Análise de Riscos e a Atividade de Inteligência

Felipe Scarpelli de Andrade
Polícia Federal - Brasil

Resumo

O presente trabalho objetiva apresentar uma estrutura de Análise de Riscos como importante ferramenta de assessoramento ao processo decisório em instituições de segurança pública. Ao destacar o aspecto metodológico da atividade de Inteligência, procura-se desenvolver técnicas próprias de produção do conhecimento com foco no risco, fornecendo informações integradas para uma atuação preventiva do Estado no combate à criminalidade. Nesse sentido, analisa-se, a partir de conceitos e técnicas de gestão da informação, a viabilidade do uso de alguns instrumentos com vistas a garantir a continuidade de um processo de planejamento de longo prazo, o qual estabeleça objetivos estratégicos que baliza, delimita e ordena a ação estatal. Com efeito, expõe-se a necessidade de os organismos de Inteligência se apropriarem efetivamente de técnicas e processos de trabalho ao defini-las em práticas analíticas e sistemáticas de produção do conhecimento. Espera-se, por meio do emprego da Análise de Riscos e a sua respectiva gestão, aumentar a eficiência na tomada de decisão, na medida em que se amplia a probabilidade de alcançar os objetivos maiores do Estado, estabelecendo base confiável que conduzam os gestores à responderem os problemas e as incertezas que o tema segurança pública apresenta.

Palavras-Chave: Segurança pública. Inteligência. Metodologia da Produção do Conhecimento. Análise de Riscos. Gestão de Riscos.

Introdução

A Inteligência de segurança pública emerge no cenário nacional atual como importante instrumento de assessoramento gerencial e de combate à criminalidade. O modelo repressivo atualmente adotado pelo Estado não é suficiente para enfrentar os riscos e problemas que o tema demanda. É necessária, pois, uma política nacional que pregue a integração de informações e antecipação de cenários. É por meio da compreensão do complexo contexto da segurança pública e seus reflexos que o Estado poderá desenvolver uma atuação preventiva.

Recebido em 28 de novembro de 2016.
Aceito em 26 de outubro de 2017.
Brasília, v. 8, n. 2, p. 91-116, jul/dez, 2017.
ISSN 2178-0013
ISSN Eletrônico 2318-6917

A evolução histórica e econômica da humanidade, caracterizada por um aumento substancial de informações disponíveis, demanda dos organismos de Inteligência a especialização na procura e no tratamento de informações sensíveis para os governantes, seja na esfera da segurança pública propriamente dita, seja em temáticas que a influenciam de alguma forma.

Somam-se a esse cenário os riscos inerentes a toda organização, como os estratégicos, os de processos, os de tecnologia da informação, os de saúde e segurança do servidor, os financeiros, os legais, os sociais, os da cadeia logística, os de projeto. Esse quadro, em que diversas ações e informações se correlacionam de forma direta ou indireta, com reflexos muitas vezes imprevisíveis quando tratadas de forma isolada, pode afetar negativamente o julgamento do decisor quanto a melhor decisão a ser tomada.

Dessa forma, a incerteza resultante da quantidade de informações disponíveis para amparar deliberações nos mais diversos níveis organizacionais tem se tornado cada vez mais presente, reduzindo a capacidade de se distinguir entre diversas opções em um contexto mais amplo. É justamente o efeito que essa incerteza gera sobre os objetivos de uma organização que chamamos de risco[1].

Assim, para se obter uma decisão embasada em conhecimentos técnicos, faz-se necessário que as instituições gerenciem seus riscos, identificando-os e analisando-os, a fim de se obter sua efetiva avaliação e alicerçar a tomada de decisão, seja ela na esfera política, estratégica ou operacional.

Segundo Andrade (2012), nessa acepção, a atividade de Inteligência, definida como aquela que busca transformar dados em conhecimento por meio de metodologia própria, pode propiciar significativa contribuição aos desafios encontrados nos dias atuais.

O tomador de decisões que esteja motivado pela necessidade de prever ou controlar, geralmente enfrenta um complexo sistema de componentes correlacionados, como recursos, resultados ou objetivos desejados, pessoas ou grupos de pessoas; ele está interessado na análise desse sistema. Presumivelmente, quanto melhor ele entender essa complexidade, melhor será sua decisão (Ribeiro, 2003).

1 De acordo com a Norma NBR ISO31000/2009, risco é o efeito da incerteza nos objetivos.

A Análise de Riscos (AR) surge nessa esteira, pelo que fornece ao seu usuário conhecimentos organizados e processados com metodologia específica, sugerindo ações e medidas de prevenção ou correção das possíveis falhas detectadas em um determinado processo. Com base nessa análise, é possível assessorar com maior qualidade a tomada de decisão.

Tal entendimento vai ao encontro do conceito da atividade de Inteligência de Segurança Pública, encontrado na Doutrina Nacional de Inteligência de Segurança Pública (DNISP)[2]. Nesse sentido, destaca-se a definição da Análise de Riscos que a própria Doutrina delimita como sendo:

> *...o conjunto de procedimentos que identificam, quantificam e analisam ameaças e vulnerabilidades aos ativos da Segurança Pública e da defesa social, elaborada com a finalidade de apontar alternativas para mitigar e controlar os riscos.*

Embora a DNISP faça menção à Análise de Riscos como técnica acessória, é possível entendê-la, também, como um novo tipo de conhecimento, além daqueles elencados pela Doutrina (Informe, Informação, Apreciação e Estimativa), na medida em que possui particularidades e especificidades que a diferem, na sua essência, das demais, conforme verificar-se-á adiante.

Portanto, a Análise de Riscos aplicada à Inteligência de Segurança Pública pode, ao mesmo tempo, tratar-se de um tipo de conhecimento específico ou de uma técnica acessória na produção do conhecimento, dado que é técnica utilizada a fim de prever os perigos, as ameaças reais ou potenciais aos diversos campos da instituição.

Assim, o processo de gestão de riscos deve permear toda a organização, os seus processos ou áreas específicas, proporcionando-lhe diversas vantagens, visto que aumenta a probabilidade de se alcançarem os objetivos, estabelecendo base confiável para planejar e tomar decisões; melhora a identificação de oportunidades e de ameaças; favorece uma gestão proativa; minimiza a ocorrência de surpresas e de perdas; melhora a prevenção de incidentes; melhora os controles; permite a utilização, com maior eficácia, dos

2 "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."

recursos material e humano; melhora a eficácia e a eficiência operacional; aumenta a capacidade de resiliência da organização; preserva os ativos da instituição e melhora a governabilidade.

Embora a AR seja aplicada com maior frequência pela segurança pública no ramo da Contra Inteligência, notadamente pelo segmento da Segurança Orgânica (SEGOR), a técnica deve ser, também, adotada no ramo da Inteligência, ou seja, com a finalidade de produção de conhecimento.

A AR é uma ferramenta a ser desenvolvida em um processo mais amplo, conhecido como Gestão de Riscos (GR), ou Gerenciamento de Riscos, que é o conjunto das atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco (NBR ISO 31000:2009). Portanto, a AR é o processo por meio do qual se entende a natureza do risco e a consequente determinação de seu nível, sendo base para a Gestão de Riscos.

Dessa forma, sugere-se incluir a Gestão de Riscos no planejamento estratégico e proceder-se à análise de riscos nos processos, ou áreas em que essa organização executa. É importante sempre integrar a gestão de riscos na governança, na estratégia, no planejamento ou na gestão.

Nesse sentido, a NBR ISO[3] 31000:2009 traz um modelo para esse processo, estabelecendo princípios que devem ser atendidos para tornar a Gestão de Riscos eficaz. Os princípios de que trata a Norma são:

> *a) A gestão de riscos cria e protege valor.*
>
> *b) A gestão de riscos é parte integrante de todos os processos organizacionais.*
>
> *c) A gestão de riscos é parte da tomada de decisões.*
>
> *d) A gestão de riscos aborda explicitamente a incerteza.*
>
> *e) A gestão de riscos é sistemática, estruturada e oportuna.*
>
> *f) A gestão de riscos baseia-se nas melhores informações disponíveis.*
>
> *g) A gestão de riscos é feita sob medida.*
>
> *h) A gestão de riscos considera fatores humanos e culturais.*

3 A ISO é a sigla de *International Organization for Standardization*, ou Organização Internacional para Padronização, em português, e tem como objetivo principal aprovar normas internacionais em todos os campos técnicos, como normas técnicas, classificações de países, normas de procedimentos e processos. No Brasil, a ISO é representada pela ABNT (Associação Brasileira de Normas Técnicas).

i) A gestão de riscos é transparente e inclusiva.

j) A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.

k) A gestão de riscos facilita a melhoria contínua da organização.

Assim, a GR propõe-se a estruturar planos de ações para gerenciamento e monitoramento dos riscos identificados pela AR, a partir da definição e gestão de indicadores e desenvolvimento de atividades conforme cada tipo de tratamento definido.

Além da ISO 31000, que trata do sistema de gestão de riscos, há outra relevante norma dedicada a ferramentas e técnicas para a gestão de riscos, a ISO/IEC 31010, que descreve um método estruturado, lógico e sistemático, que contribui para a eficiência e para os resultados contínuos, consistentes, comparáveis e confiáveis. A ISO Guia 73:2009, por sua vez, estabelece padrões para a gestão de riscos na medida em que define o "vocabulário", o "conceito" e a "terminologia".

Importante destacar que as normas internacionais, aqui elencadas, foram utilizadas como referência, não como uma metodologia. Deve ser considerado que a sua descrição serve como diretriz ao apresentar uma quantidade suficiente de detalhes que permita a construção de métodos e ferramentas adequadas para o gerenciamento de riscos na esfera da atividade de Inteligência.

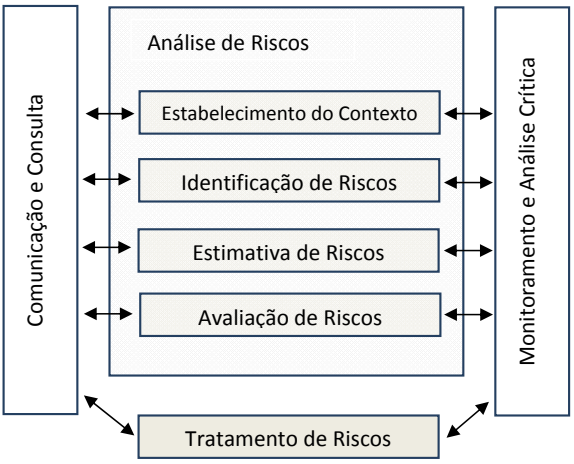
Não obstante, o processo proporciona específicos conhecimentos sobre os riscos, porquanto estabelece uma estrutura na qual são utilizadas diversas ferramentas que auxiliarão na produção do conhecimento: trata-se do Ciclo de Gestão de Riscos.

1. Ciclo de Gestão de Riscos

O ciclo da Gestão de Riscos traduz-se por meio de uma estrutura contínua e sequencial, composta por cinco fases: Estabelecimento do Contexto, Identificação de Riscos, Estimativa de Riscos, Avaliação de Riscos e Tratamento de Riscos; e dois processos: "Comunicação e Consulta" e "Monitoramento e Análise Crítica".

O ciclo da Análise de Riscos, por sua vez, não compreende a etapa de Tratamento de Risco propriamente dita, que está contida na Gestão de Riscos. Isto ocorre porque a finalidade de setores de Inteligência é assessorar e não executar. A AR não contempla, portanto, a execução dessa tarefa, cabendo à Gestão de Riscos fazê-lo.

Figura 1 – Ciclo de Gestão de Riscos



Fonte: Elaborado e adaptado pelo autor.

Embora o analista tenha que percorrer todas as etapas do Processo de Gestão para elaborar um relatório de Análise de Riscos, é possível retornar a etapas anteriores, a qualquer tempo, a fim de ajustá-las ou até mesmo retroalimentá-las.

É importante destacar que a ISO 31000 tem uma abordagem genérica e pode ser aplicada para qualquer escopo e contexto, sendo adaptável a qualquer tipo de organização. Portanto, é possível customizá-la a partir do estabelecimento do sistema a ser tratado.

A estrutura acima apresentada não pretende prescrever um determinado sistema de gestão, mas auxiliar a organização a integrar o ciclo de gestão de riscos ao seu sistema de gerenciamento global. Assim, convém que a organização adapte os componentes dessa estrutura às suas necessidades específicas.

Dessa forma, a figura acima é uma adaptação do processo de GR, extraída da ISO 31000, sugerida para a atividade de Inteligência de Segurança Pública devido à natureza específica de sua atividade.

A modificação promovida no processo de GR refere-se à inclusão da etapa "Estabelecimento do Contexto" na fase de Análise de Riscos. Entende-se que este processo pode e deve ser desenvolvido pelo próprio setor de Inteligência, uma vez que este possui conhecimento específico para tal mister.

Pretende-se, com a adaptação e customização do processo, delinear os caminhos a serem percorridos e apresentar princípios e diretrizes genéricas na Gestão de Riscos para diversas áreas de atuação, notadamente para a atividade de Inteligência de segurança pública. Logo, deve-se considerar que esta estrutura não é estanque, que há possibilidade de modificação na medida em que pode ser utilizada por uma ampla gama de atividades.

Além disso, cada organização ou sistema analisado têm necessidades específicas e, portanto, os critérios para análise e tratamento destes riscos devem ser aplicados individualmente. Não obstante, o processo aqui apresentado, na medida em que descreve uma estrutura sistemática e lógica, irá auxiliar na preparação de uma estrutura especificamente adaptada a determinada organização. Assim, as ferramentas que auxiliarão a produção da valoração dos riscos deverão ser empregadas de acordo com a realidade de cada Sistema avaliado. Para facilitar a escolha da técnica a ser utilizada em uma determinada avaliação de riscos, a ISO/IEC 31010 traz uma tabela que indica se a ferramenta é aplicável, não aplicável ou fortemente aplicável.

Frise-se que no decorrer do processo de gestão é necessário considerar dois aspectos dos quais devem ser continuamente observados e executados: a "Comunicação e Consulta" e o "Monitoramento e Análise Crítica". Não são, portanto, etapas do processo, mas procedimentos que permeiam e alicerçam as demais fases, tornando-o cíclico e permanente.

1.1 COMUNICAÇÃO E CONSULTA

A "Comunicação e Consulta" é um procedimento padrão do processo de Gestão de Riscos, no qual são desenvolvidos os planos iniciais para dar conhecimento da necessidade e da decisão tomada para a realização da respectiva análise.

Esses planos iniciais devem ser difundidos a todas as partes interessadas, sejam internas ou externas, a fim de explicitar o trabalho a ser realizado, ressaltando sua importância e necessidade de consulta aos especialistas do sistema, além de solicitar opiniões e dados existentes.

Com base nesses planos, o diagnóstico do sistema será iniciado, possibilitando a identificação preliminar dos possíveis riscos, suas causas, seus prováveis efeitos e, quando couber, algumas medidas reconhecidas para tratá-los.

A "Comunicação e Consulta" tem por finalidade fazer, por meio do diálogo, com que os públicos interno e externo compreendam as razões das decisões e das medidas que serão tomadas.

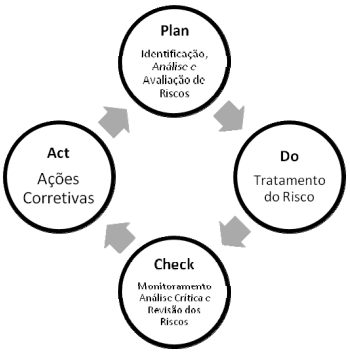
Esse procedimento, cíclico e permanente, facilita a identificação de diferentes pontos de vista e devem ser devidamente considerados, pois são importantes fontes de informação.

1.2 MONITORAMENTO E ANÁLISE CRÍTICA

Assim como na Comunicação e Consulta, o "Monitoramento e Análise Crítica" não é uma etapa, mas um procedimento padrão do processo de Gestão de Riscos. Nesse processo, ações são desenvolvidas para verificar, supervisionar, observar, controlar e revisar o funcionamento da gestão.

Trata-se, portanto, de importante procedimento de acompanhamento, cujo objetivo é a melhoria contínua da Gestão de Riscos ao considerá-lo parte essencial do Ciclo PDCA[4] (Planejar, Fazer, Checar e Corrigir):

Figura 2 – PDCA em Gestão de Riscos



Fonte: Elaborado e adaptado pelo autor.

4 "PDCA" é a sigla das palavras em inglês que designam: "Plan", planejar; "Do", fazer ou agir; "Check", checar ou verificar; e "Action", no sentido de corrigir ou agir de forma corretiva. É um método amplamente aplicado para o controle eficaz e confiável das atividades de uma organização.

Dessa forma, o processo "Monitoramento e Análise crítica" deve ser planejado como parte do gerenciamento de riscos, abrangendo a checagem e o controle regulares. Pode ser periódico ou acontecer em resposta a um fato específico.

Ao abranger todas as fases e etapas do procedimento, o Monitoramento e Análise Crítica tem como efeito:

- Garantir a eficácia das medidas de controle estabelecidas;
- Obter dados e informações adicionais para a avaliação dos riscos;
- Analisar os eventos e ocorrências, suas mudanças e tendências, buscando aumentar o aprendizado sobre elas;
- Detectar mudanças no contexto externo e interno e, se for o caso, revisá-los;

1.3 ESTABELECIMENTO DO CONTEXTO

O "Estabelecimento do Contexto" é a primeira etapa do processo, no qual se realizará um diagnóstico inicial do sistema a ser analisado. O objetivo aqui é fornecer suporte para a próxima etapa ("Identificação de Riscos") por meio de técnicas capazes de apontar as ameaças, que podem ser ações naturais e humanas, intencionais ou acidentais; e as vulnerabilidades que coloquem em risco os ativos a serem protegidos pela instituição.

Para tanto, deve-se realizar um extenso e detalhado mapeamento dos ambientes externo e interno do sistema a ser analisado. Deve ser bem delimitado e precisamente demarcado.

O contexto externo é a relação da organização com a comunidade, o país, a legislação, estrutura econômica e política e que podem impactar a consecução de seus objetivos institucionais. Entender o contexto externo é importante para assegurar que os objetivos e as preocupações de todas as partes interessadas sejam considerados no desenvolvimento dos critérios de risco.

Portanto, para sua elaboração, deve-se levar em conta, entre outros, os seguintes aspectos: localização geográfica, criminalidade, ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, quer seja internacional, nacional, regional ou local;

fatores-chave e tendências que tenham impacto sobre os objetivos da organização; e relações com as partes interessadas externas e suas percepções e valores. Esta avaliação poderá indicar possíveis ameaças aos ativos da instituição.

O contexto interno, por sua vez, é o ambiente no qual a organização busca atingir seus objetivos alinhado com a sua missão, cultura, processos, estrutura e estratégia. É considerado contexto interno tudo aquilo que se encontra dentro da organização e que pode influenciar a maneira pela qual se gerenciam os riscos. Entre outros elementos, extraem-se, desta análise, as vulnerabilidades a que está sujeita organização.

Ponto fundamental para a realização do diagnóstico é a identificação dos ativos institucionais, detalhando os tangíveis, como aspectos físicos, pessoal, materiais, projetos, planos, políticas, estratégias, documentos, e os intangíveis, como imagem, reputação, marca, símbolo, patente, propriedade intelectual, governabilidade, sensação de segurança, etc. Os ativos de uma organização são elementos essenciais em uma avaliação de risco e seu reconhecimento torna-se necessário, na medida em que o risco sempre irá influir na sua integridade.

O processo para identificá-lo pode ser simples, como o emprego de *Checklists*, ou mais detalhado, exigindo um inventário de equipamentos de capital, matriz de rastreabilidade do sistema, revisão de documentos legais, etc.

Dessa forma, para o correto estabelecimento do contexto, o analista de riscos, ao identificar os ativos, as ameaças e as vulnerabilidades, deverá confeccionar uma Apreciação, cujo conhecimento é resultante de raciocínios elaborados pelo profissional de Inteligência e expressa o estado de opinião em relação à verdade sobre fato ou situação passados e/ou presentes. É fundamental, contudo, que o analista tenha em mente a finalidade do conhecimento e sua respectiva delimitação, a fim de atender o objetivo do relatório: a Análise de Riscos.

Nesta fase, é importante levantar os antecedentes estatísticos de cada ponto, bem como colher as opiniões e as necessidades das partes interessadas e dos especialistas. Quando couber, os prognósticos sobre as potenciais consequências de um fato que podem afetar os ativos a serem protegidos são igualmente recomendados.

Conjuntamente, é indicado valer-se de algumas ferramentas acessórias que podem auxiliar o diagnóstico no "Estabelecimento do Contexto", elencadas na ISO 31010. Entre elas, destaca-se:

- *Brainstorming* – Envolver, estimular e incentivar o livre fluxo de conversação entre um grupo de pessoas "conhecedoras" para identificar os modos de falha potenciais e os perigos e riscos associados, a área estudada e os critérios para decisões e/ou opções para tratamento.
- Entrevista Estruturada: Em uma entrevista estruturada, os entrevistados são solicitados individualmente a responder a um conjunto de questões elaboradas que constam em "uma folha de indicações" que incentiva o entrevistador a ver uma situação a partir de uma perspectiva diferente e, assim, identificar os riscos e os bens a serem protegidos.
- *Checklist*: Uma lista ampla, detalhada e previamente determinada e padronizada de perigos, riscos ou falhas de controle que foram desenvolvidas como resultado de um processo de uma avaliação de riscos anterior ou como um resultado de falhas passadas.

Ao final da etapa e seu respectivo mapeamento, espera-se o estabelecimento do contexto por meio de um diagnóstico. Neste momento é indicada a implementação da análise SWOT[5], cuja finalidade é recolher dados importantes dessa análise que caracterizam os ambientes externos e internos, ao identificar, de forma resumida, os pontos fortes e fracos, as oportunidades e ameaças.

Figura 3 – Matriz SWOT em Gestão de Riscos

SWOT		
Amb. Interno Vulnerabilidades	Pontos Fortes	Pontos Fracos
Amb. Externo Ameaça	Oportunidades	Ameaças

Fonte: Elaborado e adaptado pelo autor.

Trata-se de uma ferramenta que direciona e disciplina o reconhecimento das ameaças e vulnerabilidades a fim de facilitar a futura identificação do risco. Ameaças são ações naturais e humanas, intencionais ou não (acidentes), que colocam em risco os ativos a serem protegidos. Referem-se sempre a situações externas às instituições que podem causar danos ou gerar crises. Por essa razão, geralmente não são variáveis controláveis. No entanto, em certos casos, podem ser neutralizadas, ou, ainda, controladas por meio de ações específicas.

5 SWOT é a sigla dos termos ingleses *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças) que consiste em uma metodologia bastante popular no âmbito empresarial.

Existem diversas variáveis (como capacidade e acessibilidade, por exemplo), e formas (baseada em estatísticas e dados históricos) de se analisarem as ameaças. Contudo, notadamente para a atividade de segurança pública, deve-se ter especial cuidado às pesquisas baseadas apenas em dados estatísticos. O fato de um determinado risco nunca ter ocorrido ou mesmo nunca ter sido reportado, não significa que não acontecerá ou mesmo que não esteja acontecendo.

Bertrand Russell (1980) reconhece essa questão como sendo um problema de indução (ou problema de conhecimento indutivo) ao citar as armadilhas do conhecimento adquirido por meio da observação: um peru que é alimentado diariamente; cada refeição servida reforça a crença do pássaro de que a regra geral da vida é ser alimentado diariamente por seu dono; no entanto, em uma tarde de quarta-feira que antecede o Dia de Ação de Graças, algo inesperado acontece...

As vulnerabilidades, por sua vez, são as características do ativo que facilitam a concretização da ameaça. É a suscetibilidade de o ativo sofrer ataque, a fraqueza do bem crítico a ser protegido. Ocorrem sempre em situações internas da organização e devem compor, resumidamente, o campo "Pontos Fracos", da matriz SWOT. Considerando que a vulnerabilidade é a percepção que se faz diante da ameaça, dos pontos fracos que compõem o contexto interno da organização, trata-se de uma variável com alta possibilidade de mitigação por parte da instituição.

Dessa forma, para a concepção de uma estrutura de AR, é importante que o diagnóstico esteja embasado na avaliação e compreensão do ambiente interno e externo da organização, pois é por meio dessa análise que se torna possível a identificação do risco. A matriz SWOT, de forma simples e resumida, permite a percepção dos fatores de influência e suas respectivas ameaças e vulnerabilidades, extraídas desse diagnóstico e servindo de base para a Identificação do Risco.

1.4 IDENTIFICAÇÃO DO RISCO

Após o estabelecimento do contexto por meio de um diagnóstico devidamente descrito, delimitado e mapeado, parte-se para a próxima etapa, a Identificação do Risco.

Antes, porém, faz-se necessário destacar a diferença entre "risco" e "problema", que muitas vezes não é considerada. Identificar um risco é uma oportunidade de evitar um problema, é prevenir que um evento indesejado ocorra. O problema, por seu turno, refere-se a algo já existente, que está ocorrendo e precisa ser tratado emergencialmente. Dessa forma, o risco não é, em si mesmo, um fato, mas a interpretação de fato (s), sendo que sempre se refere ao futuro e, normalmente, a algo adverso.

Importante lembrar que os riscos devem surgir a partir das ameaças e vulnerabilidades apostas na matriz SWOT. Somente haverá risco se houver uma fonte que o enseje, isto é, as ameaças devem surgir como causas com potencial para originar o risco.

As vulnerabilidades do ativo também são fatores importantes neste processo, pois, ao analisar quais ameaças são mais capazes de violar o ativo de um órgão, pode-se verificar quais as vulnerabilidades merecem ser corrigidas. Este estudo irá influir na estimativa da probabilidade de ocorrência de um determinado risco.

Isto posto, o passo seguinte é reconhecer e descrever adequadamente os riscos. Para este detalhamento, sugere-se a ferramenta adaptada 5W2H[6], uma vez que é necessário particularizar todos os elementos, as características que o envolvem. Como resultado espera-se dissecar o risco de forma precisa, ou seja, seu significado face ao sistema avaliado. Para tanto, deve-se identificar os seguintes elementos que o compõem: Quem, Quando, Onde, Porquê e Consequência. Uma vez identificados e bem delimitados, os riscos estão preparados para serem submetidos a um processo de mensuração ou valoração.

1.5 ESTIMATIVA DE RISCOS

Trata-se da etapa da Gestão de Riscos que fornece um processo estruturado para identificar como os objetivos do sistema podem ser afetados, ao analisar o risco em termos de probabilidades e impactos.

A estimativa de riscos pode ser realizada em diversos graus de detalhes e variáveis, a depender do risco, da finalidade da análise e das informações, dados e recursos disponíveis.

6 A planilha 5W2H é uma ferramenta administrativa que pode ser utilizada em qualquer empresa a fim de registrar de maneira organizada e planejada como serão efetuadas as ações, assim como por quem, quando, onde, por que, como e quanto irá custar para a empresa.

Consoante as circunstâncias, a análise pode ser qualitativa[7], semi-quantitativa ou quantitativa[8], ou uma combinação destas. Entretanto, qualquer estimativa deve levar em conta dois importantes parâmetros: a aferição da probabilidade da ocorrência do risco e, em ocorrendo, qual o impacto (consequência) que ele geraria no ativo estudado.

Assim, o risco existe quando se vislumbra um estado futuro e a probabilidade dele se materializar, sendo que a incerteza desse risco decorre da cegueira quanto ao possível estado futuro, em termos de probabilidade de sua concretude.

Dessa forma, uma vez identificados, os riscos devem ser estudados e decompostos a fim de se determinar a sua significância, o seu nível (grau). Para esta tarefa, deve-se combinar a probabilidade da ocorrência e seu impacto considerando suas consequências, sejam elas tangíveis ou intangíveis.

1.5.1 Probabilidade

Na terminologia da gestão de risco a palavra probabilidade é utilizada para referir-se a chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos.

Para a mensuração da probabilidade, deve-se elaborar uma tabela com a identificação do grau de probabilidade do risco e seu respectivo valor, escalonada em quantos patamares a equipe de análise de riscos entender razoável. Aqui, apresenta-se em cinco níveis:

Figura 4 – Tabela exemplificativa de Probabilidade

GRAU	VALOR
Extremamente provável	5
Provável	4
Ocasional	3
Remoto	2
Improvável	1

Fonte: Elaborado e adaptado pelo autor.

7 Análise que estima o valor dos riscos por meios não estatísticos, ou seja, por estimativas fornecidas por especialistas de área, que têm profundos conhecimentos sobre o assunto, baseada no saber (know-how), devendo, no entanto, serem considerados os ambientes interno e externo.

8 Análise que conta com dados em quantidade e qualidade tal que seja possível utilizar técnicas estatísticas para calcular e interpretar o risco, baseada em estatísticas, em uma análise histórica dos registros de incidentes de segurança, em experiência anterior ou em uma tempestade de ideias (*brainstorming*).

Uma vez definida a tabela de probabilidades, torna-se fundamental compreender o tipo de análise a ser desenvolvida, pois é necessário criar parâmetros para cada uma delas, ou seja, referenciá-las consoante a análise.

Assim, caso se refira a uma análise quantitativa, os parâmetros devem ser definidos de acordo com as limitações estatísticas do tema avaliado. Contudo, atenção especial deve ser dada quando a probabilidade se relacionar apenas com os dados estatísticos. A falta desses dados, sobretudo na segurança pública, não significa a sua "não ocorrência", já que pode haver diversos fatores que impediram seu aferimento, como, por exemplo, o fato de não haver atuação preventiva ou repressiva em determinado local, ou os eventos não terem sido reportados, inclusive pelas próprias forças de segurança.

Entretanto, em havendo dados estatísticos suficientes para produzir uma análise quantitativa, os parâmetros devem ser definidos de acordo com as delimitações estatísticas do tema avaliado. Sugere-se, ainda nessa hipótese, que o estudo seja focado em uma análise semiqualitativa, ou seja, valer-se de dados estatísticos para sua produção, mas não se limitar a eles. Assim como no caso de uma análise quantitativa, quando o estudo é focado em referencias qualitativas, as categorizações também são necessárias, já que torna possível relacionar, de forma objetiva, o grau de ocorrência do evento (probabilidade).

Para essa categorização, faz-se necessário descrever o que significa grau de probabilidade "extremamente provável". É a partir dessa tabela referencial que a análise se dará de forma distinta. O detalhamento, contudo, dependerá do sistema analisado. O "valor" atribuído a cada grau é igualmente definido pela equipe de análise de riscos e serve como uma espécie de peso quando da consolidação dos dados. Portanto, há diversas abordagens que podem ser empregadas para se estimarem as probabilidades: uso de dados históricos relevantes; previsão de probabilidades utilizando técnicas analíticas ou de simulação; julgamento de especialistas, entre outras.

Necessário destacar que categorizações são importantes na estimativa de risco; contudo, quando tidas como definitivas, tornam-se equivocadas, ao gerar uma redução na complexidade real e impedir a consideração imprecisa das fronteiras. Dessa forma, para que haja uma análise bem estruturada, a referência deverá ser customizada, ajustada de acordo com a análise. O detalhamento, então, dependerá do sistema analisado.

A probabilidade é a correlação de três elementos: ativo, ameaça e vulnerabilidade. Assim, ao reduzir a vulnerabilidade da instituição em relação a probabilidade de ocorrência de um determinado evento indesejado, atenuar-se-á, também, o grau desse risco.

Sugere-se o emprego do método Delphi[9], ou Mini Delphi, que consiste em combinar opiniões de especialistas que possam influenciar a estimativa de identificação na avaliação do risco, utilizando-se o resultado médio deste conjunto. A metodologia Delphi se baseia no uso estruturado do conhecimento, da experiência e da criatividade de um painel de especialistas, pressupondo-se que o julgamento coletivo, quando organizado de forma adequada, é melhor do que a opinião de um só indivíduo, ou mesmo de alguns indivíduos desprovidos de uma ampla variedade de conhecimentos especializados. Este tipo de técnica pode ser adotada para aumentar a efetividade de avaliações analíticas realizadas por especialistas.

Parte-se da premissa que uma vez que um especialista pode estar errado quanto ao futuro, a média das opiniões de vários especialistas se aproxima de uma valoração mais próxima da verdadeira. Assim, quando da avaliação do grau da probabilidade e do impacto de um determinado risco, faz-se necessário haver uma quantidade mínima de especialista a fim de se evitar os extremos na sua valoração.

O Método Mini Delphi por sua vez, pode ser conceituado como um processo estruturado de consulta a especialistas, que mantendo as principais características do método Delphi permite a realização de um estudo com grande agilidade em uma única sessão de trabalho. Uma vez mensurada a probabilidade de o risco acontecer, parte-se para a estimativa de seu impacto, em caso de ocorrência do evento.

2.5.2 Impacto

O Impacto traduz-se por meio da gravidade dos danos potenciais de uma ação hostil, verificada pela quantificação da consequência negativa pre-

9 O método Delphi surgiu em 1948 na Rand Corporation dos Estados Unidos. Segundo Wright e Giovinazzo (2000) o método passou a ser disseminado no começo dos anos 60 e tinha como objetivo original desenvolver uma técnica para aprimorar o uso da opinião de especialistas na previsão tecnológica. Sackman (1975) define Delphi como uma tentativa de elucidar a opinião de especialistas de maneira sistemática para resultados úteis.

sumível. Pode ser mensurada com base em diversos parâmetros, como a confiabilidade da imagem da organização, sensação de segurança, na repercussão na mídia, no número estimado de perdas em recursos humanos, material e do público envolvido, etc.

A análise do Impacto objetiva, por meio de um processo, associar um valor aos impactos no sistema avaliado decorrente de um risco que venha a concretizar-se. Para tanto, é fundamental levar em conta a opinião dos especialistas, análise de cenários, além de outras técnicas elencadas na norma ISO 31010. Assim como na Probabilidade, a mensuração do Impacto deve ser aplicada de acordo com cada sistema avaliado, em uma escala previamente hierarquizada, conforme se observa no exemplo abaixo:

Figura 5 – Tabela exemplificativa de Impacto

GRAU	VALOR
Catastrófico	5
Crítico	4
Moderado	3
Leve	2
Desprezível	1

Fonte: Elaborado e adaptado pelo autor.

A descrição de cada grau de Impacto é igualmente recomendada, pois ilustra a (s) característica (s) do grau de impacto, ao precisar e delimitar, em categorias, as possibilidades de análises dos envolvidos na avaliação.

Importante destacar que, tanto na avaliação da probabilidade quanto na do impacto, deve-se considerar o emprego de pessoas que efetivamente trabalham no tema. A identificação dos valores por especialista traz confiabilidade na avaliação, na medida que são eles os verdadeiros conhecedores do assunto e seus detalhes. Dessa forma, deve-se evitar que sejam processados pela própria equipe de Análise de Riscos, cabendo a estes apenas o acompanhamento.

Sugere-se, assim como no caso da probabilidade, o emprego do método Delphi, ou Mini Delphi, que consiste em combinar opiniões de especialistas que possam influenciar a estimativa de identificação na avaliação do risco.

Após a avaliação individual do Impacto, por parte dos especialistas, tira-se uma média, calculada através da soma dos valores referenciados na ta-

bela, dividido pelo número de pessoas envolvidas na estimativa. Este valor, a média deste conjunto, definirá o Impacto do risco analisado.

É possível, em alguns casos, reduzir o impacto ao isolar a ameaça, ou, ao admiti-lo, criar planos de contingência para enfrenta-lo em caso de ocorrência. Contudo, esta não é a variável com a maior oportunidade de redução ou mitigação, notadamente no campo da segurança pública.

1.6 AVALIAÇÃO DOS RISCOS

Esta etapa consiste em relacionar os níveis de probabilidade e impacto estimados do risco e seus critérios definidos de acordo com o contexto estabelecido. A partir desta relação é possível mensurar a significância de seu nível, o seu grau.

Assim, com os resultados da Estimativa identificados na etapa anterior, realiza-se a última parte da fase da AR, ao inserir em uma Matriz de Risco os valores da probabilidade e do impacto.

Conforme visto, a Probabilidade refere-se a chance de algo vir a acontecer e será medida pela definição de uma, entre as 5 faixas de níveis, aqui estabelecidas, com o seu respectivo grau.

Da mesma forma, o Impacto traduz-se por meio do valor que se atribui à repercussão de uma ocorrência. Sua estimativa dar-se-á pelo estabelecimento de uma, entre as 5 faixas de níveis, e seu peso correspondente.

O produto da Probabilidade e do Impacto permite-nos avaliar o grau de risco, identificado no sistema, através da inserção dos dados em uma matriz de dupla entrada. Portanto, por meio da integração dessas duas variáveis, obtém-se a correta avaliação do grau de risco.

A Matriz de Risco deverá ser igualmente construída pela equipe de análise de riscos, levando-se em conta o sistema a ser avaliado. Segue, abaixo, um exemplo:

Figura 6 – Matriz exemplificativa de Riscos

Grau de Probabilidade						
	MATRIZ DE RISCO	Improvável 1 (0-20%)	Remoto 2 (21-40%)	Ocasional 3 (41-60%)	Provável 4 (61-80%)	Extremamente Provável 5 (81-100%)
Grau de Impacto Negativo	**Catastrófico 5 (81-100%)**	**ME**	**ME**	**AL**	**MA**	**MA**
	Crítico 4 (61-80%)	**BA**	**ME**	**ME**	**AL**	**MA**
	Moderado 3 (41-60%)	**BA**	**BA**	**ME**	**ME**	**AL**
	Leve 2 (21-40%)	**MB**	**BA**	**BA**	**ME**	**ME**
	Desprezível 1 (0-20%)	**MB**	**MB**	**BA**	**BA**	**ME**

Legenda:	
Classificação do Risco	
MB	Muito Baixo
BA	Baixo
ME	Médio
AL	Alto
MA	Muito Alto

Fonte: Elaborado e adaptado pelo autor.

Com base no cruzamento das variáveis Probabilidade e Impacto na Matriz de Risco, obtém-se a significância do risco. Aqui, de acordo com a realidade de cada sistema, é possível empregar diversas ferramentas que auxiliarão nesse processo.

Entre elas está a Matriz Mediana, ou de Impactos Cruzados, a qual permite calcular os graus de motricidade e dependência de cada um dos riscos. Isso é feito pela soma modular dos valores dos impactos medianos constantes da matriz, obtendo, como resultado, a avaliação de quanta interdependência há entre eles.

A soma "vertical" define a motricidade, e a "horizontal", a dependência de cada Risco. Esses dois conceitos dizem respeito às capacidades de cada Risco se associar aos demais. Em outras palavras, quanto maior for o grau de motricidade desse Risco, mais ele influenciará as probabilidades de ocorrência ou não dos demais; e quanto maior o seu grau de dependência, mais a sua probabilidade de ocorrência será influenciada pelos demais.

Assim, por meio da compreensão da natureza do risco e sua influência/dependência é possível sugerir as ações mais eficazes, afim de mitigá-lo e auxiliar a condução de resultados. É possível, ainda, em função do risco com maior motricidade, indicar prioridades quanto a melhor opção de tratamento.

A depender do risco, podem ser utilizadas técnicas que auxiliam na priorização de seu tratamento. A matriz GUT[10], por exemplo, serve para classificar cada risco em função da gravidade (do risco), da urgência (de resolução) e pela tendência (piorar com rapidez ou de forma lenta).

Os tipos de conhecimentos tradicionalmente produzidos pela Inteligência são o Informe, a Informação, a Apreciação e a Estimativa. Esses relatórios são produzidos valendo-se de metodologia própria, traduzida pelo Ciclo da Produção do Conhecimento (CPC), ou Metodologia da Produção do Conhecimento (MPC), com suas fases determinadas e delimitadas. Ocorre que de acordo com essa metodologia, não é indicado sugerir ações ou prioridades a fim de se decidir o que deve ser feito. Esse papel cabe ao decisor e não ao profissional de Inteligência. Este é um ponto importante da produção do conhecimento na medida em que seu produto é organizado tecnicamente, sem inferências ou sugestões. É uma característica desse tipo de produto.

Contudo, a análise de riscos inclui, evidentemente, as condutas internas que os podem aumentar ou diminuir. Assim, é importante selecionar e apontar, no relatório de AR, uma ou mais opções pertinentes para se alterar a Probabilidade de ocorrência, o Impacto (e seu respectivo efeito), ou ambos. Trata-se do campo destinado às sugestões de tratamento de riscos. Essa possibilidade de selecionar e apontar uma ou mais opções de ações torna este tipo de relatório diferente daqueles em que a atividade de Inteligência lida ordinariamente, uma vez que doutrinariamente, para a Inteligência, não se devem sugerir decisões para o usuário do conhecimento. Como se vê, o relatório de Análise de Riscos se difere, na sua essência, dos outros tipos de conhecimento produzidos pela Inteligência.

Entretanto, ao considerar que a elaboração do relatório é concebida por profissionais de Inteligência, cuja finalidade é produzir conhecimento para o assessoramento, não lhe compete, então, executar ações de tratamento, mas apenas sugerir, indicar. A tarefa de execução é destinada

10 Sigla para Gravidade, Urgência e Tendência, é uma ferramenta utilizada na priorização das estratégias, tomadas de decisão e solução de problemas de organizações/projetos.

à etapa seguinte "Tratamento de Riscos", que está contida na Gestão de Riscos e não na Análise de Riscos.

Assim, uma vez identificadas as opções de tratamento, os dados e as informações devem ser consolidadas em um relatório de Análise de Riscos contendo o diagnóstico, os riscos identificados, sua estimativa e a avaliação com o seu respectivo campo de tratamento.

Cabe destacar que o valor de um trabalho de AR apresentado aos tomadores de decisão não se encontra no levantamento de uma determinada linha de ação, mas sim na capacidade de se distinguir entre diversas opções em um contexto mais amplo.

A fase de Análise de Riscos finda-se nesse momento e para caracterizar todo o processo como Gestão, surge a etapa de Tratamento de Riscos, procedimento no qual o setor operacional implementará as medidas sugeridas ou outras, de acordo com a decisão do usuário do conhecimento.

1.7 TRATAMENTO DOS RISCOS

Nesta etapa, integra-se um procedimento ao processo de Análise de Riscos, caracterizando-o como Gestão de Riscos. A finalidade agora é prevenir e modificar o risco negativo, a fim de o impedir, evitar, controlar, mitigar, minimizar, amenizar, reduzir, transferir; ou, no limite, aceita-se uma ocorrência ou consequência inevitável e gerenciam-se os seus efeitos e desdobramentos.

O Tratamento dos Riscos é a implementação, a execução, por um setor operacional, da decisão de um dirigente, que pode estar de acordo, ou não, com as opções e alternativas apresentadas pelo relatório de Análise de Riscos. Portanto, as sugestões inseridas em um relatório não possuem força executória ou mandatória, além de não serem exaustivas: trata-se de um instrumento de assessoramento ao planejamento e ao processo decisório, não da decisão em si; cabe ao gestor decidir o que fazer quanto ao risco, pelo que selecionar a opção mais adequada de tratamento de riscos envolve equilibrar, de um lado, os custos e os esforços de implementação e, de outro, os benefícios decorrentes dessa opção.

Ao final, o Tratamento de Riscos concretizará todo o Ciclo de Gestão de Riscos, quando o setor operacional implementará a preferência do decisor.

3. Considerações finais

A Gestão de Riscos baseia-se em princípios e boas práticas de gestão a fim de auxiliar a tomada de decisões, seja qual for seu nível hierárquico ou setor envolvidos. É por meio de uma abordagem baseada no risco que uma organização se torna proativa, ao prevenir ou reduzir os efeitos indesejados e promover a melhoria contínua.

Dessa forma, a Gestão de Riscos voltada para a visão, missão e valores da organização auxilia o processo decisório na busca de se atingirem os objetivos institucionais, já que se trata de técnica capaz de antecipar ameaças e oportunidades, proporcionando às organizações a capacidade de agir preventivamente.

Ao apresentar em linhas gerais uma metodologia de Análise de Riscos inserida no contexto de Gestão de Riscos, verifica-se que se trata de técnica eficaz e plenamente aplicável a uma extensa gama de atividades, tanto no serviço público quanto no privado. Quando empregada pela Inteligência de Segurança Pública, a Gestão de Riscos torna-se importante ação especializada, pelo que atende ao princípio da eficiência, imposto à administração pública, na medida em que proporciona, ao subsidiar com conhecimentos técnicos e uteis, maior qualidade no assessoramento para a tomada de decisão.

Conhecendo os riscos, sua probabilidade de ocorrência e o seu impacto, bem como compreendendo suas ameaças e vulnerabilidades, o processo decisório certamente terá maior segurança na escolha da opção mais vantajosa para alcançar seus objetivos ao adotar uma abordagem sistemática e disciplinada para a avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, de controle e de governança corporativa.

O processo aqui apresentado, procurou delinear os caminhos a serem percorridos e apresentar princípios e diretrizes genéricas na Gestão de Riscos, que devem ser adaptados a cada instituição. O objetivo é auxiliar na preparação de uma estrutura para que uma organização, um setor ou uma área, possam gerenciar o risco, customizando as diversas ferramentas disponíveis em função da finalidade do assessoramento.

Na conjuntura das atividades de inteligência, o conhecimento e a sua gestão passam a ter papel relevante, pois qualificam a informação e se

apresentam como forma que permite diminuir incertezas, ampliar as possibilidades dos processos decisórios e potencializar as ações e estratégias organizacionais e operacionais.

Ao considerar a necessidade de evolução da atividade de Inteligência, bem como a importância do aprimoramento de técnicas de produção do conhecimento, sugere-se que o Relatório Análise de Riscos seja classificado como um novo tipo de conhecimento para a atividade, uma vez que se difere, na sua essência, dos demais relatórios. Essa distinção, conforme observado, refere-se à possibilidade de o analista de riscos sugestionar ações a serem adotadas pelo tomador de decisão.

Nesse sentido, expõe-se a necessidade de os organismos de Inteligência apropriarem-se efetivamente de técnicas e processos de trabalho da Análise de Riscos. A possibilidade de uma melhor contextualização dos riscos por meio da Gestão de Riscos possibilita a oportunidade de o tomador de decisões avaliar e prevenir possíveis danos, evitando-se desperdícios e garantindo-se maior responsabilidade institucional.

Felipe Scarpelli de Andrade

Agente de Polícia Federal. Mestrando em Engenharia de Processos pela Universidade Federal de Pernambuco - UFPE.

E-mail: scarpelli.fsa@dpf.gov.br

Risk Analysis and Intelligence Activity

ABSTRACT

The present work aims to present a structure of Risk Analysis as an important tool to advise the decision-making process in public security institutions. By highlighting the methodological aspect of the Intelligence activity, we seek to develop our own techniques of knowledge production with a focus on risk, providing integrated information for a preventive action of the State in the fight against crime. In this sense, it is analyzed, based on information management concepts and techniques, the feasibility of using some instruments to ensure the continuity of a long-term planning process, which establishes strategic objectives that define, delimit and orders state action. In fact, it is exposed the need for intelligence agencies to effectively appropriate techniques and work processes by defining them in analytical and systematic practices of knowledge production. Through the use of Risk Analysis and its respective management, it is hoped to increase efficiency in decision-making, as the

probability of reaching the highest objectives of the State is increased, establishing a reliable basis for problems and uncertainties that the topic of public safety presents.

Keywords: Public safety. Intelligence. Knowledge Production Methodology. Risk analysis. Risk management.

Análisis de Riesgos y la actividad de Inteligencia

RESUMEN

El presente trabajo tiene como objetivo presentar una estructura de Análisis de Riesgos como importante herramienta de asesoramiento al proceso decisorio en instituciones de seguridad pública. Al destacar el aspecto metodológico de la actividad de Inteligencia, se busca desarrollar técnicas propias de producción del conocimiento con foco en el riesgo, proporcionando informaciones integradas para una actuación preventiva del Estado en la lucha contra la criminalidad. En este sentido, se analiza, a partir de conceptos y técnicas de gestión de la información, la viabilidad del uso de algunos instrumentos con objetivo de garantizar la continuidad de un proceso de planificación a largo plazo, el cual establezca objetivos estratégicos que balicen, delimiten y ordenen la acción estatal. En efecto, se expone la necesidad de que los organismos de Inteligencia se apropien efectivamente de técnicas y procesos de trabajo al definirlos en prácticas analíticas y sistemáticas de producción del conocimiento. Se espera, a través del empleo del Análisis de Riesgos y su respectiva gestión, aumentar la eficiencia en la toma de decisión, en la medida en que se amplía la probabilidad de alcanzar los objetivos mayores del Estado, estableciendo una base confiable que conduzca a los gestores a responder los problemas y las incertidumbres que el tema de seguridad pública presenta.

Palabras Clave: Seguridad pública. Inteligencia. Metodología de la Producción del Conocimiento. Análisis de Riesgos. Gestión de Riesgos.

Referências

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO 31000/2009. **Gestão de Riscos – Princípios e diretrizes**, ABNT, 2009.

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 31010/2012. **Gestão de Riscos – Técnicas para o processo de avaliação de riscos**, ABNT, 2012.

ALBUQUERQUE, Carlos Eduardo Pires. ANDRADE, Felipe Scarpelli, O Emprego da Análise de Risco como Ferramenta de Inteligência

Estratégica. **Revista Brasileira de Ciências Policiais**. Disponível em <https://periodicos.pf.gov.br/index.php/RBCP/article/view/183>, acesso em 16 de novembro de 2016.

ANDRADE, Felipe Scarpelli. Inteligência Policial: Efeitos das distorções no entendimento e na aplicação. 2012. **Revista Brasileira de Ciências Policiais**. Disponível em <https://periodicos.pf.gov.br/index.php/RBCP/article/view/57>, acesso em 03/11/2017.

AVEN, Terje. **Foundations of Risk Analysis**. Wiley, 2012.

BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidad**e. Tradução de Sebastião Nascimento. São Paulo: Ed. 34,2010.

BRODER, James F. and TUCKER, Eugene. **Risk Analysis and the Security Survey**. Elsevier, 2012.

BRASIL. **Doutrina Nacional de Inteligência de Segurança Pública**. 2012.

FENNELLY, Lawrence J. **Effective Physical Security**. Elsevier, New York, 2004.

FERRO JÚNIOR, Celso Moreira. **A Inteligência e a Gestão da Informação Policial**. Editora Fortium. Brasília/DF: 2008.

GARCIA, May Lynn. **Vulnerability Assessment of Physical Protection System**. Ed. Elsevier, 2006.

Gerenciamento de Risco, método Brasiliano.

KOVACICH, Gerald and HALIBOZEK, Edward P. **Security Metrics Management**. Elsevier, New York, 2006

LANDOLL, Douglas J. **The Security Risk Assessment Handbook**. Auerbach Publications, New York, 2006.

NORMAN, Thomas L. **Risk Aalysis and Security Countermeasure Selection**. CRC Press, 2010.

RIBEIRO, Antonio de Lima. **Teorias da Administração**. São Paulo: Saraiva, 2003.

RUSSELL, Bertrand. **Os Problemas da Filosofia**. Coimbra, 1980.

SACKMAN, H. **Delphi Critique** - Expert Opinion, Forecasting and Group Process. Massachusets. Lexington Books, 1975.

SENNEWALD, Charles A. **Effective Security Management**. Butterworth

Heinemann, New York, 2003.

TARAPANOFF, K. (org). **Inteligência Organizacional e Competitiva**. Brasília: Editora UNB, 2001.

WRIGHT, J. T. C.; GIOVINAZZO, R. A. **Delphi** – Uma Ferramenta de Apoio ao Planejamento Prospectivo. Caderno de Pesquisas em Administração, São Paulo, v. 1, n. 12, p. 54-65, 2o trim. 2000.