SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS – UEG
COORDENADORIA DE ENSINO
COORDENAÇÃO DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO
CURSO DE ALTOS ESTUDOS EM SEGURANÇA PÚBLICA - CAESP

CAMILLA RODRIGUES DE ALMEIDA

PROPOSTA DE DESENVOLVIMENTO DE UM SISTEMA DE GESTÃO DE DEMANDAS PARA A AGÊNCIA DE INTELIGÊNCIA DA POLÍCIA CIVIL DO ESTADO DE GOIÁS

GOIÂNIA-GO

2024

CAMILLA RODRIGUES DE ALMEIDA

PROPOSTA DE DESENVOLVIMENTO DE UM SISTEMA DE GESTÃO DE DEMANDAS PARA A AGÊNCIA DE INTELIGÊNCIA DA POLÍCIA CIVIL DO ESTADO DE GOIÁS

Projeto de Pesquisa apresentado como exigência parcial para conclusão da disciplina Metodologia Científica do Curso de Altos Estudos em Segurança Pública (CAESP) pela Secretaria de Segurança Pública de Goiás e a Universidade do Estado de Goiás, sob a orientação do Prof. Esp. Fábio Meireles Vieira.

GOIÂNIA-GO

2024

PROPOSTA DE DESENVOLVIMENTO DE UM SISTEMA DE GESTÃO DE DEMANDAS PARA A AGÊNCIA DE INTELIGÊNCIA DA POLÍCIA CIVIL DO ESTADO DE GOIÁS

PROPOSAL FOR THE DEVELOPMENT OF A DEMAND MANAGEMENT SYSTEM FOR THE INTELLIGENCE AGENCY OF THE CIVIL POLICE OF THE STATE OF GOIÁS

Camilla Rodrigues de Almeida[1]*
Fábio Meireles Vieira[2]**

Resumo: Este estudo propõe o desenvolvimento de um sistema informatizado de gestão de demandas para a Agência de Inteligência da Polícia Civil do Estado de Goiás (AIPCGO), com o objetivo de melhorar o fluxo de comunicação interna e a produção de conhecimento. A pesquisa aborda as necessidades operacionais de uma agência de inteligência, enfatizando a importância de um sistema unificado que promova a padronização e compartimentação de informações sensíveis. A metodologia incluiu a aplicação de um questionário aos chefes de seção da AIPCGO, revelando desafios no acompanhamento de prazos e na comunicação interdepartamental. Os resultados apontaram uma demanda por uma solução tecnológica que facilite a integração e a segurança de dados. Como conclusão, recomenda-se ampliar o diagnóstico em futuros estudos, incluindo entrevistas com gerentes e o superintendente, além de considerar os requisitos da Doutrina Nacional de Inteligência de Segurança Pública (DNISP) para garantir a conformidade normativa.
Palavras-chave: Gestão de Demandas; Segurança da Informação; Comunicação Interna; Agência de Inteligência; Sistema Informatizado.

Abstract: *This study proposes the development of a demand management system for the Intelligence Agency of the Civil Police of the State of Goiás (AIPCGO), aiming to improve internal communication and enhance knowledge production. The research highlights the operational needs of an intelligence agency, emphasizing the importance of a unified system to standardize processes and compartmentalize sensitive information. A survey conducted with section leaders of the AIPCGO identified key challenges, such as issues with deadline tracking and interdepartmental communication. The methodology includes a case study supported by a quantitative and qualitative analysis of the collected data. Based on the findings, functional and non-functional requirements were established, prioritizing features like deadline control, data compartmentalization, and activity monitoring. Although limited to section leaders, the study lays a foundation for system development aligned with operational demands. Future studies should expand the scope by incorporating interviews with managers and the superintendent and exploring the guidelines of the National Doctrine of Public Security Intelligence (DNISP) to ensure compliance with official regulations.*
Keywords: *Demand Management; Information Security; Public Security Intelligence; Communication Optimization.*

[1]*Graduada em Administração pela Faculdade Delta (2014). Atualmente, cursa o 8º período de Engenharia de Software pela UNIALFA e está finalizando a especialização no Curso de Altos Estudos em Segurança Pública (SSP-GO/UEG). E-mail: camilla.rodrigues.de.almeida@gmail.com.

[2]** Graduado em Direito pela Universidade Federal de Goiás (2009) Delegado de Polícia na Polícia Civil do Estado de Goiás. Orientador do Curso de Especialização em Gerenciamento de Segurança Pública (SSP-GO/UEG). E-mail: fabiomv@gmail.com.

1 INTRODUÇÃO

Os órgãos de segurança pública enfrentam a necessidade constante de tomar decisões para assegurar a proteção das pessoas e do patrimônio. Para cumprir sua missão constitucional, seus gestores dependem de informações precisas e oportunas, que lhes permitam tomar decisões eficazes em curto prazo (Santos; Mendonça, 2022). Assim, podem utilizar a atividade de inteligência, conforme a legislação vigente, para gerar conhecimentos que orientem os tomadores de decisão no planejamento e na execução de ações destinadas a combater atos criminosos que ameaçam a ordem pública, a integridade das pessoas e a segurança do patrimônio (Brasil, 2021).

Basicamente, a atividade de inteligência é dividida em dois ramos: inteligência e contrainteligência. A inteligência compreende a coleta, análise e disseminação de informações que, total ou parcialmente, não são acessíveis por meios convencionais. Já o papel da contrainteligência é neutralizar a inteligência adversa, proteger conhecimentos sensíveis e identificar ameaças ou oportunidades (Brasil, 2021; Santos, Mendonça; 2022).

Ribeiro, Nunes e Albuquerque (2022) destacam a importância da troca de conhecimento entre estruturas de inteligência que possuem objetivos semelhantes. No entanto, Carvalho (2015) salienta que devido a estrutura organizacional das Agências de Inteligência de Segurança Pública (AISPs) é comum diferentes equipes monitorarem o mesmo alvo sem compartilhar informações.

Nesse sentido, a Doutrina da Atividade de Inteligência (DAI) (2023, p. 77) destaca que "a cultura de segurança desejável em um organismo de inteligência inclui observar o princípio da compartimentação [...]", devendo, portanto, restringir o acesso baseado na necessidade de conhecer. A ideia central, de acordo com Ruprecht (2021) é que a probabilidade de vazamento de informações sigilosas diminui com o número de pessoas que têm acesso a elas. Assim, quanto menos pessoas souberem, menor o risco de exposição. A compartimentação é baseada no princípio de que cada membro de um projeto sigiloso deve acessar apenas as informações necessárias para sua tarefa, o que reduz o risco de comprometimento do projeto como um todo.

Diante disso, com observância dos princípios da inteligência e contrainteligência, especialmente no que tange à compartimentação de informações, à segurança na transmissão e ao controle do sigilo, torna-se oportuno o desenvolvimento de um sistema informatizado que possibilite a tramitação de documentos de maneira que atenda a esses requisitos.

Este estudo adota uma abordagem quantitativo-qualitativa e aplicada, utilizando o método hipotético-dedutivo e estudo de caso, com coleta de dados por questionários. A pesquisa visa compreender os desafios operacionais da Agência de Inteligência da Polícia Civil do Estado de Goiás, propondo soluções para a implementação de um sistema eficiente de gestão de demandas.

1.1 Problema de Pesquisa

As Agências de Inteligência (AI) operam em um ambiente dinâmico e desafiador. O grande volume de informações sensíveis e sigilosas em conjunto com a necessidade de respostas rápidas e precisas exige uma gestão eficiente de demandas. No cenário atual, o modelo de gestão precisa ser aperfeiçoado, especialmente quanto à rastreabilidade dessas demandas e à segurança dos dados, em consonância com os princípios da Doutrina Nacional de Inteligência de Segurança Pública (DNISP).

No caso da Agência de Inteligência da Polícia Civil do Estado de Goiás (AI da PCGO), atualmente não há um sistema específico para a tramitação e disseminação do conhecimento produzido. Além disso, os canais de comunicação utilizados apresentam fragilidades significativas. As demandas chegam até a AI da PCGO das mais variadas formas, como e-mail, WhatsApp e o sistema SEI, o que compromete a organização e o controle dessas demandas. A ausência de uma ferramenta dedicada para gerenciar as demandas dificulta o acompanhamento atualizado das atividades pela gestão da unidade, tornando impossível apurar com precisão as estatísticas de produção da agência.

Neste contexto, convém investigar como um sistema específico desenvolvido para gestão de demandas de Agências de Inteligência pode contribuir para otimizar o fluxo de trabalho. Tanto a rastreabilidade dos processos utilizados na produção do conhecimento, que garante a possibilidade de auditorias e verificações, quanto a segurança da informação, que protege todo o conhecimento produzido pelas equipes de análise e operações, são áreas críticas que exigem maior atenção.

Assim, o problema que se coloca, portanto, é: Como desenvolver um sistema de gestão de demandas para Agências de Inteligência que atenda às necessidades e peculiaridades operacionais, e que, ao mesmo tempo, melhore a eficiência na gestão do conhecimento?

A resposta a esta pergunta possibilita apresentar uma solução tecnológica pensada para as Agências de Inteligência, respeitando as diretrizes de segurança pública e melhorando a gestão do conhecimento.

1.2 Hipóteses

A implementação de um sistema específico para a gestão de demandas na AI da PCGO, que permita a tramitação eficiente de documentos e ofereça ao gestor uma visão abrangente das atividades realizadas e em andamento, aumentará a rastreabilidade dos processos, reduzirá as fragilidades nos canais de comunicação e aumentará a segurança das informações sigilosas, otimizando o fluxo de trabalho e fortalecendo o controle e supervisão da produção da agência.

1.3 Objetivos

1.3.1 Objetivo Geral

Este estudo tem como objetivo geral propor um modelo de sistema de gestão de demandas para a Agência de Inteligência da Polícia Civil do Estado de Goiás, visando otimizar o fluxo de trabalho, melhorar a eficiência operacional e garantir uma gestão segura e eficaz das informações sensíveis.

1.3.2 Objetivos Específicos

Para que o objetivo geral seja atingido foram definidos os seguintes objetivos específicos:

- Realizar um levantamento das principais demandas operacionais da Agência de Inteligência da Polícia Civil do Estado de Goiás, com foco em áreas críticas como gestão de informações sensíveis, priorização de demandas e comunicação interdepartamental.
- Analisar os resultados do questionário aplicado junto aos profissionais da agência, a fim de identificar padrões de necessidades e desafios operacionais nas áreas críticas previamente levantadas.
- Propor um modelo de sistema que atenda às necessidades identificadas, com funcionalidades que suportem o controle, monitoramento e priorização das demandas.

1.4 Justificativa

A segurança pública, fundamentada na Constituição Federal de 1988, tem utilizado a atividade de inteligência, que se tornou, especialmente nas últimas décadas, uma ferramenta essencial e indispensável no enfrentamento e desarticulação de organizações criminosas e na identificação do modus operandi de autores de diferentes ilícitos penais (Bueno, 2022). Nesse diapasão, a Inteligência de Segurança Pública (ISP) é essencial para o bom desempenho das instituições policiais, uma vez que o conhecimento gerado por suas agências impacta diretamente a tomada de decisões, a otimização dos serviços e a eficiência das operações de policiamento (Santos; Mendonça, 2022).

Melo, Urpia e Sartori (2021) asseveram que a Gestão do Conhecimento (GC) e a ISP lidam com dados, informações e conhecimentos, que têm características distintas. De acordo com os autores, a GC pode contribuir para o aprimoramento das instituições de Inteligência, e destacam que uma das principais dificuldades refere-se a delimitar o acesso, sigilo e a compartimentação de dados, informações e conhecimentos produzidos. Ademais, os autores, ao final do estudo realizado, sugerem a necessidade de futuras pesquisas sobre a proteção do conhecimento sensível e as possibilidades de inovação científica e tecnológica no campo da GC (Melo; Urpia; Sartori, 2021).

Uma vez produzido, o conhecimento deve ser classificado e armazenado adequadamente para que possa ser resgatado de forma eficiente quando necessário. Além disso, é crucial que o conhecimento esteja disponível dentro do prazo necessário para a tomada de decisões pelos usuários. Em uma era em que conhecimento e informação são cruciais, a segurança da informação torna-se um pré-requisito essencial para qualquer sistema de informações. Portanto, a implementação de regras rigorosas para a obtenção, processamento, disponibilização e uso da informação é fundamental e inquestionável (Souza; Trevisan; Siqueira, 2019).

Ainda é importante destacar que o tema abordado neste trabalho possui significativa relevância tanto no âmbito institucional quanto social. No contexto institucional, a criação de um sistema de gestão de demandas para agências de inteligência otimiza o fluxo de trabalho, permitindo uma atuação mais eficaz e organizada, alinhada às diretrizes de segurança pública. Já no contexto social, a implementação de tal sistema beneficiará a sociedade ao garantir que as ações das agências de inteligência sejam mais coordenadas e eficientes, contribuindo para a elucidação e prevenção de crimes.

1.5 Estrutura da Pesquisa

Este estudo está organizado em cinco seções. Na primeira seção temos a introdução ao tema da pesquisa, a identificação do problema a ser solucionado, bem como os objetivos (geral e específico), a justificativa e a estrutura do trabalho. A segunda seção abrange a revisão da literatura, que está subdividida em subseções que discutem a atividade de inteligência e os desafios operacionais e tecnológicos enfrentados na gestão de informações em Agências de Inteligência.

A terceira seção detalha a metodologia utilizada. Na quarta seção, são apresentados e discutidos os resultados obtidos com a metodologia adotada. Posteriormente temos a proposta de desenvolvimento de um sistema de gestão de demandas, visando à padronização e eficiência dos processos da SIPC. Por fim, a quinta seção traz a conclusão do estudo, ressaltando os potenciais benefícios do sistema proposto para o fluxo de comunicação e produção de conhecimento na Agência de Inteligência.

2 REVISÃO DA LITERATURA

2.1 ATIVIDADE DE INTELIGÊNCIA

A atividade de inteligência sempre desempenhou um papel de destaque na compreensão das intenções e ações de grupos e indivíduos, sendo determinante para a sobrevivência ou queda de reinos e organizações (Silva; Lima, 2021). Historicamente, a busca por informações sensíveis é uma prática destinada a auxiliar os governantes na tomada de decisões, tanto ofensivas quanto defensivas, relacionadas a interesses econômicos, políticos e, principalmente, à segurança de seus territórios (Gomes; Miranda; Chagas, 2021). Tradicionalmente, a função da atividade de inteligência era restrita ao apoio estratégico militar, todavia, com o crescimento e aprimoramento das atividades criminosas, tornou-se necessário institucionalizar os serviços de inteligência para assegurar a proteção da sociedade e do Estado (Silva; Lima, 2021).

De acordo com a Doutrina da Atividade de Inteligência (DAI), a Inteligência é uma atividade voltada para a produção e difusão de conhecimento, com o objetivo de subsidiar os tomadores de decisão com informações úteis, relevantes e oportunas (Brasil, 2023). Lavareda

(2024) assevera que, em linhas gerais, a inteligência consiste em obter dados, muitas vezes indisponíveis por consultas convencionais ou ainda de acesso negado, e processá-los a fim de gerar conhecimento inédito sobre algo, que será utilizado para orientar um usuário final sobre a melhor ação em um processo decisório.

Em outras palavras, o objetivo da atividade de inteligência é antecipar movimentos, em especial de atores-chave, para que os decisores possam atuar com previsibilidade, reduzindo surpresas e aumentando a eficiência em suas ações (Ribeiro; Oliveira Júnior; Silva, 2023). Essa atividade foca em fatos importantes para a tomada de decisões e utiliza métodos, com diferentes níveis de invasividade, para obter informações (sejam públicas ou restritas), de acordo com o impacto e interesse público envolvido (Reis Netto *et al*., 2021). Dessa maneira, a inteligência se dedica à geração de informações seguras, precisas e oportunas sobre um alvo específico, capacitando destinatário da informação a formular estratégias e garantir vantagens sobre ações externas, seja para se antecipar ou evitar desvantagens, sempre com foco na preservação da ordem interna e na proteção do sigilo das informações (Gomes; Miranda; Chagas, 2021).

Para atingir seu propósito, a atividade de inteligência é dividida em dois ramos principais: inteligência e contrainteligência. A inteligência se dedica à produção e disseminação de conhecimento sobre fatos, eventos, situações ou fenômenos relevantes, que possam representar tanto oportunidades quanto ameaças para os tomadores de decisão em um determinado contexto (Brasil, 2023).

Segundo a DAI, “a contrainteligência é o ramo da atividade que produz conhecimentos e desenvolve ações especializadas destinadas a prevenir, detectar, identificar, avaliar, obstruir e neutralizar atividades de inteligência adversa[...]” (Brasil, 2023, p. 16). Gomes, Miranda e Chagas (2021) explicam que a contrainteligência atua como protetora de informações sensíveis, sigilosas e frequentemente estratégicas. Além disso, destacam que a contrainteligência também realiza ações especializadas na obtenção de dados negados, assim como a inteligência, tendo como diferença crucial que seu foco está na proteção do conhecimento.

Ademais, a atividade de inteligência se divide em dois grupos principais: análise e operações. O elemento de análise é focado na produção de conhecimento de inteligência, com a função central de informar. Os profissionais envolvidos nesse processo coletam, processam e analisam dados, transformando-os em relatórios e outros produtos que são posteriormente disseminados para as autoridades responsáveis. Por sua vez, o grupo de operações é responsável por executar ações especializadas e sigilosas com o objetivo de cumprir metas previamente estabelecidas, tendo como missão desempenhar atividades voltadas à obtenção de informações

inacessíveis, à neutralização de ameaças adversas e à criação de cenários favoráveis aos interessados. As operações são utilizadas para superar obstáculos para alcançar os objetivos definidos em contextos de conflito e adversidade (Brasil, 2023).

Em suma, o trabalho de inteligência é materializado através de Relatórios de Inteligência (RELINT) ou Relatórios Técnicos (RT), que precisam tramitar dentro das unidades de inteligência, até o momento da difusão.

O RELINT é um documento administrativo que resulta da análise de dados e informações para apoiar o processo decisório, tendo como objetivo exclusivo informar e orientar a autoridade a que se destina (Gonçalves, 2016, p. 16 apud Bueno, 2022, p. 96). Além disso, sua disseminação é restrita às Agências de Inteligência (AIs) e não pode ser utilizado em processos administrativos ou judiciais. O RELINT é classificado como sigiloso, conforme a Lei de Acesso à Informação (Brasil, 2012), medida necessária para evitar comprometer atividades de prevenção e repressão ao crime (Zanchi, 2021).

O RT, por sua vez, é outro instrumento de grande relevância. Tradicionalmente, o conhecimento produzido pela Inteligência de Segurança Pública (ISP) era restrito ao Sistema de ISP (SISP) e às chefias dos órgãos assessorados. No entanto, o RT permitiu uma interação mais ampla entre as Agências de ISP (AISPs) e outros atores da segurança pública, inclusive aqueles fora do SISP. Além disso, possibilitou a disseminação de informações não sigilosas para fins probatórios (Lavareda, 2024).

2.2 DESAFIOS OPERACIONAIS E TECNOLÓGICOS NA GESTÃO DE INFORMAÇÕES EM AGÊNCIAS DE INTELIGÊNCIA

Silva e Lima (2021) defendem que além de converter informações brutas em conhecimento útil, é importante que a produção de inteligência seja gerada de forma integrada pelos órgãos de repressão e Segurança Pública. A troca de conhecimentos entre estruturas de Inteligência com objetivos semelhantes é amplamente reconhecida como essencial por profissionais da área de inteligência (Ribeiro; Nunes; Albuquerque, 2022).

No Brasil, esse tema é abordado pela Política Nacional de Inteligência de Segurança Pública (PNI) (Brasil, 2016; Brasil 2021), assim como pela criação do Sistema Brasileiro de Inteligência (Sisbin) e da Agência Brasileira de Inteligência (Abin), conforme previsto nos artigos 1º, 2º e 3º da legislação de 1999 (Brasil, 1999). As diretrizes expressas no anexo do Decreto Nº 10.777/2021 (Brasil, 2021), a PNI, apontam que a integração entre os órgãos de

inteligência é uma prioridade, salientando que a atividade de inteligência deve ser completa e precisa, abrangendo dados de todas as fontes possíveis e analisando o maior número de variáveis relevantes. Para isso, os órgãos do SISP devem operar de forma colaborativa, mantendo constante interação e estabelecendo conexões que otimizem seus esforços conjuntos.

Além disso, é essencial fomentar o acesso sistêmico e compartilhado de informações entre os órgãos do SISP, bem como promover cooperação em áreas como capacitação, treinamento e integração operacional (Brasil, 2021). De acordo com Ribeiro, Nunes e Albuquerque (2022), o Sisbin foi criado para integrar as atividades de planejamento e execução da inteligência no Brasil, facilitando a troca de informações relevantes e a tomada de decisões. Os autores explicam que quando foi implementado em 2002, o Sisbin era composto por 22 órgãos e expandiu gradativamente, atingindo 48 órgãos em 2021. Essa integração foi reforçada pela PNI (Brasil, 2016) e pela Estratégia Nacional de Inteligência (ENIT) (Brasil, 2017), que promovem a cooperação, atuação em rede e o compartilhamento de informações entre os órgãos.

Entretanto, Silva e Lima (2021) salientam que quase todos os órgãos de Segurança Pública possuem divisões próprias de inteligência, o que resulta em fragmentação do conhecimento e pouca cooperação efetiva. Segundo os autores, essa a falta de interação leva à dispersão de dados, muitos dos quais poderiam ser melhor trabalhados.

Nessa perspectiva, o estudo realizado por Ribeiro, Nunes e Albuquerque (2022), revelou que é preciso modernizar as ferramentas de troca de informações no Sisbin. Com base na análise de 137 participantes de 13 órgãos do Sisbin, os autores concluíram que apesar da existência de canais de comunicação, a integração entre os órgãos é limitada, prejudicando a agilidade e a segurança no processo. Outro ponto relevante ressalta a importância de melhorar a segurança da informação, implementando criptografia e controle de acesso para proteger dados sensíveis.

Um entendimento mais aprofundado sobre a necessidade de ferramentas informatizadas no controle das AIs foi apresentado por Carvalho (2015). Em seu estudo, o autor relata que, a estrutura organizacional das AISPs frequentemente apresenta subdivisão em Agências Regionais de Inteligência (ARIs) e Agências Locais de Inteligência (ALIs), formadas por equipes distintas. Essa estrutura, não raro, cria um cenário em que uma AI desconhece o trabalho que está sendo realizado por outra, ainda que pertençam à mesma instituição. Em muitos casos, diferentes equipes da AI podem monitorar o mesmo alvo, mas não compartilham informações, o que prejudica a eficiência nas investigações, dificultando uma ação coordenada (Carvalho, 2015).

Carvalho (2015) ainda argumenta que após a confecção do RELINT, cada AI adota seu próprio método de armazenar dados sobre alvos, o que gera inconsistências na organização das informações e dificulta a integração entre as agências. Esse problema de falta de padronização e comunicação resulta em relatórios dispersos e pouco eficientes, pois muitas vezes as informações ficam restritas a um agente ou arquivo local. Assim, o autor evidencia a necessidade de mecanismos para gestão dos documentos produzidos pelos órgãos de inteligência:

> Neste sentido, existe uma lacuna nos órgãos de inteligência, ou seja, a inexistência de um banco de dados sobre informações adquiridas pelos agentes. Um banco de dados com tais características poderia armazenar esses dados e informações, compartilhando com as demais agências, que teriam acesso ao conhecimento já produzido por um conjunto de agentes de inteligência. Isso resultaria, claramente, em uma redução de trabalho e em uma maior qualidade nos relatórios produzidos, auxiliando para tomada de decisões com maior precisão. (Carvalho, 2015, p. 31).

A partir dessa análise, Carvalho (2015) elaborou um modelo de banco de dados para ser aplicado na gestão da informação, que servisse como suporte às ações de inteligência policial, realizando a integração e consolidação de informações de investigações. O objetivo era facilitar a análise e a tomada de decisões pelos agentes de segurança, por meio de uma organização eficiente dos dados.

A importância desse tipo de repositório, segundo o autor, está na sua capacidade de organizar informações de maneira a otimizar a atividade de inteligência, permitindo consultas a relatórios que podem revelar conexões entre casos distintos, como redes de relacionamentos. Isso ajuda a aprimorar a compreensão do contexto criminal, fornecendo suporte a decisões estratégicas e aumentando a eficácia dos profissionais de segurança, o que contribui diretamente para o sucesso das investigações e a melhoria da segurança pública.

Todavia, é imperativo considerar que a Doutrina de Inteligência Policial do Ministério da Justiça e Segurança Pública estabelece a compartimentação como um subprincípio do sigilo, com o objetivo de restringir o acesso às atividades de inteligência apenas aos profissionais que realmente necessitam desse conhecimento. Esse conceito se baseia no princípio do "*need to know*" (necessidade de saber), que determina que o acesso a informações sensíveis ou classificadas deve ser limitado àqueles cuja função ou contribuição específica justifique tal conhecimento. Assim, a compartimentação refere-se ao fracionamento das informações e à definição criteriosa de quem terá autorização para acessá-las (Ruprecht, 2021).

Ainda de acordo com Ruprecht (2021), muitos autores apontam disfunções relacionadas à prática de compartimentação de informações sensíveis. Podemos citar, por exemplo, que em alguns casos se torna um obstáculo que impede que a informação chegue a quem realmente precisa, comprometimento da precisão e completude das análises. Nesse sentido, Ruprecht (2021) investigou os impactos da compartimentação da informação nas investigações da Polícia Federal (PF) do Brasil, dividindo as respostas dos policiais em três grupos: "a favor", "depende", e "contra" a prática. Enquanto alguns veem a compartimentação como necessária para evitar vazamentos, outros apontam que ela pode prejudicar as investigações ao limitar o compartilhamento de informações e gerar retrabalho.

Além disso, o estudo trouxe como principal sugestão de solução a criação de sistemas de informação seguros, que permitam o compartilhamento seletivo de dados entre investigações, mantendo o sigilo sem comprometer a eficiência e minimizando as disfunções da compartimentação (Ruprecht, 2021).

Desta maneira, respeitando as particularidades da atividade de inteligência policial, a implementação de sistemas informatizados para gestão do conhecimento e controle do fluxo de informações nas agências de inteligência apresenta benefícios e desafios. Esse tipo de sistema não apenas aprimora a organização e armazenamento do conhecimento produzido nas AISPs, facilitando o acesso e consulta de informações críticas, como também aprimora o acompanhamento e rastreamento das atividades em andamento em cada unidade. Ao integrar essas funcionalidades, o sistema contribui para uma gestão mais eficiente e segura, permitindo que os agentes de inteligência tomem decisões informadas e ágeis, melhorando assim a eficácia operacional.

Contudo, ao elaborar uma solução que visa informatizar o registro do conhecimento produzido pelas agências de inteligência, é essencial garantir a segurança da informação em todas as etapas do processo. Assim, tal solução deve se basear em três pilares fundamentais: confidencialidade, disponibilidade e integridade. A confidencialidade impede o acesso de usuários não autorizados às informações, a disponibilidade indica a capacidade do sistema atender às solicitações sem falhas internas, enquanto a integridade garante que as informações sejam alteradas apenas de forma autorizada, mantendo sua precisão (Barreto *et al*., 2018).

Tais requisitos estão alinhados com o que foi levantado por Ribeiro, Nunes e Albuquerque (2022), que ressaltam que é indispensável garantir a segurança da informação para proteger dados sensíveis, garantindo o acesso somente a usuários autorizados. Os autores

destacam a necessidade de implementar medidas de proteção alinhadas às diretrizes da PNI, reforçando a urgência de ações que garantam a integridade e a confidencialidade dos dados.

3 METODOLOGIA

Uma pesquisa envolve a criação de uma abordagem metodológica voltada para a resolução de um problema específico. Esses processos são adaptáveis e devem ser ajustados às necessidades do pesquisador, que precisa avaliar qual metodologia melhor se adequa às exigências da investigação (Lozada; Nunes, 2019).

Desta maneira, o presente estudo foi realizado aplicando o método hipotético-dedutivo como abordagem principal. De acordo com Lozada e Nunes (2019), o método hipotético-dedutivo combina aspectos dos métodos indutivo e dedutivo. Seus principais pontos são: inicia com a observação de fenômenos específicos para generalizar sobre toda a classe, e depois aplica leis gerais a casos concretos dentro dessa classe.

Quanto a abordagem, segundo Gil (2022), as pesquisas podem ser classificadas de maneira simplificada em quantitativas, que apresentam resultados em dados numéricos, e qualitativas, que utilizam descrições verbais. A partir do final da década de 1990, passou-se a discutir a viabilidade e a importância das pesquisas de métodos mistos, que combinam elementos de ambas as abordagens para ampliar e aprofundar o entendimento dos fenômenos, além de reforçar os resultados obtidos. Com base nisso, esta pesquisa adotou uma abordagem quantitativo-qualitativa, permitindo uma análise mais completa e detalhada do fenômeno investigado.

Ademais, o estudo é de natureza aplicada, conforme definido por Gil (2022), pois tem como finalidade resolver problemas específicos do âmbito prático, oferecendo contribuições diretas para a Atividade de Inteligência na Segurança Pública. Dessa forma, a pesquisa visa não apenas preencher lacunas teóricas, mas também proporcionar soluções práticas para os desafios concretos identificados, tornando-se relevante tanto no campo acadêmico quanto no operacional.

Quanto ao objetivo, trata-se de estudo exploratório, visto que busca proporcionar maior familiaridade com o problema investigado. Essa abordagem permite clarificar o fenômeno e construir hipóteses para futuras pesquisas e desenvolvimentos teóricos (Gil, 2022).

A metodologia central adotada foi o estudo de caso, amplamente utilizado nas ciências sociais, permitindo um conhecimento profundo e detalhado de um caso específico. Essa

abordagem facilita a análise de fenômenos complexos em seu contexto real, proporcionando uma compreensão das suas particularidades e inter-relações (Gil, 2022).

Para a realização do estudo de caso, foi aplicado um questionário contendo 10 questões objetivas aos coordenadores das divisões da Superintendência de Inteligência Policial Civil (SIPC), com o objetivo de compreender melhor a gestão de demandas e a comunicação entre as diferentes unidades da SIPC. Além disso, procedeu-se à revisão bibliográfica abrangente para fundamentar teoricamente a pesquisa, analisando livros, artigos científicos, teses e dissertações publicados nos últimos dez anos sobre o tema. Essa revisão permitiu identificar as principais contribuições teóricas e práticas recentes e a situar o estudo no contexto das pesquisas existentes.

Em síntese, a pesquisa adotou o método hipotético-dedutivo, com uma abordagem quantitativo-qualitativa, de natureza aplicada e objetivo exploratório, utilizando o estudo de caso e a revisão bibliográfica como principais metodologias. A combinação dessas abordagens permitiu identificar os principais desafios na gestão de informações em inteligência policial, orientando o desenvolvimento de um sistema de gestão eficiente e adequado às demandas do setor.

4 RESULTADOS E DISCUSSÕES

4.1 ESTUDO DE CASO: CENÁRIO ATUAL NA AGÊNCIA DE INTELIGÊNCIA DA POLÍCIA CIVIL DO ESTADO DE GOIÁS

A seguir, será apresentado o estudo de caso sobre o cenário atual da Agência de Inteligência da Polícia Civil do Estado de Goiás, focando em sua organização, nos canais de comunicação utilizados e na gestão de demandas. Essa análise visa oferecer uma compreensão da estrutura e das práticas adotadas, evidenciando os obstáculos que podem afetar a eficiência na gestão de demandas e na comunicação interna.

4.1.1 Agência de Inteligência da Polícia Civil do Estado de Goiás

A Lei Ordinária nº 16.272, de 30 de maio de 2008, foi um dos primeiros passos para consolidar uma unidade de inteligência no Estado de Goiás, ao estabelecer uma estrutura organizacional básica para a administração direta, autárquica e fundacional do Poder Executivo.

Essa lei incluiu a criação de órgãos específicos de segurança pública, como a Superintendência de Inteligência vinculada à Secretaria de Segurança Pública. Desta maneira, a Superintendência de Inteligência foi inicialmente formada por cinco gerências, dentre elas a Gerência de Operações de Inteligência da Polícia Civil (Goiás, 2008). Essa primeira formalização forneceu uma estrutura inicial para as atividades de inteligência no estado, servindo como base para as regulamentações mais robustas.

Com o tempo, essa estrutura foi expandida e integrada por meio de novas regulamentações, como a Lei Ordinária nº 17.257, de 25 de janeiro de 2011, que definiu uma reorganização administrativa, criando a Superintendência de Inteligência Integrada (Goiás, 2011). Posteriormente, a Lei nº 19.390, de 07 de julho de 2016 consolidou a coordenação das atividades de inteligência, reforçando o caráter estratégico e abrangente da inteligência na segurança pública goiana (Goiás, 2016).

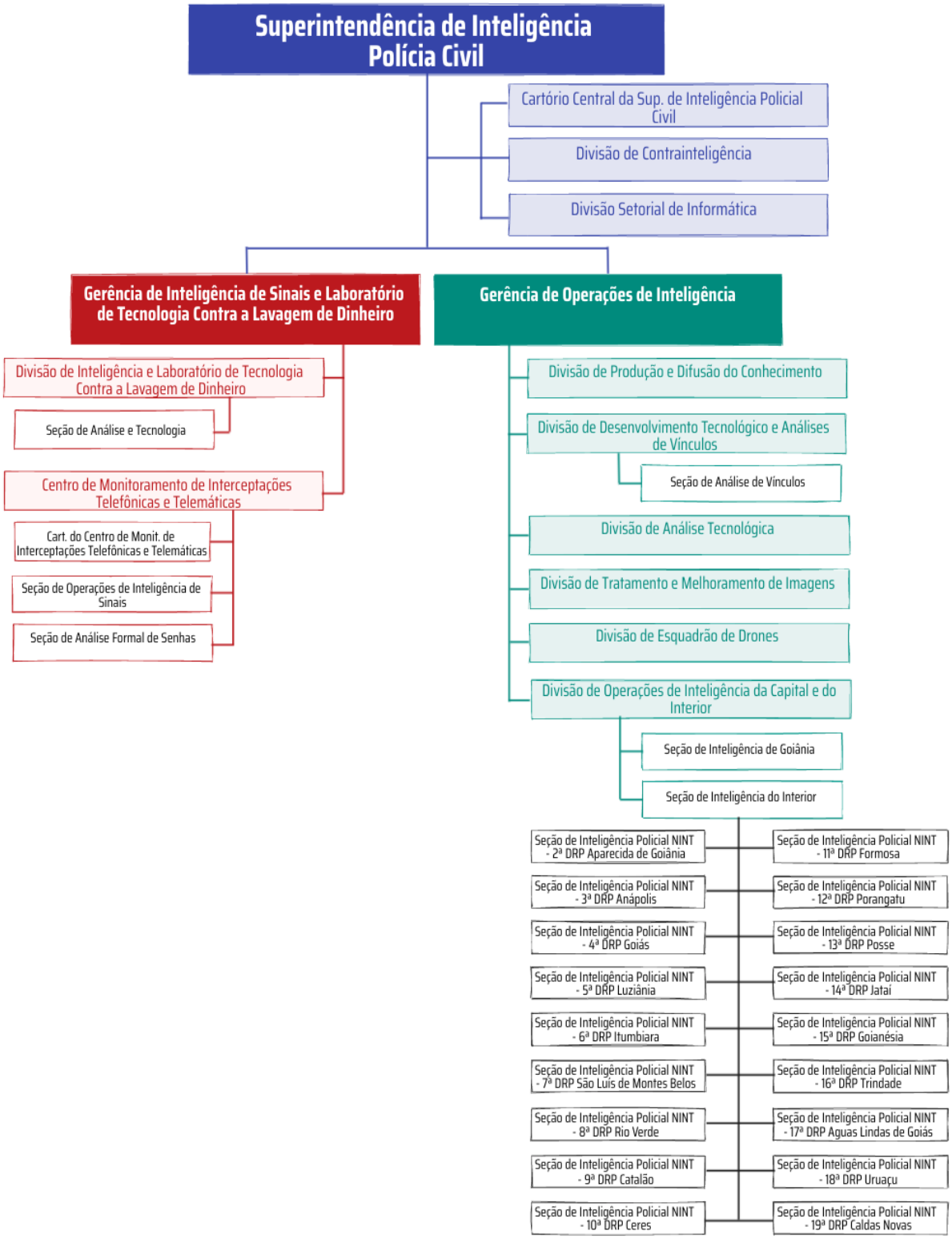
O Decreto nº 8.869, de 12 de janeiro de 2017, representou outro avanço significativo ao instituir o Sistema de Inteligência de Segurança Pública do Estado de Goiás (SISP/GO), sob a Secretaria de Estado de Segurança Pública e Administração Penitenciária. Esse sistema formalizou a integração das atividades de inteligência de segurança pública, buscando maior coordenação entre os órgãos envolvidos no combate ao crime e na promoção da ordem pública (Goiás, 2017).

Mais recentemente, a Lei nº 21.792, de 16 de fevereiro de 2023, junto ao Decreto nº 10.218, de 16 de fevereiro de 2023, atualizou a estrutura administrativa da Delegacia-Geral da Polícia Civil, estabelecendo uma organização que reflete os avanços na integração das atividades de inteligência no estado (Goiás, 2022; Goiás, 2023a). Com a Portaria nº 195/2023, houve um reforço significativo nessa estrutura: foi criada a Superintendência de Inteligência Policial Civil (SIPC), substituindo a organização anterior que contava apenas com a Gerência de Operações de Inteligência da Polícia Civil. Esta nova Superintendência detalha a organização básica e complementar da Delegacia-Geral, alinhando-se aos objetivos das legislações anteriores e fortalecendo a coordenação das atividades de inteligência (Goiás, 2023b).

A Figura 1 apresenta a estrutura atual da SIPC, conforme estabelecido pela Portaria nº 195/2023 – DGPC, a qual é composta por duas principais gerências: a Gerência de Inteligência de Sinais e Laboratório de Tecnologia contra a Lavagem de Dinheiro e a Gerência de Operações de Inteligência. No total, essa configuração abrange 11 divisões e sete seções integradas, que desempenham funções específicas e complementares dentro do sistema de inteligência estadual.

Destaca-se, ainda, a Seção de Inteligência do Interior, formada por 18 núcleos estrategicamente distribuídos para atender de forma abrangente às demandas regionais (Goiás, 2023b).

Figura 1 – Organograma da Superintendência de Inteligência Policial Civil do Estado de Goiás



Fonte: Elaborado pela autora a partir de Goiás (2024).

Conhecer a estrutura da SIPC é essencial para compreender o desafio de manter uma comunicação eficiente entre suas divisões e seções, assegurando ao mesmo tempo a compartimentação necessária das informações. Cada unidade possui funções específicas e atuações distintas, o que torna a integração e o fluxo de informações processos críticos para a eficácia das operações.

Sob essa perspectiva, o estudo realizado por Carvalho (2015), destaca a problemática da fragmentação de informações em agências de inteligência. Em muitos casos, as subdivisões internas enfrentam dificuldades para compartilhar dados relevantes entre equipes que, muitas vezes, estão investigando os mesmos alvos. O autor ressalta que essa falha de integração pode levar à duplicação de esforços e à ausência de uma visão completa sobre o alvo monitorado, prejudicando a coordenação das investigações.

A evolução da estrutura organizacional ao longo dos anos reflete o esforço contínuo em fortalecer a integração entre os diversos setores e otimizar a coordenação das atividades de inteligência. As sucessivas regulamentações e reestruturações visaram não apenas consolidar as funções de inteligência no estado, mas também adaptar as operações às crescentes demandas por segurança pública e combate ao crime organizado. A estrutura organizacional da SIPC, apresentada na Figura 1, revela um sistema complexo e interconectado, no qual a comunicação e a gestão de informações são fundamentais para a eficácia das operações e a obtenção de resultados consistentes.

Com o intuito de explorar melhor os desafios de comunicação e gestão de demandas enfrentados pela SIPC, foi aplicado um questionário aos coordenadores das divisões. O objetivo do formulário era identificar como cada divisão gerencia suas demandas e avalia a comunicação entre as diferentes unidades. Esse levantamento permitiu mapear as necessidades e dificuldades relatadas, servindo como base para propor um sistema informatizado que aumente a eficiência operacional e facilite a gestão de demandas na agência de inteligência.

4.1.2 Análise dos Resultados do Questionário sobre Gestão de Demandas e Comunicação Interna da Agência de Inteligência da Polícia Civil do Estado de Goiás

Uma das etapas iniciais no ciclo de desenvolvimento de *software* é a descoberta das funcionalidades que o *software* precisa ter para agregar valor ao usuário. Para isso, utiliza-se a elicitação de requisitos, que auxilia o analista a entender e definir o que deve ser construído. Há

várias técnicas de elicitação que envolvem interação com fontes humanas, como entrevistas, reuniões, *brainstorming*, observação e questionários (Reinehr, 2020).

Ainda segundo a autora, a técnica de questionário, também chamada de *survey* ou pesquisa de opinião, consiste em perguntas organizadas de forma lógica, podendo ser objetivas ou abertas. Embora pareça simples, a criação de um questionário eficaz exige cuidado: ele deve ser breve e fácil de responder para engajar os participantes, evitando vieses e direcionamentos nas respostas (Reinehr, 2020).

O questionário elaborado para este trabalho, composto por 10 questões objetivas, foi formulado considerando os aspectos essenciais para a pesquisa, com o objetivo de identificar os desafios e práticas na gestão de demandas e comunicação interna da SIPC. Ele foi enviado diretamente a seis coordenadores e chefes de divisão, sendo respondido por todos os destinatários, o que demonstra um elevado engajamento com a temática abordada.

A primeira pergunta do questionário, que permitia múltiplas respostas, investigou os meios pelos quais as demandas operacionais são recebidas e distribuídas na SIPC. Nenhum dos respondentes informou o uso de documentos físicos para este propósito. As respostas indicaram que as demandas são recebidas predominantemente através do SEI (Sistema Eletrônico de Informações), *e-mail*, cada um mencionado por 83,3% dos participantes. Além disso, 16,67% responderam que recebem solicitações de demandas por *WhatsApp*. Esse resultado sugere uma forte preferência por meios digitais, refletindo a modernização dos processos de comunicação na instituição.

A segunda questão destacou a variação na média mensal de demandas entre as seções, indicando que o volume de demandas pode variar consideravelmente conforme a área de atuação. Entre os respondentes, 16,7% relataram receber de 10 a 30 demandas mensais, enquanto 33,3% indicaram uma média entre 30 e 50 demandas. Outros 16,7% informaram que a média mensal varia entre 50 e 100 demandas, e 33,3% afirmaram receber mais de 100 demandas por mês. Essas diferenças evidenciam que algumas seções enfrentam cargas de trabalho significativamente maiores, o que pode impactar a alocação de recursos e influenciar as estratégias de gestão adotadas.

Na terceira pergunta foi verificado como é realizado o controle de gestão de demandas da seção atualmente. Nessa pergunta, que também permitia a seleção de múltiplas opções, todos os respondentes mencionaram o uso de planilhas eletrônicas para o controle de demandas em suas seções. Apenas dois afirmaram ter acesso a um sistema informatizado específico para essa gestão. Outras ferramentas, como controles físicos e ferramentas online de comunicação (*e-*

mail e aplicativos), foram mencionadas por 50% e 66,7% dos participantes, respectivamente. Esses dados indicam que, embora as planilhas eletrônicas sejam amplamente utilizadas, ainda há uma diversidade de métodos de controle, apontando para a necessidade de uma padronização.

A quarta questão abordou a possibilidade do sistema de gestão atual controlar acesso a informações sensíveis, um aspecto essencial na atividade de inteligência devido à necessidade de compartimentação. Metade dos respondentes afirmaram que o sistema atual não permite um controle adequado de acesso com base na "necessidade de conhecer", enquanto os outros 50% indicaram que possuem algum nível de controle. Esse resultado demonstra que há uma lacuna significativa na capacidade de garantir a segurança das informações sensíveis, o que é um ponto crítico para a eficácia da atividade de inteligência.

A quinta questão buscou identificar a frequência com que as informações sobre o andamento e prazos das demandas são atualizadas e compartilhadas com outros setores ou membros da equipe diretamente envolvidos com a demanda. Os resultados revelaram uma diversidade nas práticas de atualização, com 50% dos respondentes afirmando que realizam esse compartilhamento apenas quando solicitados. Outros 33,3% indicaram que fazem as atualizações de forma semanal, enquanto apenas 16,7% compartilham informações diariamente. Essa variação nas práticas de atualização pode refletir diferenças nas demandas e recursos de cada seção, mas também aponta para uma possível necessidade de padronização para melhorar a consistência e eficiência na gestão de demandas.

Nesse sentido, a sexta pergunta revelou que apenas 33,3% dos respondentes consideram a comunicação interdepartamental eficaz em relação às demandas compartilhadas entre seções. Em contraste, 66,7% classificaram essa comunicação como pouco eficiente ou ineficiente, destacando a necessidade de melhorias na integração e fluxo de informações entre as seções. Esse dado indica um obstáculo relevante para a gestão colaborativa de demandas.

Essa dificuldade fica evidente quando analisamos o resultado da pergunta seguinte. Os respondentes foram perguntados se consideram que o compartilhamento de informações entre seções deve ser melhorado. Para 83,3% dos respondentes, a implementação de um sistema unificado melhoraria o compartilhamento de informações entre as seções. Nenhum participante sugeriu que mais reuniões seriam uma solução eficaz, enquanto 16,7% afirmaram estar satisfeitos com o compartilhamento atual. Esses resultados reforçam a preferência por soluções tecnológicas, evidenciando uma demanda por ferramentas que facilitem a integração e a troca de informações.

Na oitava pergunta, que também permitia múltiplas respostas, 66,7% dos respondentes indicaram que a principal dificuldade enfrentada atualmente está relacionada ao acompanhamento de prazos. Outras dificuldades mencionadas incluíram a falta de integração entre os departamentos e a falta de padronização nos canais utilizados para recebimento e envio de demandas. Esses obstáculos sugerem áreas críticas onde intervenções poderiam melhorar a eficiência e a gestão de demandas.

A nona questão investigou a percepção dos respondentes sobre a possível melhoria na eficiência operacional com a implementação de um sistema informatizado para gestão de demandas. Os resultados indicaram que 66,7% dos participantes acreditam que a adoção de um sistema informatizado contribuiria para aprimorar a eficiência das operações. Outros 33,3% responderam “talvez”, sugerindo uma abertura à ideia, mas com possíveis dúvidas sobre a eficácia ou adequação de tal sistema para atender às necessidades específicas da instituição. Nenhum dos respondentes optou por “não”, o que indica um consenso sobre o potencial benefício de um sistema informatizado, embora com diferentes níveis de certeza.

Essa predominância de respostas favoráveis aponta para uma demanda latente por ferramentas que otimizem o gerenciamento de demandas e promovam uma maior agilidade e integração entre as divisões. A análise sugere que um sistema informatizado seria bem-vindo pela maioria e poderia representar um avanço na organização e na comunicação interna.

Nesta última questão, cada respondente poderia selecionar até cinco práticas de segurança da informação consideradas essenciais para um sistema de gestão de demandas. As práticas mais citadas incluíram a compartimentação de informações, o monitoramento de acessos e a criptografia de dados, todas mencionadas por 83,3% dos participantes. Além disso, 66,7% apontaram para a importância da auditoria de atividades. Essa preferência por controles de segurança robustos indica a preocupação dos coordenadores em proteger dados sensíveis e garantir a integridade da informação.

Os resultados do questionário reforçam a importância de implementar um sistema informatizado para gestão de demandas na SIPC, capaz de integrar as diferentes seções e melhorar a comunicação interna. A predominância de respostas favoráveis à adoção de uma solução unificada indica que um sistema moderno e seguro poderia otimizar o acompanhamento de prazos, reduzir a duplicidade de esforços e assegurar a compartimentação das informações sensíveis, atendendo de forma mais eficaz às necessidades operacionais da agência de inteligência.

4.2 PROPOSTA DE DESENVOLVIMENTO DE UM SISTEMA DE GESTÃO DE DEMANDAS PARA A AGÊNCIA DE INTELIGÊNCIA DA POLÍCIA CIVIL DO ESTADO DE GOIÁS

Diante dos desafios e das necessidades identificadas na análise do cenário atual da Superintendência de Inteligência Policial Civil (SIPC) da Polícia Civil do Estado de Goiás, este capítulo apresenta uma proposta de desenvolvimento de um sistema informatizado de gestão de demandas. A criação desse sistema visa solucionar as dificuldades operacionais e de comunicação relatadas pelos coordenadores das divisões, proporcionando um ambiente mais integrado, seguro e eficiente para a gestão das demandas da AIPCGO.

De acordo com Reinehr (2020), os requisitos representam a especificação do que precisa ser implementado no sistema, descrevendo como ele deve se comportar ou definindo uma propriedade ou atributo necessário para seu funcionamento. Um requisito funcional (RF) é uma funcionalidade específica exigida pelos *stakeholders* para alcançar um objetivo de negócio, indicando o que os desenvolvedores precisam implementar para que os usuários realizem suas atividades. Já os requisitos de qualidade, também conhecidos como requisitos não funcionais (RNF), dizem respeito a como o *software* deve operar em determinadas condições. Eles abrangem aspectos como desempenho, disponibilidade, usabilidade, portabilidade e escalabilidade (Reinehr, 2020). Portanto, os requisitos funcionais especificam o que o sistema deve realizar, enquanto os requisitos não funcionais determinam como o sistema deve executar essas funcionalidades.

Nesse contexto, com base no cenário identificado no questionário aplicado e nas informações obtidas durante a revisão bibliográfica, foram listados inicialmente 12 requisitos funcionais para a implementação de um sistema de gestão de demandas na SIPC, conforme detalhado no Quadro 1.

Conforme podemos observar, o RF01 - Cadastro de Demandas está alinhado à primeira questão do questionário, que revelou uma preferência clara por meios digitais para o recebimento de demandas (como SEI, *e-mail* e *WhatsApp*). A inclusão de um cadastro padronizado permitirá centralizar essas informações e organizar os registros de origem, natureza e unidade demandante.

Quadro 1 – Requisitos Funcionais

CÓDIGO	REQUISITO FUNCIONAL	DESCRIÇÃO
RF01	Cadastro de Demandas	Permitir registro de novas demandas com informações como origem, natureza, unidade, demandante, observações, anexos, data de cadastro e criador.
RF02	Atribuição de Responsáveis	Permitir designação e alteração de responsáveis (pessoa ou equipe) com preenchimento obrigatório do prazo de conclusão.
RF03	Acompanhamento de Status	Acompanhar status das demandas (pendente, em andamento, em atraso, concluída) e registrar histórico de mudanças.
RF04	Controle de Prazos	Monitorar prazos e gerar alertas automáticos para responsáveis próximos ao vencimento.
RF05	Compartimentação	Implementar níveis de acesso com restrição de visualização conforme o princípio da "necessidade de conhecer".
RF06	Registro de Interações	Permitir registro de comentários e atualizações no histórico da demanda com data e hora.
RF07	Relatórios e Estatísticas	Gerar relatórios sobre demandas criadas, concluídas e pendentes, incluindo tempo médio de atendimento.
RF08	Busca e Filtro de Demandas	Funcionalidades de busca avançada e filtros com identificação de termos parciais em campos relevantes. Salvar filtros frequentes.
RF09	Controle de Acesso por Perfil	Permitir criação de diferentes perfis de usuário com permissões específicas e gestão pelos administradores.
RF10	Histórico de Alterações	Registrar alterações realizadas nas demandas, incluindo usuário responsável, data e hora.
RF11	Notificações Automáticas	Enviar notificações automáticas configuráveis por e-mail ou no sistema sobre eventos importantes.
RF12	Dashboard Geral	Oferecer visão geral das demandas com status (pendente, em andamento, em atraso, concluída) e resumo por responsável.

Fonte: Elaborado pela autora (2024).

Em seguida, ao especificarmos o RF02 - Atribuição de Responsáveis responde à necessidade de distribuir as demandas de forma clara, definindo responsáveis e prazos, conforme destacado nas perguntas sobre práticas de gerenciamento. A exigência de prazos obrigatórios busca reduzir o risco de atrasos, apontado por 66,7% dos participantes na oitava pergunta como uma das principais dificuldades. Ainda nessa perspectiva, os RF03 - Acompanhamento de Status e RF04 - Controle de Prazos são essenciais para monitorar o progresso e atender às expectativas de acompanhamento de prazos.

A falta de ferramentas padronizadas de acompanhamento, com seções que ainda utilizam planilhas segundo as respostas da terceira pergunta do questionário, sugere a necessidade de um sistema que registre o progresso e gere alertas automáticos para manter a eficiência nas operações. Assim, RF11 - Notificações Automáticas responde ao desafio de acompanhamento de demandas em tempo real, apontado por 50% dos participantes que dependem de atualizações sob demanda. Esse requisito reforça a eficiência operacional, permitindo que responsáveis sejam alertados sobre prazos e mudanças de status de forma proativa.

Ademais, o RF06 - Registro de Interações reflete a necessidade de documentar atualizações e interações em cada demanda, permitindo um histórico detalhado que favoreça o acompanhamento contínuo. Esse requisito responde ao desafio da comunicação interna, pois oferece um canal formal para registrar informações relevantes sobre cada demanda, facilitando a consulta entre setores.

Com base nos 83,3% dos respondentes que citaram a compartimentação como prática essencial, o sistema deve permitir um controle granular de acesso, com base no princípio da "necessidade de conhecer." Isso inclui a implementação de perfis de usuário e níveis de acesso, limitando a visualização de informações conforme o cargo e a função de cada usuário. Desta forma, os requisitos RF05 e RF09 estão alinhados com o que foi identificado na pergunta 10 do questionário.

O RF05 - Compartimentação é fortemente fundamentado pela resposta à quarta pergunta, que evidenciou uma lacuna no controle de acesso a informações sensíveis. Metade dos respondentes indicou que o sistema atual não atende plenamente à necessidade de compartimentação, o que reforça a importância de implementar controles de acesso que garantam a segurança das informações.

Ainda nesse diapasão, os RF09 - Controle de Acesso por Perfil de Usuário e RF10 - Histórico de Alterações, foram incluídos para endereçar a necessidade de controle de segurança

e acesso, conforme as práticas de segurança apontadas na última pergunta. A compartimentação e o monitoramento de acessos são considerados essenciais para proteger dados sensíveis, garantindo que cada usuário acesse apenas o necessário para sua função.

Outra funcionalidade que deverá ser implementada para otimizar o trabalho é a Busca e Filtro de Demandas (RF08), que responde à dificuldade identificada em localizar demandas e consolidar informações sobre alvos ou pessoas relacionadas, conforme indicado pela preferência por sistema unificado na pergunta sete do questionário. Essa funcionalidade permitirá um acesso rápido e eficiente a dados específicos, incluindo a possibilidade de busca em descrições parciais, o que é essencial para investigações. No entanto, o uso desses filtros avançados será restrito a determinados perfis de usuário, assegurando que apenas aqueles com autorização tenham acesso a essa funcionalidade (RF09).

Por fim, os RF07 - Relatórios e Estatísticas de Demandas e RF12 - Dashboard com Visão Geral das Demandas foram projetados para atender a demanda por uma visão consolidada das operações. Os resultados das perguntas sobre atualização de demandas e controle de prazos apontam a necessidade de relatórios e indicadores que possibilitem análises estratégicas, ajudando os gestores a tomar decisões baseadas em dados confiáveis.

Adicionalmente, é imprescindível observar os requisitos não funcionais (RNF). Reinehr (2020), salienta a importância de identificar, por exemplo, o requisito de processo, que impõe, por exemplo, restrições sobre as tecnologias usadas, definindo como o produto deve ser desenvolvido. Esses requisitos de qualidade são mais difíceis de elicitar e especificar do que os requisitos funcionais (Reinehr, 2020).

A autora explica que para descobrir os requisitos não funcionais, é recomendável começar com uma lista abrangente de atributos de qualidade. Exemplos incluem usabilidade, escalabilidade, confiabilidade, desempenho e segurança (Reinehr, 2020). Nem todos os *softwares* precisarão de todos esses atributos, mas, para o caso em questão, os requisitos não funcionais prioritários são aqueles relacionados à segurança da informação, considerados fundamentais por 83,3% dos respondentes. Assim, conforme a pergunta 10 do questionário, o sistema proposto deverá implementar o RNF 01 – Segurança da Informação, com especial atenção quanto à criptografia de dados e monitoramento de acessos e auditoria das atividades.

Diante da necessidade de proteção de dados sensíveis, o sistema deve implementar criptografia em todos os dados armazenados e em trânsito. Basicamente, o controle de visibilidade de dados pode ser feito restringindo o acesso ao sistema operacional ou utilizando criptografia. Embora o controle de acesso seja comum, ele apresenta vulnerabilidades

exploráveis, como ataques de elevação de privilégios. A criptografia, por outro lado, oferece maior segurança, embora sua quebra seja possível, exigindo ataques mais complexos e direcionados (Rosini Filho; Rosine; Palmisano, 2020).

De acordo com Tolardo (2022), a criptografia destaca-se como um elemento essencial para a segurança de dados, permitindo a codificação de informações por meio de algoritmos que utilizam chaves específicas. Com o objetivo de proteger o conteúdo de mensagens ou arquivos, o método criptográfico “embaralha” os dados, tornando-os inacessíveis sem a chave correta. Assim, para criptografar ou descriptografar uma informação, é necessário utilizar a chave apropriada, o que assegura eficiência e segurança nos processos de transmissão e armazenamento de dados (Tolardo, 2022).

Nesse diapasão, Frasão (2020) assevera que a criptografia tem importância fundamental para a segurança da informação, garantindo integridade, autenticidade, não-repúdio e sigilo dos dados. Ela depende de fatores como geração e troca de chaves, tamanho e qualidade dos algoritmos. Um algoritmo eficaz impede que informações sejam recuperadas em ataques de força bruta, e o tamanho da chave deve ser ajustado conforme o tempo de proteção necessário (Frasão, 2020).

Em outras palavras, os algoritmos criptográficos têm como principal objetivo "ocultar" informações sigilosas de qualquer pessoa não autorizada a acessá-las. Esse requisito responde à preocupação dos respondentes em garantir que informações confidenciais estejam protegidas contra acessos não autorizados, reduzindo o risco de vazamento de dados.

Além disso, o sistema deverá manter registros das atividades dos usuários a fim de garantir transparência e rastreabilidade, devendo manter um *log* detalhado de atividades, incluindo quem acessou cada demanda e as alterações realizadas. Segundo Silva (2023), “o log é uma ferramenta que registra todas as alterações realizadas em um repositório de dados, como adições ou exclusões”. Freitas e Borges Neto (2018), explicam que os logs podem ser coletados tanto de hardwares quanto de softwares. Desta maneira, é possível capturar informações diversas, como por exemplo qual a data, horário e IP do dispositivo que acessou determinada demanda, ou qual usuário inseriu ou alterou algum registro salvo no banco de dados.

A análise e auditoria de logs desempenham um papel fundamental na identificação de ameaças, ajudando a compreender de forma mais detalhada o ambiente de TI (Freitas; Borges Neto, 2018). Como todas as interações com a aplicação ficam gravadas no arquivo de log, é possível criar um ambiente de monitoramento que poderá ser acessado por usuários com permissão de auditoria interna. Esse monitoramento atende à demanda por auditoria e segurança

mencionada pelos participantes do questionário, facilitando revisões periódicas e investigações, quando necessário.

5 CONSIDERAÇÕES FINAIS

A implementação de um sistema unificado de gestão de demandas é essencial para garantir a consistência e padronização nos processos da Agência de Inteligência da Polícia Civil do Estado de Goiás (AIPCGO). Com funcionalidades voltadas ao controle de prazos, compartimentação de informações e monitoramento de atividades, o sistema proposto visa não apenas atender às necessidades operacionais da AIPCGO, mas também elevar o nível de segurança e confidencialidade das informações sensíveis, contribuindo para uma comunicação eficaz entre as seções.

Os resultados do questionário aplicado aos chefes de seção evidenciaram a necessidade de melhorar a integração entre as divisões, o que poderá ajudar em casos de alvos de interesse comum. A proposta deste sistema endereça essas questões ao oferecer filtros avançados de pesquisa, histórico de atividades e controle de acesso baseado em perfis, funcionalidades que aumentam a produtividade e melhoram o fluxo de informações entre as equipes.

Embora este trabalho apresente um esboço inicial dos requisitos funcionais e não funcionais, ele não cobre todas as necessidades que o sistema deverá atender. Sugere-se que estudos futuros ampliem o diagnóstico inicial com entrevistas com gerentes e o superintendente, identificando recursos adicionais que possam agregar valor às operações da agência. Ademais, recomenda-se um estudo aprofundado da Doutrina Nacional de Inteligência de Segurança Pública (DNISP), visando assegurar que o desenvolvimento do sistema esteja em conformidade com as diretrizes e normas estabelecidas, garantindo um alinhamento robusto com as melhores práticas da atividade de inteligência.

Por fim, o foco deste trabalho se restringiu à gestão de demandas e do conhecimento, sem abordar detalhes técnicos de implementação. A proposta permanece no campo das funcionalidades e segurança do sistema. Vale ressaltar que, por questões de segurança, mesmo que o sistema seja implementado, detalhes técnicos adicionais não serão amplamente divulgados para preservar a integridade das operações da AIPCGO.

REFERÊNCIAS

BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Izabelly S.; et al. **Fundamentos de segurança da informação**. Porto Alegre: Grupo A, 2018. E-book. ISBN 9788595025875. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875/. Acesso em: 25 ago. 2024.

BRASIL. **Lei nº 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - Abin, e dá outras providências. Brasília: Presidência da República, [1999]. Disponível em: https://bit.ly/3wWb46L. Acesso em: 07 set. 2024.

BRASIL. **Decreto nº 7.724, de 16 de maio de 2012**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. Brasília, DF: Presidência da República [2012]. Diário Oficial da União. Brasília, 16 mai. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 23 ago. 2024.

BRASIL. **Decreto nº 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Brasília: Presidência da República, [2016]. Diário Oficial da União, nº124: seção 1, Brasília; DF, p. 5, 30 jun. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em: 07 set. 2024.

BRASIL. **Decreto 4.376 de 15 de dezembro de 2017** – Aprova a Estratégia Nacional de Inteligência. Brasília: Presidência da República, [2017]. Diário Oficial da União nº 241: seção 1, Brasília; DF p.36, 18 dez. 2017. Disponível em: https://bit.ly/3NFWKG9. Acesso em: 07 set. 2024.

BRASIL. **Decreto nº 10.777, de 14 de agosto de 2021**. Institui a Política Nacional de Inteligência de Segurança Pública. Brasília: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10777.htm. Acesso em: 24 ago. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. **Doutrina da Atividade de Inteligência**. Brasília: Ministério da Justiça e Segurança Pública, 2023. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023. Acesso em: 19 ago. 2024.

BUENO, Cristian Del Anhol Pereira. A Inteligência como Medida Preditiva no Combate ao Crime Organizado na Região De Fronteira: "Uma Precepção Necessária no Âmbito da PMPR". **Revista Ciências Policiais.** São José dos Pinhais: ano 2022 n. 4 p. 90-106, nov. 2022. Disponível em: https://www.apmg.pr.gov.br/Pagina/Revista-de-Ciencias-Policiais-V-4-2022. Acesso em 23 ago. 2024.

CARVALHO, Heberson. **Um Modelo de Dados Voltado ao Serviço De Inteligência Policial**. Universidade Federal de Santa (UFSC), 2015. Araranguá, Santa Catarina. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/180399/Monografia-Herbson-de-Carvalho-final-1.pdf?sequence=1&isAllowed=y. Acesso em: 24 ago. 2024.

FRASÃO, Heloisa Ferreira. **A importância da implantação de sistema de gestão de segurança da informação**. 2020. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) — Faculdade Anhanguera Educacional, Osasco, 2020. Disponível em: https://repositorio.pgsscogna.com.br/bitstream/123456789/31584/1/HELOISA_FERREIRA_FRASAO_ATIVIDADE3.pdf. Acesso em: 12 nov. 2024.

FREITAS, Rodrigo P. de; BORGES NETO, Antônio Cruvinel. A análise das ameaças por meio da auditoria de log nativo do sistema e quais as razões que dificultam sua adoção. **Revista Mirante**, Anápolis (GO), v. 11, n. 6, edição especial, p. 92-103, abr. 2018. Disponível em: https://www.revista.ueg.br/index.php/mirante/article/view/7611. Acesso em: 12 nov. 2024.

GIL, Antonio C. **Como Elaborar Projetos de Pesquisa**. Barueri - SP: Atlas: Grupo GEN, 2022. E-book. ISBN 9786559771653. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771653/. Acesso em: 12 set. 2024.

GOIÁS. **Lei n.º 16.272, de 30 de maio de 2008**. Dispõe sobre a organização da administração direta, autárquica e fundacional do Poder Executivo. Goiânia: Palácio do Governo do Estado de Goiás [2008]. Disponível em: https://legisla.casacivil.go.gov.br/api/v2/pesquisa/legislacoes/87023/pdf. Acesso em: 04 nov. 2024.

GOIÁS. **Lei n.º 17.257, de 25 de janeiro de 2011**. Dispõe sobre a organização administrativa do Poder Executivo do Estado de Goiás e dá outras providências. Goiânia: Palácio do Governo do Estado de Goiás [2011]. Disponível em: https://legisla.casacivil.go.gov.br/api/v2/pesquisa/legislacoes/98375/pdf. Acesso em: 04 nov. 2024.

GOIÁS. **Lei n.º 19.390, de 07 de julho de 2016**. Promove alterações na organização administrativa da Secretaria de Estado de Segurança Pública e Administração Penitenciária e dá outras providências. Goiânia: Palácio do Governo do Estado de Goiás [2016]. Disponível em: https://legisla.casacivil.go.gov.br/api/v2/pesquisa/legislacoes/98705/pdf. Acesso em: 04 nov. 2024.

GOIÁS. **Decreto n.º 8.869, de 12 de janeiro de 2017**. Institui o Sistema de Inteligência de Segurança Pública do Estado de Goiás - SISP/GO. Goiânia: Palácio do Governo do Estado de Goiás [2017]. Disponível em: https://legisla.casacivil.go.gov.br/pesquisa_legislacao/69612/decreto-8869. Acesso em: 04 nov. 2024.

GOIÁS. **Lei n.º 21.614, de 13 de dezembro de 2022**. Dispõe sobre a revogação de leis que especifica. Goiânia [2022]. Disponível em: https://legisla.casacivil.go.gov.br/pesquisa_legislacao/106311/lei-21614. Acesso em: 04 nov. 2024.

GOIÁS. **Decreto n.º 10.218, de 16 de fevereiro de 2023a**. Regulamenta a Lei nº 21.792, de 16 de fevereiro de 2023, que estabelece a organização administrativa básica do Poder

Executivo e dá outras providências. Goiânia [2023]. Disponível em: https://legisla.casacivil.go.gov.br/api/v2/pesquisa/legislacoes/106750/pdf. Acesso em: 04 nov. 2024.

GOIÁS. Polícia Civil. **Portaria n.º 195/2023** – DGPC, de 16 de fevereiro de 2023b. Fixa a estrutura administrativa da Delegacia-Geral da Polícia Civil. Goiânia [2023]. Disponível em: https://www.policiacivil.go.gov.br/wp-content/uploads/2023/06/portaria-n-195-2023-dgpc.pdf. Acesso em: 04 nov. 2024.

GOIÁS. Polícia Civil. **Organograma da Delegacia-Geral da Polícia Civil**, 2024. Disponível em: https://www.policiacivil.go.gov.br/wp-content/uploads/2024/06/organograma-da-policia-civil.pdf. Acesso em: 04 nov. 2024.

GOMES, Herick Wendell Antônio José; MIRANDA, Wando Dias; CHAGAS, Clay Anderson. A atividade de inteligência de segurança pública como ferramenta de assessoramento para o processo decisório do gestor público. In: REIS NETTO, Roberto Magno; MIRANDA, Wando Dias; REIS, João Francisco Garcia. **Segurança Pública e Atividade de Inteligência**: debates e perspectivas. Ananindeua: CROM, 2021. *E-book* (286p.) color. ISBN: 978-65-00-30811-2.Disponível em: https://www.researchgate.net/profile/Roberto-Reis-Netto-2/publication/355097024_SEGURANCA_PUBLICA_E_ATIVIDADE_DE_INTELIGENCIA_debates_e_perspectivas_-_V1/links/615d820450be550728899393/SEGURANCA-PUBLICA-E-ATIVIDADE-DE-INTELIGENCIA-debates-e-perspectivas-V1.pdf. Acesso em 09 set. 2024.

LAVAREDA, Mario Jessen. O Relatório Técnico na Inteligência de Segurança Pública. **Revista do Ministério Público do Estado do Rio de Janeiro.** Rio de Janeiro: ano 2024, n. 91, p. 193 - 219, jan/mar. 2024. Disponível em: https://www.mprj.mp.br/documents/20184/4920402/mario_jessen_lavareda.pdf. Acesso em: 23 ago. 2024.

LOZADA, Gisele; NUNES, Karina S. **Metodologia científica**. Porto Alegre: Grupo A, 2019. E-book. ISBN 9788595029576. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595029576/. Acesso em: 12 set. 2024.

MELO, Felipe Pereira de; URPIA, Arthur Gualberto da Cruz Bacelar; SARTORI, Rejane. A gestão do conhecimento como auxílio à inteligência de segurança pública. In: PEREIRA, Denise; CARNEIRO, Maristela (Orgs.). **Da teoria à prática em pesquisas nas ciências sociais aplicadas**. Ponta Grossa - PR: Atena, 2021. p. 27-42. DOI 10.22533/at.ed.448210104. Disponível em: https://atenaeditora.com.br/catalogo/post/a-gestao-do-conhecimento-como-auxilio-a-inteligencia-de-seguranca-publica. Acesso em: 24 ago. 2024.

REINEHR, Sheila. **Engenharia de requisitos**. Porto Alegre: SAGAH, 2020. E-book. p.36. ISBN 9786556900674. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556900674/. Acesso em: 07 nov. 2024.

REIS NETTO, Roberto Magno; MIRANDA, Wando Dias; GOMES, Herick Wendell Antônio José; CAVALCANTE, Clarina de Cássia da Silva. O sigilo do relatório produzido na

atividade de inteligência policial e o controle externo do ministério público. In: REIS NETTO, Roberto Magno; MIRANDA, Wando Dias; REIS, João Francisco Garcia. **Segurança Pública e Atividade de Inteligência**: debates e perspectivas. Ananindeua: CROM, 2021. *E-book* (286p.) color. ISBN: 978-65-00-30811-2.Disponível em: https://www.researchgate.net/profile/Roberto-Reis-Netto-2/publication/355097024_SEGURANCA_PUBLICA_E_ATIVIDADE_DE_INTELIGENCIA_debates_e_perspectivas_-_V1/links/615d820450be550728899393/SEGURANCA-PUBLICA-E-ATIVIDADE-DE-INTELIGENCIA-debates-e-perspectivas-V1.pdf. Acesso em 09 set. 2024.

RIBEIRO, Anna Carolina Mendonça Lemos; OLIVEIRA JÚNIOR, Almir de; SILVA, Marcos Paulo Hyath da. Uma visão crítica sobre a ausência de protocolo geral de integração de agências na Inteligência em Segurança Pública. **Revista Brasileira de Inteligência**, Brasília, Brasil, n. 18, p. 167–186, 2023. DOI: 10.58960/rbi.2023.18.228. Disponível em: https://rbi.abin.gov.br/RBI/article/view/228. Acesso em: 19 ago. 2024.

RIBEIRO, Cileno de Magalhães; NUNES, Rafael Rabelo; ALBUQUERQUE, Robson de Oliveira. Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E49, p. 169-183, 2022. Disponível em: https://www.researchgate.net/profile/Rafael-Nunes-4/publication/362914403_Um_diagnostico_sobre_o_processo_de_comunicacao_sigilosa_entre_os_orgaos_do_Sistema_Brasileiro_de_Inteligencia/links/630769941ddd4470210a8370/Um-diagnostico-sobre-o-processo-de-comunicacao-sigilosa-entre-os-orgaos-do-Sistema-Brasileiro-de-Inteligencia.pdf. Acesso em: 07 set. 2024.

ROSINI FILHO, Alessandro Marco; ROSINI, Alessandro Marco; PALMISANO, Angelo. The age of big data: main implications on security and privacy and new technologies that can help investigative processes and detection of real-time fraud. **RISUS – Journal on Innovation and Sustainability**, São Paulo, v. 11, n. 3, p. 13-34, mai./jun. 2020. Disponível em: https://revistas.pucsp.br/index.php/risus/article/view/49660. Acesso em: 12 nov. 2024.

RUPRECHT, Aurélio Jullbert de Assis. **A compartimentação da informação em investigações policiais: aspectos do sigilo e do controle de acesso à informação em investigações conduzidas pela Polícia Federal**. 2021. Universidade Federal de Santa Catarina - UFSC, Florianópolis, Santa Catarina. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/229135/PCIN0273-D.pdf?sequence=-1&isAllowed=y. Acesso em: 24 ago. 2024.

SANTOS, Thiago Ramos dos; MENDONÇA, Fabrício Molica de. Conceitos Introdutórios para Entender a Atividade de Inteligência e sua Utilidade na Segurança Pública. **Revista Ciências Policiais.** São José dos Pinhais: ano 2022 n. 4 p. 75-89, nov. 2022. Disponível em: https://www.apmg.pr.gov.br/Pagina/Revista-de-Ciencias-Policiais-V-4-2022. Acesso em 23 ago. 2024.

SILVA, Emerson Lopes; LIMA, Suzana Moura. Inteligência policial e atividade criminosa: Novos Paradigmas no combate à macrocriminalidade. In: REIS NETTO, Roberto Magno; MIRANDA, Wando Dias; REIS, João Francisco Garcia. **Segurança Pública e Atividade de Inteligência**: debates e perspectivas. Ananindeua: CROM, 2021. *E-book* (286p.) color. ISBN:

978-65-00-30811-2.Disponível em: https://www.researchgate.net/profile/Roberto-Reis-Netto-2/publication/355097024_SEGURANCA_PUBLICA_E_ATIVIDADE_DE_INTELIGENCIA_debates_e_perspectivas_-_V1/links/615d820450be550728899393/SEGURANCA-PUBLICA-E-ATIVIDADE-DE-INTELIGENCIA-debates-e-perspectivas-V1.pdf. Acesso em 09 set. 2024.

SILVA, Marcos Sigismundo da. **Requisitos de softwares para repositórios digitais: uma análise à luz da ISO 16363**. 2023. 100 f. Dissertação (Mestrado em Ciência da Informação) — Universidade de Brasília, Faculdade de Ciência da Informação, Brasília, 2023. Disponível em: http://icts.unb.br/jspui/bitstream/10482/48827/1/MarcosSigismundoDaSilva_DISSERT.pdf. Acesso em: 12 nov. 2024.

SOUZA, Fábio José de; TREVISAN, Rodrigo Humberto; SIQUEIRA, Jorge Antônio de Souza. **Gestão do conhecimento integrada aos sistemas inteligentes da Polícia Militar do Estado de São Paulo**. Unisanta Law and Social Science, v. 8, n. 1, p. 179-202, 2019. Disponível em: https://periodicos.unisanta.br/index.php/lss/article/view/2049. Acesso em 24 ago. 2024.

TOLARDO, Julio Cesar Cabral. **O emprego da criptografia no controle de segurança de dados no ambiente virtual**. 2022. Monografia (Bacharelado em Ciências da Computação) – Faculdade Anhanguera Educacional, Santa Bárbara D'Oeste, 2022. Disponível em: https://repositorio.pgsscogna.com.br/bitstream/123456789/50314/1/JULIO_CESAR_CABRAL_TOLARDO.pdf. Acesso em: 11 nov. 2024.

ZANCHI, Oldair. **Inteligência de Segurança Pública: O Relatório de Inteligência (RELINT) e o Processo Penal**. 2021. Universidade do Sul de Santa Catarina (UNISUL), Florianópolis, Santa Catarina. Disponível em: https://repositorio.animaeducacao.com.br/items/08294946-8f69-4525-8c64-7c08b6233101. Acesso em: 23 ago. 2024.