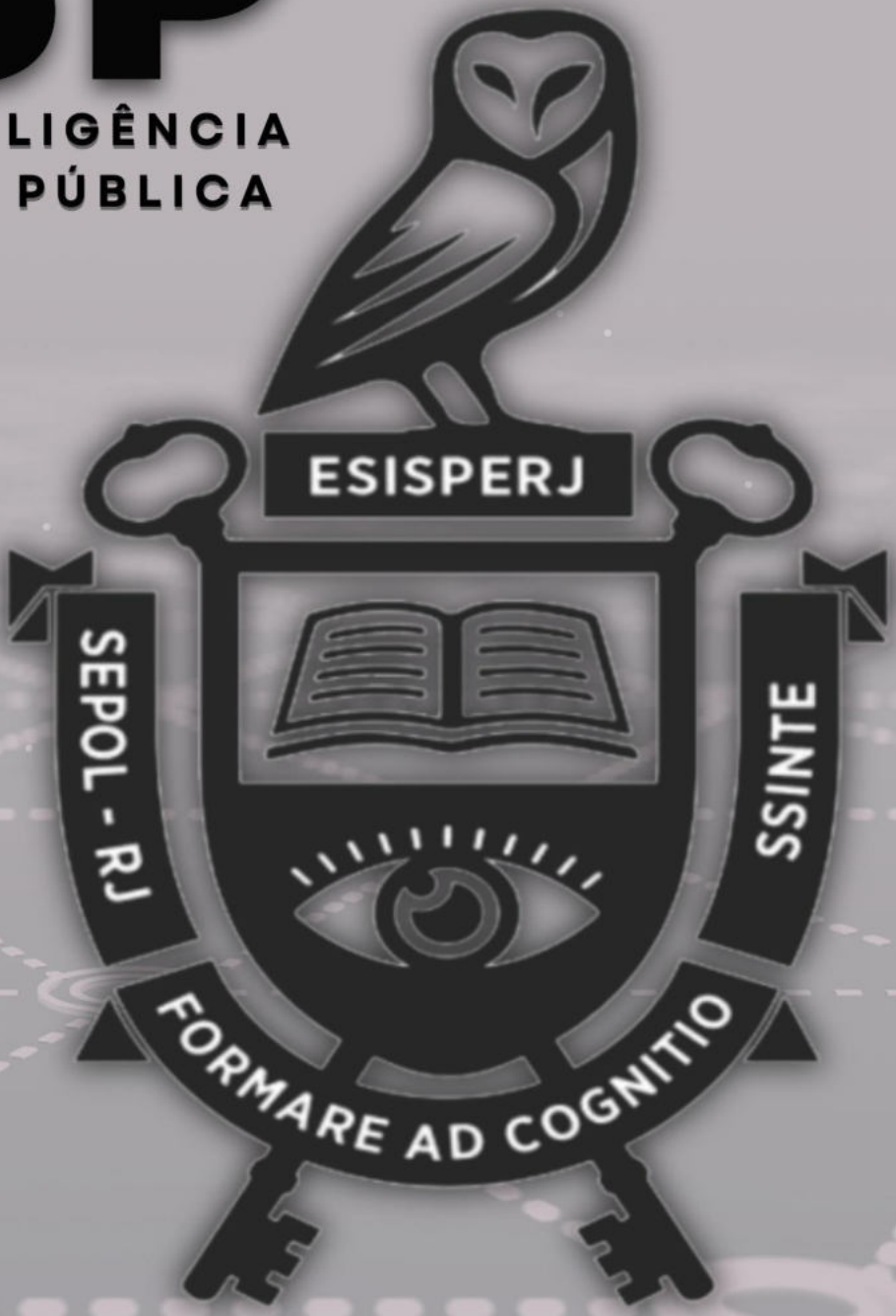
RISP

REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA



Número 9
2025

ISSN 2675-7168 ; 2966-0254

https://esisperj-ead.pcivil.rj.gov.br

risp.esisperj@pcivil.rj.gov.br

RISP – Revista de Inteligência de Segurança Pública

Número 9 – 2025

ISSN 2675-7168 (Impressa); 2675-7249 (CD-Rom); 2966-0254 (Online)

Esta obra está licenciada com uma Licença
Creative Commons Atribuição – Não Comercial 4.0 Internacional

EXPEDIENTE

Secretaria de Estado de Polícia Civil
Subsecretaria de Inteligência
Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro

Governador do Estado do Rio de Janeiro
Cláudio Bomfim de Castro e Silva

Secretário de Polícia Civil
Felipe Lobato Curi

Subsecretário de Inteligência
Flávio Marcos Amaral de Brito

Diretora-Geral da ESISPERJ
Carolina Salomão Albuquerque

Editora Chefe da RISP
Carolina Salomão Albuquerque

Editor Executivo da RISP
Leandro Martins de Paiva Passos

Revisores
Alessandra de Oliveira Rodrigues de Paiva Passos
Anderson Pereira Tavares
Maria Isabel Maia Marmello Henderson
Rafaela Silva Santos

Disponível em:
https://esisperj-ead.pcivil.rj.gov.br/login/index.php
https://www.policiacivil.rj.gov.br/publicacoesRisp

Conselho Editorial
• Carlos Augusto Neto Leba, SEPOL
• Carolina Salomão Albuquerque, SEPOL
• Fernando Antônio Paes de Andrade Albuquerque, SEPOL
• Flávio Porto de Moura, SEPOL
• Luiz Lima Ramos Filho, SEPOL
• Marcos Felipe Pereira Gonçalves da Mota, SEPOL
• Marcus Castro Nunes Maia, SEPOL

Comitê Editorial
• Flávio Marcos Amaral de Brito
• Marcelo Luiz Santos Martins
• Renata Teixeira de Assis
• Pablo Valentim
• Sergio Sahione Ferreira

Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro
Rua do Lavradio, 162. Centro. Rio de Janeiro, RJ.
Tel: (21) 3132-3007 e 3132-3007. E-mail: esisperj@pcivil.rj.gov.br

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

Revista de Inteligência de Segurança Pública [online] [impressa] [CD-Rom]/Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro, Subsecretaria de Inteligência, Secretaria de Estado de Polícia Civil. Número 9 (2025). Rio de Janeiro: ESISPERJ, 2025.

Anual
ISSN 2675-7168(Impressa);2675-7249(CD-Rom);2966-0254 (Online).

1. Inteligência – periódicos. 2. Segurança Pública – periódicos. 3. Segurança e Defesa – periódicos. 4. Educação Profissional e Inteligência – periódicos. Secretaria de Estado de Polícia Civil, Subsecretaria de Inteligência, Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro.

CDD 300

Dados internacionais de catalogação na publicação (CIP)

As opiniões expressas em artigos e entrevistas por autores são de responsabilidade exclusiva destes e não refletem, necessariamente, a posição institucional da ESISPERJ/SSINTE/SEPOL.

Sumário

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

EDITORIAL

No ano de 2024, a Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro realizou alguns cursos inovadores, somados às tradicionais capacitações amplamente conhecidas pela comunidade de Inteligência. O 1º Curso de Operações de Inteligência de Segurança Pública com Drones (1º COID/2024), o 1º Curso Básico de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (1º CTIR/2024) e o 1º Curso de Inteligência de Segurança Pública na Prevenção de Ataques à Escolas (1ºCISPPAE/2024), foram realizados no ano passado. Recentemente, foi realizado o Curso de Introdução à Análise de Riscos (1º CIAR/2025), em sua primeira edição. Todos são exemplos de inovação no ensino de ISP e esta edição da Revista de Inteligência de Segurança Pública (RISP) traz artigos relacionados a estes temas. Orgulhosamente, a escola pioneira no ensino de ISP do Brasil segue tradicional e alerta às demandas atuais da Inteligência.

No primeiro artigo, intitulado "A importância da Contrainteligência perante Incidentes Cibernéticos na Segurança Pública", o autor Anderson Tavares analisa o papel da Contrainteligência na Inteligência de Segurança Pública (ISP), focando na defesa contra ameaças cibernéticas. Aponta a necessidade de uma defesa cibernética robusta, sobretudo nos dias atuais, tendo em vista a inevitável dependência da internet e de sistemas computacionais nas atividades de segurança pública.

No segundo artigo, "Estudo sobre o Uso de Drones no BOPE para a Inteligência de Segurança Pública", de autoria de Henrique Machado, é abordada a utilização de drones como ferramenta de inteligência pelo Batalhão de Operações Policiais Especiais (BOPE), da Secretaria de Estado de Polícia Militar do Rio de Janeiro. O autor avalia o impacto da tecnologia nas operações da unidade, considerando benefícios, desafios e regulamentações.

Os autores Leonardo Luis e Guilherme Lopes, no terceiro artigo desta edição, "Análise de Risco para Locais de Eventos com Dignitários (ARLED): Análise de Risco para o Assessoramento ao Processo Decisório e ao Planejamento de Segurança de Eventos com a Participação de Dignitários", apresentam a metodologia de análise de risco que visa aperfeiçoar a segurança de altas autoridades em participação de eventos. Combinando aspectos da metodologia de Análise de Riscos de Pessoas (ARP) e da Análise de Riscos em Segurança

Orgânica (ARSO), a ARLED propõe uma abordagem integrada e estruturada para identificar e analisar ameaças e vulnerabilidades.

O quarto e último artigo, de autoria de Débora Rinaldi, com título "Violência Escolar: uma Discussão para Avaliar como a Atividade de Inteligência de Segurança Pública (ISP) pode Contribuir na Prevenção e Cuidado", explora como a ISP pode contribuir para prevenir a violência escolar no Brasil. Demonstra como o uso de ferramentas específicas para identificar sinais de alerta de violência e análise de perfis de potenciais agressores favorece a segurança no ambiente escolar.

Ótima leitura!

Carolina Salomão
Editora-chefe da RISP

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

A IMPORTÂNCIA DA CONTRAINTELIGÊNCIA PERANTE INCIDENTES CIBERNÉTICOS NA SEGURANÇA PÚBLICA

Anderson Pereira Tavares[*]

RESUMO

O presente estudo tem por objetivo analisar a atuação da Contrainteligência no contexto da Inteligência de Segurança Pública (ISP), com foco específico nos desafios e estratégias contemporâneos de defesa contra ameaças e incidentes cibernéticos, que se multiplicam a cada dia. A ISP, responsável por ações especializadas de defesa contra ameaças à segurança pública, encontra no ramo Contrainteligência a função primordial de proteger instituições, agentes e conhecimentos sensíveis de ataques adversos, atuando em todas as fases do ciclo de vida da informação. Com a crescente dependência da internet e de sistemas computacionais nas atividades de segurança pública, a necessidade de defesa cibernética robusta torna-se cada vez mais evidente. Este estudo busca compreender a vital importância da Contrainteligência na proteção orgânica das agências de Inteligência de Segurança Pública frente a alguns riscos cibernéticos. Busca-se, através de metodologia baseada na revisão bibliográfica e na pesquisa exploratória, elevar o interesse do leitor no desenvolvimento de rotinas incisivas e frequentes perante eventuais ataques cibernéticos, permitindo a análise crítica de diferentes cenários de ameaças através da educação de segurança e da proposição de soluções eficazes para a proteção de sistemas e informações sensíveis, por equipes especializadas que componham a Contrainteligência das agências de inteligência.

Palavras-chave: Inteligência; Contrainteligência; educação de segurança; cibersegurança; segurança da informação.

THE IMPORTANCE OF COUNTERINTELLIGENCE REGARDING CYBER INCIDENTS IN PUBLIC SECURITY

ABSTRACT

The present study aims to analyze the performance of Counterintelligence in the context of Public Security Intelligence (ISP), with a specific focus on contemporary challenges and strategies for defending against cyber threats and incidents, which multiply every day. The ISP, responsible for specialized defense actions against threats to public security, finds in the Counterintelligence branch the primary function of protecting institutions, agents and sensitive knowledge from adversary attacks, acting in all phases of the information life cycle. With the growing dependence on the internet and computer systems in public security activities, the need for robust cyber defense becomes increasingly evident. This study seeks to understand the vital importance of Counterintelligence in the organic protection of Public Security Intelligence agencies against some cyber risks. The aim is to, through a methodology based on bibliographical review and exploratory research, increase the reader's interest in developing incisive and frequent routines in the face of possible cyberattacks, allowing critical analysis of different threat scenarios through security education and proposition of effective solutions for the protection of sensitive systems and information, by specialized teams that make up the Counterintelligence of intelligence agencies.

Keywords: Intelligence; Counterintelligence; safety education; cybersecurity; information security.

[*]Comissário da Polícia Civil do Rio de Janeiro. Graduado em Letras pela Universidade Castelo Branco. Graduado em Direito pela Universidade São José. Concluinte do 7º Curso de Contrainteligência de Segurança Pública da Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro.

INTRODUÇÃO

Os avanços tecnológicos, cada vez mais presentes em nossa rotina, seja pessoal ou profissional, sabidamente nos trouxeram facilidades em diversos aspectos da vida cotidiana, desde uma simples encomenda comercial realizada por um aplicativo de telefone celular até a complexa inteligência artificial utilizada atualmente.

Com o crescente e abrangente uso da computação e, consequentemente, da interligação de rede mundial de computadores (internet), não somente pessoas de bem se beneficiaram, mas também criminosos passaram a usar de conhecimento aprimorado para a prática dos crimes cibernéticos, também chamados de cibercrimes, através de fraudes, sequestros de dados e outras práticas delituosas.

Visando à proteção institucional pela redução de vulnerabilidades e antecipação a ameaças, a atividade de Inteligência cumpre papel essencial na salvaguarda do Estado, das pessoas e das instituições. Nesse contexto, a Contrainteligência, como ramo da Inteligência de Segurança Pública (ISP), passa a ter grande importância na prevenção e no combate aos crimes virtuais em face de infraestruturas críticas, que possam levar a risco seus analistas, seus ativos institucionais e, por conseguinte, a segurança da população.

O estudo ora apresentado busca evidenciar a necessidade da capacitação e atualização de analistas de inteligência para a obtenção de resultados significativos na defesa de Agências de Inteligência de Segurança Pública (AISP), no que tange à chamada segurança cibernética, objetivando levar ao público-alvo, ou seja, aos profissionais de segurança, conhecimento útil e oportuno ao desempenho de suas funções na proteção da AISP.

Para isso, serão abordados alguns conceitos básicos, mas essenciais ao entendimento do presente trabalho, associados à ISP e, sobretudo, à Contrainteligência, assim como abordaremos a atuação desta na proteção de dados, infraestruturas críticas e ativos sensíveis. Também serão tratados a necessidade da educação de segurança dos analistas e os ataques cibernéticos mais comuns, envolvendo técnicas de engenharia social, além de alguns métodos de defesa e estatísticas referentes a incidentes cibernéticos recentes.

Considerando o objetivo deste estudo, a metodologia prevalecente será a revisão bibliográfica, com ênfase na pesquisa exploratória e na coleta de dados por meio da documentação indireta, somada a uma breve análise na forma quantitativa, envolvendo incidentes cibernéticos no Brasil.

O propósito deste estudo é despertar no leitor a necessidade de desenvolver rotinas de segurança cibernética incisivas e regulares. Através da análise crítica de diversos cenários de ameaças, busca-se fomentar a educação de segurança e a proposição de algumas soluções eficazes para a proteção de sistemas e informações sensíveis. A pesquisa enfatiza o papel crucial da contrainteligência em agências de inteligência como elemento central na implementação dessas medidas de segurança.

1 BREVES CONCEITOS DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA E DE CONTRAINTELIGÊNCIA

A Constituição Federal prevê que a segurança pública é dever do Estado, direito e responsabilidade de todos, sendo exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio (BRASIL,1988). Assim sendo, a segurança é um direito fundamental do cidadão brasileiro. Para garantir esse direito, as instituições de segurança necessitam de meios eficazes, destacando-se a Inteligência de Segurança Pública (ISP).

Conforme a Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ, 2015), a ISP abrange o conjunto de ações especializadas e permanentes, destinadas a subsidiar os tomadores de decisão através da identificação, avaliação e acompanhamento de ameaças, sejam reais ou potenciais, que atentem à ordem pública, à incolumidade das pessoas e do patrimônio.

As atividades de ISP são estruturadas em dois ramos interdependentes: Inteligência e Contrainteligência. Aquela possui como objetivo principal a produção de conhecimento, a partir da coleta, análise e interpretação de dados relevantes para a segurança pública, enquanto esta atua de forma complementar, visando proteger tanto a produção de conhecimento, quanto a própria instituição e seus agentes de ameaças internas e externas.

A Estratégia Nacional de Inteligência de Segurança Pública, define a Contrainteligência de Segurança Pública como:

> A atividade que objetiva prevenir, detectar, obstruir e neutralizar ações que constituam ameaça à atividade de Inteligência de Segurança Pública e à instituição a qual pertence e salvaguardar dados e conhecimentos sensíveis (BRASIL, 2021).

Já a Política Nacional de Inteligência de Segurança Pública complementa e estabelece que a Contrainteligência de Segurança Pública:

> Visa à prevenção, à detecção, à neutralização e à obstrução de ações e atividades que constituam ameaça à consecução plena da atividade de Inteligência de Segurança Pública e à atuação livre dos órgãos de segurança pública e das suas

> estruturas de inteligência, nas quais se incluem os dados e os conhecimentos sensíveis em poder do Estado (BRASIL, 2021).

Desse modo, cabe à Contrainteligência o desenvolvimento de atividades destinadas à proteção de dados, conhecimentos e infraestruturas críticas, todas sensíveis e sigilosas, em virtude de seus interesses estratégicos para a segurança nacional. Assim como o ramo Inteligência, a Contrainteligência também se destina à produção de conhecimentos, sempre no intuito da proteção e salvaguarda dos ativos institucionais de interesse da sociedade.

Para manter sua atuação de forma objetiva e estruturada, a Contrainteligência conta com segmentos qualificados para cada atividade específica, denominados Segurança Ativa (SEGAT), Segurança de Assuntos Internos (SAI) e Segurança Orgânica (SEGOR).

A SEGAT objetiva estabelecer, em caráter ofensivo, medidas e normas para detectar e neutralizar ações de inteligência adversa, sobretudo através da contrapropaganda, da contraespionagem, da contrassabotagem e do contraterrorismo. A SAI busca, em síntese, prevenir, identificar, obstruir e neutralizar possíveis desvios de conduta dos servidores da instituição. Já a SEGOR propõe um conjunto de normas, medidas e procedimentos, para garantir o funcionamento da agência de forma segura, atuando defensivamente frente a eventuais ameaças.

Portanto, a SEGOR visa efetivar a prevenção e neutralizar ameaças, sejam estas de qualquer natureza, através de medidas de proteção sobre as áreas e instalações, o pessoal, os materiais, os documentos, as operações de inteligência, as comunicações e a informática.

Conforme exposto até aqui, entende-se que cabe à Contrainteligência, por meio de seu seguimento denominado Segurança Orgânica (SEGOR), a responsabilidade pelo emprego de recursos humanos e tecnológicos destinados à proteção da infraestrutura de comunicações e da informática, abrangendo os conhecimentos sigilosos produzidos pelas agências de inteligência (AI).

2 ATUAÇÃO DA CONTRAINTELIGÊNCIA NA PROTEÇÃO DE DADOS, INFRAESTRUTURAS CRÍTICAS E ATIVOS SENSÍVEIS

A chamada OpSec (*Operational Security*), que pode ser traduzida como Segurança Operacional, busca identificar, quantificar e mitigar os riscos de ameaça às informações sensíveis de uma organização. Richard Brito Guedes de Sousa (2023) define OpSec como “medidas adotadas para proteger informações sensíveis e evitar que sejam exploradas por adversários”.

A Contrainteligência, por meio de sua SEGOR, deve utilizar a OpSec de maneira contínua, visando identificar e mitigar possíveis deficiências nas medidas de proteção empregadas, sempre balanceando suas medidas de controle e as fragilidades identificadas.

Assim, utilizando-se da OpSec, a Contrainteligência traçaria algumas medidas, iniciando pela medição do nível de risco a que a instituição está exposta e comparando as ações de segurança já implementadas com as vulnerabilidades existentes e potenciais.

A partir da identificação das fraquezas e das limitações do sistema de segurança de informações, torna-se possível admitir medidas para fortalecê-lo, reduzindo o risco de incidentes e, consequentemente, de ataques cibernéticos aos dados sensíveis das agências de Inteligência de Segurança Pública.

Relevante diferenciar, de forma básica, a espionagem cibernética e o ataque cibernético, cabendo àquela a coleta clandestina de informações, sem a intenção destrutiva, e a este a manipulação, exposição, alteração ou a destruição do sistema de dados atacados, seja de forma parcial ou total. Porém, cabe salientar que para as duas ações podem ser utilizadas as mesmas técnicas.

Sabe-se que os ataques cibernéticos, também chamados de ciberataques, trazem aos sistemas ameaças de interrupção, interceptação e modificação nos bancos de dados de inteligência. Em suma, tais ameaças colocam em risco a chamada tríade de pilares da segurança da informação: confidencialidade, integridade e disponibilidade.

Conforme a ISO 27001, norma elaborada para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI), os pilares supracitados são assim definidos:

> A disponibilidade está relacionada ao tempo e à acessibilidade que se tem dos dados e sistemas da organização, esse princípio é de suma importância, pois, falhas de indisponibilidade comprometem o serviço prestado pela organização (ISO 27001:2006).
> Integridade é que garante a veracidade da informação e restringe o acesso e/ou alteração da informação por pessoas não autorizadas, garante a completude e preservação da precisão da informação, para que não haja perda de partes da informação (ISO 27001:2006).
> A confidencialidade é o que garante o sigilo de informação e impede que elas não sejam roubadas ou acessadas por pessoas não autorizadas (ISO 27001:2006).

A perda do sigilo de informações constantes nos bancos de dados de uma agência de inteligência, provocada pelo acesso indevido, viola um dos princípios básicos da segurança da informação, ou seja, o princípio da confidencialidade.

Certamente, a execução de um Plano de Resposta a Incidentes Cibernéticos pela instituição é de extrema importância para a prevenção, o tratamento e a resposta a eventuais ataques cibernéticos, trazendo formas rápidas e eficazes de segurança.

Dentre as medidas previstas no supracitado plano, a efetiva compartimentação do acesso aos conhecimentos sigilosos deve ser observada, assim como a análise constante de *logs* (registros) no sistema, efetuada através de auditorias, e a realização de *backups* (cópias) frequentes para garantir a recuperação de dados eventualmente modificados ou destruídos.

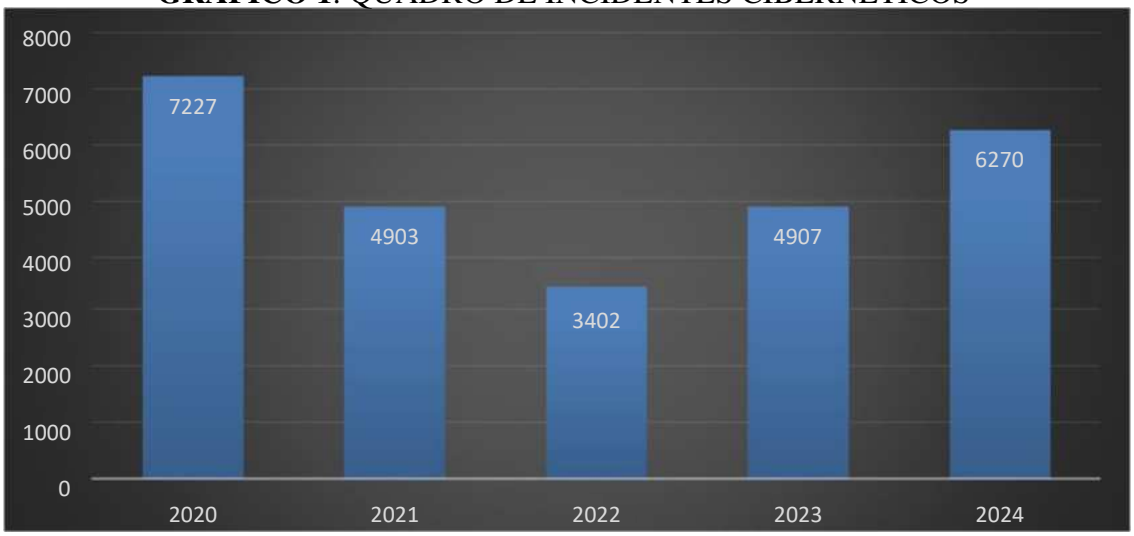
Como objeto de estudo, cabe apresentar possíveis e mais recomendadas ações de defesa, como *Firewalls*, sistemas de detecção de intrusão (IDS), sistemas de prevenção de intrusão (IPS) e antivírus, que monitoram a rede em busca de atividades suspeitas, detectam, bloqueiam e removem malwares, ou seja, softwares maliciosos.

A atualização dos softwares de proteção das redes, como os antivírus, deve ser efetuada constantemente, utilizando-se as versões mais atuais.

Compõem outras medidas importantes o uso de criptografias na transmissão de documentos sigilosos e a possível segmentação de redes, que pode limitar o impacto de uma possível invasão. O estabelecimento de um canal técnico adequado e seguro entre agências é de suma importância.

Segundo informações do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov), já foram registrados mais de seis mil incidentes em 2024. O CTIR Gov define um incidente de segurança como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores. Segue gráfico apresentando a evolução dos incidentes a partir do ano de 2020.

GRÁFICO 1: QUADRO DE INCIDENTES CIBERNÉTICOS



Fonte: Elaborado pelo autor a partir dos dados contidos no CTIR Gov. 2024

Pelos dados apresentados no gráfico acima, que registram incidentes cibernéticos até 13/09/2024, já vemos números superiores aos anos anteriores, que sugerem que ultrapassaremos o recorde registrado em 2020. Esse fato reforça a relevância do presente estudo e, consequentemente, do papel da Contrainteligência na efetiva defesa dos ativos institucionais sensíveis, como os conhecimentos produzidos pelos órgãos de inteligência.

3 A IMPORTÂNCIA DA EDUCAÇÃO DE SEGURANÇA EFETUADA PELA CONTRAINTELIGÊNCIA

Preliminarmente, cumpre estabelecer uma diferenciação básica quanto às ameaças, cabendo duas classificações: as externas e as internas.

As ameaças externas são provenientes de agentes não autorizados a usar uma rede ou um dispositivo, utilizando-se de acesso clandestino e ilegal. Nesse grupo podem-se incluir criminosos organizados, hackers profissionais ou até mesmo agentes patrocinados pelo Estado para objetivos escusos. Os chamados "hacktivistas", criminosos que invadem dispositivos por motivações políticas ou sociais, também estão incluídos nesse rol.

Quanto às ameaças internas, são oriundas de usuários que possuem acesso autorizado e legítimo aos ativos de uma instituição e o utilizam de modo indevido, provocando prejuízos reais ou potenciais no sistema, mesmo que de forma acidental.

Para evitar tais comportamentos, a Contrainteligência, por intermédio da SEGOR e de suas medidas de segurança de pessoal, possui um conjunto de normas e procedimentos denominado Processo de Recrutamento Administrativo (PRA). Essas medidas são voltadas para a segura admissão, o acompanhamento das atividades e o correto desligamento dos recursos humanos de uma agência de inteligência.

Um dos procedimentos presentes no Processo de Recrutamento Administrativo prevê que os analistas sejam submetidos à rotina de educação de segurança, que abrange três formas de orientação: inicial, específica e periódica.

A orientação inicial aos servidores ingressos na agência visa apresentar todas as medidas de segurança orgânica exigíveis pela agência para atuação na instituição, antes do início efetivo do desempenho de sua função. A orientação específica, a cargo da chefia imediata, deverá apresentar aos servidores os procedimentos de segurança inerentes às funções que irão desempenhar, orientando-os quanto aos procedimentos de Segurança Orgânica a serem observados no exercício da função, assegurando a salvaguarda da agência e dos conhecimentos sigilosos. Já a orientação periódica visa abordar as medidas de segurança vigentes, a importância de seu cumprimento, as possíveis vulnerabilidades e

o comportamento esperado dos servidores no sentido de preveni-las.

Dentre as medidas de segurança, deve-se orientar os analistas para a proteção e o uso de senhas fortes de acesso aos sistemas sensíveis. Comportamentos estranhos e eventuais ameaças ou ataques devem ser reportados imediatamente à SEGOR, atendendo à cultura eficaz de segurança, salientando que a segurança da agência é dever de todos.

Ressalta-se que um analista que armazena informações confidenciais de forma descuidada, não obedecendo aos princípios da compartimentação e do sigilo das informações, não está cometendo um ataque cibernético.

Entretanto, um analista que usa intencionalmente seus privilégios de acesso para realizar atividades mal-intencionadas, provocando o vazamento de informações sigilosas e atingindo de maneira nociva os ativos institucionais sensíveis da agência, está sujeito à imputação de crime de violação de sigilo funcional, além de outros possíveis crimes conexos.

> Art. 325. Revelar fato ou circunstância de que tem ciência em razão do cargo ou função e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa, se o fato não constitui crime mais grave. (BRASIL, 1940)

As causas mais comuns do vazamento de dados e informações sigilosas são a insatisfação, a vingança e os motivos financeiros. Para evitar essas atitudes, que podem comprometer os dados sensíveis da agência, a SEGOR deve atentar-se sempre aos comportamentos estranhos, cabendo a possível atuação do seguimento de Segurança de Assuntos Internos (SAI) nos casos de desvios de conduta. Vale lembrar que os seguimentos de Contrainteligência devem atuar de forma complementar, colaborativa, integrada e harmônica entre si.

4 ANALISTAS E OS ATAQUES DE ENGENHARIA SOCIAL

Conforme apresentado no tópico anterior, fica evidente que ações imprudentes ou negligentes dos analistas podem facilitar a ocorrência de incidentes cibernéticos nas agências de inteligência.

Para Mitnick (2003), “engenharia social é uma técnica de ataque que explora a vulnerabilidade humana, por intermédio da persuasão e enganação para conseguir informações, utilizando-se da tecnologia ou não”.

Pelo teor deste estudo, que cadencia para a educação de segurança dos analistas, cumpre apresentar, como forma de exemplificação, ataques cibernéticos que envolvem práticas de engenharia social, visto que exploram vulnerabilidades humanas. Vejamos algumas técnicas:

- *Phishing*: uma das técnicas mais utilizadas pelos criminosos, que se utilizam de emails ou outras mensagens fraudulentas para reproduzir empresas ou pessoas

conhecidas a fim de obter informações confidenciais. A vítima, enganada, acaba por passar senhas ou outros dados pessoais e sigilosos;

- *Pretexting*: consiste em criar um cenário falso para obter informações confidenciais ou ganhos financeiros. Através desse ataque, a vítima é ludibriada por uma história inventada e acaba expondo a agência;
- *Baiting (quid pro quo)*: através desse ataque, os criminosos oferecem um incentivo ou uma facilidade para que a vítima execute uma ação maliciosa. Citamos como exemplo o oferecimento de uma assinatura gratuita, durante um período, de uma plataforma paga. Frente ao suposto benefício, ao acessar um link infectado, o agente acaba se expondo ao ataque;
- *Vishing*: envolve mais interações humanas, já que ocorre através de contatos telefônicos fraudulentos, com o intuito de extrair informações sigilosas das vítimas, como por exemplo, senhas de acesso, ao passar-se o criminoso por um representante empresarial ou pessoa confiável;
- *Pharming*: possui práticas semelhantes ao *Phishing*, pois busca informações pessoais, porém caracteriza-se por ações fraudulentas praticadas especificamente através do direcionamento das vítimas a um site falso na internet, geralmente muito similar ao legítimo, não despertando desconfiança no usuário, que acaba por ter seus dados coletados de forma ilegal.

Diante do apresentado, torna-se crucial a educação de segurança dos analistas, posto que as orientações específicas visam à conscientização e ao treinamento para melhores práticas de segurança, como identificar e evitar ataques de engenharia social, para que não exponham os conhecimentos sigilosos produzidos nas agências.

CONCLUSÃO

Uma agência de inteligência, pela essência de sua atribuição, que objetiva a produção de conhecimento oportuno e útil, naturalmente dispõe de informações sigilosas, sejam elas classificadas como reservadas, secretas ou ultrassecretas. Por isso, é importante que a proteção dessas informações sensíveis seja um dos objetivos principais da Contrainteligência, posto que sua exposição pode acarretar danos à organização e à sociedade de modo geral.

Neste estudo, vimos que cabe à Contrainteligência atuar com eficiência diante dos desafios advindos da evolução constante dos crimes cibernéticos e da eventual vulnerabilidade de infraestruturas críticas ligadas às Agências de Inteligência de Segurança Pública.

Por meio de ações especializadas, a Contrainteligência busca prevenir, detectar, identificar e neutralizar ações adversas que

visem ao acesso não autorizado ou à manipulação indevida de dados e informações sensíveis, protegendo assim os recursos humanos, materiais e informacionais da instituição.

Sendo assim, conclui-se que cabe à Segurança Orgânica, como seguimento da Contrainteligência, obstruir e frustrar eventuais ameaças cibernéticas, mitigando os riscos de acesso clandestino aos conhecimentos e dados sensíveis armazenados nos dispositivos informáticos e àqueles transmitidos pela rede de computadores, seja ela privada (intranet ou extranet) ou pública (internet).

Conforme visto, a educação de segurança dos analistas torna-se essencial para que estes não coloquem em risco o sistema e o banco de dados das agências de inteligência, seja por atos negligentes, imprudentes ou amadores. Nesse sentido, tornam-se primordiais as orientações previstas no Processo de Recrutamento Administrativo dos analistas.

Além disso, demonstra-se crucial a criação e o treinamento de uma equipe de resposta a incidentes, responsável por lidar com incidentes de segurança inerentes aos bancos de dados da instituição.

As ameaças e os ataques cibernéticos estão em constante evolução, logo as estratégias de defesa também devem ser atualizadas regularmente. A segurança cibernética deve ser vista como um processo contínuo, a ser promovido por todos os integrantes de uma agência de inteligência, sobretudo aos analistas que compõem o efetivo da Contrainteligência.

REFERÊNCIAS BIBLIOGRÁFICAS

ASER SECURITY. Os 7 tipos de ataques cibernéticos mais comuns. Disponível em: https://www.aser.com.br/os-7-tipos-de-ataques-ciberneticos-mais-comuns/. Acesso em: 15 ago. 2024.

BRASIL. Código Penal Brasileiro. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 06 jan. 2017.

BRASIL. Decreto nº 10.778, de 24 de agosto de 2021 Aprova a Estratégia Nacional de Inteligência de Segurança Pública. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/ENINT.pdf. Acesso em: 10 set. 2024.

BRASIL. Doutrina da Atividade de Inteligência. 4. ed. - Brasília: Agência Brasileira de Inteligência, 2023.

CTIPs. CREST. O que é inteligência contra ameaças cibernéticas e como ela é usada? 2019. Disponível em: https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf. Acesso em: 10 fev. 2024.

CTIR Gov. Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 13 set. 2024.

GUEDES, Richard. O Emprego da OpSec. Disponível em: <https://dciber.org/o-emprego-do-opsec/>. Acesso em: 18 set. 2024.

IBM. O que é um ataque cibernético? Disponível em: https://www.ibm.com/br-pt/topics/cyber-attack. Acesso em: 10 set. 2024.

MICROSOFT CORPORATION. O que é Segurança Cibernética. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-cybersecurity. Acesso em: 16 set. 2024.

MINISTÉRIO DA JUSTIÇA. Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública – DNISP. Brasília, 2023.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar: ataques de harckers: controlando o fator humano na segurança da informação. São Paulo: Person Education, 2003.

RIO DE JANEIRO. Decreto nº 45.126, de 13 de janeiro de 2015. Aprova a nova Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ) e dá outras providências.

WOLOSYN, André Luis. Inteligência Militar: o emprego no Exército Brasileiro e sua evolução. Rio de Janeiro: Biblioteca do Exército, 2018.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

ESTUDO SOBRE O USO DE DRONES NO BOPE PARA A INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Henrique de Souza Machado[*]

RESUMO

Este estudo aborda a utilização de drones pelo Batalhão de Operações Policiais Especiais (BOPE) como ferramenta de inteligência e reforço à segurança pública. Com o avanço tecnológico e a crescente sofisticação das ações do crime organizado no Brasil, os drones se consolidaram como recursos estratégicos para monitoramento, vigilância e mitigação de riscos em operações táticas. O objetivo central desta pesquisa é analisar o impacto da adoção dessa tecnologia nas atividades do BOPE, considerando sua aplicação prática, benefícios operacionais, desafios enfrentados e conformidade com as regulamentações vigentes, especialmente as normativas da Agência Nacional de Aviação Civil (ANAC) e do Departamento de Controle do Espaço Aéreo (DECEA). Para isso, foi realizada uma abordagem qualitativa, baseada na análise de dados operacionais e estudos de caso. Os resultados indicam que o uso de drones proporciona vantagens significativas, incluindo a redução de custos operacionais, ampliação da segurança dos agentes, coleta de dados em tempo real e maior precisão na tomada de decisões estratégicas. Além disso, a pesquisa destaca a necessidade de treinamento contínuo e desenvolvimento de protocolos específicos para otimizar o emprego desses equipamentos em cenários de alto risco. Dessa forma, conclui-se que a incorporação de drones nas operações do BOPE representa um avanço tecnológico essencial para o fortalecimento das ações policiais especializadas.

Palavras-chave: drones; BOPE; inteligência; segurança pública.

STUDY ON THE USE OF DRONES IN BOPE FOR PUBLIC SECURITY INTELLIGENCE

ABSTRACT

This study addresses the use of drones by the Special Police Operations Battalion (BOPE) as an intelligence tool and a reinforcement for public security. With technological advancements and the increasing sophistication of organized crime activities in Brazil, drones have become strategic resources for monitoring, surveillance, and risk mitigation in tactical operations. The central objective of this research is to analyze the impact of adopting this technology in BOPE's activities, considering its practical application, operational benefits, challenges faced, and compliance with current regulations, especially the standards set by the National Civil Aviation Agency (ANAC) and the Department of Airspace Control (DECEA). To achieve this, a qualitative approach was conducted, based on the analysis of operational data and case studies. The results indicate that the use of drones provides significant advantages, including reduced operational costs, enhanced officer safety, real-time data collection, and greater accuracy in strategic decision-making. Furthermore, the research highlights the need for continuous training and the development of specific protocols to optimize the use of these devices in high-risk scenarios. Thus, it is concluded that the incorporation of drones into BOPE operations represents an essential technological advancement for strengthening specialized police actions.

Keywords: drones; BOPE; intelligence; public security.

[*] Pós-graduado em História do Rio de Janeiro, Graduado em Gestão de Segurança Pública pela UNESA, concluinte do 1º Curso de Operações de Inteligência de Segurança Pública com drones da ESISPERJ/SSINTE/SEPOL, Primeiro-sargento da Polícia Militar do Estado do Rio de Janeiro. Endereço eletrônico: machados.henriques@gmail.com

INTRODUÇÃO

A segurança pública no Rio de Janeiro enfrenta desafios significativos e complexos, especialmente em comunidades que possuem atuação e/ou domínio de facções criminosas. A utilização de drones na atividade de Inteligência tornou-se uma ferramenta crucial no enfrentamento desses desafios de forma eficaz, subsidiando a tomada de decisões e contribuindo para a eficiência e a eficácia das ações operacionais do comando da unidade (Agência Brasil, 2024).

No cenário brasileiro, esse avanço tecnológico ganha particular relevância na atuação de unidades especializadas, como o Batalhão de Operações Policiais Especiais (BOPE), da Secretaria de Estado de Polícia Militar, que integra essas tecnologias para aprimorar suas ações de inteligência e segurança pública. Apesar de seu grande potencial, o uso de drones também impõe desafios relacionados à regulamentação, segurança operacional e ao controle do espaço aéreo, aspectos fundamentais para garantir a eficácia dessas tecnologias (Souza; Santos, 2019).

O cenário atual revela a crescente demanda por soluções tecnológicas que complementem e otimizem as operações policiais, principalmente em áreas urbanas densamente povoadas ou em regiões de difícil acesso. O uso de drones no BOPE, especificamente, tem se mostrado uma ferramenta estratégica para a obtenção de informações em tempo real, permitindo uma análise precisa das movimentações criminosas e a coordenação das ações em campo. Contudo, o uso dessa tecnologia levanta uma série de questões, como a adequação das regulamentações, os custos operacionais e a efetividade na prevenção de crimes em tempo real. Além disso, os drones desempenham um papel crucial na mitigação de riscos para os agentes de segurança, garantindo operações mais seguras e eficazes, o que se torna especialmente relevante em operações de alto risco, como as realizadas em áreas dominadas por facções criminosas (Jorge, 2020; Rezende, 2020; Bastos; Roldão, 2019).

Considerando o conceito de atividade de Inteligência de Segurança Pública (ISP), disposto na Doutrina de Inteligência de Segurança Pública do Estado do Rio de Janeiro (DISPERJ), o drone é uma ferramenta essencial a ser inserida nas ações de ISP para reunir dados.

A atividade de Inteligência de Segurança Pública (ISP) é o exercício permanente e sistemático de ações especializadas para a identificação, acompanhamento e avaliação de ameaças reais ou potenciais na esfera da Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os governantes e tomadores de decisões, para um planejamento

mais adequado e para a execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza ou atentatórios à ordem pública (DISPERJ, 2015).

O uso de tecnologias avançadas, como os drones, é considerado fundamental para a obtenção de dados negados através de outros meios, revelando os aspectos ocultos da atuação criminosa que seriam de difícil constatação pelos meios clássicos de buscas na atividade de ISP.

A hipótese está relacionada entre os possíveis benefícios proporcionados pelo uso de drones nas operações do BOPE. A real eficácia dessa tecnologia pode ser limitada por fatores como a falta de uma regulamentação adaptada à rápida evolução tecnológica, a complexidade do controle do espaço aéreo e a integração eficaz com outras plataformas de monitoramento. Assim, embora os drones representem um avanço para a segurança pública, sua efetividade depende de uma série de ajustes, incluindo a capacitação dos operadores e a constante atualização das normas regulatórias.

A justificativa para o estudo do uso de drones no BOPE para a Inteligência de Segurança Pública reside na necessidade de aprimorar as estratégias de monitoramento e intervenção policial em um contexto de crescente sofisticação das organizações criminosas. A integração das tecnologias aéreas, como os drones, na rotina das operações do BOPE pode proporcionar uma abordagem mais eficiente e coordenada na coleta de informações, além de permitir uma resposta mais ágil a movimentações criminosas. O emprego dessas ferramentas contribui diretamente para a segurança dos agentes e a redução de danos colaterais, como evidenciado em operações anteriores em que a tecnologia foi utilizada de forma eficaz. Este estudo se justifica, portanto, pelo potencial dos drones em transformar as práticas operacionais do BOPE, promovendo um modelo de atuação mais eficiente, seguro e com menores custos operacionais (Jorge, 2020; Machado, 2024).

O objetivo geral deste estudo é analisar o impacto da utilização de drones nas Operações de Inteligência e de Segurança Pública realizadas pelo Batalhão de Operações Policiais Especiais (BOPE), da Polícia Militar do Estado do Rio de Janeiro.

Para isso, consideram-se os seguintes objetivos específicos: investigar de que maneira os drones são empregados em operações de Inteligência, vigilância e intervenção; examinar as vantagens oferecidas pelos drones, como a redução de custos operacionais e o aumento da segurança para os agentes de segurança pública; analisar como a utilização de drones pode ser coordenada com outras plataformas de monitoramento; investigar como a transmissão de dados e imagens em tempo

real entre os drones e as equipes em campo pode impactar a tomada de decisão; estudar como o uso de drones pode reduzir a exposição das equipes policiais a situações de perigo; e avaliar a conformidade das operações de drones do BOPE com as normativas da ANAC (Agência Nacional da Aviação Civil), DECEA (Departamento de Controle do Espaço Aéreo), ANATEL (Agência Nacional de Telecomunicações) e outras regulamentações pertinentes.

1 O USO DE DRONES NA SEGURANÇA PÚBLICA

Os drones proporcionam a capacidade de realizar vigilância furtiva e não intrusiva sobre áreas sensíveis, permitindo a obtenção de dados sem alertar as pessoas atuantes no ato ilícito. Essa discrição é essencial para manter o efeito surpresa durante as operações especiais e garantir a segurança das equipes de Inteligência (Jorge, 2020).

A utilização de drones permite uma grande resolução temporal, ou seja, o levantamento sem custos altos, realizados repetidas vezes. A coleta de dados de forma aérea e contínua possibilita a identificação de padrões de comportamento da localidade monitorada. Os drones podem sobrevoar áreas por longos períodos, registrando atividades rotineiras e destacando desvios que podem indicar a presença de atividades criminosas, assim como de seus autores (Bastos, Roldão, 2019).

O mapeamento detalhado oferecido pelos drones pode fornecer informações sobre a topografia, estruturas físicas e redes de ruas. Isso é crucial para o planejamento estratégico das operações especiais, permitindo que os tomadores de decisão visualizem e compreendam completamente o terreno antes da execução das ações (Rezende, 2020).

O aspecto em tempo real do monitoramento por drones é de grande importância. A transmissão instantânea e em tempo real por vídeo permite que as forças de segurança respondam rapidamente a eventos dinâmicos, coordenando de forma eficaz as operações e ajustando estratégias conforme o necessário (Rezende, 2020).

Drones fornecem uma visão aérea abrangente que facilita a identificação de rotas de fuga e esconderijos diversos, utilizados por membros de facções criminosas e outros meliantes. Isso é crucial para o correto planejamento de rotas a serem evitadas e/ou bloqueadas de forma eficiente, antes, durante e mesmo depois das operações policiais, aumentando as chances de captura dos criminosos, desmantelamento de estruturas montadas, bem como da apreensão de materiais ilícitos escondidos (Jorge, 2020).

Ao avaliar previamente áreas de operação, os drones permitem que as forças de segurança minimizem riscos potenciais, como emboscadas e armadilhas. Isso

contribui para a segurança e eficácia das operações, protegendo os agentes envolvidos e, principalmente, possibilitando a redução drástica de efeitos colaterais indesejados. Cabe ressaltar que o levantamento de Inteligência possibilita a tomada de decisão acerca do custo-benefício, mesmo antes de iniciar as ações (Rezende, 2020).

O uso de drones proporciona um conhecimento detalhado, permitindo o desenvolvimento de estratégias mais eficientes e adaptáveis, resultando em economia de recursos, capacidade de ajustar táticas com base em informações precisas, aumentando a probabilidade de sucesso e a habilidade de adaptar estratégias em tempo real. Atendendo as demandas de cenários em constante evolução, por meio de dados obtidos pelos sensores embarcados nos drones, que são destacados como cruciais, possibilitando um planejamento estratégico, dinâmico e ajustes contínuos que maximizam a eficácia das ações das Unidades Operacionais (Bastos, Roldão, 2019).

A importância do uso de drones na atividade de Inteligência de Segurança Pública vai além do simples monitoramento aéreo, sendo uma ferramenta essencial para a coleta de dados e produção de conhecimentos estratégicos, planejamento operacional eficiente e, em última instância, o enfrentamento bem-sucedido das facções criminosas, tendo como principal ponto a geração de informação de qualidade (Bastos, Roldão, 2019).

2 CASOS DE SUCESSO EM 2023

Durante algumas operações conduzidas pelo BOPE entre os meses de abril e dezembro de 2023 (08 meses), a Agência de Inteligência da unidade desempenhou um papel crucial, assessorando ativamente as equipes no terreno, resultando em apreensões significativas, prisões fundamentadas e mitigação do efeito colateral. Como exemplos de material apreendido, temos: 7 (sete) fuzis; 8 (oito) pistolas; uma espingarda calibre 12; 20 (vinte) granadas de mão; 147 (cento e quarenta e sete) munições para fuzil; 95 (noventa e cinco) munições para pistola; 5 (cinco) munições para espingarda calibre 12; 5 (cinco) rádios transmissores; 1 (uma) mira telescópica; 22 (vinte e dois) presos e farto material entorpecente, como maconha, cocaína, crack e loló.

Dos vinte e dois criminosos presos, alguns são oriundos de outros estados, que se homiziaram nas comunidades cariocas. A implementação dessas tecnologias aéreas resultou em um ambiente operacional mais controlado e estrategicamente gerenciado. Durante as operações policiais, não houve registro de feridos por disparos de arma de fogo, tanto entre os agentes de segurança quanto entre os cidadãos, evidenciando a

eficácia da ferramenta na mitigação de danos internos e colaterais.

O levantamento contínuo, realizado pelos drones, possibilitou a identificação precisa de alvos, permitindo uma resposta imediata a movimentações suspeitas e ações criminosas.

A comunicação em tempo real estabelecida entre as equipes no terreno e os operadores de drones foi essencial para o sucesso das operações. As informações obtidas pelos drones foram transmitidas instantaneamente, permitindo uma tomada de decisão ágil e adaptável às condições dinâmicas do ambiente operacional.

A localização de criminosos específicos foi possível por meio do levantamento de dados realizado pelos drones. As equipes no terreno receberam informações precisas sobre a localização dos alvos, permitindo uma condução eficiente até o objetivo.

Os drones desempenharam um papel crucial na realização de varreduras ao longo do trajeto das equipes, mitigando potenciais emboscadas dos criminosos. A capacidade de monitoramento constante permitiu a identificação antecipada de áreas de risco, proporcionando um deslocamento mais seguro das forças de segurança.

Em síntese, a integração de drones nas operações do BOPE em 2023 exemplifica a convergência eficaz entre a Inteligência, tecnologia aérea e as equipes táticas. O resultado foi a obtenção de dados precisos, ações estratégicas coordenadas e o alcance bem-sucedido dos objetivos operacionais, demonstrando a eficácia do uso técnico de drones na Inteligência de Segurança Pública.

3 A REGULAMENTAÇÃO BRASILEIRA SOBRE O USO DE DRONES

A regulamentação do uso de drones voltados à segurança pública no Brasil é fundamental para garantir a segurança operacional e a eficácia das operações aéreas, especialmente em missões táticas e de Inteligência. A Agência Nacional de Aviação Civil (ANAC) estabelece as normas gerais para a utilização de aeronaves não tripuladas (RPAs) por meio do Regulamento Brasileiro de Aviação Civil Especial (RBAC-E) nº 94, que define requisitos para aeronaves civis, incluindo aspectos técnicos e operacionais. Além disso, a Agência Nacional de Telecomunicações (ANATEL) regula o uso do espectro eletromagnético, assegurando que os sistemas de radiocomunicação dos drones operem sem interferir nas comunicações essenciais para a segurança pública.

O Departamento de Controle do Espaço Aéreo (DECEA) também desempenha um papel crucial, delineando as normas que permitem o acesso seguro dos drones ao espaço aéreo brasileiro, prevenindo colisões com aeronaves tripuladas e garantindo que as operações de drones sejam

conduzidas em consonância com as normas internacionais, conforme elencadas na ICA 100-40 - Aeronaves não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro, e no MCA 56-5 – Aeronaves não Tripuladas para Uso Exclusivo em Operações Aéreas Especiais (BRASIL, 2017, 2020, 2021).

A regulamentação é reforçada pelo Código Brasileiro de Aeronáutica (Lei nº 7.565, de 1986), que estabelece a base legal para o uso de aeronaves no país, incluindo as não tripuladas, e pela Resolução nº 6055 da Polícia Militar do Estado do Rio de Janeiro, Boletim PM nº 049 de 04 de julho de 2024 (PMERJ), que define as diretrizes específicas para o uso de RPAs na corporação. Essas normas são essenciais para coordenar o uso dos drones em missões de segurança pública, garantindo a conformidade legal e minimizando riscos operacionais (RIO DE JANEIRO, 2024).

4 O USO COORDENADO DO ESPAÇO AÉREO E A INTELIGÊNCIA DE FORMA ABRANGENTE

À medida que a complexidade das ameaças à segurança pública aumenta, é imperativo que exploremos meios inovadores para otimizar nossas operações. Nesse contexto, é destacada a importância do uso coordenado do espaço aéreo, integrando nas ações de Segurança Pública as operações com drones e helicópteros durante missões policiais.

A combinação estratégica de drones e helicópteros amplia nossas capacidades de vigilância e resposta. Drones, com sua agilidade e discrição, são ideais para tarefas de reconhecimento, enquanto os helicópteros oferecem vantagens logísticas, transporte rápido e uma plataforma mais robusta para operações especializadas.

O uso simultâneo de drones e helicópteros proporciona uma visão abrangente e detalhada do cenário operacional. Drones podem mapear áreas complexas, identificando alvos específicos, enquanto helicópteros fornecem uma perspectiva mais ampla e capacidade de deslocamento rápido, garantindo cobertura completa durante as operações.

A complementaridade entre drones e helicópteros reduz os riscos inerentes às operações policiais. Drones podem explorar áreas críticas previamente, identificando potenciais ameaças e rotas de fuga, permitindo uma abordagem mais segura por parte das equipes de intervenção a bordo dos helicópteros.

A utilização simultânea de drones e helicópteros permite uma adaptação dinâmica às mudanças no Teatro ou Área de Operações. A comunicação eficiente entre as plataformas aéreas possibilita ajustes em tempo real, maximizando a eficácia operacional e minimizando a vulnerabilidade frente a adversidades inesperadas.

De forma crítica, todas as operações devem observar as normativas da ANAC, ANATEL, DECEA, em conjunto com o Manual do Comando da Aeronáutica 56-5. O uso coordenado do espaço aéreo exige uma coordenação rigorosa para garantir a segurança e a conformidade legal de todas as aeronaves envolvidas. Para Souza e Santos (2019), a combinação de drones e helicópteros representa uma evolução estratégica para nossas operações policiais.

Aproveitar ao máximo as capacidades únicas de cada plataforma de forma integrada, não apenas aprimora nossa resposta a ameaças, mas também estabelece um novo paradigma para a Segurança Pública (Lopes, 2021). Neste sentido, a implementação desse modelo integrado e inovador em futuras operações promoverá não apenas uma eficácia operacional aprimorada, mas também um aumento substancial na segurança das equipes e na efetividade da missão.

Cabe salientar que toda e qualquer necessidade que seja verificada pelas forças, não sendo contempladas pelos órgãos reguladores pode e deve ser informada e discutida com os órgãos competentes, com a intenção de buscar soluções que atendam às necessidades operacionais, sem que se perca o nível de segurança operacional.

CONCLUSÃO

A análise sobre o impacto do uso de drones nas operações de segurança pública, especialmente no contexto do Batalhão de Operações Policiais Especiais (BOPE) da Polícia Militar do Estado do Rio de Janeiro, revela os avanços significativos dessa tecnologia. Os drones, sem dúvida, têm o potencial de transformar as operações de inteligência, sobretudo em vigilâncias, oferecendo vantagens como a redução de custos operacionais, o aumento da segurança dos agentes e a possibilidade de transmissão em tempo real de dados e imagens, o que otimiza a tomada de decisões em campo. Esses benefícios são particularmente evidentes em situações de risco elevado, como operações em áreas de difícil acesso ou em cenários de confronto com organizações criminosas.

A aplicação precisa desta tecnologia representou um marco significativo no aprimoramento das capacidades de inteligência e operacionais da unidade, promovendo ganhos substanciais em eficácia e segurança. A utilização de drones, de acordo com as regulamentações estabelecidas pela ANAC, ANATEL e pelo DECEA, assegura não apenas a legalidade das operações, mas também uma credibilidade jurídica e segurança operacional no espaço aéreo brasileiro.

Os resultados das diligências realizadas com o apoio dessas aeronaves não

tripuladas foram impressionantes. O emprego da assessoria aérea em tempo real, comunicação instantânea e a localização precisa de alvos, destacam-se como fatores decisivos nas apreensões de armamento, drogas e nas detenções de membros de organizações criminosas.

A necessidade de capacitação contínua dos operadores e de ajustes nas normas regulatórias é imperativa para garantir que os drones sejam empregados de maneira eficiente e dentro dos parâmetros legais.

Contudo, a operação coordenada entre as equipes no terreno e os operadores de drones demonstrou uma convergência técnica exemplar, permitindo adaptações dinâmicas em tempo real, maximizando a eficácia das ações e, crucialmente, preservando a integridade das forças de segurança. Neste contexto, este estudo aponta a necessidade do investimento e aprimoramento de nossa capacidade de Inteligência por meio do uso estratégico de drones. Esta tecnologia não só representa um avanço na resposta aos desafios impostos por organizações criminosas, mas também uma oportunidade de excelência no contexto da segurança pública.

REFERÊNCIAS

BASTOS, F.; ROLDÃO, V. O uso de drones no monitoramento de áreas de risco, como pontos de tráfico de drogas, e as vantagens táticas dessa tecnologia. Goiânia: Academia de Polícia Militar de Goiás, 2019.

BRASIL. Código Brasileiro de Aeronáutica. Lei nº 7.565, de 19 de dezembro de 1986. Diário Oficial da União: Seção 1, Brasília, DF, p. 19613-19626, 22 dez. 1986.

BRASIL. Agência Nacional de Aviação Civil. Regulamento Brasileiro de Aviação Civil Especial (RBAC-E) nº 94: Requisitos gerais para aeronaves não tripuladas de uso civil. Brasília: ANAC, 2017.

BRASIL. Departamento de Controle do Espaço Aéreo. ICA 100-40: Aeronaves não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro. Rio de Janeiro: DECEA, 2021.

BRASIL. Departamento de Controle do Espaço Aéreo. MCA 56-5: Aeronaves não tripuladas para uso exclusivo em operações aéreas especiais. Rio de Janeiro: DECEA, 2020.

JORGE, A. Aeronaves Remotamente Pilotadas (RPAs) e enfrentamento da criminalidade no Brasil. Revista Eletrônica Direito & TI, v. 1, n. 9, p. 5, 2020.

KOLODZEI, A. A popularização do termo "drone" e a diferença entre a terminologia genérica e o uso técnico de RPAs. RECIMA21 - Revista Científica Multidisciplinar, v. 5, n. 9, e595647, 2024.

LOPES, M. Drones, proteção de dados pessoais e direitos conexos. Revista Electrónica de Direito, RED, v. 25, n. 2, p. 210-236, 2021.

MACHADO. H. DE. S. Estudo sobre o uso de drones no Bope para a Inteligência de Segurança Pública. Online, Piloto Policial, 2024. Disponível em: https://www.pilotopolicial.com.br/estudo-sobre-o-uso-de-drones-no-bope-para-a-inteligencia-de-seguranca-publica/

OLIVEIRA, L.; FÁVERO, F. Benefícios dos drones para a segurança pública, incluindo vigilância, busca e resgates, e a utilização de sensores de temperatura. Brazilian Journal of Development, v. 8, n. 9, p. 63064-63090, 2022.

PEY, L. Estudo sobre o emprego de drones em operações de inteligência de segurança pública. Dissertação de Mestrado. Brasília: Universidade de Brasília, 2022.

REZENDE, M. Drones em áreas de alta criminalidade: a visão estratégica que proporcionam às forças de segurança. Ciências Aeronáuticas – Unisul Virtual, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/8207. Acesso em 26 jan. 2025.

RUSSO, A. N. et al. Quadrilhas articuladas de terceira geração: Estudo de caso sobre criminosos que utilizam explosivos, drones, armas de assalto em área urbana para a prática de crimes contra o patrimônio. Instituto Brasileiro de Segurança Pública (RIBSP), v. 6, n. 14, p. 10-18, 2023

RIO DE JANEIRO (Estado). Polícia Militar. Resolução nº 6055, de 28 de junho de 2024. Estabelece diretrizes para o uso de aeronaves não tripuladas no âmbito da Corporação. Boletim da Polícia Militar do Estado do Rio de Janeiro, n.o 049, 04 jul. 2024.

SILVA, Eduardo Araújo. Operações aéreas especiais: drones, busca e salvamento e resposta a desastres. Monografia (Bacharelado em Segurança Pública e Social) – Departamento de Segurança Pública, Instituto de Estudos Comparados em Administração de Conflitos, Universidade Federal Fluminense, Rio de Janeiro, 2023.

SOUZA, R. L.; SANTOS, S. B.O uso de drones na segurança pública: avanços e desafios. Revista Brasileira de Segurança Pública, v. 12, n. 3, p. 98-112. 2019.

ZATERRA, A. Emprego de aeronaves remotamente pilotadas na área operacional de inteligência, subsidiando ações ostensivas da Polícia Militar do Paraná. RECIMA21 - Revista Científica Multidisciplinar, v. 3, n. 10, p. 12-19, 2022.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

ANÁLISE DE RISCO PARA LOCAIS DE EVENTOS COM DIGNITÁRIOS (ARLED): Análise de risco para o assessoramento ao processo decisório e ao planejamento de segurança de eventos com a participação de dignitários.

Guilherme Lopes Maddarena[1]
Leonardo Luis da Silva de Araújo[2]

RESUMO

A Análise de Risco para Locais de Eventos com Dignitários (ARLED) é uma metodologia de análise de risco que visa aperfeiçoar a segurança de altas autoridades em participação de eventos. Combinando aspectos da metodologia de Análise de Risco de Pessoas (ARP) e da Análise de Risco em Segurança Orgânica (ARSO), a ARLED propõe uma abordagem integrada e estruturada para identificar e analisar ameaças e vulnerabilidades. A metodologia considera as variáveis ambientais, políticas e de momento, utilizando uma matriz de risco adaptada para avaliar o nível dos elementos do risco relacionados à probabilidade, possibilitando o melhor planejamento de segurança e a tomada de decisão.
Palavras-chave: risco; dignitários; vulnerabilidades; ameaça; e assessoramento.

RISK ANALYSIS FOR EVENT LOCATIONS WITH DIGNITIES (ARLED): Risk analysis to advise on the decision-making process and security planning for events with the participation of dignitaries.

ABSTRACT

Risk Analysis for Event Venues with Dignitaries (ARLED) is a risk analysis methodology that aims to improve the safety of senior authorities participating in events. Combining aspects of People Risk Analysis (ARP) methodology and Organic Security Risk Analysis (ARSO), ARLED proposes an integrated and structured approach to identify and analyze threats and vulnerabilities. The methodology considers environmental, political and current variables, using an adapted risk matrix to assess the level of risk elements related to probability, enabling better security planning and decision making.
Keywords: risk; dignitaries; vulnerabilities; threat; and advice.

[1] Delegado de Polícia Federal, Coordenador de Aviação Operacional da Polícia Federal. MBA em Gerenciamento de Projetos pela Universidade da Grande Fortaleza e Estágio de Gerenciamento Avançado da Prevenção de Acidentes – Militar – EGAP-MIL (CENIPA). E-mail: maddarena.glm@pf.gov.br
[2] Policial Militar do Paraná há 18 anos, mobilizado na Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública (Senasp/MJSP), lotado na Diretoria de Operações Integradas e de Inteligência. Pós-Graduado em Segurança Pública, História Militar e Inteligência de Segurança Pública, pela Faculdade Unina e pela Academia Nacional de Polícia (ANP). Atualmente cursa a especialização em Segurança Pública Contemporânea, pela ANP. Endereço eletrônico: leo.araujo444@gmail.com

INTRODUÇÃO

A segurança de locais de eventos com a participação de altas autoridades depende de planejamento prévio e dinâmico, subsidiado de análise de risco. Dessa forma, visando assessorar o processo decisório e o planejamento de segurança, tornou-se relevante analisar metodologias de análise de risco atualmente utilizadas para pessoas e instalações, verificar a aplicabilidade para a análise de risco destinada à segurança de locais de eventos com dignitários e adaptar às necessidades da segurança de autoridades.

A partir dessas observações, no exercício das atividades funcionais desempenhadas na segurança de eventos com altas autoridades governamentais, durante o ano de 2023, surgiu a necessidade do desenvolvimento de uma metodologia de análise de risco específica para locais de eventos com dignitários, que envolve necessidades a serem consideradas tanto do ponto de vista técnico e metodológico, quanto logístico e operacional. Dessa maneira, surgiu a Análise de Risco para Locais de Eventos com Dignitários – ARLED.

Do ponto de vista técnico e metodológico, pela própria natureza da função, o dignitário é uma figura de alta exposição e atratividade para pessoas ou grupos que desejem visibilidade ou projeção para uma causa ou pauta. Figuras públicas, como artistas, empresários e políticos, já foram alvos de diversas ações de cunho moral, como o lançamento de tinta e objetos, manifestações vexaminosas, durante reuniões e eventos fechados, entre outros.

Por conseguinte, o dignitário naturalmente passa a ser um alvo em potencial para agentes descontentes no campo político, por exemplo, muitos dos quais potencialmente dispostos a praticar atos extremos, inclusive contra a vida, para alterar a ordem política, social ou chamar a atenção para algum aspecto, conforme o seu entendimento.

Por outro lado, assegurar as condições de segurança de um local com dignitários muitas vezes é um desafio logístico e operacional, pois estes frequentemente participam de eventos inopinados e têm uma agenda substancialmente concorrida, resultando em compromissos sequenciais, com pouca antecedência para a preparação de segurança. O mesmo entendimento pode ser aplicado aos seus cônjuges e familiares. Portanto, é essencial que a segurança analise rapidamente os riscos desses locais para reduzir a probabilidade de sucesso de ações adversas contra a integridade física e moral dos dignitários.

Destarte, ao desenvolver uma metodologia de análise de risco para locais de eventos com dignitários, é fundamental equilibrar a complexidade e a objetividade, sob pena de o modelo adotado se tornar inexequível, na prática, não se prestando à

finalidade para a qual foi concebido ou adotado.

1 DISCUSSÃO TEÓRICA

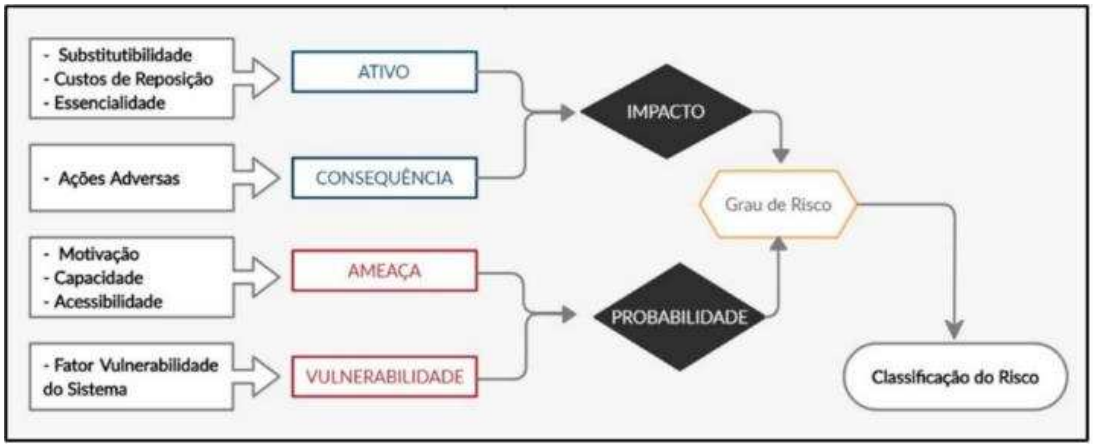
Risco pode ser definido como a correlação dos componentes "probabilidade" e "impacto", que precisam ser analisados caso um evento indesejado ocorra (AVEN, 2015). Análise de riscos, por sua vez, é um processo de identificação e avaliação dos elementos do risco que integram respectivamente esses componentes, quais sejam: "ameaça" e "vulnerabilidade"; "ativo" e "consequência".

Nessa perspectiva, a avaliação de riscos de locais de eventos com dignitários requer a conjugação de fatores da análise de risco de pessoas, destinada à proteção de pessoas, e da análise de riscos em segurança orgânica, destinada à segurança de instalações sensíveis.

Portanto, trata-se de um modelo misto, pois por um lado a proposta aborda a segurança de altas autoridades, aplicando-se em grande parte a doutrina de segurança de dignitários, mas, por outro lado, o foco desta avaliação está em uma instalação física ou um ambiente específico, visando à preparação deste para a proteção do dignitário, enquanto presente no local.

Nesse sentido, cabe apresentar o fluxo da metodologia de Análise de Risco em Segurança Orgânica (ARSO), abaixo representado, o qual prevê a existência de variáveis de impacto e probabilidade como componentes do grau de risco.

FIGURA 1: FLUXO DA METODOLOGIA ARSO

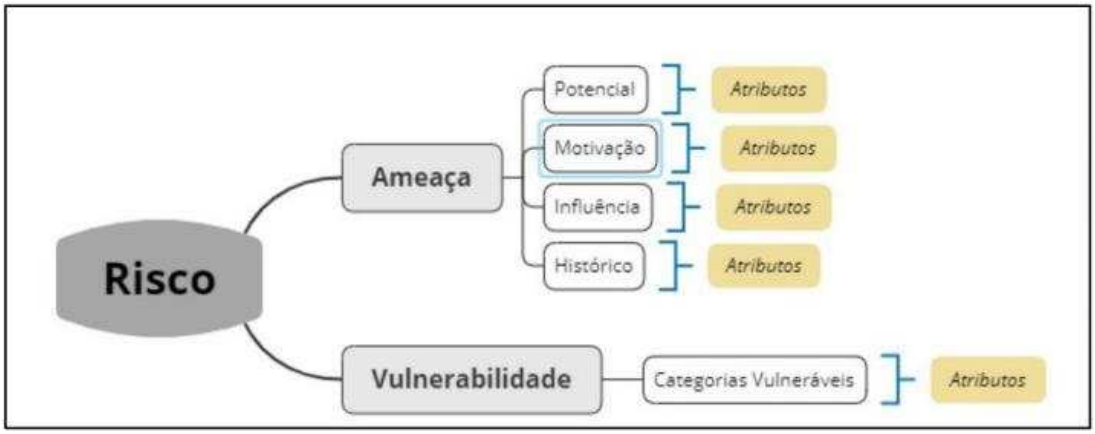


Fonte: Elaborado pelos Autores da ARSO – ANDRADE, F. S.; ROCKEMBACH, S. J.

Considerando que o ativo a ser protegido na ARLED não é negociável, neste caso, dignitários (pessoas), e que o objetivo da metodologia é preservar e assegurar a integridade física destes, não há negociação quanto à avaliação das variáveis do impacto, que não podem ser aceitas neste estudo. Em resumo, considerando que a equação do risco é baseada na análise da probabilidade e do impacto, o foco da Análise de Risco para Locais de Eventos com Dignitários deve estar centrado nos elementos da probabilidade, ou seja, "ameaça" e "vulnerabilidade".

Esse entendimento está, inclusive, alinhado a outra metodologia, a da Análise de Risco de Pessoa (ARP), que considera que "a Análise de Risco de Pessoa é uma função da probabilidade de um evento indesejado ocorrer e o subjacente impacto caso ele se materialize, e que este não é uma variável – já que a incolumidade do indivíduo não será negociada" (ANDRADE, 2022), conforme a metodologia representada a seguir.

FIGURA 2: FLUXO DA METODOLOGIA ARP



Fonte: Elaborado pelos Autores da ARP - ANDRADE, F. S; DOS REIS, A. R.; SANCHES, M.

Entretanto, diferencia-se a ARLED da ARP pura por dois motivos: primeiro, a ARLED tem seu foco principal no local físico onde se desenvolverá o evento, ainda que em função da presença do dignitário e, segundo, porque a ameaça, apesar de existir e dever ser considerada, tem de ser tratada dentro do contexto que a autoridade representa, aplicável especificamente ao local que está sendo preparado para a visita. Enquanto a metodologia ARP considera para a contextualização da ameaça os ambientes e os locais que o dignitário costuma frequentar.

Além disso, as ameaças tratadas na ARP são, de forma geral, ameaças mais concretas, praticadas por grupos ou pessoas identificados ou identificáveis, enquanto a análise das ameaças na ARLED deve ser focada em uma visão mais abrangente, que considera as condições políticas e conjunturais que afetam aquele local, devendo a análise, portanto, preocupar-se com ameaças potenciais que, apesar de não externadas, possam estar aptas a se concretizarem naquele evento, caso se façam presentes determinadas condições.

Outras metodologias de análise de risco já foram consideradas e estudadas por especialistas em trabalhos anteriores e podem ter servido de inspiração para o desenvolvimento de metodologias próprias. Entretanto, a criação da ARLED, a partir da adaptação das metodologias ARSO e ARP, mostra-se mais adequada, uma vez que estas se encontram mais alinhadas com a finalidade da proposta.

1.1 Risco

Ao longo do desenvolvimento de métodos e pesquisas de análise de risco surgiram diversas definições de risco. Para a *International Organization for Standardization* (ISO), ele é descrito como o "efeito da incerteza nos objetivos" (ISO 31000, 2018).

Por se tratar de um conceito voltado ao futuro, o risco não possui uma existência objetiva. No entanto, abordá-lo por meio de um processo metodológico permite, mesmo diante das incertezas, delinear cenários que favoreçam o planejamento e a tomada de decisões.

Desse modo, a análise de risco se torna uma ferramenta essencial, pois, ao utilizar técnicas analíticas, possibilita identificar e interpretar essas incertezas, expressando-as em diferentes níveis e classificação de risco.

1.2 Análise de Risco

A Análise de Risco (AR) é um processo estruturado e sistematizado que se realiza por meio de uma metodologia específica, com o propósito de avaliar ou determinar o nível ou grau de risco envolvido. “Trata-se de um procedimento voltado a compreender como a incerteza pode impactar um objetivo específico” (ANDRADE, 2022).

Apesar de algumas instituições já considerarem a Análise de Risco um tipo de conhecimento, segundo a Doutrina Nacional de Inteligência de Segurança Pública (DNISP, 2016), a AR é uma técnica acessória que utiliza metodologia própria e que pode auxiliar na produção do conhecimento, por meio de procedimentos que identificam e analisam ameaças e vulnerabilidades, a fim de identificar alternativas para mitigar e controlar os riscos.

Nesse sentido, não obstante a existência de diversas metodologias de Análise de Risco, tais como Análise de Risco em Segurança Orgânica – ARSO (ANDRADE, 2018) e Análise de Risco de Pessoa – ARP (ANDRADE, 2022), para que a análise chegue o mais próximo da verdade real, mediante mecanismos sistematizados de AR, “a estratégia de análise deve ser estruturada e delineada, consoante o seu propósito” (ABNT ISO 31000, 2018), se possível em metodologia específica, como a que se apresenta a ARLED para a segurança de locais de eventos com dignitários.

2 ANÁLISE DE RISCO PARA LOCAIS DE EVENTOS COM DIGNITÁRIOS (ARLED)

Os critérios de mensuração da probabilidade do risco na ARLED são os elementos do risco “Ameaça” e “Vulnerabilidade”. Ambos analisados de forma abrangente e unificada, que, após as devidas mensurações, são aplicados na matriz de risco específica desse método.

2.1 Ameaças

As ameaças relacionadas à segurança de dignitários não devem ser tratadas de forma individualizada nem restritas apenas às ameaças concretas. É fundamental que sejam analisadas e tratadas, considerando o contexto político, social e situacional específico do momento e do local preparado para a visita do dignitário.

Para fins de aplicação da metodologia, "local" é considerado como as instalações físicas escolhidas para o evento, podendo ter o conceito ampliado para o território do município ou a região metropolitana onde se encontra inserido o evento. Em alguns casos, a depender da avaliação do responsável pela análise de risco, este conceito pode ser alterado para englobar áreas de fácil ou rápido acesso ao local do evento, o que deve ser verificado caso a caso.

Uma diferença significativa em relação ao contexto da ARP diz respeito ao fato de que, nesta metodologia, a ameaça geralmente é conhecida quando se trata de pessoas que requerem proteção. No caso dos dignitários, entretanto, as ameaças tendem, em grande parte, a ser potenciais e não claramente visíveis.

Além disso, os dignitários recebem – ou podem receber – frequentemente uma quantidade indeterminada de mensagens de desagravo decorrentes do próprio sistema democrático e, por vezes, uma quantidade igualmente relevante de mensagens de cunho ameaçador. Essas mensagens podem chegar a quantidades exorbitantes, dependendo da função do dignitário e do momento político e social, não podendo ser consideradas individualmente para fins de aferição do nível de ameaça, mas também não podem ser desconsideradas.

Não se trata de ignorar elementos de ameaça que eventualmente possam atentar contra a vida dos dignitários, pois estas são tratadas individualmente na seara adequada, possivelmente nos campos da inteligência estratégica e da polícia judiciária. O que se chama a atenção aqui é que, para fins de análise de risco, o nível de ameaça deve ser considerado de forma mais abrangente e, portanto, ágil, analisando-se o cenário atual como um todo, sem o tratamento extensivo de cada reporte individual, mas levando-se em conta, primeiro, a quantidade de reportes como um item de aferição do cenário e, em seguida, os mais graves em nível individual para a aferição e o tratamento, formando em conjunto o nível de ameaça. Outrossim, vale destacar que, para fins de análise da ameaça, nesta metodologia, o enfoque é nas ameaças humanas e não nas naturais.

Ainda, para fins desta análise de risco, não se deve esquecer que a ameaça considerada deve ser com foco no local do evento, tanto na sua perspectiva de ação humana contra uma determinada pessoa (RENN, 1992), quanto um evento – ou um

cenário – capaz de ocasionar prejuízo a esta pessoa, o que inclui não somente o prejuízo físico, mas também à imagem, à honra e outros bens jurídicos da instituição que representa o dignitário, como por exemplo, Presidente da República e Governadores, passíveis de tutela e preservação. Ou seja, o elemento territorial da ameaça é de extrema relevância, pois há locais em que essas autoridades não enfrentam a presença de determinados grupos ou pessoas contrárias em específico, enquanto em outros locais esta presença pode ser muito relevante.

Nesse sentido, as variáveis da ameaça (potencial, motivação, influência e histórico) inicialmente previstas na ARP são utilizadas, mas de forma adaptada, visto que os dignitários normalmente são figuras públicas e sujeitas às manifestações positivas e negativas de diversas origens, algumas podendo configurar ameaças reais e outras sendo apenas manifestações de desagrado a esta ou aquela medida, em específico.

Nesse contexto, na ARLED propõe-se a adaptação dessas variáveis para os seguintes conceitos, classificações e pesos, bem como gradação de valores, seguindo a escala de pesos de 1 a 5 tradicionalmente conhecida como escala Likert:

Potencial: capacidade técnica, logística e financeira para que uma das ameaças potenciais ou concretas identificadas sejam realizadas no ambiente em estudo. (Classificações: Muito Baixa, Baixa, Média, Alta e Muito Alta; Valores: 01, 02, 03, 04 e 05; e Peso 40%).

Motivação: percepção de que há um clima ou ambiente político, social ou conjuntural favorável à concretização de uma das ameaças identificadas. (Classificações: Muito Baixa, Baixa, Média, Alta e Muito Alta; Valores: 01, 02, 03, 04 e 05; e Peso 40%).

Influência: refere-se ao poder que o ambiente tem de servir como vetor favorável à concretização de uma das ameaças em potencial (por exemplo, ambiente que favorece aglomerações e contato direto de pessoas não credenciadas com o dignitário). (Classificações: Muito Baixa, Baixa, Média, Alta e Muito Alta; Valores: 01, 02, 03, 04 e 05; e Peso 10%).

Histórico: refere-se à existência de registros pretéritos de ações perpetradas contra autoridades em condições semelhantes naquele local. (Classificações: Muito Baixa, Baixa, Média, Alta e Muito Alta; Valores: 01, 02, 03, 04 e 05; e Peso 10%).

Ressalta-se que o valor da ameaça será um valor único e genérico, baseado nas análises supracitadas e na fórmula do cálculo para ameaça a seguir.

FIGURA 3: **FÓRMULA DO CÁLCULO PARA AMEAÇA**.

CÁLCULO: $A * 0,4 + B * 0,4 + C * 0,1 + D * 0,1 = XX$

Fonte: Elaborado pelos autores desta pesquisa (2024).

2.2 Vulnerabilidades

Segundo a metodologia ARP, "as vulnerabilidades são identificadas a partir da compreensão das atitudes e comportamentos adotados, direta ou indiretamente pela pessoa a ser protegida" (ANDRADE, 2017). Vulnerabilidades também podem ser definidas como "características intrínsecas de algo que resultam em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência" (ABNT ISO 73, 2009).

No contexto da segurança de locais de eventos com dignitários, vulnerabilidade pode ser vista como uma fragilidade presente no espaço físico de realização de um evento, que pode ser explorado por um agente motivado e com meios disponíveis para buscar êxito na concretização de uma ação adversa. É, portanto, um elemento que aumenta a probabilidade de o risco se concretizar.

Tendo em vista a ARLED, vale destacar que a ameaça não é uma variável controlável, por se tratar de elemento do contexto externo organizacional, que em certos casos pode ser neutralizada, isolada ou ainda controlada, por intermédio de ações específicas. Por outro lado, as vulnerabilidades se encontram no contexto interno da organização, de responsabilidade da segurança orgânica e, portanto, trata-se de uma variável com alta possibilidade de incidir na redução do risco, por meio de medidas preventivas.

Posto isso, para facilitar o trabalho do analista, propõe-se a análise das vulnerabilidades do local, por meio de categorias vulneráveis, quais sejam:

- ✓ **Acesso ao Local**: condições de chegada e saída do dignitário do local do evento.
- ✓ **Áreas e Instalações**: conformação física geral do local.
- ✓ **Recursos Humanos**: pessoas que atuarão no evento, perfil do público e pessoas que terão contato direto com o dignitário.
- ✓ **Materiais e equipamentos**: recursos materiais e equipamentos de proteção que serão empregados na segurança do evento e da autoridade, como equipamentos de controle de acesso, recursos de monitoramento, anteparos balísticos, recursos de contramedidas (ex.: cancelas, detector de metais, CFTV, blindagens, equipamentos de varredura etc.);
- ✓ **Medidas de Segurança**: adoção das medidas de segurança específicas para o

evento, como varredura, vigilância, credenciamento, controle de acesso etc.

Diante do cenário do evento, o analista avalia as categorias de vulnerabilidade com base nas condições do local e nas medidas de adequação e segurança adotadas, orientando a classificação e o grau da vulnerabilidade. (Classificações: Muito Baixa, Baixa, Média, Alta e Muito Alta; e Graus: A, B, C, D e E).

Ressalta-se que, para a avaliação das vulnerabilidades, utiliza-se o recurso conhecido como Lista de Verificação. Cada categoria vulnerável possui acordos semânticos para cada grau de vulnerabilidade, bem como uma lista de itens a serem verificados, que deve ser dinâmica e continuamente aperfeiçoada, conforme os eventos. Esse recurso, além de ser fundamental para uma análise precisa das vulnerabilidades, permite o constante aprimoramento da avaliação desse elemento da análise de risco durante o processo analítico.

Na análise do elemento vulnerabilidade, será aplicada a teoria do elo mais fraco, ou seja, a categoria avaliada mais vulnerável é a dominante no estudo. Dessa forma, a categoria que tiver a nota (grau) mais alta é aquela a ser aplicada na matriz de risco.

2.2.1 – Categoria de Vulnerabilidade Especial – Adesão aos protocolos de segurança

Considerando que a metodologia ARLED é específica para a segurança de dignitários, é fundamental avaliar o comportamento destes no que tange à adesão aos protocolos de segurança. Nesse sentido, essa metodologia conta ainda com a categoria vulnerável "Adesão aos Protocolos de Segurança". Essa categoria tem como critérios de valoração apenas as opções POSITIVO ou NEGATIVO para a adesão ou não dos protocolos e, no caso Negativo, a avaliação final de vulnerabilidades é majorada com o acréscimo de um nível, como, por exemplo: quando a análise de vulnerabilidades resultar no grau/classificação de vulnerabilidade "D/Alta" e a avaliação desta categoria diferenciada tiver o resultado "Negativo", a avaliação final de vulnerabilidades tem o resultado "E/Muito Alta".

Destaca-se que o valor da avaliação de vulnerabilidade não será alterado quando já estiver no grau/classificação "E/Muito Alta". Outrossim, vale registrar que, se o evento tiver a participação de mais de um dignitário, a avaliação será sempre em relação ao dignitário de nível mais elevado.

Por fim, esta categoria é praticamente invariável para o mesmo dignitário, só sendo alterada quando houver alguma modificação consistente em seu comportamento ou quando houver a alteração do dignitário objeto da análise.

2.3 Estimativa de Risco

Após a apuração das variáveis com base nos dados disponíveis, somados aos de inteligência, a informes diversos e à observação, durante a preparação do local do evento, sugere-se a adoção da seguinte escala para dimensionamento da ameaça e da vulnerabilidade:

FIGURA 4: MATRIZ DE RISCO ARLED

AMEAÇA			VULNERABILIDADE		
Classificação	Descrição	Grau	Grau	Classificação	Descrição
MUITO ALTA	É provável que haja presença hostil no local, agressiva e em grande número	5	E	MUITO ALTA	O local não possui controle ou o controle utilizado é complemente inadequado e ineficiente.
ALTA	É provável que haja presença hostil no local	4	D	ALTA	O controle existe, mas é muito inadequado, tornando o local permeável a pessoas com conhecimento das instalações.
MÉDIA	Improvável, mas pode ocorrer a presença de elementos hostis no local	3	C	MÉDIA	O controle existe, é adequado, mas a sua eficiência demandaria ajustes, pois o local é potencialmente acessível a pessoas com acesso a outras áreas.
BAIXA	Existe, mas não há manifestações ou ações efetivas registradas	2	B	BAIXA	O controle existe, é bastante adequado, mas a sua eficiência demandaria pequenos ajustes na forma de execução.
MUITO BAIXA	Quase inexistente	1	A	MUITO BAIXA	O controle existe, é adequado e eficiente e o local tem um nível alto de segurança.

Fonte: Elaborado pelos autores desta pesquisa (2024).

Com base na metodologia, pode-se notar que os níveis mais altos devem ser evitados, mas que há uma possibilidade maior de se suportar a elevação moderada de um dos fatores, caso seja compensada pela preservação do outro em níveis suficientemente baixos.

Em outras palavras, hipoteticamente é possível a realização de um evento em local hostil, desde que a vulnerabilidade do estabelecimento onde o evento esteja sendo realizado seja muito baixa, e vice-versa, mas é altamente desaconselhável a realização de um evento em local hostil e vulnerável, por exemplo.

Ressalta-se que a vulnerabilidade do local é a variável que permite maior nível de atuação por parte da segurança do evento, uma vez que está sob o controle orgânico, ao contrário da ameaça. A necessidade desse controle se torna ainda mais premente à medida que se constata o aumento no nível da ameaça. Note-se, ainda, que não há a hipótese de ameaça inexistente, assim como não há local invulnerável.

Assim, ações mínimas para a preservação da segurança da autoridade

protegida são sempre necessárias. Determinados os níveis de ameaça e a vulnerabilidade do local, aplicam-se os dois valores encontrados (ameaça e vulnerabilidade) na matriz de risco a seguir, tornando-se possível identificar o grau e a classificação do risco a que o dignitário está exposto em determinado evento.

2.4 Matriz de Risco

Matriz de risco é a representação do grau/classificação do risco, por meio de tabela com gradação, para subsidiar tecnicamente o planejamento e o processo decisório. Tendo em vista que o objetivo da ARLED é a segurança de locais de eventos com dignitários, a matriz tem que considerar os elementos da probabilidade do risco – ameaça e vulnerabilidade.

FIGURAS 5 E 6 – MATRIZ E CLASSIFICAÇÃO DE RISCO ARLED

AMEAÇA X VULNERABILIDADE	MUITO ALTA	ALTA	MÉDIA	BAIXA	MUITO BAIXA
MUITO ALTA	5E	5D	5C	5B	5A
ALTA	4E	4D	4C	4B	4A
MÉDIA	3E	3D	3C	3B	3A
BAIXA	2E	2D	2C	2B	2A
MUITO BAIXA	1E	1D	1C	1B	1A

COR	CLASSIFICAÇÃO	DESCRIÇÃO (ACORDO SEMÂNTICO)
PRETO	MUITO ALTO	Situação de ameaça alta ou muito alta e local altamente vulnerável.
VERMELHO	ALTO	Locais de vulnerabilidade média a alta e níveis de ameaça médio a alto, mas não em combinação de ambos elevados de alto a muito alto.
AMARELO	MÉDIO	Trata-se aqui das hipóteses em que ambos os elementos são moderados ou um deles é alto ou muito alto, mas o outro é baixo ou muito baixo
VERDE	BAIXO	Este é um nível em que há baixa ameaça e o local é pouco vulnerável. Normalmente pode ser verificado em tempos de estabilidade política razoável e em eventos realizados em palácios governamentais e afins

Fonte: Elaboradas pelos autores desta pesquisa

Por se tratar de análise de riscos atinentes a altas autoridades, não é considerado o nível muito baixo, conforme pode ser percebido na matriz da ARLED.

2.5 Encaminhamento/Tomada de Decisão

Conforme se eleva o nível do risco, é necessária a ativação de escalões mais elevados no processo decisório. Por esta razão, sugere-se que a avaliação seja informada pelo menos aos seguintes níveis (seguindo a cadeia hierárquica), conforme o nível de risco identificado, sem prejuízo das providências dinâmicas típicas de preparação do evento previstas nos respectivos manuais de eventos, como comunicação com o cerimonial, demais órgãos de segurança envolvidos e assessoria do dignitário.

FIGURA 7: CLASSIFICAÇÃO DE NÍVEIS PARA TOMADA DE DECISÃO

FAIXA DE RISCO	INFORMAÇÃO/NÍVEL DE DECISÃO
PRETA	Político/Estratégico
VERMELHA	Estratégico
AMARELA	Tático
VERDE	Operacional

Fonte: Elaborado pelos autores desta pesquisa (2024).

CONSIDERAÇÕES FINAIS

O trabalho de avaliação de risco para locais de eventos com dignitários é tão

dinâmico quanto o ambiente em que se insere a autoridade protegida. Isso significa que, em pouco tempo, pode ser necessário atualizar e adaptar a análise, redimensionando-a sempre que as condições presentes se alterarem.

É comum que a notícia da presença do dignitário protegido e a proximidade da data do evento alterem o panorama político e social do local, podendo, em razão disso, ocorrer mudanças no nível de ameaça. Da mesma forma, devido às vicissitudes da atividade política de um dignitário, por exemplo, não é raro que a configuração de um evento se modifique várias vezes até a data de sua realização, exigindo que o avaliador atualize a análise e reposicione os responsáveis quanto a eventuais alterações no nível de risco apresentado.

Por fim, deve-se sempre ter em mente que a avaliação de risco está ligada à identificação de probabilidades. Assim, quando se estima um nível de risco baixo, isso significa que ainda existe, embora reduzida, a probabilidade de uma ação adversa ocorrer.

Grande parte do trabalho de gerenciamento de risco depende do conhecimento dos fatores que compõem seus elementos, ou seja, o risco é gerenciado com base no conhecimento obtido e em fatores estimados. Como é impossível garantir que foram coletados todos os elementos de conhecimento relacionados a um local ou evento específico, sempre há uma margem de probabilidade de que o indeterminado aconteça.

Dessa forma, independentemente do nível de risco encontrado, é indispensável que todos os envolvidos mantenham o mais elevado nível de alerta, durante todo o período do evento, pois o sistema de segurança é constituído pela soma de suas partes, as quais, quanto melhor preparadas estiverem, melhor desempenharão seu papel, reduzindo as chances de ocorrência do imponderável.

REFERÊNCIAS

ANDRADE, F S. Análise de Riscos e a Atividade de Inteligência. Revista Brasileira de Ciências policiais. 2017. Disponível em: <https://periodicos.pf.gov.br/index.php/RBCP/article/view/462/311> Acesso em 13 de julho de 2018.

ANDRADE, F. S. ROCKEMBACH, S. J. Metodologia ARSO: Análise de Riscos em Segurança Orgânica. Revista Mercopol. Edición Paraguay. Año XI, nº11. ISSN 2236-9236. 2018.

ANDRADE, F. S; DOS REIS, A. R.; SANCHES, M. Análise de risco de pessoa: a convergência das medidas de proteção com os procedimentos de segurança adequados. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO GUIA 73: gestão de riscos: vocabulário. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 31000: gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018.

BRASIL.SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA. DNISP - Doutrina Nacional de Inteligência de Segurança Pública, Brasília-DF, 2015.

CAPLAN, J. M.; KENNEDY, L. W.; MILLER, J. Risk Terrain Modeling: Brokering Criminological Theory and GIS Methods for Crime Forecasting. Justice Quarterly, v. 28, n. 2, p. 360–381, abr. 2011.

KENNEDY, L. W.; CAPLAN, J. M.; PIZA, E. Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies. Journal of Quantitative Criminology, v. 27, n. 3, p. 339–362, set. 2011.

RENN, O. Concepts of risk: a classification. In: Social theories of risk. Westport, Conn, 1992. p. 53-79. DOI: http://dx.doi.org/10.18419/opus-7248. Disponível em: https://elib.uni-stuttgart.de/handle/11682/7265. Acesso em: 08 de ago. de 2021.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

VIOLÊNCIA ESCOLAR: Uma discussão para avaliar como a atividade de Inteligência de Segurança Pública (ISP) pode contribuir na prevenção e cuidado.

Deborah Karla Rinaldi Paiva[*]

RESUMO

A atividade de Inteligência de Segurança Pública (ISP) na contribuição da prevenção da violência escolar, como objeto de estudo, planeja discutir, de que forma a atividade poderia contribuir na promoção de políticas públicas mais eficazes na prevenção da violência escolar no Brasil. A parceria entre o poder público e a atividade de ISP, o uso de ferramentas específicas para detectar gatilhos na prevenção da violência, a identificação de corpo discente adequado no que tange à mediação de conflitos e ainda, a análise de perfil de eventuais agressores são abordagens deste artigo cujo objetivo é auxiliar o poder público e, consequentemente, toda uma sociedade em face de possíveis eventos criminosos em âmbito escolar. Trata-se de pesquisa básica, de natureza explicativa, a partir de fontes bibliográficas.

Palavras-chave: violência escolar; atividade de inteligência; perfil de adolescentes agressores; ataques às escolas no Brasil.

SCHOOL VIOLENCE: A discussion to evaluate how public security intelligence activity can contribute to prevention and care.

ABSTRACT

The Public Security Intelligence (PSI) activity in contributing to the prevention of school violence, as an object of study, plans to discuss how the activity could contribute to the promotion of more effective public policies in the prevention of school violence in Brazil. The partnership between the public authorities and the PSI activity, the use of specific tools to detect triggers in the prevention of violence, the identification of a suitable student body with regard to conflict mediation and also the analysis of the profile of potential aggressors are approaches of this article whose objective is to assist the public authorities and, consequently, society as a whole in the face of possible criminal events in the school environment. This is basic research, of an explanatory nature, based on bibliographic sources.

Keywords: School violence; intelligence activity; profile of teenage aggressors; attacks on schools in Brazil.

[*] Graduada em Processamento de Dados, graduanda em Licenciatura em Matemática e Pós-Graduada em Comércio Exterior. Servidora da Secretaria de Administração Penitenciária do Estado do Rio de Janeiro, lotada na Subsecretaria de Inteligência e exercendo a função de Coordenadora Pedagógica da Escola de Inteligência Penitenciária. Endereço eletrônico:deborahkrs@gmail.com.

INTRODUÇÃO

No Brasil, a violência nas escolas vem se tornando cada vez mais comum devido às pressões psicológicas submetidas aos jovens através do uso das mídias sociais e por conta do convívio, muitas vezes, nada harmonioso, no ambiente escolar. Nesse contexto, a violência nas escolas é um fenômeno que afeta, além dos estudantes, toda uma sociedade. A abordagem desse tema tem por objetivo discutir de que forma a atividade de Inteligência de Segurança Pública (ISP) poderia contribuir na promoção de políticas públicas mais eficazes na prevenção da violência escolar. Além disso, é necessário identificar e listar, especificamente, os gatilhos que promovem a violência escolar, descrever a atividade de ISP no âmbito da prevenção deste fato e reconhecer a interação entre a atividade e a implementação de medidas públicas para que tal problemática seja solucionada.

Antes de analisarmos esses objetivos, devemos refletir: de que forma a atividade de ISP poderia contribuir, a ponto de evitar/ minimizar a violência escolar?

A justificativa está relacionada à atividade de inteligência, como sendo uma atividade de cunho basicamente preventivo, tendo uma contribuição relevante para estabelecer diretrizes de políticas públicas nacionais mais efetivas na prevenção a esse tipo de delito, objetivando, portanto, benefícios não só à comunidade escolar, mas à sociedade como um todo.

Outrossim, o estudo em tela é extremamente importante para a atividade de ISP, no tocante à identificação de tendências e padrões que corroboram para a violência escolar. O intuito é o monitoramento direcionado a partir dessa identificação, para, através da cooperação interinstitucional, prevenir e proteger, oportunamente, a sociedade brasileira da violência que assola as escolas.

Importante ressaltar que este estudo possui abrangência nacional. A escolha dessa delimitação, se deve ao simples fato de que diferentes países podem apresentar contextos socioeconômicos, culturais, comportamentais e políticos distintos, que influenciam diretamente na dinâmica da violência escolar sofrida. Compreender essas especificidades permite desenvolver estratégias de prevenção e intervenção mais eficazes, adaptadas às necessidades brasileiras, objetivando a sugestão de promoção de políticas públicas direcionadas à adequação da nossa legislação.

Para confecção deste artigo, foram examinadas várias publicações em revista da Doutora em Educação Telma Pileggi Vinha, pesquisadora com ênfase em violência e mediação de conflitos interpessoais no ambiente escolar, do Instituto de Estudos Avançados da Unicamp. A partir da leitura das pesquisas feitas pela Drª Telma, foram buscados, para embasamento na elaboração

deste estudo, artigos, livros e revistas sobre o *bullying*, *cyberbullying*, prevenção à violência virtual, convivência escolar saudável, ética nas escolas, mediação de conflitos, ataques escolares de violência extrema, dentre outros aplicados ao direito à educação e políticas públicas no Brasil.

Em relação à legislação aplicada, foram examinadas a Constituição da República Federativa do Brasil (CFRB/88), o Estatuto da Criança e do Adolescente (ECA), a legislação correlata à Inteligência de Segurança Pública (ISP), a instituição do Sistema Brasileiro de Inteligência (SISBIN), a instituição do Subsistema de Inteligência de Segurança Pública (SISP), a fixação a Política Nacional de Inteligência (PNI), a organização do SISBIN e ainda, a Doutrina Nacional de Inteligência de Segurança Pública (DNISP), por se tratar de estudo de delimitação nacional.

Quanto às ferramentas específicas de inteligência, foram adotados estudos sobre inteligência e investigação em fontes abertas, ferramentas de geolocalização, técnicas de engenharia social, técnicas operacionais de inteligência e técnicas de entrevista.

Aprofundando o assunto relacionado às políticas públicas, foram explorados os Núcleos de Inteligência e Segurança Escolar (NISE), sua criação e aplicabilidade em diversos estados do Brasil.

A metodologia utilizada neste artigo foi a pesquisa básica, de natureza explicativa, a partir de fontes bibliográficas.

1 UM BREVE CONTEXTO JURÍDICO SOBRE OS DIREITOS À EDUCAÇÃO DAS CRIANÇAS E ADOLESCENTES

A segurança nas escolas envolve diversas questões jurídicas e sociais, as quais estão diretamente ligadas aos princípios do direito à educação, à dignidade da pessoa humana e à proteção dos direitos das crianças e adolescentes, conforme garantidos pelo ordenamento jurídico brasileiro.

Conforme descrito no art. 6º da Constituição da República Federativa do Brasil (CFRB/88), "São direitos sociais a educação, a saúde, o trabalho, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição" (BRASIL, CRFB/88, Art. 6º).

Em consonância, o art. 205 da CRFB/88 enfatiza a educação como direito de todos, sendo um dever do Estado e da família, destacando a colaboração da sociedade na sua promoção e incentivo.

> A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. (BRASIL, CRFB/88, art.205)

Complementando os artigos anteriores, o artigo 227 da Constituição determina a educação como sendo dever da família, da sociedade e do Estado, bem como a vida, a saúde, a alimentação, o lazer, a cultura, dentre outros.

> A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. (BRASIL, CRFB/88, Art.227)

Além dos referidos artigos da CRFB/88, citados anteriormente, podemos mencionar ainda o Estatuto da Criança e do Adolescente (ECA), promulgado através da Lei Federal nº 8.069/1990, cujo objetivo é garantir os direitos das crianças e dos adolescentes, direcionando como obrigação do Estado, da família e da sociedade, salvaguardá-los e promovê-los, conforme mencionado, por exemplo, em seu art. 53: "A criança e o adolescente têm direito à educação, visando ao pleno desenvolvimento de sua pessoa, preparo para o exercício da cidadania e qualificação para o trabalho" (BRASIL, Lei Federal 8069/1990, Art. 53).

2 A ATIVIDADE DE ISP NO BRASIL E UM BREVE HISTÓRICO DE SUA REGULAMENTAÇÃO

O primeiro Plano Nacional de Segurança Pública (PNSP) que se tem conhecimento, foi apresentado no período pós-redemocratização em abril de 1991, durante o governo de Fernando Collor de Mello.

Em 1999, através da a Lei Federal nº 9.883/1999, foi criada a Agência Brasileira de Inteligência (ABIN), que é um órgão da Presidência da República dedicado à produção de conhecimentos para subsidiar as decisões do Presidente da República e de seus ministros.

Posteriormente, um novo PNSP foi lançado em 2000, pelo Ministério da Justiça (MJ), durante o segundo governo de Fernando Henrique Cardoso, já na vigência da Secretaria Nacional de Segurança Pública (SENASP). O plano foi estruturado em 35 (trinta e cinco) páginas e era subdividido em 15 (quinze) compromissos de atuação da União com a segurança pública.

Esse plano, em seu 4º compromisso, previa a implementação de um Subsistema de Inteligência de Segurança Pública (SISP). Assim, em 21 de dezembro de 2000, através do Decreto nº 3.695, foi criado o SISP, no âmbito do Sistema Brasileiro de Inteligência (SISBIN), objetivando coordenar e integrar as atividades de ISP no Brasil.

Em 2007, foi proposta a primeira versão da Doutrina Nacional de Inteligência de Segurança Pública (DNISP), através da SENASP. Com o constante crescimento dos assuntos direcionados às questões de segurança pública e, consequentemente, de ISP, a DNISP, depois de diversas revisões,

chegou a sua 4ª edição, publicada em 20 de janeiro de 2016.

Em novembro de 2023, a ABIN publicou a Doutrina da Atividade de Inteligência (DAI) que não sobrepõe as doutrinas já existentes e sim prevê a possibilidade da integração de órgãos federados ao SISBIN, atendidos os critérios legais e procedimentais.

> Toda a atividade de inteligência conduzida no Brasil deve seguir os mesmos princípios, os quais conformam as premissas básicas da atual Doutrina da ABIN. Nos termos da Lei nº 9.883/1999, da Política Nacional de Inteligência, instituída pelo Decreto nº 8.793/2016, e do Decreto nº 11.693/2023, complementados por outros dispositivos legais e administrativos legitimamente estabelecidos, a atividade de inteligência no Estado brasileiro é exercida por organizações públicas, de forma constante e metódica, por profissionais especializados, lotados em estruturas próprias de trabalho contínuo, conhecidas como organismos de inteligência. (DNISP, 2023, p15)

3 A VIOLÊNCIA NAS ESCOLAS – DESDOBRAMENTOS ALÉM DOS MUROS ESCOLARES

Em 20 de abril de 1999, o massacre de Columbine, ocorrido no estado do Colorado, Estados Unidos da América (EUA), chocou o mundo como sendo um dos mais aterrorizantes atos de violência envolvendo jovens em ambiente escolar. Os estudantes Eric Harris e Dylan Kleebold promoveram um ataque à escola de Columbine utilizando armas de fogo e explosivos, resultando em 13 (treze) mortes e 24 (vinte e quatro) feridos. Após o massacre, ambos cometeram suicídio. Columbine serviu de inspiração para ataques ocorrido no Brasil a partir de 2001.

Diante disso, traz-se à tona calorosas discussões buscando entendimentos sobre as possíveis motivações para uma atitude tão perturbadora, que afeta a sociedade como um todo.

FIGURA 1: IMAGEM REAL DO ATAQUE NA ESCOLA DE COLUMBINE

Fonte: Wikipedia.org , 2024.

3.1 Índices da violência nas escolas brasileiras e o perfil do agressor

O Brasil, infelizmente, é o segundo país com mais casos de violência escolar no mundo.

Segundo o estudo de junho de 2023 da Drª Telma Pileggi Vinha (2023), ilustrado na imagem abaixo, nos últimos 22 (vinte e dois) anos, foram registrados no Brasil 32 (trinta e dois) ataques, cometidos por estudantes e ex-estudantes, em 33 (trinta e três) escolas, sendo, 15 (quinze) escolas estaduais, 12 (doze) escolas municipais e 06 (seis) escolas particulares.

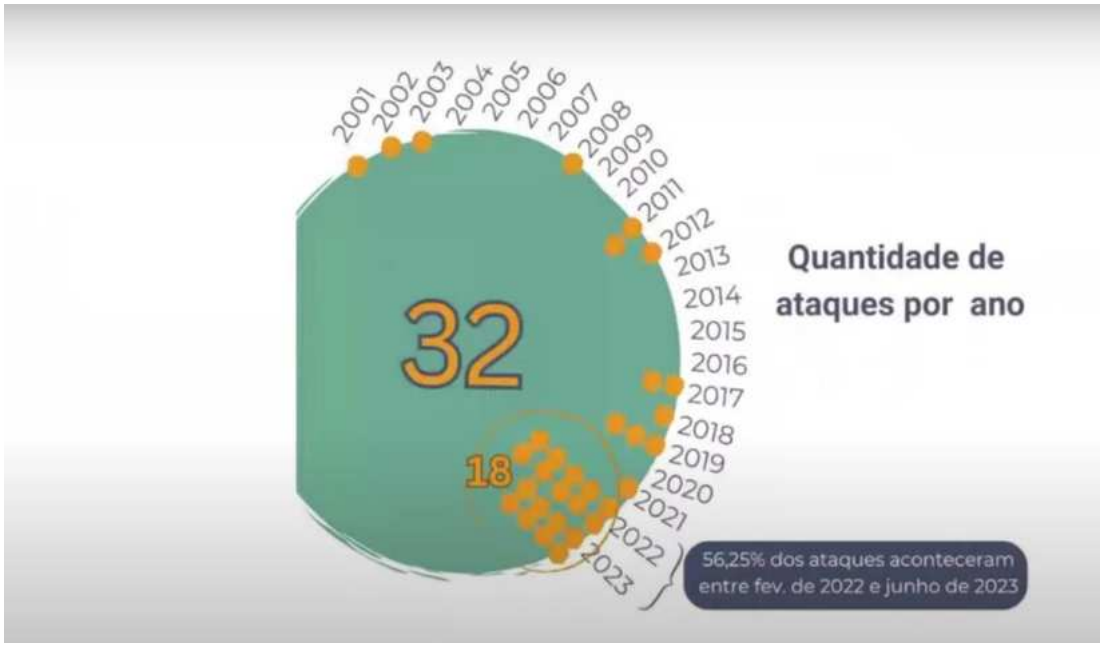
FIGURA 2: ATAQUES DE VIOLÊNCIA EXTREMA, COMETIDOS POR ALUNOS E EX-ALUNOS, EM ESCOLAS NO BRASIL

Fonte: Youtube, 2024 - Palestra: Ataques de Violência Extrema em Escolas do Brasil e a Construção da Cultura de Paz – MINISTÉRIO PÚBLICO DE RONDÔNIA.

Os anos 2022 e 2023 foram os que registraram os maiores índices de ataques em escolas. O isolamento social e os impactos psicológicos decorrentes da pandemia de Covid-19, possivelmente contribuíram para esse aumento significativo de ataques.

Foram contabilizadas 38 (trinta e oito) vítimas fatais, das quais 27 (vinte e sete) estudantes, 04 (quatro) professores, 02 (dois) profissionais da educação e 5 (cinco) atiradores por suicídio, conforme demonstrado na figura 4.

FIGURA 3: QUANTIDADE DE ATAQUES EM ESCOLAS POR ANO, DE 2021 A 2023



Fonte: Youtube, 2024 - Palestra - Ataques de Violência Extrema em Escolas do Brasil e a Construção da Cultura de Paz – Ministério Público de Rondônia.

.

FIGURA 4: VÍTIMAS FATAIS DOS ATAQUES DE VIOLÊNCIA EXTREMA EM ESCOLAS DO BRASIL

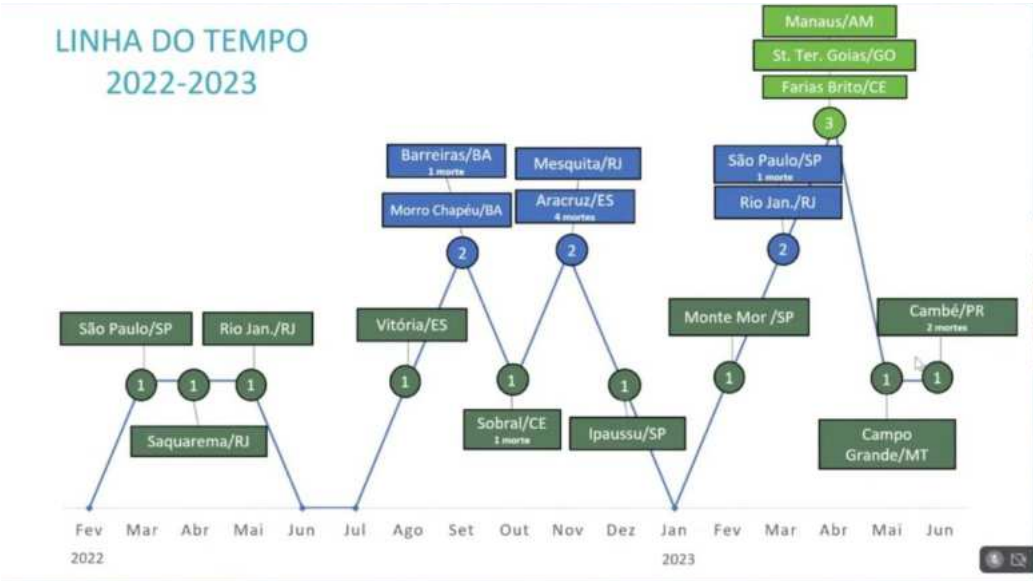
Fonte: Youtube, 2024 - Palestra - Ataques de Violência Extrema em Escolas do Brasil e a Construção da Cultura de Paz – Ministério Público de Rondônia.

O perfil predominante dos autores é de jovens entre 10 (dez) e 25 (vinte e cinco) anos, brancos, do sexo masculino, com gosto pela violência e culto a armas, além de possuírem indícios de transtornos mentais variados.

Esses jovens, em sua maioria, possuem valores extremamente opressores e enxergam a realidade de forma completamente distorcida. São motivados por diversos tipos de preconceitos. A intolerância e a aversão total à existência de um determinado grupo são causas que fomentam o desejo latente de vingança, caracterizado pela autocrítica do não pertencimento sentida pelo agressor. Identificam-se como desfavorecidos e se julgam excluídos da sociedade como um todo.

Na figura abaixo, além de visualizar os meses que foram registradas ocorrências de 2022 a 2023, também é possível visualizar os estados brasileiros em que ocorreram.

FIGURA 5: ATAQUES DE VIOLÊNCIA EXTREMA EM ESCOLAS NOS ESTADOS DO BRASIL - LINHA DO TEMPO



Fonte: Youtube, 2024 - Palestra - Ataques de Violência Extrema em Escolas do Brasil e a Construção da Cultura de Paz – Ministério Público de Rondônia

.

3.2 Forma de atuação dos agressores escolares

Observou-se que todos os ataques às escolas não foram acidentais, e sim articulados e planejados anteriormente.

Como os jovens agressores não se sentem acolhidos pela sociedade, procuram, por meio de redes sociais, de jogos violentos e de fóruns *on-line*, perfis de pessoas que se assemelhem a eles. Utilizam-se muitas vezes, de acessos não rastreáveis, como, por

exemplo, *Deep Web* e *Dark Web*, pela preferência pelo anonimato. Quando encontram comunidades caracterizadas por indivíduos de comportamento opressor, adeptos da subcultura extremista e discursos de ódio, identificam-se e trocam experiências agressivas, racistas, misóginas, buscando a violência, como forma de poder. Essa nova comunidade em que estão inseridos, reforça suas tendências agressivas, gerando o tão sonhado pertencimento, pelos objetivos e gostos em comum. Costumam vangloriar terroristas, neonazistas e extremistas. Como acham que fazem parte de um movimento, inspiram-se em outros ataques para arquitetar seu próprio, no desejo de virarem ícones. Diante disso, estes agressores focam em indivíduos que consideram repugnantes, condicionando-os como responsáveis por sua exclusão social e insatisfação pessoal para, em um momento oportuno, promover um massacre justificado, em nome de uma causa maior.

3.3 Alguns casos de ataques às escolas no Brasil

Alguns casos de ataques às escolas foram de grande comoção no Brasil. Todos desencadearam uma onda de insegurança em suas comunidades locais e circunvizinhas, alertando todas as forças de segurança. Foram eles:

ARACRUZ (ES), 2022

Em 25 de novembro, um adolescente de 16 anos deixou quatro pessoas mortas - três professoras e uma aluna de 12 anos - após invadir duas escolas em Aracruz, no norte do Espírito Santo. No momento do crime, o adolescente ostentava uma suástica (símbolo nazista) em um dos braços, além de roupa tática e duas armas (uma pistola .40 e um revólver 38) pertencentes ao pai policial. Ele foi apreendido e cumprirá até três anos de internação em unidade socioeducativa.

SOBRAL (CE), 2022

Um estudante de 15 anos morreu e dois ficaram feridos após um adolescente, também de 15 anos, disparar contra os três colegas na Escola Professora Carmosina Ferreira Gomes, em Sobral, no dia 8 de outubro. Ele estava com uma arma de fogo registrada no nome de um CAC (colecionador, atirador desportivo e caçador) e foi apreendido.

SUZANO (SP), 2019

Um ataque na Escola Estadual Raul Brasil, em Suzano, na Grande São Paulo, deixou dez mortos, incluindo os dois atiradores, e 11 feridos. Os autores do massacre, Luiz Henrique de Castro, de 25 anos, e G.T.M., de 17, eram ex-alunos da instituição. Um dos atiradores acabou matando o comparsa e depois cometeu suicídio.

MEDIANEIRA (PR), 2018

Um estudante de 15 anos do ensino médio pegou uma arma e atirou nos colegas em uma escola estadual da pacata cidade de

Medianeira, a 60 quilômetros de Foz do Iguaçu, no oeste do Paraná. Tinha uma lista para livrar os amigos - no fim, dois acabaram baleados. O atentado aconteceu no Colégio Estadual João Manoel Mondrone. Segundo a polícia, o autor do ataque seria vítima de bullying na escola.

GOIÂNIA (GO), 2017

Um adolescente de 14 anos matou a tiros dois colegas e feriu outros quatro em uma sala de aula do Colégio Goyases, em Goiânia, em 20 de outubro de 2017. Filho de policiais militares, ele usou a arma da mãe, que havia levado à escola particular, escondida na mochila. Segundo a Polícia Civil, o rapaz sofria bullying e o crime foi premeditado.

REALENGO (RJ), 2011

Considerado à época como o maior massacre em escolas brasileiras até então, a tragédia em Realengo, zona oeste do Rio de Janeiro, deixou 12 crianças mortas. O crime foi cometido por um ex-aluno de 23 anos que levou dois revólveres à Escola Municipal Tasso da Silveira e disparou contra os alunos, todos de 13 a 15 anos. Depois de invadir duas salas de aula, ele foi atingido na barriga pela polícia e disparou um tiro na própria cabeça.

4 A PARCERIA ENTRE A ATIVIDADE DE ISP E O PODER PÚBLICO NA PREVENÇÃO À VIOLÊNCIA NAS ESCOLAS BRASILEIRAS

Conforme o estudo da Dr.ª Telma Pileggi Vinhas, mencionado anteriormente na seção 3.1, dos 32 (trinta e dois) ataques às escolas brasileiras nos últimos 22 (vinte e dois) anos, 18 (dezoito) deles ocorreram entre fevereiro de 2022 e junho de 2023, demonstrando um crescimento expressivo da violência nas escolas do Brasil. Diante disso, viu-se a necessidade de direcionar os olhares para a temática Segurança X Educação X Saúde, assunto que vem se tornando destaque nos estudos e discussões acadêmicas como objeto de pesquisa.

A parceria entre a atividade de ISP e o poder público é fundamental para o desenvolvimento de estratégias adequadas visando salvaguardar a sociedade de atividades violentas, transgressoras e criminosas em ambiente escolar.

A partir da necessidade de um olhar mais direcionado em relação à segurança nas escolas e ao seu redor, foram desenvolvidos os Núcleos de Inteligência e Segurança Escolar (NISE) em diversos estados brasileiros, que atuam em conjunto com outras forças de segurança, como polícias, bombeiros, guardas municipais e civis etc. na reunião de dados e produção de conhecimento, visando garantir a segurança da comunidade escolar. Atualmente, não existe uma lista oficial e atualizada de todos os estados que possuem NISE e é possível que nem todos tenham implementado esses núcleos. Os Núcleos também não atuam de forma padronizada, alguns pertencem à

estrutura da secretaria de educação, outros na estrutura da secretaria de segurança pública, com dinâmicas de subordinação distintas. A ausência do NISE pode ocasionar vulnerabilidade a ataques e impacto na segurança pública, uma vez que a falta de informações prejudica a identificação de padrões de violência e, consequentemente, a elaboração de políticas públicas eficazes para combater e/ou mitigar atos infracionais e criminais. Porém, alguns estados já implementaram esses núcleos, demonstrando um compromisso crescente com a segurança no ambiente escolar, como, por exemplo, Amazonas (AM), Mato Grosso (MT), Mato Grosso do Sul (MS) e Rio de Janeiro (RJ).

Embora o tema da segurança escolar seja de interesse nacional e o governo federal atue em diversas frentes relacionadas a ele, a criação e implementação desses Núcleos são iniciativas que partem dos governos estaduais, considerando a autonomia para lidar com as questões de segurança pública e educação, previstas na Constituição Federal (1988). Esses NISE foram desenvolvidos com base nas preocupações com os ataques ocorridos no interior das escolas no Brasil. É um canal direto que colhe, organiza e analisa informações para produção de conhecimento de segurança pública no ambiente escolar.

O estado do Rio de Janeiro instituiu o NISE-RJ através da resolução SEEDUC nº 6.176 de 19 de junho de 2023, publicada no Diário Oficial (DOERJ) nº 112, de 21 de junho de 2023, subordinado à Secretaria Estadual de Educação, "com o objetivo de criar mecanismos que visem erradicar ou mitigar eventos de qualquer natureza violenta que comprometa a dinâmica escolar" (DOERJ, 2023).

O estado do Mato Grosso do Sul criou o NISE-MS através do Decreto nº 16.276 de 14 de abril de 2023, publicado em 20 de setembro de 2023.

No Mato Grosso, o Decreto Estadual nº 282, de 11 de maio de 2023, dispõe sobre a Estrutura Organizacional da SEDUC. O NISE-MT foi criado por meio de uma parceria entre a SEDUC-MT e a Secretaria de Estado de Segurança Pública do Estado do Mato Grosso (SESP-MT) e conta com o monitoramento do Centro Integrado de Operações de Segurança Pública (CIOSP) para 647 (seiscentos e quarenta e sete) unidades escolares dos municípios de Cuiabá e Várzea Grande. O NISE-MT visa identificar, avaliar e inibir ataques e ameaças, sugerindo ações e medidas de proteção nas unidades escolares.

No estado do Amazonas, há o NISE-AM, instalado na sede da SEDUC-AM. Foi criado através do Decreto Estadual nº 47.235 de 10 de abril de 2023 que instituiu o Comitê Institucional de Proteção, Monitoramento, Guarda e Segurança Escolar, objetivando assegurar à criança, ao adolescente e ao

jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Vale ressaltar que os NISE são recentes, visando proporcionar segurança aos alunos, professores e funcionários, além de direcionar esforços no tocante a inibir ataques, ameaças, racismo, *bullying, cyberbullying* e quaisquer outras ações consideradas transgressoras no ambiente escolar.

Os Núcleos citados são apenas alguns exemplos dos inúmeros casos de parceria entre a atividade de inteligência e o poder público na prevenção à violência escolar no Brasil, não sendo objeto deste estudo aprofundá-los.

A iniciativa da criação dos NISE se deu após a gravidade das ocorrências de ataques às instituições de ensino, como, por exemplo: o assassinato de duas estudantes no Colégio Sigma, em Salvador, em 28 de outubro de 2002; o ataque à escola Tasso da Silveira, no bairro de Realengo-RJ, em 07 de abril de 2011; o ataque à escola Professor Raul Brasil, em Suzano-SP, em 13 de março de 2019; dentre outros.

Há departamentos ou setores na estrutura da Secretaria de Educação, ou da Segurança Pública, que possuem ações semelhantes aos NISE. Porém, é necessário que sejam criados núcleos de inteligência e segurança escolar em todos os estados do Brasil e ainda que estes tenham cunho de Agência de Inteligência, objetivando facilitar a comunicação e trâmite de documentos de inteligência visando à prevenção da violência escolar.

O estado do Rio de Janeiro, por exemplo, além de ter o NISE na estrutura da SEEDUC-RJ, também conta com a Coordenação de Inteligência de Prevenção a Ataques em Escolas (CIPAE), subordinada ao Departamento Geral de Inteligência (DGI) da Subsecretaria de Inteligência (SSINTE), que pertence à estrutura da Secretaria de Estado de Polícia Civil (SEPOL). A CIPAE tem como atribuição a produção de conhecimento de inteligência pertinente a ataques em escolas. Considerando que a SSINTE é Agência Central do Sistema de Inteligência do Estado do Rio de Janeiro (SISPERJ), a atuação da CIPAE promove uma rede de integração consolidada, fortalecendo interfaces interinstitucionais.

5 A ATIVIDADE DE ISP E SUAS FERRAMENTAS PARA A PREVENÇÃO DA VIOLÊNCIA ESCOLAR NO BRASIL

A violência escolar não só afeta a comunidade escolar, mas a sociedade como um todo, ela ultrapassa os muros da escola comprometendo o desenvolvimento social, emocional e intelectual dos alunos, gerando impactos negativos a longo prazo para a sociedade além da promoção da sensação de insegurança.

Com técnicas, ferramentas e metodologias específicas de reunião de dados, análise e produção de conhecimento, a atividade de ISP pode auxiliar na detecção de gatilhos que vulnerabilizem a segurança nas escolas brasileiras.

A referida atividade, como de cunho preferencialmente preventivo, possui, na maioria das vezes, uma base de dados alimentada sistematicamente com dados, informações e estatísticas sobre infrações, crimes, infratores, criminosos, locais, lideranças criminosas, facções criminosas, dentre outros. Uma sólida base de dados mostra-se imprescindível para o planejamento de ações, objetivando direcionar a estrutura da agência no fomento de atividades de prevenção, visando a eficiência dos resultados na antecipação da atividade delitiva.

5.1 As técnicas de engenharia social, geolocalização e análise de redes sociais para reunião de dados e monitoramento de atividades nocivas na internet

Muitas técnicas e ferramentas da atividade de ISP são utilizadas para a prevenção da violência escolar. Contudo, este estudo limita-se às técnicas de engenharia social, geolocalização, análise de redes sociais para a reunião de dados, monitoramento dos atacantes e exemplo de como a ação de busca vigilância poderia ser aplicada.

A Engenharia Social é uma técnica psicológica para a manipulação de comportamentos, com o intuito de focar no estudo do indivíduo. A criação de um enredo baseado na motivação humana, manipula as emoções e os instintos das pessoas, de forma a serem induzidas a tomar atitudes inocentes, nem sempre de seu interesse.

Essa técnica, aliada à criação de um perfil não rastreável, objetivando a interação e confiança de um referido grupo, pode ser utilizada na atividade de ISP para cooptar a atenção de grupos reservados e de perfis com potencial risco para a execução de atividades criminosas.

O analista, uma vez logrando êxito em fazer parte de uma determinada comunidade digital, consegue interagir com um ou mais jovens, participando de fóruns, conversas, trocando opiniões, recebendo, inclusive, informações de possíveis ataques.

Além disso, uma correta utilização do recurso de pesquisas em fontes abertas, por analistas bem capacitados, torna-se um excelente aliado no constante rastreamento de possíveis atividades suspeitas e articulações criminosas.

Em consonância, mediante técnicas de inspeção e análise de códigos-fonte, além de softwares de análise de vínculos em redes sociais, profissionais preparados são capazes de identificar outros perfis associados, que passam a ser monitorados. Esse monitoramento, aliado à experiência do profissional de ISP, identifica articulações e planejamentos de ataques, acionando oportunamente os órgãos de segurança e evitando, consequentemente, que tal fato ocorra.

Por conseguinte, um cuidadoso rastreamento através do recurso da geolocalização possibilita identificar, quase que em tempo real, a iminência de um possível ataque.

Diante das técnicas mencionadas, verifica-se como a atividade de ISP é capaz de identificar, monitorar e interagir com jovens e grupos com potencial tendência à prática de atividades extremistas e criminosas, reunindo dados e produzindo conhecimento, constatando assim, através da análise, as vulnerabilidades na segurança escolar. Dessa forma é possível assessorar o tomador de decisão objetivando, em parceria com o poder público, antecipar e evitar quaisquer atividades delitivas.

Importante ressaltar que os analistas de inteligência, que atuam no processo de interação nos grupos de jovens, devem receber, de forma sistemática e constante, capacitações e treinamentos, no que tange aos programas de rastreamento de dados e ainda no tocante às linguagens, gírias e comportamento adequado aos grupos, facilitando assim, sua interação.

5.2 Mapeamento de perfil comportamental para criação de base de dados

Inicialmente, através de estatísticas e casos reais, é primordial que seja traçado o perfil do possível agressor para cada caso.

Considerando a dinâmica do NISE de cada estado, o desenho desse perfil pode ser feito através da coleta de dados, principalmente nas redes sociais, combinada à ação de busca vigilância, pelo NISE ou órgão ao qual é subordinado. São iniciativas favoráveis para reunir dados pertinentes aos comportamentos dos alunos de uma determinada instituição escolar, preferencialmente aquelas que sabidamente podem sofrer algum tipo de influência.

Os dados desses perfis comportamentais seriam analisados e confrontados pelos analistas, considerando o perfil já traçado anteriormente, como de potencial agressor. O resultado é a sugestão

de possíveis novos agressores com tendências ao cometimento de atos de violência no ambiente escolar.

Essa análise seria determinante para a promoção de medidas sistemáticas de acompanhamento comportamental, voltadas aos alunos, observados na pesquisa instrumental.

FIGURA 6: CASOS DE SUCESSO ALCANÇADOS ATRAVÉS DO TRABALHO CONTÍNUO DA INTELIGÊNCIA DE SEGURANÇA PÚBLICA (ISP)

Fontes: Carta Capital, 2023[1]. G1, 2023[2]. g1 Rio e TV Globo, 2023[3].

5.3 A cooperação da atividade de inteligência na identificação de problemas sociais e familiares referentes ao corpo discente

Sabe-se haver vários direcionamentos de ações educacionais humanizadas como ferramentas para a conscientização e formação do indivíduo, focadas na empatia, no acolhimento, no respeito familiar, no respeito ao próximo e na aceitação de grupos diversos, objetivando uma saudável convivência coletiva, como forma de prevenção da ruptura da harmonia escolar. O que se propõe neste tópico é utilizar o conhecimento de inteligência produzido para uma ação direcionada a jovens já

[1]Disponível em: https://www.cartacapital.com.br/educacao/policia-diz-que-jovem-preso-em-pernambuco-e-mentor-intelectual-de-ataque-em-colegio-do-parana/.
[2]Disponível em: https://g1.globo.com/rj/sul-do-rio-costa-verde/noticia/2023/04/11/preso-jovem-suspeito-de-publicar-ameacas-de-ataque-a-escolas-de-barra-do-pirai.ghtml
[3]Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2023/03/24/apos-alerta-da-interpol-menor-suspeito-de-planejar-ataque-a-escola-no-rio-e-apreendido.ghtml

identificados como tendenciosos à prática de ações criminosas.

Conforme mencionado na subseção 5.2, após a análise do mapeamento comportamental do corpo discente e destacamento de possíveis agressores, um relatório poderia ser enviado aos NISE, ou gerado por eles (dependendo da subordinação do Núcleo), que, com o apoio de profissionais da saúde e da educação, adotariam métodos relevantes, voltados ao trato da saúde mental, inserção social e apoio familiar, direcionados aos indivíduos já destacados.

A finalidade dessa ação dirigida, em consonância com o princípio da conveniência e oportunidade, seria a identificação dos gatilhos do possível agressor, seu tratamento personalizado e antecipado, prevenindo, por conseguinte, massacres e vidas ceifadas.

Importante ressaltar que quando os pais permitem ou reforçam abertamente a agressão, é possível que as crianças/jovens se comportem agressivamente em casa e, por generalização, em outros lugares em que sintam ser a agressão permitida, esperada ou encorajada. A presença de um adulto permissivo favorece a expressão do comportamento agressivo. Quando problemas de relações familiares são identificados pelos analistas, este fato deverá ser encaminhado a um setor de saúde especializado em tratamento familiar, para que profissionais especializados direcionem o tratamento indicado ao jovem e sua família.

5.4 A participação da atividade de inteligência na adequação de profissionais e educadores

Sabe-se que a escola pode auxiliar na formação dos adolescentes e contribuir muito para o desenvolvimento de um indivíduo, podendo até frear o avanço da violência escolar.

Para tanto, é preciso que a escola promova políticas norteadas por um plano de engajamento e inserção. Uma abordagem de conteúdos de forma mais humanizada, baseada em respeito mútuo, possui um poder transformador. Desta forma, é necessário um corpo docente motivado, capacitado e preparado para lidar com a especificidade escolar e na possível mediação de conflitos.

A atividade de inteligência, na estrutura organizacional de setores como o da educação e da segurança pública, pode promover processos de recrutamento e gestão de pessoas, baseados em técnicas de entrevista para análise de aptidões pessoais, objetivando adequar o perfil profissional consonante a cada tipo de função escolar. Além disso, uma análise criminal dos profissionais que lidam com o corpo discente é imprescindível para a preservação de um ambiente seguro. Assim, ao analisar profissionais que interajam diariamente com jovens e crianças, contribui-se

grandiosamente para garantir a prevenção da violência escolar no Brasil.

CONCLUSÃO

Em vista dos argumentos apresentados neste estudo, a parceria entre a atividade de ISP e o poder público torna-se fundamental para prevenir e evitar ataques nas escolas do Brasil. A elaboração de leis que obriguem a identificação de usuários de redes de internet, inclusive com sua localização, evitaria o suposto anonimato dos usuários e seus desdobramentos, facilitando o trabalho da inteligência. É importante salientar que o anonimato é um fator encorajador de ações nada ortodoxas e fomenta a livre divulgação de ideias sem qualquer tipo de responsabilização. O acompanhamento dos perfis nocivos e perigosos pelos profissionais de ISP seria aperfeiçoado e a criminalização mais assertiva. O objetivo da identificação obrigatória de usuários, sob pena de responsabilidade, não possui o cunho de censura ou de controle, até porque os rastros digitais são invariavelmente detectáveis. Além disso, devemos nos conscientizar de que anonimato e privacidade não possuem o mesmo significado. A privacidade, conforme art. 5º da CRFB/88, é um direito constitucional que assegura a proteção de informações pessoais: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, CRFB/88, art. 5º, inciso X).

Com a leitura do referido artigo, infere-se, no entanto, que o direito à privacidade protege apenas as informações pessoais, mas não dispensa sua identificação. Já o anonimato é o ato de não divulgar sua própria identidade. O que se procura aqui é o equilíbrio entre a liberdade de expressão e a autonomia permissiva disfarçada de anonimato, com o propósito do cometimento de ações transgressoras e delituosas. A coleta e o tratamento de dados de adolescentes e jovens realizados por profissionais de inteligência, mesmo que cuidadosamente avaliados para não violar seus direitos à privacidade, liberdade e imagem (Art. 31 da Lei 12.527/2011 – Lei de Acesso às Informações, § 1º), é possível e proporcional visto a gravidade e impacto social dos ataques.

No que tange ao aspecto social, a intimidação sistemática sofrida pelos discentes na rede nacional de ensino forma, como consequência, um sentimento de ódio e repúdio aos agressores, como foi comprovado pelo pedagogo e filósofo brasileiro Paulo Freire, em sua célebre frase do livro Pedagogia do Oprimido: "Quando a educação não é libertadora, o sonho do oprimido é ser o opressor" (FREIRE, 2011, p.269).

Nessa sucinta fala de Freire, podemos observar que determinados alunos

podem ter comportamentos bastante previsíveis. Subentende-se, portanto, que esses jovens, ao internalizar a dor sofrida, acabam identificando a escola como palco de seu sofrimento e assim começam a arquitetar sua vingança. Neste cerne, a atividade de ISP combinada a outras medidas preventivas com profissionais das áreas de saúde e da educação, consegue traçar o delineamento do perfil do possível agressor, sendo eficaz na prevenção do cometimento de atos extremistas que culminariam em massacres e mortes violentas. Podemos ainda ressaltar que um efetivo processo de recrutamento, norteado por profissionais da inteligência, é capaz de identificar requisitos e qualidades necessárias, direcionadas à especificidade escolar, sugerindo um corpo docente preparado para mediar conflitos, adequando cada colaborador à sua competência profissional.

Finalmente, foram relacionadas diversas formas da atuação da Inteligência de Segurança Pública, sendo demonstrada a capacidade da atividade na constatação de índices que vulnerabilizem a segurança no âmbito escolar. A interação da ISP com o poder público pode promover a propositura de implementação de políticas públicas efetivas, objetivando antecipar e evitar quaisquer atividades delitivas, transgressoras e criminosas, relacionadas à violência nas escolas do Brasil.

Cabe ressaltar que as ações sugeridas são um desafio a ser assumido por todas as partes implicadas.

REFERÊNCIAS

AMAZONAS, Decreto nº 47.235, de 10 de abril de 2023. Institui o Comitê de Proteção, Monitoramento, Guarda e Segurança Escolar. Manaus, AM: Governo do Estado, 2023. Disponível em: https://acesse.dev/dec472352023. Acesso em 10 de jun. de 2024.

BOZZA, T.C.L.; VINHA, T. P. Cyberbullying, cyber agressão e riscos on-line: Como a escola pode atuar diante dos problemas da (cyber) convivência. Revista Ibero-Americana de Estudos em Educação, Araraquara, v.18, n.00, e023059, 2023. Disponível em: https://doi.org/10.21723/riaee.v18i00.18444. Acesso em 15 de jun. de 2024.

BOZZA, T.C.L.; VINHA, T. P. Um programa para a promoção da convivência saudável e prevenção da violência virtual:"A Convivência Ética On-line". Revista@mbienteeducação, São Paulo, v.16, n.00, e023007, 2023. Disponível em: https://doi.org/10.26843/ae.v16i00.1262. Acesso em: 16 de jun. de 2024.

BRASIL. [Constituição (1988)] Institui a Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, 1988. Disponível em: https://acesse.dev/crfb1988. Acesso em: 10 de jun. de 2024.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Institui o Estatuto da Criança e do Adolescente (ECA). Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 de jun. de 2024.

BRASIL. Lei nº 9.883, de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência (SISBIN), cria a Agência Brasileira de Inteligência (ABIN). Brasília, DF: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em: 10 de jun. de 2024.

BRASIL. Decreto nº 3.695, de 21 de dezembro de 2000. Institui o Subsistema de Inteligência de Segurança Pública (SISP), no âmbito do Sistema Brasileiro de Inteligência (SISBIN). Brasília, DF: Presidência da República, 2000. Disponível em: https://acesse.one/dec3695-2000. Acesso em 10 de jun. de 2024.

BRASIL. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência (PNI). Brasília, DF: Presidência da República, 2016. Disponível em: https://l1nk.dev/DEC8793-2016. Acesso em: 10 de jun. de 2024.

BRASIL. Lei nº 11.693, de 06 de setembro de 2023. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência (SISBIN). Brasília, DF: Presidência da República, 2023. Disponível em: https://l1nk.dev/dec11693-2023. Acesso em 10 de jun. de 2023.

BRASIL, Doutrina Nacional de Inteligência de Segurança Pública (DNISP). Brasília, DF: Presidência da República, 2023. Disponível em: https://acesse.one/DNISP2023. Acesso em 10 de jun. de 2024.

CIALDINI, Robert B.; Korytowsk, Ivo. As armas da persuasão: como influenciar e não se deixar influenciar. Rio de Janeiro: Sextante, 2012. Disponível em: https://acesse.dev/armas-dapersuasao. Acesso em: 14 de jun. de 2024.

FREIRE, Paulo. Pedagogia do Oprimido. São Paulo: Paz & Terra, 1987. Disponível em: http://www.letras.ufmg.br/espanhol/pdf/pedagogia_do_oprimido.pdf. Acesso em: 13 de jun. de 2024.

GONÇALVES, Joanisval Brito. Atividade de inteligência e legislação correlata. Niterói: Impetus, 2018.

MACEDO, Epaminondas Silva. O Direito à Educação e às Políticas Públicas no Brasil: uma história de exclusão, omissão e reformas educacionais. Curitiba: Appris, 2023.

MATO GROSSO DO SUL, Decreto nº 16.276, de 20 de setembro de 2023. Institui o Núcleo de Inteligência de Segurança Escolar (NISE/MS), no âmbito da Secretaria de Estado de Educação (SED/MS). Campo Grande, MS: Governo do Estado, 2023. Disponível em: https://acesse.dev/16276-23. Acesso em: 10 de jun. de 2024.

MATO GROSSO, Decreto nº 282, de 11 de maio de 2023. Dispõe sobre a Estrutura Organizacional da Secretaria de Estado de Educação (SEDUC). Cuiabá, MT: Governo do Estado, 2023. Disponível em: https://legislacao.mt.gov.br/mt/decreto-n-282-2023-mato-grosso-dispoe-sobre-a-estrutura-organizacional-da-secretaria-de-estado-de-educacao-seduc-a-redistribuicao-de-cargos-em-comissao-e-funcoes-de-confianca?origin=instituicao. Acesso em: 10 de jun. de 2024.

MAURMANN, A. P.; PINTO, M. V. Guia de Entrevista Investigativa: uma coletânea das melhores práticas para obtenção de testemunhos e declarações. Brasília: Pró Consciência, 2020.

PACHECO, J. C.; GOMES, C. B. Violência nas Escolas: uma realidade a ser transformada. Curitiba: Juruá, 2013. Disponível em: https://www.jurua.com.br/bv/conteudo.asp?id=23247&pag=25. Acesso em 12 de jun. de 2024.

PEIXOTO, Mário César Pintaudi. Engenharia Social e Segurança da Informação na Gestão Corporativa. Uberaba: Brasport, 2018.

PEREIRA, J. Peixoto. Investigação Digital e Rastreamento de Dados. Natal: Cyber Trackers, 2023.

RESCHKE, Cristiano; WENDT, Emerson; MATSUBAYACI, Mayumi. Infiltração Policial: da tradicional a virtual. Rio de Janeiro: Brasport, 2021.

RIBEIRO, Neide Aparecida. Cyberbullying: práticas e consequências da violência virtual na Escola. Palmas: Juspodivm, 2019. Disponível em: https://juspodivmdigital.com.br/cdn/arquivos/jus0320_previa-do-livro.pdf Acesso em 14 de jun. de 2024.

RIO DE JANEIRO, Decreto nº 48.803, de 17 de novembro de 2023. Altera, sem aumento de despesas, a Estrutura Organizacional da Secretaria de Estado de Educação (SEDUC). Rio de Janeiro, RJ: Governo do Estado, 2023. Disponível em: https://encr.pw/48803-23. Acesso em: 10 de jun. de 2024.

SCHAEFER, Jack; KARLINS, Marvin. Manual de persuasão do FBI. São Paulo: Universo dos Livros, 2015.

SILVA, Iracema. Atividade de Inteligência: novos paradigmas para a polícia Judiciária. Belo Horizonte: Dialética, 2021.

TOGNETTA, L. R. P.; VINHA, T. P. Até quando? Bullying na escola que prega a inclusão social. Universidade Federal de Santa Maria (UFSM), Santa Maria, v.35 n.3, p. 449-464, 2009. Disponível em: https://doi.org/10.5902/198464442354. Acesso em: 15 de jun. de 2024.

TORREMORELL, Maria Carme Boqué. Mediação de conflitos na escola: modelos, estratégias e práticas. São Paulo: Sumus, 2021.

VINHA, T. P.; TOGNETTA, L. R. P. Construindo a autonomia moral na escola: os conflitos interpessoais e a aprendizagem dos valores. Revista Diálogo Educacional, Paraná, v.9, n.28, p. 525-540, 2009.
Disponível em: https://periodicos.pucpr.br/dialogoeducacional/article/view/3316. Acesso em: 15 de jun. de 2024.

VINHA, T. P.; GARCIA, Cleo. Ataques de violência extrema em escolas no Brasil: causas e caminhos. Relatório de Política Educacional, São Paulo, 2023. Disponível em: https://l1nq.com/ataquesdeviolenciaextremaemescolasnobrasil. Acesso em 16 de jun. de 2024.

WENDT, Emerson; BARRETO, Alessandro G. Inteligência e Investigação em Fontes Abertas. São Paulo: Braspot, 2024.

ZECHI, J.A.M.; VINHA, T. P. A convivência ética em escolas públicas: Análise de um programa de intervenção a partir das perspectivas dos profissionais da escola. Revista Ibero-Americana de Estudos em Educação, Araraquara, v.17, n. 2, p.1293-1310, 2022. Disponível em: https://periodicos.fclar.unesp.br/iberoamericana/article/view/15032. Acesso em: 19 jun. 2024.

RISP
REVISTA DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA
ISSN 2675-7168 ; 2966-0254

A ESISPERJ

Criada oficialmente pelo Decreto Estadual nº 40.254/2006, renomeada pelo Decreto Estadual nº 44.528/2013, posteriormente reorganizada e vinculada à Subsecretaria de Inteligência através da Resolução SESEG nº 737/2013 (DOERJ nº 002/2013), a Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ) busca, através de seus cursos, seminários, ações, *workshops* etc. a uniformização da atuação das Agências de Inteligência de Segurança Pública (AISP) formando, especializando e treinando os servidores nelas lotados, com ênfase nos seguintes pilares:

MISSÃO: qualificar os profissionais da Comunidade de Inteligência e manter atualizada a Doutrina de ISP, por meio da pesquisa e produção de conhecimento, visando potencializar a capacidade de atuação estatal na área finalística da Segurança Pública.

VISÃO: ser referência em ensino, doutrina, pesquisa e extensão em Inteligência de Segurança Pública (ISP) para a Comunidade de Inteligência.

VALORES: produção de conhecimento em ISP; valorização do ambiente democrático; fortalecimento de rede; integração; profissionalização técnica; respeito à diversidade; interoperabilidade; e excelência científica e tecnológica.

A RISP

A Revista de Inteligência de Segurança Pública (RISP) é uma publicação continuada, da Escola de Inteligência de Segurança Pública do Estado do Rio de Janeiro (ESISPERJ). Idealizada como um canal de acesso ao conhecimento de forma oficial, objetiva e transparente, a revista visa divulgar manuais e estudos científicos, resenhas, pesquisas atuais, além das melhores e mais apuradas práticas, contribuindo assim para a desmistificação do tema. A RISP é, portanto, voltada para a comunidade acadêmico-científica, profissionais do setor e demais interessados em aprofundar seus conhecimentos na área de Inteligência, notadamente vinculados às questões da segurança pública.

CONDIÇÕES GERAIS PARA SUBMISSÃO

O envio dos textos, em recebimento de fluxo contínuo, deve ser realizado para o e-mail: risp.esisperj@pcivil.rj.gov.br, em formato <.doc/.docx> (*Microsoft Office Word*). No mesmo e-mail, deve ser encaminhado o Termo de Cessão de Direitos Autorais, assinado e salvo em formato <.pdf>, além do arquivo contendo elementos pré-textuais. Visando facilitar esse processo, todos os modelos destes e outros documentos, além das Diretrizes para Autores, podem ser obtidos na página da ESISPERJ (https://esisperj-ead.pcivil.rj.gov.br/).

Como parte do processo de submissão, os autores são obrigados a verificar a sua conformidade em relação a todos os itens listados nas diretrizes. As submissões em desacordo com as normas serão recusadas e/ou devolvidas aos autores para adequação. Os textos devem seguir os padrões de estilo e requisitos bibliográficos descritos e adotados pelo padrão vigente da ABNT, apresentados nas Diretrizes para Autores.

Os textos devem ter como escopo a atividade de inteligência, com foco na atividade de Inteligência de Segurança Pública, podendo tomar como objeto todas as dimensões e aspectos inerentes à ISP. É necessário que sejam produções intelectuais inéditas dos respectivos autores, atentando-se para que não haja inserção de conteúdo publicado sem menção da fonte, de modo a não ferir a política editorial adotada pela ESISPERJ e a ética científica.

DECLARAÇÃO DE DIREITO AUTORAL

Autores que publicam nesta revista concordam com os seguintes termos:

1) Autores mantêm os direitos autorais e concedem à revista o direito de primeira publicação, sob a Licença *Creative Commons Attribution,* que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista.

2) Autores têm autorização para assumir contratos adicionais separadamente, para distribuição não exclusiva da versão do trabalho publicada nesta revista (ex.: publicar em repositório institucional ou como capítulo de livro), com reconhecimento de autoria e publicação inicial nesta revista.

3) Autores têm permissão e são estimulados a publicar e distribuir seu trabalho *online* (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado.