Análise de Riscos e a Doutrina Nacional de Inteligência Penitenciária

Bruno César Gomes da Rocha
Departamento Penitenciário Nacional – Brasil

Resumo

O presente trabalho tem por objetivo propor um modelo específico de Análise de Riscos como importante ferramenta de assessoramento para o Departamento Penitenciário Nacional a partir da sua inclusão na Doutrina Nacional de Inteligência Penitenciária. Para tanto, será apresentado um breve histórico sobre o aumento da violência nos estabelecimentos penitenciários, a Lei de Execução Penal, o Sistema Penitenciário Federal, a gestão de riscos e seus *frameworks* mais conhecidos, com ênfase na adoção na Norma ISO 31000:2018 como ponto de partida. A partir daí, será abordada a evolução dos conceitos e características relacionados aos riscos, demonstrando a convergência existente entre o Ciclo da Produção de Conhecimento de Inteligência Penitenciária e o Ciclo de Análise de Riscos de Inteligência Penitenciária proposto. Acredita-se que a adoção sistemática das técnicas de Análise de Riscos no bojo da Doutrina Nacional de Inteligência Penitenciária permitirá elevar a qualidade e a eficiência da tomada de decisão dos gestores dos sistemas prisionais na tentativa de antecipar, neutralizar ou mitigar os efeitos da ocorrência de eventos de natureza crítica em estabelecimentos penitenciários.

Palavras-chave: Gestão de Riscos. Análise de Riscos. Inteligência. Inteligência Penitenciária. Produção do Conhecimento. Doutrina Nacional de Inteligência Penitenciária. Norma ISO 31000:2018.

Introdução

A formulação de políticas públicas de segurança pública no Brasil (criminal e penitenciária) não poucas vezes se caracteriza pela ausência de processos de planejamento de longo prazo, que estabeleçam objetivos estratégicos que precedam, delimitem e orientem a ação estatal (JUSTEN; FROTA, 2017).

O aumento exponencial do número de encarceramentos nos últimos 30 anos, gerou elevados índices de superlotação prisional que, somado às péssimas condições de saúde e higiene e às dificuldades administrativas dos estados na aplicação dos recursos destinados à execução dos serviços penais, impossibilitou a adequada promoção da ressocialização, o que favoreceu o aparecimento de Organizações Criminosas (Orcrims) no interior das penitenciárias brasileiras (MELO, 2018).

ISSN 2675-1895
ISSN Eletrônico 2675-1860

Diante do cenário generalizado de superlotação, proliferação de doenças e desrespeito à dignidade da pessoa humana as organizações criminosas passaram a operar dentro e fora dos presídios[1], o que culminou com a maior onda de atentados coordenados contra as forças de segurança pública jamais vista até então, que teve no estado de São Paulo o seu epicentro[2].

Apesar de estarem previstos no artigo 72, §1º[3], da Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal) e no artigo 3º da Lei nº 8.072, de 25 de julho de 1990 (Lei de Crimes Hediondos), os estabelecimentos penais federais somente foram implementados no ano de 2006, no auge da crise do sistema prisional brasileiro, por meio da reestruturação do Departamento Penitenciário Nacional (Depen), com a criação da Diretoria do Sistema Penitenciário Federal (Dispf).

O Sistema Penitenciário Federal do Departamento Penitenciário Nacional (SPF/Depen) foi apresentado como uma alternativa ao sistema carcerário ordinário, propondo um novo tipo de gestão prisional de segurança máxima, com normas mais rigorosas, focado no isolamento dos líderes organizações criminosas e dos presos mais perigosos do país.

De acordo com o § 1º do artigo 72 da Lei de Execução Penal (LEP), são atribuições do Departamento Penitenciário Nacional:

> Art. 72. [...]
>
> § 1º Incumbem também ao Departamento a coordenação e supervisão dos estabelecimentos penais e de internamento federais. (BRASIL, 1984).

No que tange, especificamente, ao Sistema Penitenciário Federal o §3º do artigo 52 da LEP prevê o seguinte:

> Art. 52 [...]
>
> § 3º Existindo indícios de que o preso exerce liderança em organização criminosa, associação criminosa ou milícia privada, ou que tenha atuação criminosa em 2 (dois) ou mais Estados da Federação, o regime disciplinar diferenciado será obrigatoriamente cumprido em **estabelecimento prisional federal** [...] (BRASIL, 1984, grifos nossos).

Apesar de impactar diretamente na desestruturação e na desarticulação das organizações criminosas ao submeter suas lideranças a

1 PAIXÃO, J. M.; SILVA, JÚNIOR, W. N. **Cartilha das Corregedorias Judiciais das Penitenciárias Federais.** Brasília: Conselho de Justiça Federal, Centro de Estudos Judiciários, 2013.

2 Disponível em: https://memoriaglobo.globo.com/jornalismo/coberturas/ataques-de-faccoes-criminosas-em-sao-paulo/maior-onda-de-ataques-da-historia-de-sao-paulo/. Acesso em: 29 jun. 2020.

3 Alteração inserida pela Lei 13.769/2018.

um regime mais rígido de cumprimento de pena, a criação do Sistema Penitenciário Federal, por si só, não conseguiu eliminar os conflitos e atentados que ainda ocorrem nos sistemas prisionais.

Nas palavras de Melo (2018) e Torres (2017), os estabelecimentos prisionais são conhecidos como verdadeiras "universidades do crime", tornando-se um campo fértil para a atuação das Orcrims que, além de se insurgir contra os órgãos de segurança pública, também visam à manutenção das suas atividades delitivas, o que tem causado uma série de massacres nos últimos anos.

Como resultado disso, observa-se o aumento considerável na ocorrência de eventos críticos de natureza violenta como motins, rebeliões, tentativas de resgate e assassinatos (de presos e servidores), todos resultantes de conflitos entre as organizações criminosas que operam dentro dos estabelecimentos penais (MELO, 2018; TORRES, 2017) e são amplamente noticiados conforme o Quadro 1.

Infelizmente, na maior parte das vezes, esses eventos adversos ocorrem sem que possam ser antecipados de maneira adequada pelos tomadores de decisão, haja vista a ausência de métodos preventivos eficazes:

Quadro 1

Seis diretores de presídios foram assassinados no Rio nos últimos oito anos (UOL, 2008).
Rebelião em RO termina com a morte de um agente e de três detentos (Folha de S. Paulo, 2006).
Diretor penitenciário é assassinado a facadas (JCNET, 2012).
Agentes revelam medo após morte de chefe do CDP: 'Nas mãos dos presos' (G1, 2014).
Agente penitenciário morre após ser baleado em casa na Zona Oeste de Natal (Tribuna do Norte, 2017).
Um dia após a rebelião em presídio, dois agentes penitenciários são mortos a tiros em Goiás (UOL, 2018).
Explosivos e artilharia antiaérea para libertar um ladrão de banco na Paraíba (El País, 2018).

Mesmo sendo considerado um sistema penal mais rigoroso e mais bem estruturado que os demais, o próprio Sistema Penitenciário Federal (SPF) já foi vítima das organizações criminosas que, nos anos de 2016 e 2017, executaram três servidores federais de execução penal e, atualmente, indicam a possibilidade de novos atentados contra o SPF, conforme Quadro 2:

Quadro 2

PCC matou 3 agentes para intimidar e desestabilizar servidores de presídios federais (UOL, 2017).
PCC planejava onda de atentados e torturas contra agentes públicos (Estadão, 2018).
PCC oferece R$ 200 milhões por "resgate" de Marcola de prisão federal, diz inteligência da polícia (Acesse Política, 2020).

Levando-se em consideração a gravidade dos problemas enfrentados pelos gestores do SPF/Depen, é primordial que se faça dotar as instituições das técnicas de gestão de riscos que levem em consideração não somente o contexto interno, mas variáveis externas à organização, geralmente não controláveis pelos dirigentes, que promovam a gestão dos riscos inerentes à dinâmica específica dos estabelecimentos prisionais.

Neste sentido, o presente trabalho busca demonstrar os benefícios da adoção, por meio da Atividade de Inteligência Penitenciária, das técnicas de Análise de Riscos (AR), aptas a identificar, analisar e avaliar as principais ameaças e vulnerabilidades dos estabelecimentos penitenciários federais e estaduais, criando protocolos específicos que permitam proteger seus ativos e, ao mesmo tempo, previnam a ocorrência de eventos não desejados, diminuindo sua probabilidade de ocorrência e/ou impacto.

A evolução do conceito analítico de Risco

Impossível tratar de risco sem antes remontar, mesmo que brevemente, às formas como vem sendo estudado ao longo da história. De acordo com Queirós, Vaz e Palma (2007), diz-se que a noção de risco, frequentemente associada a perigo, instabilidade e vulnerabilidade, é transversal aos mais diversos setores da sociedade. Por esse motivo a referida noção é alvo de amplas investigações no campo do conhecimento das ciências naturais, por meio de estudos orientados para as causas e a antecipação dos fenômenos aos quais são associados.

Para Rebelo (2001), a noção de risco é uma noção pré-científica, haja vista que começou a ser discutida antes mesmo de se falar em ciência conforme é conhecida atualmente. Apesar de existirem diferentes versões sobre a origem do conceito de risco, muitos autores o relacionam à pré-modernidade (Idade Média) ao tratar dos perigos associados às grandes navegações. Nesta fase, o conceito de risco aparece de forma tímida, comumente ligado aos fatores naturais com os quais a participação humana teria mínima ou nenhuma relação.

Com a chegada da modernidade, os avanços trazidos pelas explorações científicas e pelo pensamento racional, alternaram algumas concepções relacionadas ao risco, porque o mundo social e o natural seguem leis que podem ser quantificadas e, desta forma, previstas (LUPTON, 1999).

Nas palavras de Andrade (2017), o risco está presente em todos os lugares e no contexto de todas as organizações, do setor público ou do privado. Haja vista essa transversalidade, distintas definições são aceitas para descrevê-lo, a depender do contexto definido, como processos, segurança das instalações, meio ambiente, social, operacional, estratégico, entre outros.

Do ponto de vista mercantil, afirmava-se que os riscos se originavam da incerteza que o futuro trazia o ambiente no qual se davam os negócios, devendo ser verificadas a possibilidade de ocorrência de um evento em contraposição a seu impacto (ALBUQUERQUE; COUTO; OLIVA, 2019).

De acordo com Ortwin Renn (2008), o termo risco passou a ganhar popularidade a partir da metade do século passado quando políticos, militares, organizações civis, especialistas de instituições públicas e privadas entenderam a necessidade de sistematizar os problemas a ele relacionados. A partir desse momento, a comunidade internacional de pesquisa de risco estabeleceu sua própria sociedade profissional – a *Society of Risk Analysis* (SRA) – no ano de 1981 (RENN, 2008).

Definindo o risco como a consequência associada a uma atividade futura, Terje Aven *et al.* (2015), assevera que sua análise se divide em duas tarefas, sendo a primeira voltada para a avaliação e o gerenciamento do risco relacionado a atividades específicas e a segunda, voltada para a realização de pesquisas de desenvolvimento de risco genéricas, relacionada a conceitos, teorias, *frameworks*, abordagens, princípios, métodos e modelos para entender, avaliar, caracterizar, comunicar e governar o risco (AVEN, 2016).

Conforme se percebe, todos esses conceitos variam em função da escolha de metodologias, da complexidade das medidas de risco e das atividades operacional e social da perspectiva de risco. Entretanto, o entendimento de que risco é a incerteza dos resultados está universalmente pacificado.

Gestão de Riscos e Análise de Riscos

Enquanto a Gestão de Riscos (GR) trata do conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco (NBR ISO 31000:2018), a Análise de Riscos (AR) cuida do processo organizado e sistematizado por meio de uma metodologia específica, tendo

como objetivo final a valoração ou a definição do grau do risco, ou seja, procura entender o efeito da incerteza em um determinado contexto.

A partir da observação desses conceitos é possível notar que a Análise de Riscos se trata de uma ferramenta que está contida em um processo mais abrangente, qual seja, o Gerenciamento de Riscos. Portanto, extrai-se das palavras de Andrade (2017) que a AR é o processo por meio do qual se entende a natureza do risco e a consequente determinação de seu nível, que servirá de base para a Gestão de Riscos.

Para Heinz-Peter Berg (2010) a gestão de riscos é uma atividade que integra o reconhecimento de riscos, a sua avaliação, o desenvolvimento de estratégias para gerenciá-los e a sua mitigação por meio de recursos gerenciais que podem ser aplicados em toda a organização, independentemente das suas áreas e níveis. Na visão do autor, para elaborar uma análise de riscos é possível utilizar critérios qualitativos, semiquantitativos e quantitativos, desde que sejam observadas as características do risco, o objetivo da análise e as especificidades dos dados disponíveis (BERG, 2010).

De maneira geral, há inúmeros trabalhos e aplicações relacionados ao risco. Em 1992 o *Committee of Sponsoring Organizations* (COSO) ou Comitê das Organizações Patrocinadoras, da Comissão Nacional sobre Fraudes em Relatórios Financeiros, publicou o trabalho "Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO ERM)", com foco no gerenciamento de riscos corporativos. O COSO ERM (1992) visa formular estratégias para identificar os eventos potencialmente capazes de afetar a organização, administrando os riscos de modo a mantê-los compatíveis com o cumprimento dos seus objetivos.

No ano de 2001, o Tesouro Britânico produziu o "*Management of Risk – A Strategic Overview",* que rapidamente se tornou conhecido como *Orange Book*. Essa publicação forneceu uma introdução conceitual básica como um recurso para o desenvolvimento e implementação de processos de gerenciamento de riscos em organizações governamentais, na qual o risco pode ser entendido pela composição do cenário, das consequências e das probabilidades (UNITED KINGDOM, 2004).

No Brasil, o modelo de Gestão de Riscos mais conhecido é a Norma ISO 31000, que foi traduzida e adaptada pela Associação Brasileira de Normas Técnicas (ABNT) no ano de 2009. A ISO 31000:2009 é uma norma de gestão de riscos criada pela *International Organization for Standardization* (Organização Internacional para Padronização), que congrega agremiações de padronização e normalização de 162 países, com sede em Genebra, na Suíça.

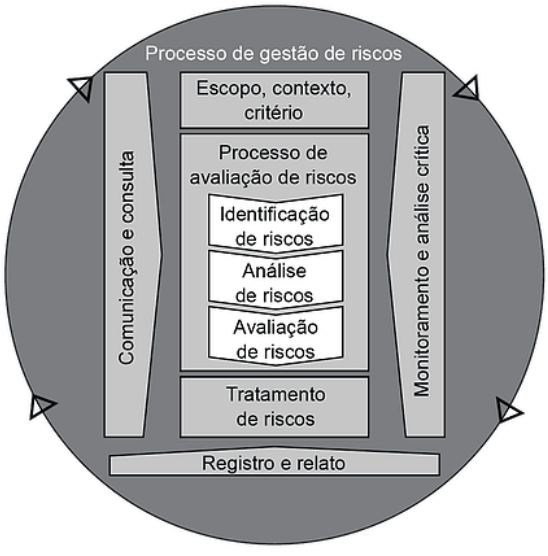
Revisada e atualizada pelo *Technical Committee Risk Management* (ISO/TC 262) no ano de 2018, a agora denominada ISO 31000 (2018) e a ISO/IEC 31010 (2009) estabelecem conceitos, princípios e orientações genéricas sobre gestão de riscos por meio de um *framework* universalmente reconhecido por tornar possível o gerenciamento de processos de diversos tipos de riscos de qualquer organização de qualquer segmento, independentemente do tamanho. As normas descrevem o processo sistemático de identificação, análise, avaliação e tratamento dos riscos, por meio de recomendações balizadas por princípios que precisam ser atendidos para tornar a gestão de riscos eficaz (ISO 31000:2018).

Framework de referência

Embora a prática do gerenciamento de riscos tenha sido desenvolvida ao longo do tempo e em muitos setores, para atender a diversas necessidades, a adoção de processos consistentes em uma estrutura abrangente ajuda a garantir que o risco seja gerenciado de forma eficaz, eficiente e coerente em toda a organização (ANDRADE, 2017).

A Norma ISO 31000 (2018) sugere como processo consistente de gestão de riscos o seguinte *framework*:

Figura 1 – Framework de Gestão de Riscos



Fonte: ISO 31000:2018

Percebe-se da Figura 1 que o modelo de gestão de riscos previsto na Norma ISO 31000 (2018) tem uma estrutura contínua, aplicada sequencialmente, sendo composta por cinco fases, além dos processos de Comunicação e Consulta e de Monitoramento e Análise Crítica, que são constantes:

a) Escopo, contexto e critério;

b) Identificação de Riscos;

c) Análise de Riscos;

d) Avaliação de Riscos; e

e) Tratamento de Riscos.

Entretanto, a Análise de Riscos é uma ferramenta sequencial autônoma, contida no Gerenciamento de Riscos. Pode-se dizer que a AR, em sentido estrito, corresponde tão somente à porção nuclear do modelo mencionado. Neste sentido, do ponto de vista da Análise de Riscos, pode-se perceber que o framework ISO 31000 (2018) acusa somente três fases: Identificação de Riscos, Análise de Riscos e Avaliação de Riscos (Figura 1).

Assim, levando em consideração que a abordagem generalista descrita nas normas ISO 31000 (2018) e ISO 31010 (2009) fornecem princípios e diretrizes básicas para o gerenciamento de riscos por meio de um modelo sistemático, transparente e confiável, que atende qualquer escopo ou contexto, reforça-se a possibilidade de se estabelecer um *framework* de Análise de Riscos que observe os preceitos da Doutrina Nacional de Inteligência Penitenciária (Dnipen).

Doutrina Nacional de Inteligência Penitenciária e a produção do conhecimento

Uma das missões institucionais do Departamento Penitenciário Nacional é a promoção de políticas públicas para a melhoria do sistema prisional. Entre elas se apresenta a elaboração e a adoção de princípios norteadores da atuação dos órgãos de administração penitenciária para a realização das atividades de Inteligência, aplicadas ao sistema prisional (BRASIL, 2020).

Partindo dessas premissas e, levando em consideração o aumento da sofisticação, da organização e da ousadia das facções criminosas no

planejamento e execução de ataques contra as instituições de Segurança Pública e da Sociedade, foi editada a Portaria nº 125, de 6 de maio de 2013, que instituiu a Doutrina Nacional de Inteligência Penitenciária (Dnipen), como instrumento orientador da atuação dos órgãos de inteligência prisional da União e das unidades federativas.

Redigida no formato de manual de instrução, a Dnipen indica as diretrizes, métodos e modelos que servem de sustentação para o exercício das atividades de inteligência no âmbito dos estabelecimentos prisionais. Atualizada pela última vez por meio da Portaria do Ministro nº 99 de 6 de março de 2020, a Doutrina Nacional de Inteligência Penitenciária não faz qualquer menção ao emprego da Análise de Riscos como um tipo próprio de conhecimento, mesmo tendo ela particularidades e especificidades que a qualifiquem para tanto.

Em sentido amplo, a produção de conhecimento de atividade de inteligência diz respeito ao tratamento dos dados obtidos (disponíveis ou não), transformados em conhecimentos avaliados, significativos, úteis, oportunos e seguros, realizado pelo profissional de inteligência, observada metodologia própria e específica.

De acordo com a Dnipen, a atividade de Inteligência Penitenciária (Ipen) é definida como:

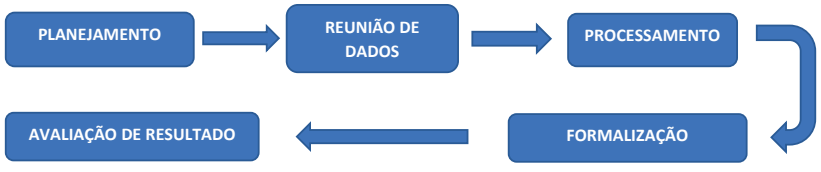
> [...] o exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais na esfera dos sistemas penitenciários, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os tomadores de decisão, para o planejamento e execução de políticas e das ações para prever, prevenir, neutralizar e reprimir atos criminosos (BRASIL, 2020).

Centrada na produção e na salvaguarda de conhecimentos utilizados no assessoramento da tomada de decisão no âmbito dos sistemas e instituições penitenciárias, a atividade de inteligência penitenciária faz uso de metodologia própria, por meio da adoção de procedimentos específicos e de técnicas voltadas para a produção do conhecimento, ficando excluídas a prática de ações meramente intuitivas ou sem orientação racional.

Portanto, a produção de conhecimento de inteligência penitenciária é definida como uma sequência ordenada de atividades, segundo a qual dados são obtidos e conhecimentos são produzidos, filtrados, protegidos e formalizados em documentos de inteligência direcionados ao tomador de decisão.

Trata-se de um processo contínuo e sequencial, que pode ser desenvolvido de forma simultânea ou alternada, cujo resultado pode gerar novos conhecimentos ou demanda. Em síntese, a metodologia da produção do conhecimento de inteligência penitenciária observa as seguintes etapas:

Figura 2 - Ciclo da Produção de Conhecimento



Fonte: Adaptado Dnipen (BRASIL, 2020)

O resultado do processo descrito na Figura 2 são os conhecimentos de inteligência. Estes são definidos e classificados pela Dnipen em quatro tipos:

a) **Informe:** é o conhecimento resultante de juízo(s) formulado(s), que expressa o estado de certeza, opinião ou de dúvida ante a verdade, sobre fato ou situação passada e/ou presente. Resulta da avaliação de situação ou fato passado ou presente quanto à idoneidade de sua fonte e à veracidade de seu conteúdo.

b) **Informação:** É o conhecimento resultante de raciocínio(s) e que expressa a certeza do analista ante a verdade, sobre fato ou situação passados e/ou presentes. A informação vai além da simples narração de fatos ou situações, contemplando a interpretação deles.

c) **Apreciação:** É o conhecimento resultante de raciocínio(s), que expressa o estado de opinião do analista ante a verdade sobre fato ou situação passados e/ou presentes. A Apreciação admite ainda a realização de projeções que resultem exclusivamente dos desdobramentos ou consequências dos fatos analisados mediante uso de técnicas prospectivas.

d) **Estimativa:** É o conhecimento resultante de raciocínio elaborado que expressa o estado de opinião sobre a evolução futura de fato ou situação. A produção requer o domínio completo das técnicas e métodos utilizados para a elaboração e acompanhamento de cenários prospectivos (BRASIL, 2020).

Partindo da premissa de que a Análise de Riscos (AR) trata da produção de conhecimentos organizados e processados, por meio de metodologia específica, a partir da qual são sugeridas ao tomador de decisão as ações e medidas de prevenção ou correção das possíveis falhas detectadas em determinado contexto, acredita-se que a AR deva ser entendida como um novo tipo de conhecimento a ser somado àqueles elencados pela doutrina (ANDRADE, 2017).

Nessa esteira, insta mencionar o que a própria Dnipen define como sendo algumas das principais finalidades de Inteligência Penitenciária a missão de "Proporcionar diagnósticos e prognósticos sobre a evolução de situações de interesse do Sistema Penitenciário, assessorando os usuários no processo decisório; [...]" (BRASIL, 2020)

Por fim, verifica-se que há precedente similar ao ora pretendido, quando se analisa o teor da Doutrina Nacional de Inteligência de Segurança Pública (Dnisp), que conceitua a Análise de Riscos como:

> [...] 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. (BRASIL, 2016)

Embora a Dnisp faça menção à Análise de Riscos como técnica assessória, acredita-se que também deva ser entendida como um novo tipo de conhecimento.

Ciclo de Análise de Riscos de Inteligência Penitenciária

Estabelecer o início do processo de Análise de Riscos é lembrar, antes de tudo que, conforme estabelecido no *framework* da ISO 31000:2018 (Fig. 1), a AR se trata de uma ferramenta autônoma, portanto, central de um processo maior que é a Gestão de Riscos. Ademais, conforme asseverado por Andrade (2017) a referida norma constitui uma abordagem genérica que pode ser adaptada a qualquer tipo de organização, de acordo com as suas necessidades específicas.

Saliente-se que o Ciclo da Análise de Riscos ora proposto para a Dnipen, não compreende a etapa "Tratamento de Risco", ou os aspectos de "Comunicação e Consulta" ou de "Monitoramento e Análise Crítica". A primeira porque a finalidade da atividade de Inteligência é produzir o conhecimento, de maneira estruturada e sistemática, com o objetivo de assessorar o tomador de decisão que definirá se, como e quando a

executará. Os dois últimos porque são constantes que permeiam todo o processo de Gestão de Riscos, tema esse que foge ao objeto da presente análise.

Partindo dessas premissas e visando a atender as características e práticas que caracterizam a atividade de Ipen, pode-se dizer que o Ciclo de Análise de Riscos de Inteligência Penitenciária deverá ser dividido em cinco fases: *Delimitação do Objeto de Análise*, *Identificação de Riscos*, *Estimativa de Riscos*, *Avaliação de Riscos* e *Encaminhamento*.

1ª Fase - Delimitação do Objeto de Análise

Assim como ocorre na fase de "planejamento" do Ciclo de Produção do Conhecimento de Inteligência Penitenciária, a *Delimitação do Objeto de Análise* deve ser considerada a primeira etapa do Ciclo de Análise de Riscos, uma vez que faz o diagnóstico inicial do contexto que se pretende analisar.

Ao delimitar o escopo que deverá ser analisado, passa-se ao emprego de técnicas que permitem identificar elementos essenciais descritos pelos conceitos de ativos, ameaças e vulnerabilidades (ISO/IEC 31010:2009):

Ativos: são os elementos valiosos para a organização sejam tangíveis, como os aspectos físicos, pessoal, materiais, projetos, planos, políticas, estratégias, documentos, ou intangíveis, como imagem, reputação, marca, símbolo, patente, propriedade intelectual, governabilidade, sensação de segurança cuja integridade pode ser afetada pelo risco.

Ameaças: ações naturais ou humanas, intencionais ou acidentais, que coloquem em risco os ativos a serem protegidos.

Vulnerabilidades: características de áreas, instalações e indivíduos, que sejam ativas e possam facilitar a concretização da ameaça.

Para que essa verificação seja possível, é necessário realizar o mapeamento detalhado dos ambientes externo e interno do "objeto" de análise, o que proporcionará uma ainda melhor delimitação.

O ambiente externo pode ser considerado como a relação que uma unidade ou sistema penitenciário tem com a comunidade, a localidade, a legislação, a estrutura econômica e política na qual está inserido e que pode impactar a consecução de seus objetivos institucionais. Portanto, a elaboração desses objetivos deverá considerar aspectos como localização

geográfica, criminalidade, ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, sejam eles internacionais, nacionais, regionais ou locais (ANDRADE, 2017).

O ambiente interno, por sua vez, é o contexto no qual a organização busca atingir seus objetivos alinhados 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 a organização.

O processo de identificação dos elementos anteriormente mencionados pode ser feito de maneira simples pelo analista de inteligência penitenciária, por meio do emprego de algumas ferramentas previstas na ISO/IEC 31010 (2009), como:

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.

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 anteriores ou como um resultado de falhas passadas.

Entrevista Estruturada: Em uma entrevista estruturada, os entrevistados são solicitados individualmente a responder a um conjunto de questões elaboradas que constam de 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.

No final dessa etapa, após o mapeamento dos elementos, espera-se o estabelecimento do contexto inicial por meio de um diagnóstico. Neste momento é indicada a implementação da chamada Matriz SWOT (Fig. 3: *strengths, weaknesses, oportunities, threats)*, 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

Fonte: Elaborado e adaptado pelo autor.

De acordo com Andrade (2017), a referida ferramenta direciona e disciplina o reconhecimento das ameaças e vulnerabilidades a fim de facilitar a futura identificação do risco. Ameaças sempre dizem respeito a situações externas às instituições que podem causar danos ou gerar crises. Por essa razão, geralmente são variáveis não controláveis que, em certos casos, podem ser controladas ou mesmo neutralizadas por meio de ações específicas.

As vulnerabilidades, por sua vez, são as características do ativo que podem facilitar a concretização da ameaça. Trata-se da suscetibilidade de um ativo em sofrer um 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 (ANDRADE, 2017).

Dessa forma, para a Delimitação do Objeto de Análise, 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.

2ª Fase - Identificação do Risco

Após a Delimitação do Objeto de Análise por meio de um diagnóstico descritivo (Apreciação), a Identificação do Risco se apresenta como

a próxima etapa de análise. Primeiramente, entretanto, faz-se necessário considerar a diferença existente entre os termos "risco" e "problema".

Enquanto o risco, em regra, é a incerteza sobre um evento futuro, identificá-lo é uma oportunidade de evitar um problema, prevenindo a sua ocorrência. O problema pode ser definido como algo concreto, que está ocorrendo e que precisa ser tratado emergencialmente. Dessa forma, o risco não é, em si mesmo, um fato, mas a interpretação do fato, sempre atinente ao futuro e, normalmente, algo negativo. A rigor, pode-se dizer que o maior objetivo da Análise de Riscos é impedir que o *risco* se torne um problema.

Ressalte-se que os riscos decorrem das ameaças e vulnerabilidades elencadas quando da elaboração da matriz SWOT. Somente haverá risco se houver uma fonte que o enseje, isto é, as ameaças devem ser analisadas conforme tenham potencial para originar o risco. As vulnerabilidades dos ativos, por sua vez, também são fundamentais nesse processo, pois, ao analisar quais ameaças são mais capazes de violar o ativo de um órgão, pode-se verificar quais são as vulnerabilidades que precisam ser corrigidas.

O passo seguinte é o reconhecimento e a descrição dos riscos por meio da planilha 5W2H adaptada, que é uma ferramenta administrativa que registra de maneira organizada e planejada como serão efetuadas as ações, a partir dos seguintes elementos: Quem, Quando, Onde, Porque e a Consequência. Uma vez identificados e bem delimitados, os riscos estão preparados para serem submetidos a um processo de mensuração ou valoração (ANDRADE, 2017).

3ª Fase - Estimativa dos Riscos: *Probabilidade x Impacto*

Trata-se da etapa do Ciclo de Análise de Riscos que fornece um processo estruturado para identificar como os objetivos de inteligência penitenciária podem ser afetados, levando 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 que está sendo analisado.

O estado de certeza sobre o risco fica caracterizado quando projetado um estado futuro, existe a probabilidade de ele se materializar. Dessa forma, uma vez identificados, os riscos devem ser estudados e decompostos de maneira a determinar o grau de sua relevância. Para tanto,

combinam-se a probabilidade da sua ocorrência e o seu impacto, considerando suas consequências, sejam elas tangíveis ou intangíveis.

Probabilidade

De acordo com a Norma ISO 31000 (2018), o termo probabilidade se refere à chance de algo acontecer, não importando se pode ser 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. No presente estudo, opta-se pela divisão em cinco níveis:

Figura 4 – Tabela de Valoração de Probabilidade

GRAU	VALOR
Extremamente Provável	5
Provável	4
Ocasional	3
Improvável	2
Raro	1

Fonte: Elaborado e adaptado pelo autor a partir da NBR ISO 31000.

Uma vez definida a tabela de probabilidades, torna-se fundamental compreender o tipo de análise a ser desenvolvida (qualitativa, quantitativa ou semiquantitativa), uma vez que será a partir dessa escolha que o analista de risco criará os parâmetros para cada uma das probabilidades, desde que haja dados que permitam que os eventos sejam mensurados.

Para que seja possível categorizar o grau de ocorrência de um determinado evento (probabilidade) em extremamente provável, provável, ocasional, improvável ou raro, deverão ser levados em consideração os conhecimentos produzidos anteriormente, bem como as opiniões dos especialistas. O detalhamento de cada um dos graus de ocorrência é importante para a *Estimativa dos Riscos*, já que, por meio dele, os especialistas conseguirão atribuir o respectivo valor, de acordo com a análise que se pretende realizar.

Do ponto de vista da doutrina de análise de riscos apresentada por meio da NBR ISO 31000 (2018), a probabilidade é a correlação de três elementos: ativo, ameaça e vulnerabilidade. Assim, pode-se dizer que reduzir a vulnerabilidade da instituição em relação à probabilidade de ocorrência de um determinado evento indesejado, necessariamente diminuirá o grau do risco analisado.

Para o levantamento das opiniões dos especialistas, sugere-se o emprego do método Mini Delphi, que consiste em combinar os apontamentos de cada um daqueles que possam contribuir com a estimativa de identificação na avaliação do risco, a partir da média dos pesos atribuídos a eles, separadamente.

A metodologia Delphi se baseia no trabalho em grupo que busca a convergência de opiniões de pessoas de notório saber com o intuito de minimizar os problemas típicos de organizações. Consiste em interrogar individualmente, por meio de sucessivos questionários, esse determinado grupo de pessoas (especialistas), dando-lhes oportunidades para que revejam suas opiniões, após conhecerem as dos demais integrantes do grupo (MARCIAL; GRUMBACH, 2013).

Para Marcial e Grumbach (2013), a estruturação do conhecimento, por meio da experiência e da criatividade dos especialistas, é melhor do que a opinião de um só indivíduo, ou mesmo de alguns indivíduos desprovidos de uma ampla variedade de conhecimentos especializados. A eficácia da metodologia leva em consideração até mesmo o erro desses especialistas. Mesmo que um deles esteja errado quanto à incerteza do futuro, a média das opiniões de vários especialistas se aproxima de uma valoração mais próxima da verdadeira.

Levando-se em consideração a dinâmica das atividades de Inteligência Penitenciária, aconselha-se a utilização do Método Mini Delphi, uma vez que, mantendo as principais características do método Delphi, o trabalho pode ser realizado com grande agilidade em uma única sessão. Uma vez mensurada a probabilidade do risco, parte-se para a estimativa do impacto de ocorrência do evento adverso.

Impacto

De acordo com Andrade (2017), diz-se que o impacto é a gravidade dos danos potenciais de uma ação hostil, sob a ótica da quantificação da consequência negativa presumível. O impacto pode ser mensurado

com base em diversos parâmetros, como a confiabilidade da imagem do sistema prisional, a sensação de segurança trazida pela unidade penal, a repercussão na mídia, no número estimado de perdas em recursos humanos, material e do público envolvido, dentre outros.

A análise do impacto permite associar um valor às consequências, normalmente negativas, decorrente de um risco que venha a se concretizar. Para tanto, assim como na probabilidade, é fundamental levar em conta a opinião dos especialistas, análise de cenários, além de outras técnicas elencadas na norma ISO 31010 (2009), conforme se observa no exemplo abaixo:

Figura 5 – Tabela de Valoração de Impacto

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

Fonte: Elaborado e adaptado pelo autor a partir da ISO 31000.

Recomenda-se que a categorização dos graus de impacto também seja descrita em detalhes, na medida que, por meio dela, os especialistas conseguirão atribuir o respectivo peso (valor), de acordo com a sua possibilidade/capacidade de análise diante do contexto.

Importante destacar que, no âmbito das unidades penais, tanto na avaliação da probabilidade quanto na do impacto, deve-se convocar pessoas que efetivamente trabalham com o tema. Neste sentido, pode-se listar como especialistas aptos a contribuir com a respectiva valoração: diretores de unidades, chefes de segurança, chefes de serviço, juízes, promotores, analistas de inteligência, dentre outros atores dos sistemas prisionais. A identificação dos valores pelos especialistas traz confiabilidade na avaliação, na medida que são eles os verdadeiros conhecedores do assunto e seus detalhes.

Assim como ocorreu no caso da probabilidade, sugere-se o emprego do método Mini Delphi, para o levantamento e combinação das opiniões dos especialistas que possam influenciar a estimativa e identificação dos riscos.

Compiladas as avaliações individuais, tira-se uma média dos pesos atribuídos pelos especialistas a cada impacto, calculada através da

soma dos valores referenciados na tabela, dividido pelo número de pessoas envolvidas na estimativa. A média deste conjunto definirá qual será o impacto do risco analisado.

Ressalte-se que, também como ocorreu no caso da probabilidade, dependendo do caso concreto, é possível reduzir o impacto, isolando a ameaça, ou aceitá-lo, criando planos de contingência como forma de mitigar a sua ocorrência (ANDRADE, 2017).

4ª Fase - Avaliação dos Riscos

A presente etapa consiste em relacionar os níveis de probabilidade e impacto estimados anteriormente de acordo com o contexto estabelecido. A partir dessa combinação, torna-se possível mensurar a real significância de cada risco.

Conforme visto anteriormente, as "grandezas" escolhidas (probabilidade e impacto) foram estabelecidas em 5 faixas que contém seus respectivos, grau e valor. Enquanto a probabilidade se refere à chance de algo vir a acontecer, o impacto se traduz por meio do valor atribuído à repercussão de uma ocorrência. Em ambas as situações, a estimativa será aferida ao se estabelecer uma, entre as 5 faixas de níveis e seu peso correspondente.

O produto dos pesos atribuídos pelos especialistas para probabilidade e impacto permite avaliar o grau de risco, 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, conforme o exemplo da Figura 6:

Figura 6 – Matriz de Riscos e Legenda

	GRAU DE IMPACTO					
Catastrófico		Médio	Médio	Alto	Muito Alto	Muito Alto
Crítico		Baixo	Médio	Médio	Alto	Muito Alto
Moderado		Baixo	Baixo	Médio	Médio	Alto
Leve		Muito Baixo	Baixo	Baixo	Médio	Médio
Insignificante		Muito Baixo	Muito Baixo	Baixo	Baixo	Médio
		GRAU DE PROBABILIDADE				
		Rara	Improvável	Ocasional	Provável	Extremamente Provável

LEGENDA:

Probabilidade	Peso	Impacto	Peso	Risco
Extremamente Provável (81 – 100%)	5	Catastrófico	5	Muito Alto
Provável (61 – 80%)	4	Crítico	4	Alto
Ocasional (41 – 60%)	3	Moderado	3	Médio
Improvável (21 – 40%)	2	Leve	2	Baixo
Rara (0 – 20%)	1	Insignificante	1	Muito Baixo

Fonte: Elaborado e adaptado pelo autor.

Por meio Matriz de Risco é possível demonstrar através da equação Probabilidade x Impacto, a real significância de cada risco e, consequentemente, das prioridades que precisam ser observadas pelos tomadores de decisão.

Superada a fase de *Avaliação dos Riscos*, passa-se à etapa que se decidiu denominar de *Encaminhamento*.

5ª Fase - Encaminhamento

Assim como os tipos de conhecimento tradicionalmente produzidos pela atividade de Inteligência Penitenciária (Informe, Informação, Apreciação e Estimativa) que são reduzidos a termo através de relatórios específicos, o produto do Ciclo de Análise de Riscos precisa ser devidamente formalizado para, na sequência, ser encaminhado para o seu destinatário, qual seja, o tomador de decisão. Em ambos os casos, há uma sequência metodológica, com fases determinadas e delimitadas.

Importante ressaltar, contudo, um dos pontos que difere o Ciclo de Produção do Conhecimento do Ciclo de Análise de Riscos. Enquanto no resultado da atividade de IPEN é contraindicado que se sugiram ações ou prioridades, a fim de se decidir o que deve ser feito. No Relatório de Análise de Riscos é importante selecionar e apontar as opções pertinentes, caso seja possível alterar a *probabilidade* de ocorrência, o efeito do seu *impacto* ou a ambos, no campo destinado às sugestões de tratamento de riscos.

Entretanto, como assevera Andrade (2017) 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 permanece destinada à uma etapa posterior:

"Tratamento de Riscos" que, como visto anteriormente, 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 consolidados em um relatório de Análise de Riscos (RAR) no qual constará o diagnóstico, os riscos identificados, sua estimativa e a avaliação com o seu respectivo campo de tratamento (ANDRADE, 2017).

Concluído o Ciclo de Análise de Riscos de Inteligência Penitenciária em comento, sugere-se a adoção desse novo tipo de conhecimento no bojo do Manual da Doutrina Nacional de Inteligência Penitenciária (BRASIL, 2020), a partir do modelo apresentado a seguir:

Figura 7 – Framework Gestão de Riscos DEPEN

Fonte: Elaborado e adaptado pelo autor

O valor de uma análise de riscos encaminhada de forma sistematizada aos tomadores de decisão não está no levantamento de uma determinada linha de ação, mas na capacidade de se distinguir entre diversas opções em um contexto mais amplo.

Assim, tem-se que a inclusão do *framework* proposto na Figura 7, além de observar as particularidades dos sistemas prisionais, reforça a importância da cultura da análise de riscos nos órgãos envolvidos na execução penal, por meio da realização da atividade de Inteligência Penitenciária.

Considerações finais

Conforme asseverado por Andrade (2019), a análise de riscos trata-se de um processo metodológico organizado e sistematizado, cujo objetivo é mensurar o efeito da incerteza em um determinado objetivo. Partindo dessa premissa, a análise de riscos pode ser estudada por meio de técnicas qualitativas, quantitativas ou mistas, a depender da quantidade de dados e informações disponíveis, principalmente quando se considera a similaridade das etapas dos *frameworks*.

Ao revisar a Doutrina Nacional de Inteligência Penitenciária, verifica-se um elevado potencial na sua aplicabilidade nos sistemas penais. Entretanto, ao buscar estudos relacionados especificamente à aplicação da análise de riscos com foco na segurança de estabelecimentos prisionais, pouquíssima menção foi encontrada e nenhum modelo foi, ao menos até o presente momento, elaborado.

Corrobora com a referida afirmação o que está previsto no item 65 do Relatório de Auditoria do Tribunal de Contas da União (BRASIL, 2017), no qual, após os estados Federados e o Distrito Federal terem sido instados a se manifestar quanto à existência de algum tipo de plano de gerenciamento de riscos de rebeliões pelos seus respectivos Tribunais de Contas, apenas cinco responderam positivamente: DF, MG, PA, PI e RS.

Essa grave ausência é mais um indicativo de que a formulação de políticas de segurança pública na área prisional é comumente caracterizada pela ausência de planejamento de longo prazo, pautando-se pela atuação reativa, ao invés de preventiva. Nas palavras de Silva (2020), se existe um mal que aflige a sociedade brasileira, e que precisa ser solucionado com urgência, é o da ausência de vontade política de questionar um modelo de justiça criminal antiquado, defasado e devastador da condição humana do delinquente.

Apesar de não ter tido o objetivo de esgotar todas as nuances que envolvem a Análise de Riscos, haja vista que detalhes mais profundos, como motricidade, dependência, gravidade, urgência de resolução e tendências do risco, por exemplo, foram propositalmente suprimidos, este trabalho se propõe a apresentar um modelo próprio de Análise de Riscos como importante ferramenta de assessoramento para o Departamento Penitenciário Nacional a partir da sua inclusão na Doutrina Nacional de Inteligência Penitenciária.

Dessa forma, a iniciativa deste trabalho vem no sentido de demonstrar a convergência existente entre o Ciclo da Produção de

Conhecimento de Inteligência Penitenciária e o Ciclo de Análise de Riscos de Inteligência Penitenciária proposto, de maneira a elevar a qualidade e eficiência da tomada de decisão dos gestores dos sistemas prisionais, na tentativa de antecipar, neutralizar ou mitigar os efeitos da ocorrência de eventos de natureza crítica em estabelecimentos penitenciários.

A adoção das práticas analíticas e sistemáticas fornecidas pela AR, além de atender os princípios estabelecidos na Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal), trata-se de elemento fundamental para a consolidação das diretrizes constantes no Plano Nacional de Segurança Pública e Defesa Social (BRASIL, 2018) e do Plano Nacional de Política Criminal e Penitenciária (BRASIL, 2019), além de estar alinhada às finalidades propostas pela Doutrina Nacional de Inteligência Penitenciária (BRASIL, 2020).

Bruno César Gomes da Rocha

Graduado em Direito pela Universidade Federal em Ouro Preto/MG, Especialização em Direito Público pelo Centro Universitário Newton Paiva, Especialização em Ciências Penais pela Universidade Anhanguera-UNIDERP, Mestrando em Administração Pública pela Universidade de Brasília.

Atua na Diretoria do Sistema Penitenciário Federal do Departamento Penitenciário Nacional. Interessa-se por Inteligência, Gestão de Riscos e Gerenciamento de Crises.
E-mail: bruno.rocha@mj.gov.br

Risk Analysis and National Doctrine of Penitentiary Intelligence

Abstract

This paper aims to propose a specific model of Risk Analysis as an important advisory tool for the National Penitentiary Department from its inclusion in the National Doctrine of Penitentiary Intelligence. To this end, a brief history will be presented on the increase in violence in penitentiary establishments, the Penal Execution Law, the Federal Penitentiary System, risk management and its most well-known frameworks, with emphasis on the adoption of ISO 31000: 2018 as a point of departure. From there, the evolution of concepts and characteristics related to risks will be addressed, demonstrating the existing convergence between the Penitentiary Intelligence Knowledge Production Cycle and the proposed Penitentiary Intelligence Risk Analysis Cycle. It is believed that the systematic adoption of Risk Analysis techniques within the scope of the National Doctrine of Penitentiary Intelligence will increase the quality and efficiency of decision-making by prison system managers in an attempt to anticipate, neutralize or mitigate the effects of the occurrence of events of a critical nature in penitentiary establishments.

Keywords: Risk management. Risk analysis. Intelligence. Penitentiary Intelligence. Knowledge Production. National Doctrine of Penitentiary Intelligence. ISO 31000:2018.

Referências

AGENTE penitenciário morre após ser baleado em casa na Zona Oeste de Natal. **Tribuna do Norte**, 10 out. 2017. Disponível em: http://www.tribunadonorte.com.br/noticia/agente-penitencia-rio-morre-apa-s-ser-baleado-em-casa-na-zona-oeste-de-natal/394402. Acesso em: 21 jun. 2020.

AGENTES revelam medo após morte de chefe do CDP: "Nas mãos dos presos"**. G1, Santos e Região, 22 ago. 2014.** Disponível em: http://g1.globo.com/sp/santos-regiao/noticia/2014/08/agentes-revelam-medo-apos-morte-de-chefe-de-cdp-nas-maos-dos-presos.html. Acesso em: 21 jun. 2020.

ALBUQUERQUE, C. E. P., ANDRADE, F. S. Análise de riscos com ênfase na segurança portuária: o processo de avaliação de riscos da CONPORTOS e o ISPS Code. **Revista Brasileira de Ciências Policiais**, Brasília, v. 10, n. 1, p. 99-124, jan./jun. 2019.

ALBUQUERQUE, M; COUTO, M. H. G.; OLIVA, F. L. **Identificação e análise dos riscos corporativos associados ao ambiente de valor do negócio de cacau da Cargill**. Cadernos EBAPE.BR, Rio de Janeiro, v. 17, nº 1, jan./mar., 2019.

ANDRADE, F. S. Análise de riscos e a atividade de inteligência. **Revista Brasileira de Ciências Policiais**, v. 8, n. 2, p. 91-116, 2017.

ANDRADE, F. S. **Análise de riscos estratégicos:** proposição de uma metodologia com foco nos valores organizacionais a partir do contexto da segurança pública. 2019. Dissertação (Mestrado em Engenharia de Produção) - Universidade Federal de Pernambuco, Recife, 2019.

AVEN, T. Risk assessment and risk management: Review of recent advances on their foundation. **European Journal of Operational Research**, v. 253, p. 1-13, 2016.

AVEN, T. et al. SRA Glossary. Committee on Foundations of Risk Analysis. **Society of Risk Analysis**, London, 2015.

BERG, H. P. Risk management: procedures, methods and experiences. **Reliability: Theory & Applications,** v. 2, n. 17, 2010.

BRASIL. Ministério da Justiça e Segurança Pública. Departamento Penitenciário Nacional. **Doutrina Nacional de Inteligência Penitenciária**. 2 ed. Brasília, DF: Depen, 2020.

BRASIL. Ministério da Justiça e Segurança Pública. Departamento Penitenciário Nacional. **Plano Nacional de Política Criminal e Penitenciária.** Brasília, DF: Depen, 2019. Disponível em: http://depen.gov.br/DEPEN/depen/cnpcp/plano_nacional-1. Acesso em: 10 maio 2020.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública**. 4. ed. Brasília, DF: Senasp, 2016.

BRASIL. Ministério Extraordinário de Segurança Pública. Secretaria Nacional de Segurança Pública. **Plano Nacional de Segurança Pública e Defesa Social.** Brasília, DF: Senasp, 2018. Disponível em:https://www.justica.gov.br/news/collective-nitf-content-1546269936.75. Acesso em: 10 maio 2020.

BRASIL. **Lei nº 7.210, de 11 de julho de 1984.** Institui a Lei de Execução Penal. Brasília, DF, julho, 1984. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7210.htm. Acesso em: 13 jul. 2020.

BRASIL. **Lei nº 8.072, de 25 de julho de 1990**. Dispõe sobre os crimes hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências. Brasília, DF, julho, 1990. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1990/lei-8072-25-julho-1990-372192-normaatualizada-pl.html. Acesso em: 13 jul. 2020.

BRASIL. **Lei nº 13.769, de 19 de dezembro de 2018**. Alterações legislativas. Brasília, DF, dezembro, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13769.html. Acesso em: 13 jul. 2020.

BRASIL. Tribunal de Contas da União. **Relatório de Auditoria**: Grupo I – Classe V – Plenário. Processo TC 003.673/2017-0. Ata 49/2017. Brasília, DF, 29 nov. 2017.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION – COSO. **Gerenciamento de riscos corporativos:** estrutura integrada, 1992.

DIRETOR penitenciário é assassinado a facadas. **JCNET.com.br,** Bauru e região, 7 out. 2012. Disponível em: https://www.jcnet.com.br/noticias/regional/2012/10/357201-diretor-penitenciario-e-assassinado-a-facadas.html. Acesso em: 21 jun. 2020.

EXPLOSIVOS e artilharia antiaérea para libertar um ladrão de banco na Paraíba**. El País,** 10 set. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/09/10/politica/1536604743_026484.html. Acesso em: 21 jun. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARTIZATION, **Risk management – Risk assessment techniques**. ISO/IEC 31010:2009. Geneva, 2009.

INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. **Risk management - Principles and guidelines**. ISO 31000:2018. Geneva, 2018.

JUSTEN, A. F.; FROTA, M. B. Planejamento e políticas públicas: apontamentos sobre as limitações em países em desenvolvimento. In: SIMPÓSIO IBEROAMERICANO EM COMÉRCIO INTERNACIONAL, DESENVOLVIMENTO E INTEGRAÇÃO REGIONAL, 8., 2017. **Anais**, v. 2. [...]. Cerro Largo, RS: RedCidir, 2017. Disponível em: https://www.uffs.edu.br/campi/cerro-largo/repositorio-ccl/anais-viii-simposio-iberoamericano-de-cooperacao-para-o-desenvolvimento-e-a-integracao-regional/planejamento-e-politicas-publicas-apontamentos-sobre-as-limitacoes-em-paises-em-desenvolvimento. Acesso em: 14 ago. 2020.

LUPTON, D. **Risk**. London: Routledge, 1999.

MARCIAL, E. C.; GRUMBACH, R. J. S. **Cenários prospectivos**: como construir um futuro melhor. 5. ed. Rio de Janeiro: Editora FGV, 2013.

MELO, F. A. L. **O dispositivo penitenciário no Brasil**: disputas e acomodações na emergência da gestão prisional**.** 2018. Tese (Doutorado em Sociologia) - Universidade Federal de São Carlos, São Carlos, SP, 2018.

PCC MATOU 3 agentes para intimidar e desestabilizar servidores de presídios federais. **UOL,** 29 jun. 2017. Seção Cotidiano. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/06/29/pcc-matou-3-agentes-para-intimidar-e-desestabilizar-servidores-de-presidios-federais.htm. Acesso em: 21 jun. 2020.

PCC OFERECE R$ 200 milhões por "resgate" de Marcola de prisão federal, diz inteligência da polícia**. Acesse Política,** Justiça, 26 jan. 2020. Disponível em: https://www.acessepolitica.com.br/faccao-oferece-r-200-milhoes-por-resgate-de-marcola-de-prisao-federal-diz-inteligencia-da-policia/. Acesso em: 21 jun. 2020.

PCC planejava onda de atentados e torturas contra agentes públicos. **Estadão**, Blog Fausto Macedo, 11 out. 2018. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/pcc-planejava-onda-de-atentados-e-torturas-contra-agentes-publicos/. Acesso em: 21 de jun. 2020.

QUEIRÓS, M., VAZ, T., PALMA, P. Uma reflexão a propósito do risco. In: CONGRESSO DA GEOGRAFIA PORTUGUESA, 6., 2007. Lisboa: Associação Portuguesa de Geógrafos, 2007.

REBELIÃO em RO termina com a morte de um agente e de três detentos. **Folha de S. Paulo**, Cotidiano, 25 jan. 2006. Disponível em: https://www1.folha.uol.com.br/fsp/cotidian/ff2501200616.htm. Acesso em: 21 jun. 2020.

REBELO, F. **Riscos naturais e acção antrópica**. Coimbra: Imprensa da Universidade, 2001.

RENN, O. **Risk Governance:** coping with uncertainty in a complex world. London: Routledge, 2008.

SEIS DIRETORES de presídios foram assassinados no Rio nos últimos oito anos. **BOL Notícias**, UOL, 16 out. 2008. Disponível em: https://noticias.bol.uol.com.br/brasil/2008/10/16/ult4733u23559.jhtm. Acesso em: 21 jun. 2020.

SILVA, L. G. Análise histórica do sistema penitenciário: subsídios para a busca de alternativas à humanização do sistema prisional. **Conteúdo Jurídico**, Brasília-DF: 24 nov. 2012. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/32634/analise-historica-do-sistema-penitenciario-subsidios-para-a-busca-de-alternativas-a-humanizacao-do-sistema-prisional. Acesso em: 29 jun. 2020.

SOCIETY FOR RISK ANALYSIS. **Foundations of risk analysis, developed.** [Discussion Paper]. 2015.

TORRES, E. N. S. **A gênese da remição de pena pelo estudo:** o dispositivo jurídico-político e a garantia do direito à educação aos privados de liberdade no Brasil. 2017. 290 f. Tese (Doutorado em Educação) – Universidade Estadual de Campinas (UNICAMP). Campinas, 2017.

UM DIA APÓS A REBELIÃO em presídio, dois agentes penitenciários são mortos a tiros em Goiás. **UOL,** Cotidiano, 2 jan. 2018. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2018/01/02/um-dia-apos-a-rebeliao-em-presidio-dois-agentes-penitenciarios-sao-mortos-a-tiros-em-goias.htm. Acesso em: 21 jun. 2020.

UNITED KINGDOM. **The Orange Book:** management of risk – principles and concepts. London: HM Treasury, 2004.