Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

ANDRÉ LUIS DECCACHE DIAS

FACILITADORES E OBSTÁCULOS PARA GESTÃO DO CONHECIMENTO EM ATIVIDADES INVESTIGATIVAS RELATIVAS A CRIMES CIBERNÉTICOS: ESTUDO NA PERCEPÇÃO DE POLICIAIS FEDERAIS

BRASÍLIA
2025

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

ANDRÉ LUIS DECCACHE DIAS

FACILITADORES E OBSTÁCULOS PARA GESTÃO DO CONHECIMENTO EM ATIVIDADES INVESTIGATIVAS RELATIVAS A CRIMES CIBERNÉTICOS: ESTUDO NA PERCEPÇÃO DE POLICIAIS FEDERAIS

Dissertação apresentada ao Curso de Mestrado Profissional em Administração Pública da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, como requisito para obtenção do título de Mestre em Administração Pública.

Orientador(a): Prof. Dr. Carlos André de Melo Alves

BRASÍLIA
2025

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

ANDRE LUIS DECCACHE DIAS

FACILITADORES E OBSTÁCULOS PARA GESTÃO DO CONHECIMENTO EM ATIVIDADES INVESTIGATIVAS RELATIVAS A CRIMES CIBERNÉTICOS: ESTUDO NA PERCEPÇÃO DE POLICIAIS FEDERAIS

Dissertação apresentada ao Curso de Mestrado Profissional em Administração Pública da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, como requisito para obtenção do título de Mestre em Administração Pública.

Data da defesa: 29 / 07 / 2025

Comissão Examinadora:

Professor Doutor Carlos André de Melo Alves - Orientador

MPA/UnB

Professor Doutor João Mendes da Rocha Neto - Examinador Interno

MPA/UnB

Professor Doutor Alexandre dos Santos Cunha – Examinador Externo

IPEA

Professor Doutor Cleidson Nogueira Dias – Examinador Suplente

PGAP/UnB

AGRADECIMENTOS

- À paciência de Fran, Cecília e Taylha, especialmente pelas inúmeras horas em que estive ausente.
- Ao colega Pablo, que desde o início do processo de seleção muito me ajudou.
- Aos colegas Góes e Freire, que participaram do processo de construção deste trabalho.
- Ao apoio dos colegas de "sala", que também são colegas de trabalho, sempre prontos a ajudar.
- À equipe da Escola Superior de Polícia (CESP/ANP), equipe sensacional e apaixonada pelo que faz.
- Aos colegas que participaram das entrevistas, com os quais aprendi mais do que seria possível expressar em qualquer texto.
- Aos professores do PPGA/UnB, por compartilharem tanto conhecimento e demonstrarem genuíno interesse no progresso dos alunos.
- Aos professores da minha banca de qualificação, que contribuíram de forma incomensurável para a realização deste trabalho.
- Ao meu professor orientador, pela orientação precisa e por indicar o caminho a ser trilhado, permitindo a realização desta etapa da vida.

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

RESUMO

O enfrentamento dos crimes cibernéticos apresenta-se como um desafio na atualidade, inclusive para as polícias em diferentes países. A este respeito, constata-se a necessidade de iniciativas sobre a gestão do conhecimento em atividades investigativas que se refiram a tais crimes. O objetivo geral desta pesquisa é descrever os facilitadores e os obstáculos para gestão do conhecimento em atividades investigativas relativas a crimes cibernéticos, na percepção de policiais federais. O quadro teórico-conceitual apresenta gestão do conhecimento (GC), facilitadores e obstáculos à GC, segurança cibernética, crimes cibernéticos e a estrutura das polícias brasileiras para investigações de tais crimes, enfatizando a Polícia Federal. Para tanto, foi realizada uma pesquisa descritiva com abordagem qualitativa. A coleta dos dados foi feita por meio de entrevistas com servidores da Polícia Federal, complementada pela coleta de documentos públicos e internos não sigilosos do referido órgão de segurança pública. Para tratamento dos dados empregou-se a análise documental e análise de conteúdo. Abordou-se na análise de conteúdo o teor do quadro teórico contendo facilitadores e obstáculos à GC, como também, a classificação dos facilitadores e dos obstáculos percebidos segundo os níveis individual, organizacional ou ambiental. Os principais resultados indicaram que os policiais percebem a definição de GC considerando oito elementos de conceito baseados na literatura. Além disso, foram identificados sete facilitadores e dez obstáculos à GC, previamente citados no quadro teórico-conceitual. Esses facilitadores e esses obstáculos não se distribuíram uniformemente entre os níveis organizacionais. Verificou-se que três facilitadores e dois obstáculos se vinculam ao nível individual; quatro facilitadores e sete obstáculos vinculam-se ao nível organizacional; e um obstáculo vincula-se ao nível ambiental. O resultado obtido nas pesquisas deu subsídios para a criação de material didático em forma de cartilha com potencial de uso por gestores e investigadores policiais que atuem na área de crimes cibernéticos. Capturar a percepção das dificuldades e dos processos bem-sucedidos na GC das investigações de crimes cibernéticos não apenas contribui para as unidades especializadas no tema, mas também para as organizações policiais envolvidas em investigações criminais, bem como para atividades correlatas que envolvam órgãos de segurança atuantes no setor público.

Palavras-Chave: Gestão do Conhecimento; Crimes Cibernéticos; Investigação Policial; Polícia Federal; Setor Público.

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

ABSTRACT

Combating cybercrime presents a contemporary challenge, including for police forces in various countries. In this context, there is a recognized need for initiatives concerning knowledge management in investigative activities related to such crimes. The general objective of this research is to describe the facilitators and obstacles to knowledge management in investigative activities related to cybercrime, from the perception of federal police officers. The theoretical-conceptual framework encompasses knowledge management, facilitators and obstacles to its implementation, cybersecurity, cybercrime, and the structure of Brazilian police forces responsible for investigating such offenses, with emphasis on the Federal Police. To achieve this, a descriptive study with a qualitative approach was conducted. Data collection involved interviews with Federal Police officers, complemented by the analysis of public and non-confidential internal documents from the institution. Data were analyzed using document analysis and content analysis. The content analysis addressed the theoretical framework on facilitators and obstacles to knowledge management, as well as the classification of these factors according to individual, organizational, or environmental levels. The main results indicated that officers understand the concept of knowledge management in terms of eight elements derived from the literature. In addition, seven facilitators and ten obstacles to knowledge management were identified, all of which were previously addressed in the theoretical-conceptual framework. These facilitators and obstacles were not evenly distributed across analytical levels: three facilitators and two obstacles were linked to the individual level; four facilitators and seven obstacles to the organizational level; and one obstacle to the environmental level. The findings supported the creation of an educational product in the form of a guidebook, with potential application by managers and investigators working in the field of cybercrime. Capturing the perception of challenges and successful practices in knowledge management related to cybercrime investigations not only contributes to specialized units but also to police organizations involved in criminal investigations and to other security-related activities within the public sector.

Keywords: Knowledge Management; Cybercrimes; Police Investigation; Brazilian Federal Police; Public Sector.

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

LISTA DE ABREVIATURAS E SIGLAS

APF	Agente de Polícia Federal
ABNT	Associação Brasileira de Normas Técnicas
DPF	Delegado de Polícia Federal
DCIBER	Diretoria de Combate aos Crimes Cibernéticos – Polícia Federal
DELECIBER	Delegacia de Repressão aos Crimes Cibernéticos – Polícia Federal
GC	Gestão do Conhecimento
GRCC	Grupos de Repressão aos Crimes Cibernéticos
IPEA	Instituto de Pesquisa Econômica Aplicada
ISO	International Organization for Standardization
PCF	Perito Criminal Federal
PGC	Política de Gestão do Conhecimento
PF	Polícia Federal
SR	Superintendência Regional da Polícia Federal
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
MGCA	Modelo de Gestão do Conhecimento na Administração Pública

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

LISTA DE FIGURAS

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

LISTA DE TABELAS

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

LISTA DE QUADROS

SUMÁRIO

1. INTRODUÇÃO

1.1. Contextualização

A revolução digital, iniciada em meados do século XX, gerou grandes mudanças sociais, levando estudiosos do tema a nomearem as primeiras décadas do século XXI de era digital (Hilbert, 2020). Tais mudanças decorrem, respeitados outros fatores, por conta de a velocidade das relações ser diretamente influenciada pela tecnologia, o que requer uma sociedade inovadora e conectada (Dhanhani & Naqbi, 2022). Essa necessidade também diz respeito à busca e à aquisição de conhecimento.

O conhecimento é reconhecido como importante elemento para sustentar a competitividade de uma organização (Lee & Choi, 2003), que deve implementar políticas e estratégias levando em conta a percepção de ser aquele um recurso crítico (Seba et al., 2012). O conhecimento diferencia-se em dois tipos, o tácito – algo inerente a quem o detém, difícil de formalizar e comunicar – e o explícito – codificado, transmissível de maneira formal e sistemática (Nonaka, 2000). Captar esse conhecimento individual e transformá-lo em material disponível oferecido a outros é um grande desafio.

Para que se possa obter resultados efetivos, faz-se uso da Gestão do Conhecimento (GC), um processo sistemático de integração entre tecnologia e aspectos humanos para ganho de competitividade dos trabalhadores e da organização, contemplando práticas e rotinas organizacionais para lidar com a criação interna ou aquisição externa de conhecimento, de forma a utilizá-lo no âmbito da organização (Jääskeläinen et al., 2022; Pellegrini et al., 2020).

A GC ganhou tração inicial em organizações privadas, e as publicações sobre o tema limitavam-se a esse tipo de organização (Agrifoglio et al., 2021). Contudo, ao longo do tempo, foi identificada uma mudança, com o surgimento de publicações tratando a GC em organizações públicas (Xanthopoulou et al., 2023). Apesar de haver a percepção de que o conhecimento é a base da eficiência que por fim contribui para o resultado lucro, é também uma ferramenta importante para organizações públicas (Seba et al., 2012), permitindo ao setor público enfatizar o bem-estar social utilizando-se de métricas que se refiram, por exemplo, à satisfação do cidadão com a prestação do serviço (Laihonen et al., 2023).

No Brasil, houve proposta de alguns modelos de implementação e avaliação de GC em organizações públicas. Por exemplo, o Modelo de GC na Administração Pública (MGCA), é difundido no setor público federal brasileiro, definido como “um método integrado de criar, compartilhar e aplicar o conhecimento para aumentar a eficácia” e que busca melhorias de

qualidade e efetividade social, consideradas relevante em virtude da necessidade de se aplicar melhor os recursos originados dos impostos cobrados da sociedade (Batista, 2012, p. 49). Importa dizer que o serviço público depende, em grande parte, da maneira como seus integrantes transferem seus conhecimentos entre si (Castro et al., 2022).

Como exemplo, os órgãos de segurança pública, representados em especial – mas não exclusivamente - pelas polícias, também necessitam de evoluções e melhorias de resultados em suas atividades (Seba & Rowley, 2010). As principais funções das polícias envolvem proteção à vida, ao patrimônio, à preservação da lei e da ordem e a investigação de crimes. Tais funções demandam conhecimentos dos profissionais, suas experiências individuais e aquisição de conhecimentos (Luen & Al-Hawamdeh, 2001; Seba et al., 2012). Assim, o trabalho policial é dependente da GC, devendo ser as polícias proativas na promoção e difusão do compartilhamento desse conhecimento (Seba et al., 2012), um recurso que pode ser usado para melhoria do desempenho da polícia (Gottschalk e Dean, 2010), inclusive em atividades investigativas relativas a crimes cibernéticos, como será exposto na sequência.

Crime cibernético pode ser definido como atividade criminal em que serviços ou aplicativos no espaço cibernético[1] são usados para, ou são alvo de, um crime, ou em que o espaço cibernético é a fonte, ferramenta, alvo ou local de um crime (Associação Brasileira de Normas Técnicas [ABNT], 2015). Tais crimes são uma ameaça constante e um desafio para a comunidade global ligada à aplicação da lei. Uma investigação pode, ao longo de seu curso, permitir a detecção do uso de tecnologias para instrumentalizar um crime cibernético, o que exige agilidade e conhecimento por parte do investigador (Hunton, 2011). A execução de crimes cibernéticos está ligada ao conhecimento – ou à sua ausência – e, para que seja possível investigá-los, faz-se necessário entender seu funcionamento (Kleve et al., 2011).

Conforme mencionado no resumo deste estudo, o enfrentamento dos crimes cibernéticos apresenta-se como um desafio na atualidade, inclusive para as polícias em diferentes países, como os EUA (Federal Bureau of Investigation, [s.d.]) e integrantes da União Europeia (Europol, 2022), em especial aqueles que aderiram à Convenção de Budapeste, como o Brasil (Brasil, 2023a; Spiezia, 2022). No Brasil, A Polícia Federal (PF) é parte do sistema de Segurança Pública, constante no art. 144 da Constituição Federal (1988), que abrange outras polícias de âmbito federal, como a Polícia Rodoviária Federal e a Polícia Penal Federal. No

[1]Para os fins deste estudo, ‘espaço cibernético’ é o ambiente complexo resultante da interação de pessoas, softwares ou serviços na internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe qualquer forma física (ABNT, 2015).

âmbito estadual/distrital, devem ser lembrados também os bombeiros militares, as polícias civis, militares e penais.

Do grupo de órgãos citados no parágrafo anterior, cabe à PF e às vinte e sete polícias civis a investigação de crimes, inclusive os crimes cibernéticos (Brasil, 1988). Cada uma das polícias citadas neste parágrafo, também chamadas de polícias investigativas, tem liberdade para estruturar a forma de lidar com os diferentes tipos de delitos previstos na legislação. Na atualidade, há a tendência de se criar grupos especializados em investigações sobre crimes cibernéticos, em virtude de muitas de suas especificidades relacionadas ao conhecimento tecnológico e à atualização de ferramentas digitais (Safernet, [s.d.]; Santos, 2022).

A importância dos crimes cibernéticos para a PF é oficializada pela Portaria n.º 2.720 – DG/DPF de 22 de novembro de 2011 que institui os Grupos de Repressão a Crimes Cibernéticos (GRCC), formalizando então as unidades especializadas e permitindo melhor capacitação dos policiais para o enfrentamento da criminalidade, inclusive a organizada. Não obstante, a formalização tem também influência das recomendações encontradas no Relatório Final nº 03/2010 da Comissão Parlamentar de Inquérito – Pedofilia, do Senado Federal (2010), para a criação de estrutura formal destinada ao combate aos crimes cibernéticos na PF.

A relevância do tema é reafirmada com a criação, em 2023 da Diretoria de Combate a Crimes Cibernéticos (DCIBER), em uma reestruturação do órgão que separa as investigações de crimes cibernéticos dos crimes físicos (Hunton, 2011) ou não cibernéticos. Com a diferenciação proposta, traz-se a definição dos crimes investigados pela DCIBER contida no Decreto n.º 11.348/2023 (Brasil, 2023b): os de alta tecnologia e contra infraestruturas críticas; de abuso sexual infantojuvenil; e relativas a fraudes eletrônicas. Cabe também a tal Diretoria o apoio a “investigações conduzidas por outras unidades que demandem o emprego de recursos ou técnicas especiais”.

Essa alteração na estrutura da organização pôde favorecer a aplicação do modelo previsto pelo próprio órgão em um grupo menor e com menos atribuições e, no caso da DCIBER, haveria mais um elemento: a alta produção e demanda por conhecimento, em virtude das especificidades da área.

1.2. Formulação do Problema

A literatura sobre GC abrangendo a PF como lócus é escassa e aponta para uma possibilidade de expansão, cabendo a realização de pesquisas que consigam contemplar a percepção sobre a GC. Apurar essa percepção pode trazer elementos para o desenvolvimento de estratégias efetivas ao referido órgão público (Menezes, 2020).

A PF teve avaliada sua maturidade em Gestão do Conhecimento na pesquisa realizada pelo IPEA (Batista, 2015), sendo indicado que a organização, à época, estava alinhada com 43% das instituições avaliadas no nível "expansão", descrito pelo autor como o nível em que se observam práticas de GC em algumas áreas da instituição, abrindo a possibilidade de se fazer uma avaliação específica de determinada atividade investigativa.

Com o enfoque na PF, o trabalho de Menezes (2020), que utilizou o MGCA proposto por Batista (2012), desenhado especificamente para a Administração Pública Brasileira, buscou compreender como o conhecimento envolvido nas atividades investigativas é gerido, deixando, contudo, em aberto a oportunidade para o estudo da GC sobre atividades investigativas específicas, como aquelas relativas a crimes cibernéticos. Como foi descrito na contextualização, a PF está envolvida em atividades investigativas relativas a crimes cibernéticos, tendo incluído em sua estrutura a DCIBER, unidade central para tratar o assunto de forma específica no órgão.

Acrescente-se que a opção por buscar a percepção dos policiais federais que atuam nas investigações sobre crimes cibernéticos é motivada pelo entendimento de ser o conhecimento, em seu nível mais básico, gerado por indivíduos em processos técnicos e cognitivos (Nonaka, 2000). A descrição da percepção desses policiais pode, inclusive, indicar a existência de facilitadores e de obstáculos relativos à GC em atividades investigativas relativas a crimes cibernéticos.

O estudo desses facilitadores e obstáculos à GC pode trazer evidências que auxiliem o aprimoramento das atividades investigativas relativas a crimes cibernéticos em diferentes níveis organizacionais, contribuindo para um diagnóstico que pode ser segmentado em individual, organizacional ou ambiental (Oliveira & Abib, 2023).

Diante do exposto previamente na introdução, na contextualização e nesta seção, o problema proposto nesta pesquisa é o seguinte: quais são os facilitadores e os obstáculos para a gestão do conhecimento em atividades investigativas relativas a crimes cibernéticos, na percepção de policiais federais?

1.3. Objetivos da Pesquisa

1.3.1. Objetivo geral

O presente trabalho tem como objetivo descrever os facilitadores e os obstáculos para Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos, na percepção de policiais federais.

1.3.2. Objetivos específicos

De forma a alcançar o objetivo geral do trabalho, tem-se os objetivos específicos:

a) Caracterizar o conceito de gestão do conhecimento, na percepção de policiais federais;
b) Identificar, a partir da percepção de policiais federais, os facilitadores e os obstáculos para a Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos;
c) Classificar os facilitadores e os obstáculos previamente identificados segundo os níveis individual, organizacional e ambiental;
d) Propor recomendações à Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos, com base nos facilitadores e obstáculos previamente identificados.

1.4. Justificativas

A literatura internacional apresenta poucos trabalhos específicos sobre a GC no Setor Público (Alvarenga et al., 2020), com escassos autores especializados no tema e pouca interação entre tópicos e autores (Massaro et al., 2015). A GC e suas práticas mantêm-se pouco explorada no setor público (Al Ahbabi et al., 2019; Laihonen et al., 2023; Pepple et al., 2022), havendo pesquisas em menor número quando comparadas com o setor privado (Ganapathy et al., 2019). Uma constatação adicional é a ausência de trabalhos especificamente sobre serviços públicos, dentre eles as organizações policiais (Massaro et al., 2015; Seba et al., 2012, 2013).

Os trabalhos encontrados na literatura sobre GC no serviço público nacional buscam avaliação através da ótica da gestão da organização, mas não enfatizam a percepção dos servidores públicos sobre o tema (Menezes, 2020). A organização pública depende de tais

servidores para o alcance de seus objetivos, justificando a tentativa de identificar se conhecem sobre GC, inclusive seus facilitadores e obstáculos.

Além da atividade investigativa da polícia ser fortemente dependente de conhecimento, os profissionais que atuam em atividades investigativas podem ser considerados *knowledge workers* em virtude do volume de conhecimento produzido durante os procedimentos investigatórios (Gottschalk & Dean, 2010; Luen & Al-Hawamdeh, 2001) o qual deve ser reaproveitado para uma maior eficiência e eficácia em outras investigações. Este entendimento pode, inclusive, ser aplicado a atividades investigativas relativas a crimes cibernéticos.

Não obstante, compreender os contrastes e convergências das visões das coordenações da DCIBER e dos investigadores de crimes cibernéticos sobre a GC, seus facilitadores e obstáculos, pode trazer melhorias nos processos, ferramentas e políticas de GC na organização e, principalmente, nos procedimentos investigativos, permitindo a qualificação constante dos policiais e a reutilização de cada passo realizado. Ressaltam-se os achados de Menezes (2020), que apontam para iniciativas estanques por parte dos investigadores – em geral, projetos individuais não aproveitados pela organização – e para projetos organizacionais que não entram de maneira efetiva em uso.

O trabalho proposto busca suprir a lacuna de pesquisa relacionada às instituições policiais, em especial à própria PF, ao tema GC no Serviço Público Federal e a percepção dos trabalhadores da base hierárquica sobre o conhecimento e sua gestão, por meio daqueles que atuam em um tópico com densidade de conhecimento e demanda por sua rápida aquisição em virtude das frequentes inovações. Seu resultado, contudo, pretende atender não apenas à DCIBER, mas também às demais Diretorias da instituição, podendo ser replicado em outras instituições policiais.

Dessa forma, a proposta de entrevistar os policiais da PF para colher suas percepções sobre a GC na organização se justifica por auxiliar a gestão da organização a compreender os eventuais problemas e amplificar sucessos no escopo da DCIBER, além de contribuir para os estudos em GC no setor público, especialmente nas organizações policiais. Ao buscar categorizar os facilitadores e obstáculos nos níveis individual, organizacional e ambiental, pretende-se compreender em qual desses níveis devem concentrar-se os esforços para permitir melhorias na GC da organização.

Capturar a percepção das dificuldades e dos processos bem-sucedidos na GC das investigações de crimes cibernéticos não apenas contribui para as delegacias especializadas no

tema, mas também para a instituição como um todo, incluindo as demais atividades além das investigações criminais. Não obstante, outros órgãos que atuam com investigações criminais também poderão se beneficiar dos resultados obtidos por meio da pesquisa, pois a GC em investigações criminais contribui para investigações mais ágeis e com maior índice de resolutividade.

O produto deste trabalho é apresentado em forma de cartilha, a qual visa disseminar o conceito de GC e propor medidas que contribuam para o seu aprimoramento no âmbito organizacional. A cartilha apresenta sugestões práticas direcionadas a gestores, supervisores e burocratas de nível operacional, com o objetivo de fortalecer a aplicação da GC na tomada de decisões e na otimização de processos. Esse formato foi escolhido por sua acessibilidade e facilidade de disseminação, configurando-se como um produto técnico-tecnológico de caráter educativo e instrumental para o público-alvo. Por fim, a contribuição do trabalho alcança o meio acadêmico ao trazer pesquisa sobre Gestão do Conhecimento na administração pública brasileira e na segurança pública, em especial na Polícia Federal, além de estabelecer a relação entre o espaço cibernético e criminalidade.

1.5. Estrutura do Trabalho

O trabalho está estruturado em quatro partes ou capítulos. O Capítulo 1 corresponde à introdução. Ele abrange a contextualização, formulação do problema, descrição dos objetivos, justificativas e a estrutura do trabalho.

O Capítulo 2 consiste em um artigo teórico-empírico dividido em cinco partes. Na primeira parte, encontra-se a introdução do artigo; em seguida, é exposto o referencial teórico, que traz revisão da literatura sobre GC, tratando também da GC no serviço público e, especificamente, em organizações policiais; e, por fim, aborda-se Segurança Cibernética e Crimes Cibernéticos. Na terceira parte, são descritos métodos e técnicas da pesquisa, apresentando instrumentos de pesquisa e o perfil dos entrevistados, assim como métodos de coleta e análise de dados; na quarta parte são apresentados e discutidos os resultados sobre os conceitos de GC para os entrevistados, os facilitadores e obstáculos à GC em investigações de crimes cibernéticos no âmbito da PF e a classificação dos níveis de análise dos facilitadores e obstáculos encontrados. Por fim, na quinta parte do artigo, apresentam-se as conclusões da pesquisa realizada.

O Capítulo 3 aborda o Produto Técnico-Tecnológico resultante desta pesquisa, materializado em uma cartilha que reúne os facilitadores e obstáculos à GC identificados pelos policiais nas atividades investigativas relacionadas aos crimes cibernéticos. O objetivo principal da cartilha é incentivar e ampliar os elementos facilitadores, além de propor a revisão e o aprimoramento dos obstáculos identificados, visando otimizar o aproveitamento do conhecimento gerado dentro das organizações. Embora o material tenha sido desenvolvido a partir da realidade da Polícia Federal, sua aplicabilidade se estende a qualquer organização que atue na investigação de crimes cibernéticos, oferecendo diretrizes práticas e sugestões valiosas para gestores, supervisores e burocratas de nível operacional.

Por fim, o capítulo 4 traz as considerações finais sobre a pesquisa, apresentando os achados, recomendações e as limitações da pesquisa realizada, possibilitando à Polícia Federal avaliar e incorporar as sugestões apresentadas.

2. PERCEPÇÃO DE POLICIAIS FEDERAIS SOBRE FACILITADORES E OBSTÁCULOS PARA GESTÃO DO CONHECIMENTO EM ATIVIDADES INVESTIGATIVAS RELATIVAS A CRIMES CIBERNÉTICOS

2.1. INTRODUÇÃO

Crimes cibernéticos se tornaram problema relevante para países e organizações, causando graves prejuízos de toda a ordem à sociedade. Fruto do avanço tecnológico e de sua inserção no cotidiano dos povos, cabe às polícias o combate inicial, exigindo dos investigadores de crimes cibernéticos especialização no tema e a capacidade de lidar com os conhecimentos adquiridos durante investigações.

Para gerenciar tais conhecimentos, é necessário utilizar a Gestão do Conhecimento (GC), conceituada como a gestão voltada ao conhecimento, visando ao aprendizado contínuo e à melhoria de resultados. Esse processo inclui a otimização da identificação, criação, análise, representação, distribuição e aplicação do conhecimento, com o objetivo de gerar valor organizacional (ISO, 2018). A GC ainda é pouco explorada no setor público, com escassa produção acadêmica e limitada articulação entre autores e temas (Al Ahbabi et al., 2019; Massaro et al., 2015; Pepple et al., 2022). Esse cenário é ainda mais evidente no contexto dos serviços públicos especializados, como as organizações policiais, para as quais a literatura apresenta lacunas significativas.

A Polícia Federal (PF), dentre suas diversas funções, é responsável por investigar crimes cibernéticos. Em 2023, com a criação da Diretoria de Combate a Crimes Cibernéticos (DCIBER), observa-se um aumento da importância atribuída a esta área. Diante disso, torna-se essencial compreender a gestão dos conhecimentos gerados em tais investigações, destacando-se os facilitadores e obstáculos ao fluxo deste conhecimento e indicando em quais níveis de análise se encontram para permitir um melhor direcionamento dos esforços por parte da gestão da organização (Jilke et al., 2019).

Esta pesquisa tem como objetivos: 1- caracterizar o conceito de gestão do conhecimento, na percepção de policiais federais; 2- identificar, a partir da percepção de policiais federais, os facilitadores e os obstáculos para a Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos; e 3- classificar os facilitadores e os obstáculos previamente identificados segundo os níveis individual, organizacional e ambiental.

O quadro teórico-conceitual apresenta a conceituação de GC, de facilitadores e obstáculos à GC, de níveis de análise, de segurança cibernética e de crimes cibernéticos,

assuntos diretamente conectados com a gestão dos conhecimentos envolvidos em atividades investigativas relativas a crimes cibernéticos.

Quanto ao método, este trabalho é fruto de uma pesquisa descritiva, de natureza qualitativa, fruto de pesquisa bibliográfica, pesquisa documental, que inclui documentos não-sigilosos produzidos pela organização, e entrevistas com policiais atuantes no combate a crimes cibernéticos na PF. O tratamento de dados inclui análise de conteúdo, complementada por análise documental. As análises têm como base o quadro teórico-conceitual produzido, que é confrontado com as entrevistas e documentos não sigilosos identificados.

Diante disso, este trabalho busca suprir a lacuna na literatura acadêmica que trata da GC no âmbito da Administração Pública, em especial na segurança pública, ao investigar as percepções desses profissionais sobre os facilitadores e obstáculos à GC, contribuindo para a qualificação dos processos investigativos e o fortalecimento das políticas institucionais de tais organizações, em especial da PF, objeto deste estudo.

Por meio de entrevistas e categorização dos fatores nos níveis de análise individual, organizacional e ambiental, objetiva-se oferecer subsídios práticos voltados à melhoria da GC na PF, com potencial de replicação em outras organizações policiais e contribuição ao debate acadêmico sobre GC na administração e segurança públicas brasileiras.

Este trabalho está estruturado da seguinte forma: além desta introdução (2.1), o quadro teórico conceitual (2.2), métodos e técnicas (2.3), resultados e discussão (2.4) e, por fim as conclusões (2.5).

2.2. QUADRO TEÓRICO-CONCEITUAL

2.2.1. Gestão do Conhecimento

A organização, ao lidar com ambientes dinâmicos, precisa processar informações de modo eficiente, criar informações e gerenciar conhecimento (Nonaka, 2000). A criação da informação leva à continua inovação, trazendo vantagem competitiva (Dhanhani & Naqbi, 2022; Nonaka & Takeuchi, 1995). Quando gerenciadas e processadas, essas informações podem resultar em desempenhos superiores (Alves et al., 2022). Informação e conhecimento não são claramente diferenciados na literatura (Amayah, 2013; Nonaka, 2000), sendo por vezes tratados como sinônimos embora não o sejam, pois o fluxo de informações gera transformações no conhecimento (Nonaka, 2000).

A informação traz novos pontos de vista sobre eventos ou objetos, enquanto conhecimento pode ser definido como um processo humano dinâmico de justificar crenças pessoais através da "verdade" - um conceito ligado ao sistema de valores do indivíduo (Nonaka & Takeuchi, 1995). O conhecimento consiste em uma coleção de experiências, valores, informações contextualizadas e uma visão profunda que permite criar estruturas para avaliar e integrar novas experiências e informações, as quais são geradas e implementadas nas organizações (Amayah, 2013; Dhanhani & Naqbi, 2022).

O conhecimento possui dois estágios, o tácito e o explícito. Enquanto o primeiro é inerente ao indivíduo, dependente de sua percepção de mundo e ligado às capacidades técnicas e cognitivas, sendo de difícil externalização, o segundo é a informação documentada, sistematizada e em condições de ser transmitida (Nonaka, 2000). Para que o fluxo de conhecimento ocorra efetivamente, é necessário que ele transite do tácito para o explícito e vice-versa, um processo descrito como Espiral do Conhecimento por Nonaka & Takeuchi (1995).

A GC engloba quatro dimensões principais: construção, incorporação, disseminação e uso do conhecimento. Essas dimensões são sustentadas pelas interações sociais dos trabalhadores, que são cruciais para o fluxo eficaz do conhecimento e estão profundamente conectadas às políticas de eficiência de pessoal implementadas pela organização (Mcadam & Reid, 2000). Uma implementação eficaz da GC pode aumentar o compromisso e o desempenho dos *knowledge workers* (Razzaq et al., 2019), incentivando-os a documentar e armazenar conhecimento de forma acessível para os novos membros da equipe, facilitando o aprendizado autônomo (Duan et al., 2023). Portanto, conclui-se que uma função essencial da GC é coordenar o conhecimento existente e redistribuí-lo uniformemente por toda a organização. Isso se mostra especialmente relevante no setor público, que detém um vasto acervo de conhecimentos técnicos (Lartey et al., 2021).

A iniciativa da International Organization for Standardization (ISO), por meio da norma ISO 30.401 (2018), traz definições sobre a conversão e a transformação do conhecimento, caracterizando-as como atividades sistemáticas com objetivo de apoiar um sistema de gestão do conhecimento. As definições presentes na referida norma e as propostas por Nonaka & Takeuchi (1995) apresentam semelhanças.

A GC nas organizações é um tema complexo em ciências sociais, dada a diversidade de concepções que incluem orientações ao processo, às pessoas, ao sistema ou à tecnologia

(Xanthopoulou et al., 2023). É importante destacar que as ferramentas que utilizam tecnologias - como computadores, *internet*, *data mining* - integram as boas práticas de GC. Essas ferramentas contribuem tanto para a gestão das empresas quanto para a gestão do conhecimento produzido e adquirido (Oliva e Kotabe, 2019). Além disso, possibilitam o reuso de conhecimento codificado e facilitam comunicações que permitem a criação, compartilhamento, armazenamento e uso do conhecimento (Lee & Choi, 2003).

Construída sobre as perspectivas de ser a GC entendida como um processo ou objeto, o avanço dos estudos sobre o tema incluiu o fator humano como elemento observado, vez que é a visão humana elemento central na implementação da GC (Dhanhani & Naqbi, 2022), sendo mais do que digitalização de documentos, configuração de sistemas ou aplicação de tecnologia da informação - TI (Yeh et al., 2006).

A GC tem reconhecida relevância no ambiente corporativo, seja público ou privado, estando intrinsecamente ligada ao fator humano, culturalmente orientado e tratado como resposta para problemas societais complexos (Chong et al., 2011; Laihonen et al., 2023; Salleh et al., 2011). Também auxilia as organizações a enfrentarem novos desafios e a implementarem novas práticas de gestão, resultando em melhorias de processos, produtos e serviços para a sociedade (Batista, 2012).

Facilitadores são conceituados como mecanismos organizacionais para desenvolver o conhecimento de forma consistente (Lee & Choi, 2003) e dar suporte ao planejamento e implantação da GC (Joshi & Chawla, 2019) através de um contexto a ser oferecido pela organização de maneira a permitir que a espiral do conhecimento ocorra (Nonaka & Takeuchi, 1995), enquanto obstáculos são fatores que bloqueiam a implementação de uma ideia vital para o desenvolvimento de uma associação (Kaldeen, 2019). Os facilitadores e os obstáculos à GC serão tratados adiante neste trabalho.

Organizações do setor público existem para prestar serviços essenciais e possuem motivações para competir que não são baseadas exclusivamente no lucro (Lartey et al., 2021). A GC em organizações do setor público apresenta algumas peculiaridades quando comparadas ao setor privado, contemplando alguma complexidade em suas estruturas e processos e a sofrer interferências políticas e maior influência dos governos, do Tesouro e das responsabilidades sociais. (Marques et al., 2019; Mc Evoy et al., 2019).

A despeito da importância da GC para as organizações, enquanto muito se produziu para o setor privado, há lacunas a serem estudadas na GC do setor público (Ganapathy et al., 2019;

Pepple et al., 2022), não obtendo a devida atenção de pesquisadores do tema (Laihonen et al., 2023). A literatura indica que os investimentos em GC no setor público receberam aumento, mas sem a contrapartida de evidências empíricas dos possíveis impactos no volume entendido como necessário para compreensão do fenômeno (Mc Evoy et al., 2019; Pee & Kankanhalli, 2016). Apesar dos estudos apontarem para um baixo volume de publicações, percebe-se uma tendência de aumento nas pesquisas neste campo (Xanthopoulou et al., 2023).

A GC nas organizações do setor público é elemento central para a formulação de políticas de desenvolvimento - como segurança pública e serviços de saúde - auxiliando no atendimento das exigências para que tais organizações inovem na entrega de serviços assim como melhorem seu desempenho (Pee & Kankanhalli, 2016). Além disso, o setor público possui objetivos voltados para o bem-estar da sociedade, sendo esperado que o valor gerado ao alcançar esses objetivos seja revertido para os cidadãos. As organizações públicas também utilizam informações para a tomada de decisões, que são de natureza distinta das adotadas pelas organizações privadas (Laihonen et al., 2023).

É importante ressaltar o papel da TI, que dentre outros papéis facilita a criação e ampliação de redes – inclusive transnacionais - de forma a compartilhar o conhecimento através das fronteiras nacionais, permitindo a colaboração em questões globais (Pee & Kankanhalli, 2016). Contudo, mesmo organizações públicas que possuem estruturas de TI adequadas podem encontrar dificuldades para executar de forma apropriada os processos de captura, criação, armazenamento e compartilhamento do conhecimento (Ganapathy et al., 2019), visto não ser um fator exclusivo para o sucesso da GC.

As polícias frequentemente tratam de investigações dependentes de intenso conhecimento, sendo necessário o desenvolvimento de competências em GC, em especial o compartilhamento do conhecimento, para o sucesso de suas missões. Este desenvolvimento ocorre tanto no âmbito organizacional como individual, com a melhoria na capacidade dos investigadores em solucionar casos. Além disso, a relevância da GC se estende à esfera ambiental, tanto nacional quanto internacional, devido à globalização do crime organizado, embora o fluxo do conhecimento possa ser mais lento quando atravessa fronteiras (Adekannbi & Bello, 2021; Birdi et al., 2020).

A disponibilidade de conhecimento é essencial para o sucesso da investigação policial, representando um desafio significativo para a GC em uma atividade que depende intensamente deste recurso (Gottschalk, 2006; Luen & Al-Hawamdeh, 2001). Quando se trata de GC nas

atividades investigativas da polícia, a tendência é haver foco em procedimentos e diretrizes que permitam conhecer fatos e a obtenção de evidências (Dean et al., 2006). A atividade policial é complexa e possui caráter pluralista, devendo também atender às expectativas de redução dos crimes e da sensação de insegurança (Abrahamson & Goodman-Delahunty, 2014).

Em complemento, no que tange a atividades investigativas da polícia, a TI faz-se necessária para auxiliar na GC (Gottschalk, 2006; Luen & Al-Hawamdeh, 2001) e na agilidade requerida para a realização da investigação, que pode ser dividida em duas fases: a primeira focada na obtenção de evidências suficientes para a prisão do suspeito e a segunda na obtenção de evidências e testemunhas que levem a convicções sobre o fato investigado, o que torna importante não apenas capturar informações, mas também permitir que sejam acessadas (Gottschalk, 2006).

A norma ISO 30401 (2018) busca oferecer entendimento comum sobre GC, apresentando seus conceitos, princípios e elementos centrais, criando um suporte para as organizações estruturarem suas estratégias sobre a matéria (Carvalho et al., 2020). A norma conceitua GC como "gestão no que diz respeito ao conhecimento", por meio de uma abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados, que incluem a otimização da identificação, criação, análise, representação, distribuição e aplicação do conhecimento para gerar valor organizacional (ISO, 2018), definição adotada por este trabalho. A opção pela citada norma justifica-se por ser um modelo proposto internacionalmente e que visa auxiliar a implementação de sistemas de GC nas organizações. A Tabela 1 traz os elementos que compõem o conceito de GC na norma ISO 30401/2018:

Tabela 1 - Elementos do conceito de GC na norma ISO 30.401:2018

Elemento do Conceito de GC	Fatores		Elemento do Conceito de GC	Fatores
EC1	Gestão voltada ao conhecimento		EC5	Análise
EC2	Abordagem holística e sistêmica		EC6	Representação
EC3	Identificação		EC7	Distribuição
EC4	Criação		EC8	Aplicação

Fonte: o autor, baseado na norma ISO 30401(2018)

Legenda:

EC1 - Gestão voltada ao conhecimento
EC2 - Abordagem holística e sistêmica
EC3 - Identificação
EC4 - Criação
EC5 - Análise
EC6 - Representação
EC7 - Distribuição
EC8 – Aplicação

2.2.2. Facilitadores e Obstáculos à Gestão do Conhecimento

Os facilitadores são fatores críticos que colocam os conceitos de GC em prática de maneira a torná-la efetiva (Ho, 2009). Eles contribuem para formar um sistema capaz de estimular os membros da organização a ampliarem seus conhecimentos, transporem as barreiras ao crescimento e encorajá-los a compartilhá-los (Yeh et al., 2006), estabelecendo um ambiente propício a iniciativas que promovam inovação (Shehzad et al., 2022) e o desenvolvimento constante do conhecimento (Lee & Choi, 2003). Esses facilitadores são necessários para o sucesso da implementação dos processos de GC (Nordin et al., 2009; Sahibzada & Mumtaz, 2023).

Facilitadores referem-se a estruturas administrativas que permitem a gestão da aprendizagem organizacional e dos sistemas de GC (Kaldeen, 2019). São categorizados em internos e externos. Internamente, liderança, cultura organizacional e sistemas de recompensa desempenham papéis fundamentais, com a cultura organizacional emergindo como o fator mais influente (Pham et al., 2023; Shehzad et al., 2022). Externamente, competidores, parceiros comerciais, clientes e influências governamentais impulsionam a GC, especialmente nas cadeias de suprimento globais (Özlen, 2021).

A literatura sobre GC destaca o compartilhamento e a criação de conhecimento como elementos essenciais, ambos fortemente influenciados pela liderança, que se mostra um facilitador crítico desses processos (Goswami & Agrawal, 2023). A cultura organizacional, crucial para estabelecer valores necessários à inovação sustentável, é complementada pela importância da TI (Lee & Choi, 2003; Ho, 2009; Yeh et al., 2006) e por canais de comunicação individuais, coletivos, dentro ou fora da organização, educação e treinamento, além do interesse do servidor em participar da GC (Birdi et al, 2020; Dhanhani & Naqbi, 2022; Gaur et al., 2019; Kaldeen 2019; Salleh et al., 2011; Smith & Johnson 2023; Syed-Ikhsan & Rowland 2004). *Frameworks* de GC frequentemente integram esses elementos, destacando a sinergia entre os aspectos humanos e técnicos na eficácia da GC (Heisig 2009).

No Brasil, o modelo de GC proposto para a administração pública identifica fatores cruciais para o sucesso da GC, incluindo liderança, que reforça a visão e estratégias, estruturas de governança, tecnologia para gestão e comunicação do conhecimento, educação e capacitação das pessoas envolvidas, e processos que transformam insumos em produtos e facilitam todas as fases da GC (Batista, 2012). Este

modelo sublinha a interdependência entre tecnologia, processos, liderança e desenvolvimento humano para o sucesso da GC.

A norma ISO 30401 (2018) afirma que os facilitadores devem apoiar os objetivos do sistema de GC, priorizando a cobertura dos fatores capital humano, processos, tecnologia e infraestrutura, governança, e cultura de GC. Contudo, os diversos autores na literatura propõem fatores distintos, não havendo um padrão definitivo de facilitadores e obstáculos para a GC, lacuna esta que a norma ISO 30401/2018 busca preencher. O Quadro 1 apresenta exemplos de facilitadores à GC. Para fins deste trabalho foi adotado o termo "fatores", pois a literatura não é unânime ao definir um termo que indique a aglutinação de facilitadores ou obstáculos em algo como grupos temáticos para fins de organização.

Quadro 1 - Exemplos de facilitadores à GC obtidos na literatura

EXEMPLOS DE FACILITADORES	REFERENCIAS SELECIONADAS
Apoio da liderança à cultura de compartilhamento do conhecimento	Chong et al. (2011); Xanthopoulou et al. (2023)
A presença de canais formais de comunicação com outras instituições para permitir a troca de informações	Birdi et al. (2020); Dhanhani & Naqbi (2022)
Evidência da participação ativa do servidor em redes sociais promovendo a circulação de informações que subsidiam suas atividades	Dhanhani & Naqbi (2022); Kaldeen (2019); Smith & Johnson (2023)
Utilização de novas Tecnologias da Informação e Internet	Kaldeen (2019)
O (alto) nível educacional e o conhecimento especializado dos empregados	Kaldeen (2019); Smith & Johnson (2023); Syed-Ikhsan & Rowland (2004)
Cultura corporativa para a GC	Özlen (2021); Syed-Ikhsan & Rowland (2004)
A existência de Infraestrutura de Tecnologia da Informação e Comunicação	Chong et al. (2011); Dhanhani & Naqbi (2022); Syed-Ikhsan & Rowland (2004)
Posicionamento dos trabalhadores nas funções / Rotatividade das funções	Syed-Ikhsan & Rowland (2004)
Conter avaliações e medições contínuas no uso de redes sociais para processos de GC	Dhanhani & Naqbi (2022)
A efetividade das práticas aplicadas na GC para documentar e compartilhar as melhores práticas para o projeto	Dhanhani & Naqbi (2022)
Fluxos de comunicação	Syed-Ikhsan & Rowland (2004)

Busca por atender expectativas de clientes/usuários	Özlen (2021)
Diretivas políticas	Syed-Ikhsan & Rowland (2004)
A existência de cursos e treinamentos na área de atuação do servidor	Kaldeen (2019); Salleh et al (2011); Smith & Johnson (2023); Syed-Ikhsan & Rowland (2004)
Manifestação da habilidade e do Interesse dos servidores em Adquirir, Compartilhar e Utilizar Conhecimentos	Birdi et al. (2020); Dhanhani & Naqbi (2022); Gaur et al. (2019); Smith & Johnson (2023); Syed-Ikhsan & Rowland (2004)

Fonte: o autor, adaptado do quadro teórico conceitual

Obstáculos à GC incluem comportamentos dos empregados como a falta de compartilhamento de conhecimento e confiança, frequentemente ligados à ausência de recompensas e reconhecimento adequados (Salleh et al., 2011). Outras barreiras envolvem a escassez de pessoal especializado e resistência ao uso de tecnologias percebidas como inseguras, tal qual *e-mails* e bancos de dados obsoletos.

Os obstáculos são fatores que bloqueiam a criação e o compartilhamento de conhecimento, variando de acordo com o contexto organizacional e não restritos a uma lista definitiva, evidenciando a complexidade e a extensão desses desafios na implementação eficaz da GC (Kaldeen, 2019; Rios-Ballesteros & Fuerst, 2022). A literatura raramente conecta facilitadores e obstáculos no contexto de um projeto, e considera tecnologia e cultura organizacional tanto como facilitadores como obstáculos ao compartilhamento do conhecimento (Alves et al., 2022).

Rotatividade de pessoal, sigilo legal, falta de uniformidade em relação a informações e conhecimento, priorização de execução de tarefas em detrimento da GC, ausência de políticas de GC, comunicação ineficiente sobre fontes de conhecimento, falta de comprometimento da liderança, de recursos adequados, de confiança em relação aos outros e falta de vontade ou motivação para GC são exemplos de obstáculos (Abrahamson & Goodman-Delahunty, 2014; Alves et al., 2022; Ashok et al., 2021; Birdi, 2020; Dhanhani & Naqbi, 2022; Kaldeen, 2019; Oliva, 2014; Rios-Ballesteros & Fuerst, 2022; Seba et al., 2012; Smith & Johnson, 2023; Syed-Ikhsan & Rowland, 2004; Xanthopoulou et al., 2023). O Quadro 2 apresenta exemplos de obstáculos à GC.

Quadro 2 - Exemplos de obstáculos à GC obtidos na literatura

EXEMPLOS DE OBSTÁCULOS	REFERÊNCIAS SELECIONADAS
Falta de vontade ou motivação para compartilhar informações ou conhecimento	Abrahamson & Goodman-Delahunty (2014); Dhanhani & Naqbi (2022); Oliva (2014)
O impacto da mudança nas estruturas organizacionais na motivação para GC	Dhanhani & Naqbi (2022)
Liderança não comprometida com GC	Abrahamson & Goodman-Delahunty (2014); Xanthopoulou et al. (2023)
Falta de confiança em relação aos outros na GC	Asrar-ul-Haq, M., & Anwar, S. (2016); Dhanhani & Naqbi (2022); Rios-Ballesteros & Fuerst (2022)
Priorização de execução de tarefas em detrimento da aquisição do conhecimento	Alves et al. (2022); Abrahamson & Goodman-Delahunty (2014); Kaldeen (2019); Seba et al., (2012); Smith & Johnson (2023)
Comunicação ineficiente sobre fontes de informação e de conhecimento e sobre iniciativas de capacitação	Birdi et al. (2020); Oliva (2014)
Ausência de políticas para promover a gestão e compartilhamento de conhecimento	Alves et al. (2022); Dhanhani & Naqbi (2022); Kaldeen (2019); Oliva (2014)
Falha em fornecer treinamento adequado sobre como usar ferramentas de Tecnologia da Informação para compartilhar conhecimento	Dhanhani & Naqbi (2022)
Restrição do acesso às informações necessárias para a atividade investigativa em decorrência do sigilo legal	Abrahamson & Goodman-Delahunty (2014); Ashok et al. (2021); Syed-Ikhsan & Rowland (2004)
A influência externa de fatores como crises globais para a GC	Dhanhani & Naqbi (2022); Özlen (2021)
Ausência de sistemas de GC por falta de orçamento	Al-Ahbabi et al. (2017); Birdi et al. (2020)
Decisões políticas (não comprometidas com a GC)	Xanthopoulou et al. (2023)
Rotatividade de pessoal sem transmissão de conhecimento	Kaldeen (2019); Smith & Johnson (2023); Syed-Ikhsan & Rowland (2004)
Falta de recursos adequados para Gestão do Conhecimento	Dhanhani & Naqbi (2022); Rios-Ballesteros & Fuerst (2022)
Falta de uniformidade nos procedimentos de compartilhamento de informações e conhecimento	Abrahamson & Goodman-Delahunty (2014)

Fonte: o autor, adaptado do quadro teórico conceitual

Como demonstrado, a literatura sobre GC se firmou trazendo vários fatores em que se pode focar os estudos, sendo possível apontar liderança, pessoas e tecnologia como as mais citadas. Ocorre que há necessidade de, por vezes, especificar se os facilitadores

ou obstáculos estão no âmbito da organização ou fora de seu controle, se passam por decisões internas ou se estão relacionadas somente ao indivíduo e seu comportamento.

2.2.3. Níveis de Análise em estudos de Administração Pública

Assim como no modelo proposto por Oliva (2014), que avalia as barreiras à GC em grandes empresas no Brasil com divisões nos níveis humano, organizacional e ambiental, Jilke et al. (2019) defende uma classificação semelhante para pesquisas em Administração Pública. Essa classificação facilita a integração das pesquisas na citada área em qualquer um desses níveis ou mesmo em todos simultaneamente. Tais níveis de análise permitem indicar precisamente as implicações teóricas e empíricas nas pesquisas neste campo de estudo.

Os estudos em Administração Pública são analisados em três níveis distintos: o nível individual, focado nos processos cognitivos, comportamentos e interações dos indivíduos; o nível organizacional, essencial devido às ações coletivas nas atividades governamentais; e o nível ambiental, que examina as estratégias governamentais e seus impactos na estrutura do Estado (Jilke et al., 2019). Essa estrutura permite categorizar facilitadores e obstáculos à GC, possibilitando uma análise detalhada das influências de cada nível e identificando áreas para melhorias. O Quadro 3 traz a descrição dos níveis apresentados.

Dada a estrutura dos níveis de análise em estudos de Administração Pública, o presente trabalho adotará a nomenclatura de Níveis de Análise Individual, Organizacional e Ambiental para classificar facilitadores e obstáculos à GC, com o objetivo de explorar as implicações específicas de cada nível dentro das organizações, permitindo uma análise mais aprofundada dos aspectos que podem ser melhorados ou replicados no contexto da GC.

Oliva (2014) faz considerações sobre a pouca influência dos fatores ambientais como obstáculos à GC, apresentando os fatores individuais como os mais relevantes, seguido pelos fatores organizacionais. Já Dhanhani & Naqbi (2022), dos cinco principais obstáculos identificados, os dois mais presentes se referem à organização.

Quadro 3 - Níveis de análise em estudos de Administração Pública

NÍVEL DE ANÁLISE	DESCRIÇÃO
MICRO (Individual)	Está relacionado aos aspectos cognitivos, comportamentais e emocionais dos indivíduos, influenciado por áreas como psicologia e administração pública. Ele é fundamental para entender a motivação e a tomada de decisão no serviço público, especialmente na atuação dos trabalhadores de linha de frente. Por ser o nível mais básico de análise, contribui para a compreensão dos níveis organizacional e ambiental.
MESO (Organizacional)	O nível organizacional (ou meso) envolve o estudo de grupos como equipes, agências ou organizações, sendo central na Administração Pública por tratar de ações coletivas. Ele busca entender como essas interações influenciam o desempenho e a prestação de serviços. Além disso, serve como ponte entre os níveis individual e macro nas pesquisas.
MACRO (Ambiental)	O nível macro analisa estratégias governamentais, decisões políticas e como essas influenciam os níveis individual e organizacional. Ele busca entender o ambiente político e sua influência sobre administradores públicos, atuando como moderador entre os demais níveis. Embora historicamente menos explorado, é essencial para compreender como indivíduos em posições de autoridade moldam a governança democrática.

Fonte: baseados nos conceitos de *Jilke et al. (2019)*

2.2.4. Segurança Cibernética e Crimes Cibernéticos

O tema da segurança cibernética ganhou grande interesse e relevância na literatura, que oferece diversas definições sobre o assunto (Von Solms & Van Niekerk, 2013). Nesta subseção, serão apresentadas definições de segurança cibernética, exemplificados conceitos de ameaças cibernéticas, e citados documentos selecionados a partir da literatura que recomendam boas práticas para minimizar tais ameaças.

As diretivas para a segurança de sistemas de informação e redes (NIS - *Network and Information Systems*), são regulamentações da União Europeia que estabelecem requisitos de segurança e notificação de incidentes para operadores de serviços essenciais e fornecedores de serviços digitais. A norma NIS2, uma atualização da diretiva original, define segurança cibernética como o conjunto de atividades necessárias para proteger redes e sistemas de informação, incluindo seus usuários e outras pessoas impactadas. Esta revisão busca aumentar a resiliência contra ameaças cibernéticas (Conselho da União Europeia [CEU], 2022). A NIS2 representa uma iniciativa legislativa da União Europeia, especificamente voltada para reforçar a segurança cibernética, estendendo seu alcance a mais setores e aumentando as obrigações das partes afetadas (Vandezande, 2024).

Por sua vez, a norma ABNT NBR ISO/27032:2015[2] define segurança cibernética como a preservação da confidencialidade, integridade e disponibilidade das informações no espaço cibernético. O referido espaço cibernético, conforme exibido na Nota 1 deste estudo, é o ambiente complexo resultante da interação de pessoas, softwares ou serviços na *internet* por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe qualquer forma física (Associação Brasileira de Normas Técnicas [ABNT], 2015).

As referências da NIS2 e da ISO 27032:2015 visam oferecer não apenas definições, mas também orientações práticas para prestadores de serviço, infraestruturas críticas, organizações e pessoas, tanto em contextos comerciais quanto domésticos (ABNT, 2015; CEU, 2022). A introdução da NIS2 foi motivada pela necessidade de se enfrentar as mudanças ocorridas em poucos anos, especialmente após a massiva adoção do teletrabalho durante e logo após a pandemia de COVID-19, demonstrando a necessidade de um nível mais alto de resiliência para a proteção de estruturas essenciais (Vandezande, 2024).

O teor das referências citadas no parágrafo anterior busca minimizar a exposição das organizações e usuários finais a ameaças cibernéticas. Ameaça cibernética pode ser entendida como "uma circunstância, um evento ou uma ação potenciais suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas" (CEU, 2022).

A respeito dessas ameaças cibernéticas, Almeida et al. (2023) apresenta como exemplos não exaustivos o sequestro de dados (*ramsonware)*, uso de códigos digitais maliciosos (*malware)* e o emprego de engenharia social (*phishing),* conforme detalhado no Quadro 4, sendo as principais ameaças vinculadas aos crimes cibernéticos o *phishing* (22%) e o *malware* (20%) (Djenna et al., 2023).

[2] É importante salientar que a norma internacional ISO/IEC 27032 recebeu atualização em 2023, ainda não gerando reflexos nas normas ABNT, sendo a última versão disponível a ABNT NBR ISO/IEC 27032:2015, baseada na norma ISO/IEC 27032:2012 (ABNT, 2015).

Quadro 4 - Exemplos de Ameaças Cibernéticas

Ameaça Cibernética	**Descrição detalhada da ameaça cibernética**
Ramsomware	Modalidade de ameaça cibernética comum, que explora vulnerabilidades. O agente invasor sequestra e criptografa o sistema da vítima (inclusive o disco rígido); posteriormente, exige resgate em dinheiro (criptomoedas) para supostamente fornecer a chave de reversão da criptografia de dados.
Malware	Trata-se de um *software* malicioso (também identificado como vírus ou *Trojan*) que pode capturar credenciais, roubar dados, identificar outros alvos na rede e criptografar ou destruir dados, entre outros danos. Ele é infiltrado na organização por meio de um agente invasor que explora vulnerabilidades em dispositivos de usuário final, anexos de e-mail, páginas da web, serviços em nuvem, dispositivos móveis e mídias removíveis.
Phishing	Consiste numa ameaça consubstanciada por *e-mail* (ou outra forma de interação por meio eletrônico) capaz de enganar o destinatário, apelando para determinado interesse em informação. Trabalhadores do setor público que não adotem cautelas ou não estejam precavidos podem abrir anexos de e-mail ou mensagens eletrônicas e ficar exposto aos efeitos desse tipo de ameaça.

Fonte: Almeida et al. (2023)

Os procedimentos e controles de segurança cibernética visam reduzir a exposição a ameaças cibernéticas através de práticas estabelecidas em documentos e *frameworks*, incluindo a ISO/IEC 27032:2015 e a NIS2, além do *framework* do *National Institute of Standards and Technology* (NIST) (Barret, 2018). Essas diretrizes permitem que organizações, independentemente do tamanho ou setor, adotem medidas robustas de segurança cibernética para minimizar riscos, demonstrando que a implementação de boas práticas é crucial para quaisquer empresas (Ogar et al., 2023).

A criação de autoridades governamentais especializadas em segurança cibernética não só melhora a prevenção contra ameaças, mas também possibilita informar à população sobre os fundamentos e as maneiras pelas quais organizações comerciais e governamentais protegem seus dados sensíveis contra os ataques cibernéticos (Kalogiannidis et al., 2023). Exemplos de estruturas governamentais são a ENISA (Parlamento Europeu e Conselho da União Europeia, 2019), a *UK National Cyber Security Center - NCSC* (Kemp, 2023) e a CISA, congênere americana que tem como foco os setores de infraestrutura críticas (Jimoh, 2023).

No Brasil, o Decreto nº 11.856, de 26 de dezembro de 2023, estabeleceu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança, visando promover medidas preventivas contra ameaças cibernéticas (Brasil, 2023c). Em nível setorial, reguladores têm autoridade para criar normas que fortaleçam a prevenção de ameaças cibernéticas em entidades tanto públicas quanto privadas. Um exemplo é a Resolução nº

4.893 do Conselho Monetário Nacional (CMN), de 26 de fevereiro de 2021, que determina às instituições financeiras autorizadas pelo Banco Central do Brasil a implementação de políticas de segurança cibernética (CMN, 2021).

2.2.4.1. Crimes Cibernéticos

O crime cibernético pode ser compreendido de diversas maneiras. Uma definição envolve a atividade criminal na qual serviços ou aplicativos no espaço cibernético são utilizados para cometer um crime, ou quando são eles mesmos o alvo do crime. O espaço cibernético também pode ser a fonte, ferramenta, alvo ou local de um crime (ABNT, 2015). Outra abordagem define estas ações como tentativas de burlar a segurança de sistemas de informação para acessar dados sobre seus usuários, diferenciando-se de outros crimes pela inviabilidade de sua execução sem esses sistemas (Arpaci & Ateş, 2023).

O espaço cibernético se tornou lócus para a realização de crimes cibernéticos. Exemplos de atividades que podem ensejar tais crimes são a engenharia social (Hweidi & Eleyan, 2023), roubo de identidade, ameaças por códigos digitais maliciosos, fraudes por meio digital, inclusive com a publicação de páginas falsas na *internet* (Mishra, 2023), crimes de ódio, crimes sexuais, fraudes, roubo de dados pessoais, de identidade, fraudes bancárias (Arpaci & Ateş, 2023) e *defacement*, onde a invasão busca alterar a página *web* de uma organização, demonstrando falhas graves em sua cibersegurança (Perkins et al., 2023), também chamado de cibervandalismo (Ogar et al., 2023).

O crime cibernético envolve ações planejadas por indivíduos ou grupos contra usuários, empresas ou governos, e é amplificado por comunidades *online* que compartilham recursos e coordenam ataques sofisticados (Yarovenko et al., 2023). Os perpetradores, conhecidos como *hackers*, ganham eficácia e senso de pertencimento através dessas redes, que incentivam ataques em larga escala e reconhecem seus feitos (Hoffman et al., 2024).

A criminalidade cibernética apresenta um crescimento alarmante, de seis vítimas por hora em 2001 para noventa e uma em 2021. Reconhecido pelo Fórum Econômico Mundial em 2022 como um dos dez maiores riscos globais, estes crimes são vistos como um entrave ao desenvolvimento econômico, causando prejuízos estimados em US$ 6 trilhões em 2023, ultrapassando os lucros do tráfico de drogas ilícitas (Yarovenko et al.,

2023; Brici e Achim, 2023; Kassab et al., 2023). A Índia, por exemplo, registrou aumento significativo de registros de crimes cibernéticos, em especial ligados a transações monetárias fraudulentas e notícias falsas em redes sociais, passando de 12.317 registros em 2016 para 50.035 em 2020, em aumento ligado ao período da pandemia de COVID-19 (Sharma et al., 2023).

No Brasil, segundo o Fórum Brasileiro de Segurança Pública (2024), houve um aumento de 13,6% no crime de estelionato por meio eletrônico no ano de 2023 frente ao ano anterior, chegando a 235.393 ocorrências registradas por polícias civis estaduais. Além disso, os crimes de pornografia infanto-juvenil registraram 2.790 ocorrências, representando aumento de 42,6% de 2022 para 2023. Importante salientar que, segundo o documento consultado, nem todos os estados informaram seus dados. Sobre os dados da Polícia Federal, em todo o ano de 2023 e até o mês de agosto de 2024 foram realizadas 1.316 operações, mais de 98% referentes a material de abuso infantil (Polícia Federal, 2024b).

É relevante observar que o número de investigações policiais iniciadas é significativamente menor do que os incidentes de segurança reportados pelo CERT.br, definido como um Grupo de Resposta a Incidentes de Segurança de responsabilidade nacional, que registrou 621.537 notificações de incidentes cibernéticos em 2024 (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [CERT.br], 2024).

Cabe ressaltar que crime é um conceito jurídico definido por legislação específica, originado de leis locais relativas ao uso de tecnologia e computadores. Essa definição legislativa não se opõe ao que a literatura descreve sobre crimes cibernéticos (Kleve et al., 2011). A este respeito, a Convenção de Budapeste é um documento editado no âmbito da União Europeia, contemplando definições e tipificações que contribuem para o entendimento e o combate aos crimes cibernéticos. O tratado permite a integração de outros países fora da União Europeia por força de seu artigo 37, o que possibilitou a adesão do Brasil, resultando no Decreto nº 11.491, de 12 de abril de 2023, que incorpora a referida convenção no ordenamento jurídico brasileiro. O citado decreto, em seu Capítulo 2, apresenta sugestões para que se tornem criminosas determinadas ações (Brasil, 2023a).

A legislação brasileira já define uma série de crimes cibernéticos, sendo o Código Penal (Brasil, 1940) o principal veículo, além do Estatuto da Criança e do Adolescente

(Brasil, 1990), que trata de crimes envolvendo mídias de abuso sexual infantil. É digno de registro que a primeira legislação sobre o tema é a Lei 12.737/2012 (Brasil, 2012), chamada Lei Carolina Dieckmann, que altera o Código Penal inserindo crimes ligados à invasão de dispositivos, obtenção, adulteração ou destruição de dados sem autorização.

Em complemento, o combate aos crimes cibernéticos exige conhecimentos específicos, abrangendo aqueles sobre segurança cibernética, prevenção contra ameaças cibernéticas, bem como sobre forense digital, descrito como a capacidade de preservar evidências e analisar dispositivos eletrônicos, tornando possível extrair informações encriptadas e ocultas no meio digital (Djenna et al., 2023).

Por fim, para atuar no combate ou na repressão aos crimes cibernéticos, a polícia necessita do devido treinamento, podendo, ainda, compartilhar o conhecimento a respeito das atividades investigativas sobre tais crimes, tanto por meio de cooperação internacional, a exemplo daquela que abrange a cooperação de esforços por meio da Interpol como o *Interpol Innovation Centre*, que permite o fluxo de conhecimento sobre novas tecnologias e ameaças cibernéticas (Interpol, [s.d.]-c) quanto na própria jurisdição do país em que a polícia atua.

Cabe esclarecer que a PF é responsável por representar as forças de segurança brasileiras frente à Interpol (Interpol, [s.d.]-a), além de tratar da cooperação com polícias e organizações estrangeiras - como a integração ao programa "*No More Ransom*" de iniciativa da Europol (PF, 2023c); a atuação conjunta com a Polícia Judiciária de Portugal no combate ao crime de abuso sexual infantojuvenil (PF, 2024c); e a assinatura de acordo de cooperação policial com a polícia inglesa *National Crime Agency*, visando o combate a uma série de tipos criminais, incluindo financeiros e cibernéticos (PF, 2024f).

No Brasil, as investigações policiais são previstas no art. 144 da Constituição Federal e ficam à cargo das polícias civis (PC), uma por Estado, a quem cabe apurações de infrações penais, excetuadas as militares e ressalvadas a competência da União. Cabe à PF, dentre outras funções, apurar "crimes cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme" (Brasil, 1988).

Desta forma, no caso de crimes cibernéticos, a polícia que ficará a cargo da investigação será definida pelo local do crime, por exemplo, a localidade do endereço IP identificado, em geral sob responsabilidade da PC. Existindo potencial internacionalidade, interesse da União ou repercussão interestadual, cabe atuação da PF.

Cada PC é responsável por desenvolver sua estrutura de acordo com o que melhor atende ao interesse público. Algumas criam delegacias especializadas (Polícia Civil do Distrito Federal, 2024); outras, núcleos ou divisões (Polícia Civil do Estado do Paraná, 2022) enquanto algumas outras não diferenciam as investigações de crimes cibernéticos dos demais crimes.

Na PF, a DCIBER é dividida em quatro eixos temáticos: repressão ao abuso sexual infantil; aos crimes de ódio pela Internet (ainda não existindo formalmente na estrutura da PF); às fraudes bancárias por meios eletrônicos; e repressão a crimes de alta tecnologia. No âmbito das SRs, existem as delegacias especializadas em crimes cibernéticos, as Deleciber, responsáveis pelas investigações de crimes cibernéticos em qualquer dos eixos mencionados (Brasil, 2023a).

Cada Coordenação é responsável pela doutrina e disponibilização de meios para o cumprimento dos objetivos nas investigações de crimes cibernéticos. Como exemplo, há o Projeto Tentáculos, que centraliza as notícias-crime sobre fraudes bancárias em repositório único, evitando retrabalho e possibilitando vínculos de autoria nas investigações decorrentes (Febraban, 2023). Outro exemplo é o uso da base de dados ICSE[3], gerenciada pela Interpol, que permite identificação de crianças e adolescentes vítimas de exploração sexual pelas polícias de mais de 68 países, evitando retrabalho e possibilitando a identificação do local e dos autores dos crimes (Interpol, [s.d.]-b).

Findo o quadro teórico-conceitual, é apresentado o modelo proposto para o estudo dos facilitadores e obstáculos à GC na perspectiva de policiais federais (Figura 1).

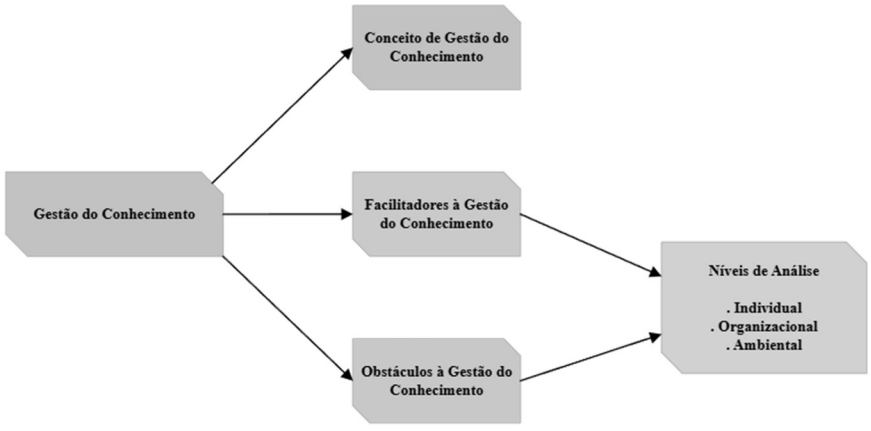


Figura 1 - Modelo proposto para o estudo.

Fonte: o autor, considerando o quadro teórico.

[3] International Child Sexual Explotaition

2.3. MÉTODOS E TÉCNICAS

2.3.1. Tipologia da pesquisa

Este trabalho traz a realização de uma pesquisa descritiva. O caráter descritivo possibilita coletar informações sobre os conceitos ou variáveis a que se referem, com o compromisso de caracterizar uma população ou um fenômeno específico (Sampieri et al., 2013). Em adição, a pesquisa adota uma abordagem qualitativa, permitindo estudar ambientes e trazer reflexões sobre o fenômeno pesquisado (Sampieri et al., 2013). A coleta de dados da pesquisa é transversal, num momento específico do tempo, em uma espécie de "fotografia" do objeto pesquisado (Zangirolami-Raimundo et al., 2018). O nível de análise é organizacional, e a organização selecionada como lócus do estudo é descrita na sequência.

2.3.2. Perfil dos participantes e da organização

A organização que foi selecionada como lócus do estudo é a PF. Justifica-se a escolha dessa organização por suas atribuições e envolvimento com a repressão de crimes cibernéticos em nível interestadual no País e em investigações abrangendo a cooperação internacional do Brasil com outros países, conforme citado na Seção 2.2.4deste estudo. A estrutura da PF possui quatorze diretorias e vinte e sete Superintendências Regionais (SR), uma em cada capital estadual (PF, 2023b).

Cada Superintendência da PF possui em sua estrutura uma Delegacia de Repressão a Crimes Cibernéticos (Deleciber). Há também a Divisão de Investigações e Operações Especiais (DIOE), integrando a estrutura da DCIBER, com funções semelhantes às Deleciber nas SRs, totalizando vinte e oito locais que atuam direta e especificamente com investigações criminais no tema Crimes Cibernéticos na Estrutura da PF (Apêndice C).

Em relação ao perfil dos potenciais participantes do estudo, foi realizado sorteio que apontasse: o primeiro entrevistado, se do Órgão Central (DCIBER) ou SR, e neste último caso se lotado em Setec ou Deleciber. Na PF, a Carreira Policial Federal é composta por cinco cargos com funções distintas (Brasil, 1996). Dos cinco cargos, somente os PCFs atuam em estrutura administrativa separada dos demais nas SRs, sendo lotados exclusivamente nos SETECs. Apenas os PCFs da área de conhecimento em TI (PF, 2021b) atuam em investigações envolvendo crimes cibernético. Os demais cargos

citados ocupam funções nas Deleciber. A Tabela 2 apresenta os dados demográficos dos entrevistados, capturados nas perguntas 5 a 7 do roteiro.

Tabela 2 - Perfil dos entrevistados

Tipo de lotação	Cargo	Tempo de PF (em anos)	Tempo de atuação em crimes cibernéticos (em anos)
SR	PCF	18	14
DCIBER	DPF	10	6
SR	APF	9	4
DCIBER	APF	21	20
SR	PCF	4	4
DCIBER	DPF	16	2
SR	DPF	22	7
DCIBER	PCF	19	2

Fonte: dados da pesquisa.

Legenda:

SR – Superintendência Regional
DCIBER – Diretoria de Combate a Crimes Cibernéticos
APF – Agente de Polícia Federal
DPF – Delegado de Polícia Federal
PCF – Perito Criminal Federal

2.3.3. Caracterização do instrumento de pesquisa

A pesquisa se utilizou de roteiro de entrevista semiestruturado (Apêndice B) para coleta de dados primários. Tal opção decorreu da necessidade de se obter mais informações sobre o tema do trabalho, exigindo um roteiro, mas devendo permitir flexibilidade ao entrevistador para colher dados dos entrevistados (Sampieri et al., 2013), por serem capazes de expressar suas práticas, maneiras de pensar e ser representante de seu grupo ou fração dele (Poupart, 2014).

O roteiro possui oito perguntas, divididas em dois módulos. O primeiro módulo aborda cinco perguntas, dentre elas sobre o conceito de GC, os facilitadores e os obstáculos à GC nas atividades investigativas envolvendo crimes cibernéticos. As perguntas do primeiro módulo baseiam-se nos autores descritos no quadro teórico-conceitual, especialmente na Subseção 2.2. O segundo módulo apresenta três perguntas de caráter demográfico, baseadas em Tormin (2022) e Menezes (2020).

2.3.4. Procedimentos de coleta dos dados

A coleta de dados primários foi precedida de teste piloto, que consistiu em realizar entrevistas iniciais para validar o questionário com três servidores da PF que já atuaram em atividades investigativas de crimes cibernéticos ou envolvidos diretamente em Gestão do Conhecimento (Alexandre & Coluci, 2011). Após essa validação, foram realizadas as entrevistas com os servidores da PF previamente inseridos no perfil dos participantes descritos na Seção 2.3.2, envolvidos nas atividades investigativas relativas a crimes cibernéticos.

Na etapa seguinte deu-se início as entrevistas com servidores da PF, complementada pela coleta de documentos públicos e internos não sigilosos do referido órgão de segurança pública. Com o objetivo de equilibrar a representatividade entre as entrevistas realizadas com servidores de superintendências e órgão central, estas foram conduzidas de forma alternada entre os setores do órgão central DCIBER (coordenações e divisão) e as SRs. A ordem das entrevistas respeitou a sequência original definida no sorteio, iniciando pelo órgão central e alternando com SRs. Os convites foram feitos aos chefes dos citados setores, solicitando que ou participassem ou indicasse quem poderia participar. Os nomes de chefes e coordenadores foram obtidos através das portarias de nomeação publicadas no Diário Oficial da União.

A quantidade final de entrevistados foi de oito participantes, conforme perfil ilustrado na Tabela 2. Essa quantidade foi estabelecida com base no critério de saturação teórica, definido como o ponto em que novas entrevistas não acrescentam informações relevantes à pesquisa (Falqueto et al., 2018; Rego et al., 2018). O período de coleta ocorreu entre 19 de novembro de 2024 e 15 de janeiro de 2025. As entrevistas foram conduzidas de maneira remota por meio da plataforma *Microsoft Teams*, que foi selecionada devido à dispersão geográfica dos entrevistados e por ser a ferramenta padrão utilizada pela organização. Esta plataforma possibilitou o registro dos conteúdos audiovisuais para consultas futuras, além de permitir a transcrição automática dos diálogos, que posteriormente foram revisados manualmente.

Os dados secundários não sigilosos utilizados para subsidiar o exame da estrutura organizacional da PF, dos conceitos de GC, e de seus facilitadores e obstáculos em atividades investigativas relativas à crimes cibernéticos foram obtidos de fontes internas e externas. As fontes internas consistiram em normativos que abordam a GC ou algum dos fatores evidenciados nas entrevistas. Já as fontes externas incluíram documentos

publicamente disponíveis no sítio eletrônico da PF, com destaque para informações sobre o organograma da instituição, com foco em superintendências, delegacias e DCIBER, além de legislações relacionadas a crimes cibernéticos. Uma descrição dos principais documentos coletados consta do Apêndice D.

Por fim, a coleta das entrevistas e de documentos internos foram devidamente autorizadas pela DCIBER e pela DIREN – Diretoria de Ensino – responsável pelo acompanhamento de pesquisas referentes à PF, com encaminhamento de pedido efetuado nos termos do Apêndice A.

2.3.5. Procedimentos para análise dos dados

Os dados foram analisados com o emprego da análise de conteúdo, que pode ser entendida como um conjunto de técnicas de análise de comunicações visando obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores que permitam a inferência de conhecimentos relativos às condições de produção e recepção destas mensagens (Bardin, 1977, p. 42).

A análise de conteúdo foi conduzida após a transcrição dos dados coletados por meio de entrevistas, utilizando-se a ferramenta *Atlas.ti* para apoiar a codificação das categorias e organização dos dados. Os códigos foram definidos com base no conceito de GC e nos Quadros 1 e 2, todos apresentados no quadro teórico-conceitual, e posteriormente ajustados mediante a identificação de novos elementos emergentes durante a análise, utilizando a abordagem de grade mista, sendo frases e parágrafos tratados como unidades de análise, não se limitando a perguntas específicas (Vergara, 2006).

Adicionalmente, os facilitadores e os obstáculos relacionados à GC em atividades investigativas de crimes cibernéticos, conforme exemplificados nos Quadros 1 e 2 do quadro teórico-conceitual, foram analisados. O uso da grade mista permitiu aprimorar os facilitadores e os obstáculos oriundos da literatura, enriquecendo a análise dos dados coletados. Todos os facilitadores e os obstáculos mencionados pelos entrevistados foram corroborados pela literatura.

Após a identificação dos facilitadores e dos obstáculos à GC em atividades investigativas relativas a crimes cibernéticos, foi possível classificar os referidos facilitadores e os obstáculos segundo os níveis de análise, com base no proposto por Jilke

et al (2019), conforme o Quadro 3, no Quadro Teórico-Conceitual. O resultado foi apresentado em figura que indica os facilitadores e os obstáculos apontados pelos entrevistados e a qual nível organizacional pertencem.

Os procedimentos para análise de dados envolveram a triangulação das fontes de evidências das entrevistas e dos documentos coletados (Yin, 2015), pontuando-se com o teor do Quadro Teórico-Conceitual. A cada entrevista foi feita a revisão da transcrição, a codificação dos trechos relevantes para a pesquisa, fossem tais elementos já citados por outros entrevistados ou novos (Falqueto et al., 2018; Fontanella et al., 2011; Rego et al., 2018). Por fim, os resultados são apresentados com emprego de mapas mentais, figuras e quadros para auxiliar a descrição, análise e discussão dos resultados.

2.4. RESULTADOS E DISCUSSÃO

Nesta subseção, apresentam-se os resultados oriundos das análises realizadas com base nas evidências descritas na metodologia. A Tabela 3 ilustra o processo de alcance da saturação teórica ao longo das entrevistas, indicando a presença ou ausência de novos elementos relevantes para o estudo, considerando três categorias: conceito de GC, Facilitadores da GC e Obstáculos à GC.

O conceito de GC foi considerado saturado na terceira entrevista, tendo sido todos os elementos extraídos da definição contida na norma ISO 30401:2018 citados e nenhum elemento diverso foi incluído pelos demais entrevistados. Da mesma forma, os Facilitadores também chegam à saturação teórica na terceira entrevista. For fim, os Obstáculos apresentam saturação na sexta entrevista, assim como a saturação geral. As entrevistas foram levadas até o total de oito, de maneira a reforçar a percepção de saturação, por não haver mais inclusões de elementos novos considerando a sétima e oitava entrevistas (Fontanella et al., 2011).

Tabela 3 – Elementos inclusos e recorrentes nas entrevistas, segmentado por categorias.

Categoria	E1	E2	E3	E4	E5	E6	E7	E8	Total de Recorrências
Conceito de GC	I	I	I	R	R	R	R	R	5
Facilitadores da GC	I	I	I	R	R	R	R	R	5
Obstáculos à GC	I	I	I	R	I	I	R	R	3
Total de Inclusões	3	3	3	0	1	1	0	0	

Fonte: dados da pesquisa

Legenda:

E1 – Entrevista 1
E2 – Entrevista 2
E3 – Entrevista 3
E4 – Entrevista 4
E5 – Entrevista 5
E6 – Entrevista 6
E7 – Entrevista 7
E8 – Entrevista 8
I – Elementos incluídos
R – Elementos recorrentes

Feitas as considerações sobre saturação teórica, apresenta-se estrutura do trabalho a seguir: a Seção 2.4.1 apresenta o detalhamento dos resultados sobre o conceito de gestão do conhecimento na visão dos policiais federais. A Seção 2.4.2 trata os facilitadores e os obstáculos na percepção dos policiais federais. Por fim, a Seção 2.4.3 apresenta os níveis de análise, com base nos facilitadores e obstáculos previamente identificados.

2.4.1. Conceito de Gestão do Conhecimento na visão de policiais federais

O objetivo de questionar o conceito de GC aos entrevistados foi verificar suas percepções sobre o assunto, bem como a viabilidade de obter respostas sobre seus facilitadores e obstáculos, evitando dificuldades caso o conceito fosse completamente desconhecido. Para analisar o conteúdo apresentado pelos entrevistados sobre GC, percebeu-se ser adequado confrontá-lo com conceito que advém da norma ISO (2018), que trata de Sistemas de Gestão do Conhecimento e traz definições sobre o tema. Buscando compreender quais elementos do conceito de GC da ISO 30401 foram apontados pelos entrevistados, assim como outros possíveis conceitos, apresenta-se a Tabela 4, indicando quais elementos do conceito de GC foram incluídos (**I**), são recorrentes (**R**) ou estão ausentes (A) nas entrevistas:

Tabela 4 - Presença e ausência de elementos do conceito de Gestão do Conhecimento por entrevistado

Elemento do Conceito de GC	E1	E2	E3	E4	E5	E6	E7	E8	Total de Recorrências
EC1	**I**	**R**	A	A	A	**R**	A	A	**2**
EC2	A	**I**	A	A	**R**	**R**	A	A	**2**
EC3	A	**I**	**R**	**R**	A	A	A	**R**	**3**
EC4	A	**I**	**R**	A	A	A	A	**R**	**2**
EC5	A	**I**	A	A	**R**	A	A	A	**1**
EC6	**I**	A	**R**	A	**R**	A	A	A	**2**
EC7	A	A	**I**	**R**	A	A	**R**	**R**	**3**
EC8	**I**	**R**	A	A	**R**	**R**	**R**	**R**	**5**
Total de Inclusões	**3**	**4**	**1**	**0**	**0**	**0**	**0**	**0**	

Fonte: o autor, considerando dados da pesquisa

Legenda:

EC1 - Gestão voltada ao conhecimento
EC2 - Abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados
EC3 - Identificação do conhecimento
EC4 - Criação do conhecimento
EC5 - Análise do conhecimento
EC6 - Representação do conhecimento
EC7 - Distribuição do conhecimento
EC8 - Aplicação do conhecimento
I – Inclusão do elemento de conceito
R – Recorrência do elemento de conceito
A - Ausência de citação do elemento de conceito

A seguir são apresentadas as análises sobre os elementos de conceito de GC resultantes das entrevistas realizadas:

EC1 - Gestão voltada ao conhecimento: a GC visa as maneiras que organizações criam e usam conhecimento, o processo de ativar o conhecimento tácito e explícito, mas não há uma definição única aceita (Alves et al., 2022; ISO, 2018). Um dos entrevistados afirma que "é exatamente conhecimento da unidade ficar na unidade". Na Política de Gestão do Conhecimento (PGC) criada pelo órgão, o conceito encontrado é definido como conjunto de processos sistematizados que incrementam a habilidade de gestores e servidores em criar, organizar e transferir conhecimento (DPF, 2015).

EC2 - Abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados: ao definir a GC como holística, entende-se ser algo que abrange toda a organização, suas estruturas, seu pessoal, sua cultura, em busca de capturar o conhecimento tácito, transformá-lo e difundi-lo como conhecimento explícito, o que envolve vários níveis da organização e fora dela (ISO, 2018; Nonaka & Takeuchi, 1995). Na fala de um dos entrevistados foi encontrada no trecho "desde a mais básica do nível operacional até o nível estratégico da organização. Não só procedimentos, né? Mas procedimentos, ferramentas, recursos humanos, todos os elementos.". No PGC, a definição de GC traz a ideia de articulação dos processos sistematizados que podem até mesmo incluir o cidadão como produtor de conhecimento coletivo (DPF, 2015).

EC3 - Identificação do conhecimento: a identificação do conhecimento deve levar em conta o que é importante para a organização, quais conhecimentos trazem valor às suas atividades e a quem deve ser dirigido (ISO, 2018). Um dos depoimentos trouxe a questão do uso do conhecimento: "vamos lá, a gente tem 2 tipos de conhecimento, na minha opinião, [...] dentro da PF: o conhecimento de inteligência e um conhecimento formal, que é o que está ali nos inquéritos [...]". O PGC fala em coletar conhecimentos que possam auxiliar em tomada de decisões.

O uso da expressão “formal” na resposta está relacionado ao conteúdo dos inquéritos policiais, que possuem formalidades estabelecidas pela legislação e se restringem a informações que embasem uma eventual acusação criminal, enquanto inteligência se preocupa com informações que contribuam para tomada de decisões em várias instâncias e, em seu limite, contribuir para investigações policiais (PF, 2022a). Nesse sentido, a distinção entre conhecimentos formais e de inteligência configura-se como uma etapa da identificação do conhecimento (EC3), permitindo reconhecer quais dados são relevantes e qual encaminhamento devem receber.

EC4 - Criação do conhecimento: está ligado à obtenção de conhecimento não existente na organização ou mesmo adaptação do conhecimento já existente (ISO, 2018). Um dos depoimentos, ao se referir a um material apreendido durante uma operação, traz a percepção de que “o grande diferencial é a gente estudar vínculos que a pessoa não sabe que a gente conhece, para desenvolver um trabalho melhor”, ou seja, a adaptação de um conhecimento já existente. No PGC há expressamente o verbo criar descrito no conceito de GC (DPF, 2015).

EC5 - Análise do conhecimento: se trata de manejar conhecimentos inválidos ou obsoletos que podem levar a erros ou ineficiência, mas passa também por curadoria, arquivamento e atualização (ISO, 2018). A fala “[...] essa agenda é informação demais. Talvez não coubesse adicionar no dossiê desse cara. Só que informação é poder [...]” traz consigo a questão da seleção do que deve ou não constar formalmente na investigação, o que deve ser organizado e arquivado para uso futuro – auxiliando em tomada de decisão, como rumos de outras investigações, no caso – ou simplesmente descartado. No conceito apresentado no PGC, não há explicitamente “análise”, mas os verbos “coletar” e “organizar” constantes no texto, com objetivo de apoiar tomada de decisão (DPF, 2015), implica em analisar se o conhecimento é válido e se é aplicável naquele momento ou deve ser guardado para uso futuro.

EC6 - Representação do conhecimento: o conhecimento externo é aquele que foi analisado, combinado e sistematizado para que sua transmissão seja acessível, compreensível e útil, que pode se dar por manuais, aulas, vídeos instrucionais, por exemplo (ISO, 2018; Nonaka & Takeuchi, 1995). Nas entrevistas, é trazido na fala “é documentar e armazenar, né? O histórico, né? Do conhecimento e procedimentos da unidade”. No PGC pode-se apontar o termo “organizar” como reconhecimento da necessidade da representação do conhecimento.

EC7 - Distribuição do conhecimento: trata-se das maneiras como o conhecimento flui na organização. Pode tanto ser por meio de sistemas de computadores, conversas, documentos, materiais didáticos, de forma a possibilitar sua aplicação, difusão e recombinação (ISO, 2018; Nonaka & Takeuchi, 1995). O trecho de entrevista "gerir o conhecimento é... é não só produzir o conhecimento, mas é tornar isso acessível e de maneira segura" apresenta este elemento, que se encontra nos termos "transferir" e "compartilhar" da definição de GC no PGC (DPF, 2015).

EC8 - Aplicação do conhecimento: é o uso efetivo do conhecimento para gerar novos conhecimentos, auxiliar no processo decisório e aumentar as habilidades dos trabalhadores, através do "aprender fazendo" (ISO, 2018; Nonaka & Takeuchi, 1995). A afirmação coletada em entrevista "tenho que ter um histórico disso internamente que possa ser acompanhado e correlacionado para uso futuro" deixa clara a ideia de gerar conhecimento para que possa ser aplicado. A PGC indica claramente aplicações possíveis para o conhecimento, como tomada de decisões ou gestão de políticas públicas (DPF, 2015).

Chamam a atenção alguns comentários afirmando que o compartilhamento deve ser com segurança, que envolve negar acesso a partes não interessadas. Tal percepção envolve tanto a própria ideia de gestão - que inclui proteção de ativos da organização - como a consciência do relevante papel da distribuição do conhecimento e seu fluxo:

> Gestão do conhecimento acho que passa, necessariamente pelo compartilhamento com responsabilidade, né? Compartilhamento com observância das regras de sigilo [...]
>
> [...] primeiro colocar todo esse conhecimento, seja ele de inteligência, ou seja, ele formal, em algum lugar, em algum banco de dados e tornar isso acessível. Obviamente que tem toda a segurança, né?

Em relação aos documentos pesquisados sobre o tema, a PF insere a GC em sua agenda ao instituir a PGC (DPF, 2015). Esta portaria traz conceituação alinhada com o conceito de GC adotado neste trabalho, mesmo sendo focada no processo decisório e na investigação policial.

Desta forma, considera-se que todos os entrevistados demonstraram adequada compreensão sobre o conceito de GC durante as entrevistas, permitindo o alcance do objetivo específico 1.

A Figura 2 apresenta o mapa mental sobre as percepções do conceito de GC. A figura traz os conceitos adotados pelo trabalho, buscando dar ideia do número de citações pelo tamanho das figuras de cada conceito. Na figura relativa à "identificação do conhecimento", foi apresentada a diferenciação percebida entre conhecimentos ligados ao inquérito policial e aqueles ligados ao conceito de inteligência.

Figura 2 - Mapa mental dos conceitos percebidos pelos entrevistados sobre Gestão do Conhecimento
Fonte: o autor, a partir de dados da pesquisa.

2.4.2. Facilitadores e Obstáculos à Gestão do Conhecimento na percepção de policiais federais

Esta subseção apresenta os resultados da descrição e análise dos facilitadores da GC e dos obstáculos à GC. Inicialmente, a Tabela 5 apresenta facilitadores resultado da identificação dos facilitadores da GC nas entrevistas.

Tabela 5 – Inclusões e Recorrências dos facilitadores da Gestão do Conhecimento por entrevistas

Facilitador da GC	E1	E2	E3	E4	E5	E6	E7	E8	Total de Recorrências
F1	**I**	**R**	**R**	**R**	**R**	**R**	A	**R**	**6**
F2	**I**	A	**R**	A	A	A	A	**R**	**2**
F3	**I**	A	A	A	A	A	A	**R**	**1**
F4	A	**I**	**R**	**R**	A	**R**	**R**	**R**	**5**
F5	A	**I**	A	**R**	A	A	A	**R**	**2**
F6	A	**I**	A	**R**	A	**R**	**R**	**R**	**4**
F7	A	A	**I**	A	A	**R**	**R**	A	**3**
Total de inclusões	**3**	**3**	**1**	**0**	**0**	**0**	**0**	**0**	

Fonte: o autor, considerando dados da pesquisa.

Legenda de Facilitadores (F):

F1 - A existência de Infraestrutura de Tecnologia da Informação e Comunicação
F2 - Apoio da liderança à cultura de compartilhamento do conhecimento
F3 - A existência de cursos e treinamentos na área de atuação do servidor
F4 - A presença de canais formais de comunicação com outras instituições para permitir a troca de informações
F5 - O (alto) nível educacional e o conhecimento especializado dos empregados
F6 - Manifestação da habilidade e do Interesse dos servidores em Adquirir, Compartilhar e Utilizar Conhecimentos
F7 - Evidência da participação ativa do servidor em redes sociais promovendo a circulação de informações que subsidiam suas atividades
I – Inclusão do facilitador
R – Recorrência do facilitador
A - Ausência de citação do facilitador
E1 a E8 – Entrevistas

O primeiro fator citado na Tabela 5 é **F1**, indicando 'a existência de Infraestrutura de Tecnologia da Informação e Comunicação' (TIC)**.** Algumas citações relacionadas a este fator são "Tudo hoje em dia tem na intranet [...]", "Bom, são os nossos sistemas, né? Nosso sistema, informação, *software* específico... nós temos hoje, por exemplo, na Criminalística, o Siscrim [...]" e "não sei se você tem conhecimento disso [...] mas no nosso caso a gente tem a *Wiki*[4]".

A estrutura de TIC deve promover a captura e tanto do conhecimento tácito como explícito, além de facilitar e dar suporte ao compartilhamento do conhecimento por toda a organização (Chong et al., 2011, Syed-Ikhsan & Rowland, 2004). Foi o fator de maior recorrência, até mesmo com entrevistados nominando ferramentas oficiais utilizadas,

[4] "Wiki" é termo "usado para designar uma coleção de documentos em hipertexto que fornece suporte à produção colaborativa de conteúdos a partir de um browser". Ramalho, L., & Tsunoda, D. F. (2007, 28–31 de outubro). *A construção colaborativa do conhecimento a partir do uso de ferramentas wiki*. In Anais do VIII Encontro Nacional de Pesquisa em Ciência da Informação (GT3 – Mediação, circulação e uso da informação, pp. 1–9). Salvador, BA, Brasil. Recuperado de http://enancib.ppgci.ufba.br/artigos/GT3--240.pdf

indicando haver um esforço da organização neste sentido. A PF conta com estrutura de TIC que oferece ferramentas colaborativas para construção e difusão de conhecimento (2022b). Conforme o depoimento, em virtude de haver informações relevantes acessíveis pela infraestrutura de TIC, é possível obter o conhecimento necessário para a atuação diária.

O segundo fator da Tabela 5 é o **F2**, que diz respeito a 'Apoio da liderança à cultura de compartilhamento do conhecimento', trazidas por alguns entrevistados, como em "[...] O gestor percebeu a importância disso [...] então acho que às vezes o gestor perceber a importância dessa gestão é fundamental", além de:

> [...] Passa pela realização de cursos, treinamentos, a elaboração de manuais que é... dentro da DCIBER a gente tem um manual de contatos com os provedores, né? Que facilitou nosso trabalho, é uma lista de provedores que a gente, quando precisa fazer uma consulta ao provedor, a gente sabe para onde encaminhar o contato.

O apoio da liderança é um dos principais fatores facilitadores à GC, devendo tanto os níveis de supervisão como a alta gestão estarem comprometidos, o que demanda formação para incorporarem a GC em suas decisões (Chong et al., 2011; Xanthopoulou et al., 2023). Os depoimentos que apontam este facilitador fazem referência a posturas da alta gestão do órgão, até por alguns entrevistados ocuparem cargos de supervisão. Formação contínua de gestores consta no planejamento estratégico na PF (2024e), mas nada diretamente vinculado à GC.

O terceiro fator da Tabela 5, **F3**, dispõe sobre 'a existência de cursos e treinamentos na área de atuação do servidor', e pode ser identificado nas falas como "Capacitação, os cursos que são oferecidos na área é um facilitador, porque ele promove a distribuição do conhecimento." e:

> [...] aí em 2024 a gente já começou a... já tinha os fluxos mais ou menos melhor mapeados dentro da diretoria, né? E aí a gente começou a também pensar na capacitação das Deleciber principalmente.

A oferta por parte da organização e consequente participação em cursos e treinamentos permitem que o investigador esteja em linha com novas tecnologias e formas criminosas de atuação, além das técnicas tradicionais de investigação policial (Pagon, 1996), sendo apontado como relevante para o enriquecimento do conhecimento organizacional, pois os investigadores que não recebem constante treinamento não conseguem criar, usar e compartilhar conhecimento (Syed-Ikhsan & Rowland, 2004). A

oferta de cursos e estrutura necessária está prevista em documentos pesquisados (ANP, 2021).

O Fator **F4** aponta para a presença de canais formais de comunicação com outras instituições para permitir a troca de informações. Algumas das referências apresentadas por entrevistados incluem "A exemplo da CBAN, que tem muito contato com outras instituições, eu acho que é bem por aí [...]" e:

> É, e por fim, eu acho que podia citar também a cooperação Internacional e Nacional, não é? Acho que a gente tem uma experiência muito boa em mapear essa necessidade de cooperação, tanto Polícia Federal, polícia civil, quanto a Polícia Federal, a polícia de outros países. Porque, afinal de contas, no cibernético, a gente vai precisar da cooperação Internacional.

A existência de canais de comunicação com outras instituições é de grande relevância para o acesso ao conhecimento (Grant, 1996). Podem ser levadas em conta como partes interessadas, por exemplo, outras polícias, brasileiras ou não; organizações internacionais, como a Interpol; ou mesmo organizações privadas, como bancos (Dhanhani & Naqbi, 2022). O contato com outras instituições consta no Planeamento Estratégico da organização (PF, 2024e).

O Fator **F5,** o (alto) nível educacional e o conhecimento especializado dos empregados, é relacionado com a formação prévia e o conhecimento individual como ferramenta com poder de influenciar as práticas de GC e as atividades rotineiras (Kaldeen, 2019). Apresenta-se depoimentos referentes a tal fator, "[...] aí quando o colega lá que tá já com algum conhecimento bom, adiantado de informática, isso é ótimo. É, já consegue adiantar bastante coisa" e:

> Os agentes e escrivães de recentemente... terem pedido *[em concurso]* um conhecimento muito grande de administração e contabilidade. Isso aí adiantava algumas perguntas que poderiam ser sacadas *[percebidas]* pelos peritos. Mas um colega que talvez não tivesse esse conhecimento prévio podia demorar mais para fazer.

Importa considerar que a literatura indica que ausência de educação formal é um obstáculo ao fluxo do conhecimento em algumas áreas de atuação (Smith & Johnson, 2023). Educação indica um conhecimento mais amplo, formal (Abrahanson et al., 2014; Pagon, 1996). A exigência educacional para os cargos – todos de nível superior - é definida em normativos, havendo flexibilidade da organização para direcionar os conhecimentos específicos desejáveis no momento da seleção de novos servidores (Brasil, 1996; PF, 2021c).

O Fator **F6,** a manifestação da habilidade e do interesse dos servidores em adquirir, compartilhar e utilizar conhecimentos se refere à atitude do indivíduo frente ao conhecimento. Considerações apresentadas por alguns entrevistados:

> Mas isso também é muito da minha personalidade, né? Eu não tenho curso, por exemplo, de análise de RIF, quebra bancária, mas eu nunca me deixei limitar por isso, sempre corria atrás, [...] quando não tinha coisa ligava até Brasília.

> Eu não enxergo na nossa área de cibernético uma restrição pessoal dos colegas em compartilhar conhecimento. Não enxergo isso. Isso é uma percepção minha, tá? Diferentemente de quem trabalha na área de enfrentamento à corrupção, tem muito, é, vamos dizer assim, freios em compartilhar conhecimento em relação à pessoa.

Assim sendo, buscar, compartilhar e utilizar conhecimentos como comportamento individual é relevante para a GC na organização (Alves et al., 2020; Dhanhani & Naqbi, 2022; Gaur et al., 2019; Smith & Johnson, 2023; Syed-Ikhsan & Rowland, 2004). Na documentação pesquisada, este fator se contrapõe a problemas com o comprometimento de servidores com a PF detectados em diagnóstico interno, mas não citado especificamente como relacionado à GC (PF, 2023d).

Por fim, o Fator **F7** da Tabela 5, evidência da participação ativa do servidor em redes sociais promovendo a circulação de informações que subsidiam suas atividades, envolve os contatos interpessoais, privados ou em grupos, como instrumento para GC (Dhanhani & Naqbi, 2022). Alguns dos depoimentos obtidos: "Na nossa área, eu acho que ela foi bem melhor do que nas outras áreas, né? Não só porque a gente tem grupos de *WhatsApp*, *Teams*... [...]" e:

> Há uma troca muito boa, entendeu? Então, claro, existe um contato pessoal que eu acho que pode ter a melhor ferramenta do mundo digital. Às vezes, o contato pessoal é importante, não é? É importante para facilitar essa disseminação do conhecimento.

Tais contatos são relevantes mesmo que geograficamente distantes, através de instrumentos de TIC, como aplicativos de comunicação e correio eletrônico (Kaldeen, 2019), que permitem a troca de conhecimento entre os envolvidos na etapa de socialização do conhecimento (Nonaka & Takeuchi, 1995). Documentos internos da PF dão conta de uso relevante tanto das ferramentas e *e-mail* quanto de reuniões, comunicações em grupo e privadas através de aplicativo contratado pela organização (PF, 2022b).

Em relação aos obstáculos à GC, a Tabela 6 apresenta um mapa de inclusões (**I**), recorrências (**R**) e ausências (A) dos obstáculos nas entrevistas.

Tabela 6- Inclusões e Recorrências dos obstáculos identificados por entrevistas

Fator Obstáculo	E1	E2	E3	E4	E5	E6	E7	E8	Total de Recorrências
O1	**I**	A	A	A	A	**R**	**R**	A	**2**
O2	**I**	**R**	**R**	A	**R**	A	**R**	A	**4**
O3	**I**	A	**R**	A	A	A	A	A	**1**
O4	A	**I**	A	**R**	A	A	**R**	**R**	**3**
O5	A	**I**	A	A	**R**	**R**	A	A	**2**
O6	A	**I**	**R**	**R**	A	**R**	A	A	**3**
O7	A	A	**I**	**R**	A	A	**R**	A	**2**
O8	A	A	**I**	**R**	**R**	A	A	A	**2**
O9	A	A	A	A	**I**	A	A	A	**0**
O10	A	A	A	A	A	**I**	A	A	**0**
Total de inclusões	**3**	**3**	**2**	**0**	**1**	**1**	**0**	**0**	

Fonte: o autor, considerando o quadro teórico.

Legenda de Obstáculos (O)

O1 - Rotatividade de pessoal sem transmissão de conhecimento
O2 - Restrição do acesso a informações necessárias para a atividade investigativa em decorrência do sigilo legal
O3 - Falta de uniformidade nos procedimentos de compartilhamento de informações e conhecimento
O4 - Priorização de execução de tarefas em detrimento da aquisição do conhecimento
O5 - Ausência de políticas para promover a gestão e compartilhamento de conhecimento
O6 - Comunicação ineficiente sobre fontes de informação e de conhecimento e sobre iniciativas de capacitação
O7 - Liderança não comprometida com GC
O8 - Falta de recursos adequados para Gestão do Conhecimento
O9 – Falta de confiança em relação aos outros na Gestão do Conhecimento
O10 - Falta de vontade ou motivação para compartilhar informações ou conhecimento
I – Obstáculo incluído
R – Recorrência do Obstáculo
A – Ausência de citação do facilitador
E1 a E8 – Entrevistas

O Fator **O1**, rotatividade de pessoal sem transmissão de conhecimento, registrado na Tabela 6, considera a movimentação de investigadores para outras atividades ou localidades sem que haja documentação ou compartilhamento por parte de quem sai para quem chega, se tornando um obstáculo dada a perda de conhecimento (Kaldeen, 2019, Smith & Johnson, 2023).

> Porque volta e meia um servidor, sai, é removido, né? E às vezes, o conhecimento tá com ele, né? E não, não fica na unidade, então muitos casos que passaram, né? Muito conhecimento que ele adquiriu na investigação, e isso aí pode se perder

> [...] unidades aqui como a nossa, onde tem muita rotatividade. Então, ferramenta, qualquer ferramenta, assim que promova gestão do conhecimento, é fundamental [...]

Como se pode observar, os depoimentos mostram ser uma constante a movimentação de pessoal, assim como a preocupação para que se aproveite o conhecimento daquele que sai. A rotatividade de pessoal por si só também é indicada como facilitador à GC, especialmente no setor público, por parte da literatura (Chong et al., 2011). Ocorre que para se tornar um facilitador à GC, a rotatividade de pessoal deve ser acompanhada da conversão do conhecimento tácito em explícito, caso contrário se torna um obstáculo em virtude da perda daquele conhecimento (Syed-Ikhsan & Rowland, 2004), o que foi indicado nas entrevistas.

Em diagnóstico interno, são apontados vários fatores negativos ligados à rotatividade de pessoal, como "falta de incentivo à permanência de servidores" e "dificuldade de retenção de servidores qualificados" (2023d), mostrando ser realidade na PF a movimentação de pessoal, mas nada diretamente ligado à GC.

O Fator **O2,** restrição do acesso a informações necessárias para a atividade investigativa em decorrência do sigilo legal, aparece em vários depoimentos. Abaixo alguns exemplos:

> Seria a parte de sigiloso também, né? Daí eu acho que a pesquisa não funciona para esses casos aí, tipo assim, eu, se eu tivesse interesse no caso, né? [...] São os problemas também, né, [...] da investigação policial, né? Do sigilo necessário. [...] parte da própria natureza intrínseca da investigação policial.

> Então, acho que o sigilo judicial dos casos é um obstáculo. É ao menos, parcial. Pro compartilhamento das informações, né? Para gestão desse conhecimento.

O obstáculo descrito em virtude do sigilo das investigações está previsto no art. 20 do Código de Processo Penal (Brasil, 1941), que engloba eventuais riscos para a investigação em virtude de vazamentos (Abrahamson & Goodman-Delahunty, 2014; Ashok et al., 2021; Syed-Ikhsan & Rowland, 2004). Foi o obstáculo com maior recorrência entre entrevistados, mesmo que sempre havendo ponderação sobre a inviabilidade de mudanças.

O Fator **O3, f**alta de uniformidade nos procedimentos de compartilhamento de informações e conhecimento, aparece em alguns depoimentos, como" de certa forma já indiquei algumas sugestões de como poderia ser melhorado, né? Mas é isso, é que nem tudo isso tem que ser uma... tem que ser de cima para baixo [...]" e "Então não morreu,

está morrendo o histórico das investigações dentro da polícia federal, é extremamente relevante esse conhecimento do histórico das investigações".

Este obstáculo trata de barreiras impostas ao fluxo do conhecimento pela própria organização por não valorizar a GC (Abrahamson & Goodman-Delahunty, 2014). Conforme os depoimentos apresentados, há expectativa que a alta gestão proponha meios para que conhecimentos da organização sejam disponibilizados e acessíveis aos interessados. Este fator é expresso de diferentes formas no diagnóstico interno da organização havendo menção expressa a "inexistência de gestão do conhecimento" (PF, 2023d).

O Fator **O4,** priorização de execução de tarefas em detrimento da aquisição do conhecimento, surge em quatro entrevistas. Alguns dos depoimentos são "[...] a gente evita, está tentando evitar que a unidade se encha de muitos casos, porque a gente vai perder a qualidade" e:

> Fora que as pessoas que trabalham na delegacia não ficam só voltadas para o serviço da Delegacia, tem outros serviços. É, e a gente tem que participar com missões fora, não é isso? Acaba dificultando que a pessoa que trabalhe continuamente na área aí, possa é... manter sempre atualizado esses conhecimentos, né?

O obstáculo em tela apresenta um problema comum no setor público, em especial nas polícias, que é o excesso de atividades a serem realizadas aliada à pressão por resultados, que acabam por não permitir um espaço para que o indivíduo adquira, gere e compartilhe conhecimento (Abrahamson & Goodman-Delahunty, 2014; Alves et al. 2022; Kaldeen, 2019; Seba et al., 2012; Smith & Johnson, 2023), fato que pode ser claramente identificado nas entrevistas. Cabe pontuar que dos cinco entrevistados que podem ser classificados como burocratas de rua, quatro apontaram tal obstáculo, o que não foi ponderado pelos entrevistados das coordenações.

Em diagnóstico interno, três fatores corroboram o obstáculo achado nas entrevistas: "gestão de pessoas ineficiente", "falta de estudos de dimensionamento da força de trabalho" e "falta de política de ingresso regular de servidores", apesar de não haver citação expressa sobre carga de trabalho (PF, 2023d).

O Fator **O5** faz referência a ausência de políticas para promover a gestão e compartilhamento de conhecimento, conforme se constata nos depoimentos a seguir:

“Então, por exemplo, tem um procedimento que eu faço. Aqui tá na minha cabeça, mas eu, poxa, eu posso fazer um pop? Como é para fazer um pop[5]?” e:

> Mas então vejo um colega lá mandando um e-mail para um problema que eu já tive, pô, vou parar responder, pode ser que eu não saiba explicar bem e tal. Deixa pra lá, né? [...] Vejo como obstáculo, né, de ter até um incentivo de dizer... não sei de que forma poderia incentivar isso. Vamos incentivar os colegas que nós estamos aqui, né? Na PF como um todo.

No caso, o obstáculo se refere a ausência de fomento ou apoio por parte da organização para que os servidores participem dos processos de GC. A cultura de gestão e de compartilhamento de conhecimento é apresentada na literatura como importante facilitador à GC, apresentada como regras não escritas, valores, princípios, normas e procedimentos na organização (Alves et al., 2022; Oliva, 2014). No diagnóstico interno da instituição são encontrados fatores como “ausência de cultura de dados” e “falta de manuais e difusão de boas práticas” (PF, 2023d).

O Fator **O6**, comunicação ineficiente sobre fontes de informação e de conhecimento e sobre iniciativas de capacitação, surge em algumas das respostas, como em “Então, se tem uma comunicação, uma comunicação falha, é, eu não vou ter uma gestão eficiente, né?” e:

> Então, a gente tenta criar mecanismos aí de melhorar a comunicação. Eu acho que isso também dificulta um pouco da gestão do conhecimento. Como é que o cara vai saber que tem um curso? Não chega lá na delegacia, fica lá na superintendência, né? Então eu acho que essa comunicação tem que melhorar, né? O compartilhamento de conhecimento, enfim, dentro da PF, acho que é isso.

O citado obstáculo indica problemas no fluxo de informações na organização, que se torna barreira para o conhecimento (Oliva, 2014). Sendo o conhecimento determinante para o sucesso nas atividades da organização, é relevante haver meios adequados para que o conhecimento flua e esteja disponível (Chong, 2019, Alves et al., 2022). Nos discursos há citações sobre comunicação pouco clara em relação a cursos oferecidos e onde encontrar conhecimento explícito. No diagnóstico interno, podem ser citados a “inexistência de cultura de multiplicação da capacitação” e “falta de manuais e difusão de boas práticas”, mas também a “cultura de resistência à utilização dos recursos

[5] POP: Procedimento Operacional Padrão. “[...] uma espécie de estudo técnico que procura descrever requisitos e atividades necessários para alcance de um determinado resultado esperado”. Ministério da Justiça e Segurança Pública. (2024, 10 de setembro). *Procedimento Operacional Padrão*. Recuperado de https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/pop/procedimento-operacional-padrao

disponíveis no *Microsoft Teams*" (PF, 2023d), que podem explicar essa desconexão entre eventuais informações disponibilizadas e a recepção por parte do servidor.

O Fator **O7**, liderança não comprometida com GC, em depoimentos como os abaixo**:**

> Muitas vezes, o pessoal que faz o curso, ele volta, não é utilizado em nada, né? Então, até o exemplo, [...] o colega fez 3 vezes o mesmo curso [..], mas quando chegava para fazer essa análise, quem fazia análise era um outro colega que nunca tinha feito o curso.
>
> Os cursos né? Muitas vezes, é um benefício, mas às vezes há uma dificuldade, não é, de você reunir o efetivo, da chefia liberar também, e participar desse compartilhamento de conhecimento às vezes, né?

Este obstáculo versa sobre problemas com lideranças, impedindo o fluxo de conhecimento e a própria GC (Abrahamson & Goodman-Delahunty, 2014) sendo necessário que a liderança apoie e fomente as iniciativas de GC que envolvam seus liderados (Seba et al., 2012). As referências negativas tratam dos treinamentos, em que por vezes não há liberação da chefia imediata para participação ou é enviado alguém que não atuará naquela área de conhecimento. "Desestímulo à capacitação", "gestores com perfil inadequado", além de "falta de treinamento em gestão e liderança para chefes e servidores em geral" estão consignados no diagnóstico interno da instituição (PF. 2023d), corroborando as percepções de alguns entrevistados.

O Fator **O8**, falta de recursos adequados para Gestão do Conhecimento, foi detectado em respostas como "Informações estarem espalhadas em sistemas muito diferentes, então é obstáculos de ter acesso, né?" e "[...] outro ponto de cada unidade de ter o seu próprio sistema que não se conversa, né?"

O obstáculo faz referência a recursos tecnológicos insuficientes, que se tornam barreiras à comunicação e compartilhamento do conhecimento, sendo a falta de integração de sistemas uma das características do conceito (Abrahamson & Goodman-Delahunty, 2014; Alves et al. 2022; Birdi et al., 2020; Dhanhani & Naqbi, 2022). Os depoimentos coletados apontam para a existência de uma estrutura adequada na PF, mas a falta de integração dos sistemas é um obstáculo claro ao conhecimento e à GC, fator identificado em diagnóstico interno como "falta de integração de dados" e "multiplicidade de sistemas não integrados" (PF, 2023d).

O Fator **O9**, falta de confiança em relação aos outros na Gestão do Conhecimento, foi identificado no seguinte depoimento:

> [...] hoje todo mundo tem acesso a todos os sistemas de pesquisa, mesmo assim ainda há obstáculos nesse ponto, porque "ah, vou compartimentar informação porque é de uma certa diretoria". [...] O mau uso, ele vai responder por aqui. Então a gente ainda tem essa inversão de valores assim: não, só vou liberar para alguns porque pode ter mau uso.

O fator aponta para a falta de confiança em relação aos outros dentro da organização referente ao conhecimento existente, até mesmo como forma de controle e poder (Asrar-ul-Haq & Anwar, 2016). Interessante perceber que a fala do entrevistado se refere a dados da organização como um todo, não apenas na área de crimes cibernéticos, indicando haver decisões de concessão de acesso a sistemas pautadas pelo medo de haver uso indevido. Nos documentos pesquisados, não se encontrou menção a tal obstáculo, talvez por estar atrelado a questões de sigilo na percepção da instituição.

Por fim, o Fator **O10**, falta de vontade ou motivação para compartilhar informações ou conhecimento, último apresentado na Tabela 66, é apresentado na seguinte fala:

> Então, não só o compartilhamento, porque temos a necessidade de compartimentar, né? [...] de saber o que compartilhar tem esse ponto, mas também tem aquela questão mesmo de ter pessoas mais suscetíveis a compartilhar, compartilhar no sentido de contribuir mesmo, né? Dizer, pô, vim aqui, ó, esse material aqui é legal, pô.

Este obstáculo refere-se à postura do indivíduo em relação ao compartilhamento de conhecimento, negando-se a fazê-lo, seja por crenças, falta de estímulo, seus valores pessoais, o que se torna importante barreira ao fluxo de conhecimento na organização (Abrahamson & Goodman-Delahunty, 2014; Dhanhani & Naqbi, 2022; Oliva, 2014). O diagnóstico interno da PF pode ter identificado o obstáculo, possivelmente relacionado a "desmotivação e reatividade de parte do efetivo" e "falta de comprometimento dos servidores com a instituição", porém não de maneira direta (PF, 2023d).

2.4.3. Níveis de análise dos facilitadores e obstáculos identificados

Identificados os facilitadores e obstáculos à GC, passa-se a classificação dos níveis de análise dos fatores percebidos pelos entrevistados. A classificação é uma forma de apresentar os fatores considerando taxonomia presente na literatura (Jilke et al., 2019; Oliva, 2014) e previamente citada na metodologia deste estudo, que os segmenta em individual, organizacional e ambiental. A Figura 4 apresenta os facilitadores e obstáculos identificados no nível individual. Foram identificados três fatores facilitadores e dois

obstáculos. A inclusão de tais fatores no citado nível advém dos elementos analisados: a educação e conhecimento individual, a habilidade, a capacidade e a ausência de vontade ou motivação, amoldando-se à descrição do nível de análise proposto, que é ligado ao indivíduo, atributos, comportamentos e interações (Jilke et al., 2019).

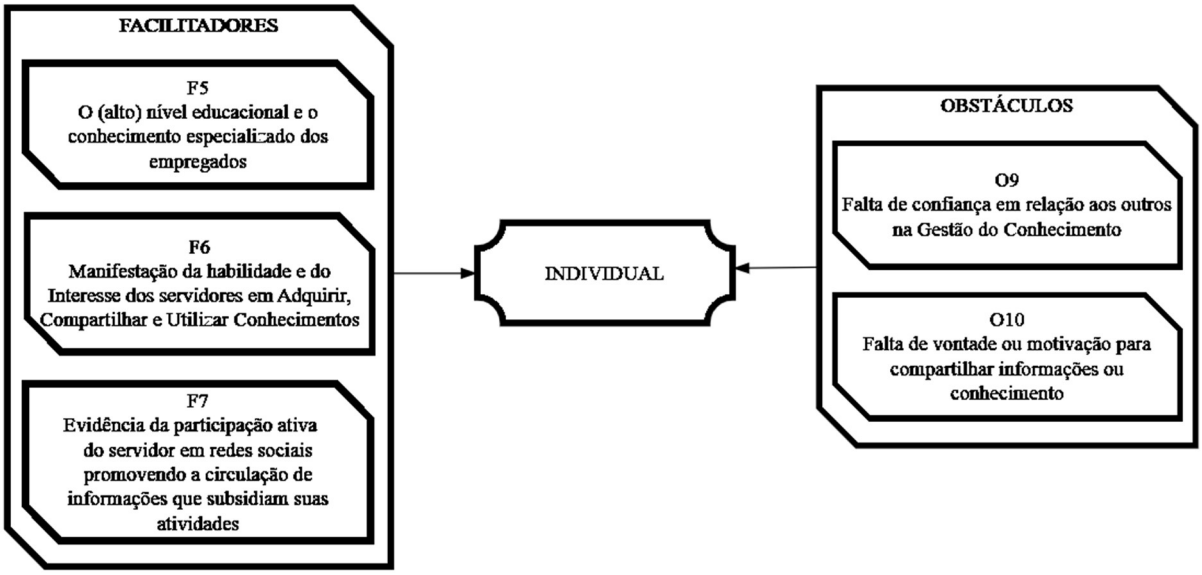


Figura 3 - Fatores no nível de análise individual identificados

Fonte: dados da pesquisa, considerando os resultados das tabelas 5 e 6

Adicionalmente, a Figura 5 apresenta quatro facilitadores e sete obstáculos classificados no nível organizacional, no total de onze, demonstrando preponderância de ações e características da organização como principal fonte de percepções dos entrevistados. Este nível engloba a relação entre indivíduos, grupos, organizações e suas estruturas, abarcando os atos de gestão, como existência de infraestrutura de TI, posicionamento e capacitação das lideranças e de liderados, comunicação institucional entre as estruturas internas e outras organizações (Jilke et al., 2019). A Figura 4 apresenta as conclusões sobre o nível organizacional.

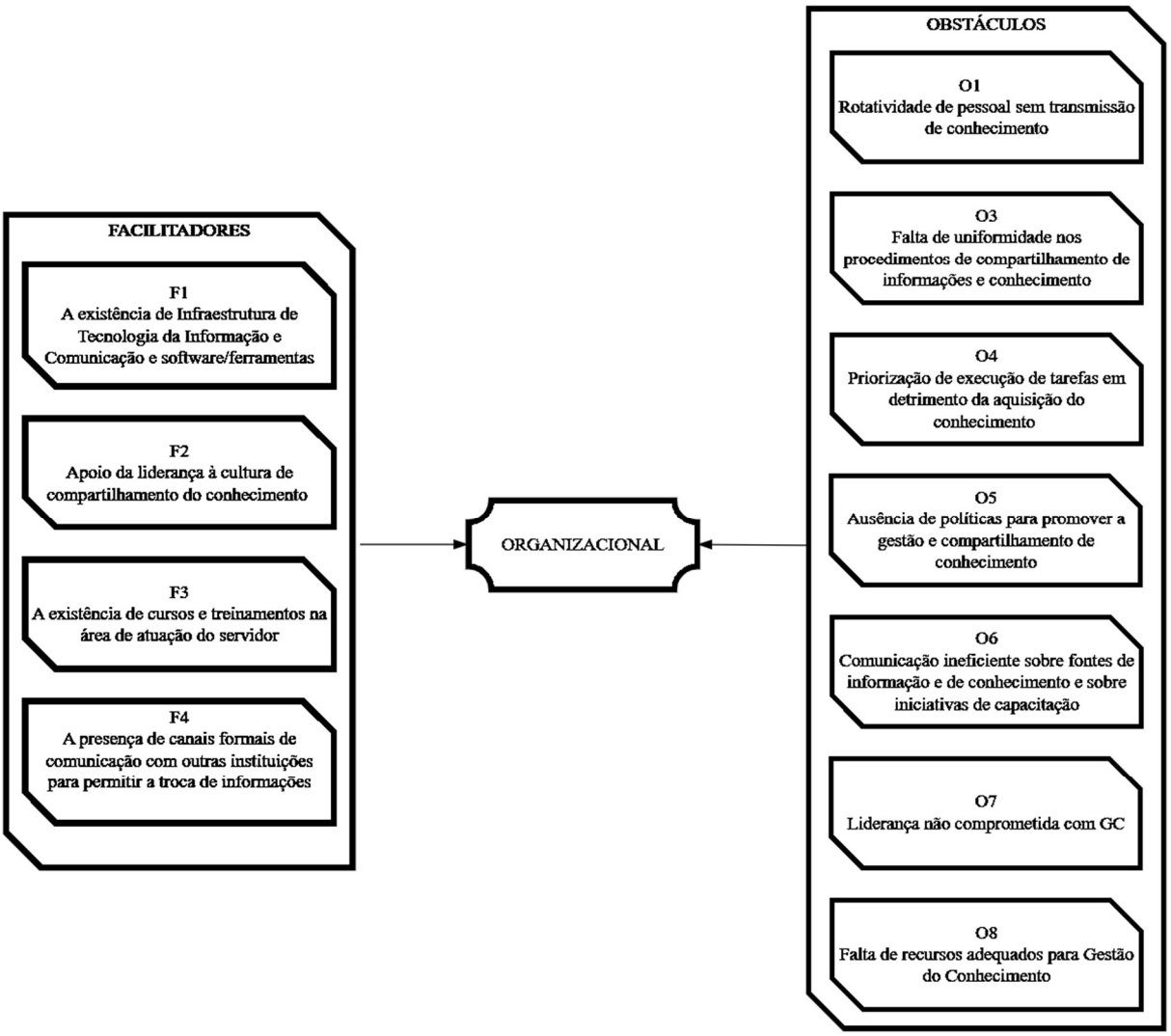


Figura 4 - Fatores em nível de análise organizacional identificadas

Fonte: dados da pesquisa, considerando os resultados das tabelas 5 e 6

Por fim, identificou-se somente o obstáculo "sigilo legal em inquéritos policiais e documentos de inteligência" como fator ambiental. Ainda que as falas possam trazer a ideia de uma falta de vontade de partes da organização no compartilhamento de certas informações, de fato existem restrições expressas na legislação pátria, estando então qualquer eventual alteração ligada a decisões políticas em âmbito nacional (Jilke et al., 2019). A Figura 5 mostra o fator ambiental identificado.

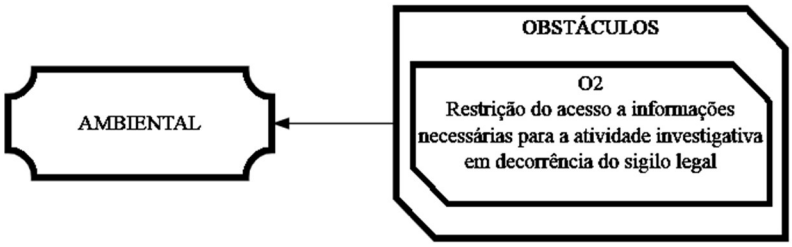


Figura 5 – Fator em nível de análise ambiental identificado

Fonte: dados da pesquisa, considerando os resultados das tabelas 5 e 6

Os resultados encontrados são corroborados pela literatura apresentada no quadro teórico-empírico deste trabalho, a qual reconhece a relevância dos níveis individual e organizacional na gestão do conhecimento, comumente associados tanto a facilitadores quanto a obstáculos. Embora a ênfase atribuída a cada nível varie entre os estudos analisados (Dhanhani & Naqbi, 2022; Oliva, 2014), nesta pesquisa observou-se a predominância do nível organizacional em termos de evidências empíricas, seguido pelo nível individual e, por fim, pelo nível ambiental, que foi o menos representado.

A análise da classificação dos fatores segundo os níveis de análise contribui significativamente para os estudos sobre organizações, ao oferecer subsídios para a compreensão de como diferentes dimensões da estrutura institucional influenciam a gestão do conhecimento (Jilke et al., 2019). Cada facilitador ou obstáculo identificado representa um ponto a ser abordado pela organização, e a atribuição de seu nível de análise (individual, organizacional ou ambiental) permite orientar intervenções específicas, aumentando a efetividade das ações de melhoria, como implantação de políticas de estímulo ao compartilhamento individual de conhecimento ou de conscientização de gestores para a importância da GC.

2.5. CONCLUSÕES

O objetivo deste estudo foi descrever os facilitadores e os obstáculos para a GC em atividades investigativas relativas a crimes cibernéticos, na percepção de policiais federais. Como meio de alcançar tal resultado, foi realizada uma pesquisa descritiva, com abordagem qualitativa e de caráter transversal.

Para a obtenção de dados foram realizadas entrevistas com policiais lotados em Superintendências Regionais - mais precisamente nas delegacias especializadas em

crimes cibernéticos e nos setores técnicos-científicos, onde atuam os peritos em informática – além de gestores da divisão e das coordenações subordinadas à DCIBER, de modo a garantir maior diversificação de opiniões. Como fonte secundária de dados foi realizada análise documental em documentos não sigilosos oriundos da organização estudada, com a devida autorização. As entrevistas passaram por análise de conteúdo, e todos os elementos obtidos foram confrontados com o conhecimento apresentado no quadro teórico-conceitual deste trabalho.

O primeiro objetivo específico deste estudo foi caracterizar, na percepção de policiais federais, o conceito de gestão do conhecimento. Para tanto, adotou-se a definição da ISO (2018) que a apresenta como a "gestão no que diz respeito ao conhecimento", por meio de uma abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados, incluindo a otimização da identificação, criação, análise, representação, distribuição e aplicação do conhecimento para gerar valor organizacional. Os entrevistados reconheceram a GC como gestão voltada ao conhecimento, embora não tenham citado individualmente cada elemento de definição adotada, mas que, no conjunto das entrevistas, foram todos citados. Desta maneira, ficou claro que todos possuíam entendimento suficiente do conceito para prosseguir com as entrevistas.

O segundo objetivo específico foi identificar, a partir da percepção de policiais federais, os facilitadores e os obstáculos para a Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos. Foram identificados sete facilitadores na percepção dos policiais federais, todos respaldados pela literatura.

Em relação aos obstáculos, foram identificados dez obstáculos na percepção dos policiais federais com respaldo na literatura pesquisada. À exceção de "Restrição do acesso a informações necessárias para a atividade investigativa em decorrência do sigilo legal", os demais também aparecem em diagnósticos realizados pela própria PF com todo o efetivo.

O terceiro objetivo específico - classificar os facilitadores e os obstáculos previamente identificados segundo os níveis de análise individual, organizacional e ambiental - aponta para predominância do nível organizacional, em total de onze, sendo quatro facilitadores e sete obstáculos citados, indicando que a Administração, na visão dos policiais federais, tem grande impacto na Gestão do Conhecimento das atividades relativas a crimes cibernéticos. O nível individual contou com cinco fatores identificados,

três facilitadores e dois obstáculos. O nível ambiental contou com um obstáculo, sem facilitadores identificados.

Conclui-se que a identificação e classificação dos facilitadores e obstáculos em níveis individual, organizacional e ambiental fornece um roteiro preciso para a instituição direcionar intervenções pontuais. Essa abordagem permite, por exemplo, a implementação de políticas de incentivo ao compartilhamento de conhecimento entre os indivíduos e a promoção de programas de capacitação e conscientização voltados aos gestores sobre a importância da gestão do conhecimento, o que potencializa a eficácia das ações de aprimoramento organizacional.

Entende-se como limitação do trabalho a dificuldade em extrapolar resultados, em virtude de tratar especificamente de uma organização, que podem sofrer influências das realidades específicas dos estados onde cada entrevistado trabalha, assim como o fator temporal, visto ser uma pesquisa transversal, que identificou as percepções em determinado momento.

Como sugestão para futuras pesquisas, recomenda-se a ampliação do número de entrevistas nas Superintendências Regionais e inclusão das lotações do interior, de forma a capturar percepções considerando o Estado em que cada entrevistado atua. Tal abordagem pode revelar variações significativas devido à diversidade das realidades brasileiras. Apesar do proposital foco na PF neste trabalho, é importante que os policiais atuantes em atividades investigativas relativas a crimes cibernéticos de outras organizações – em especial as polícias civis estaduais – sejam ouvidos, pois cada uma possui realidade distinta, tanto da PF quanto de suas congêneres. Além disso, a realização de pesquisa semelhante nas polícias civis pode revelar novos cenários sobre o tema.

3. PRODUTO TÉCNICO TECNOLÓGICO (PTT) – CARTILHA SOBRE GESTÃO DO CONHECIMENTO EM ATIVIDADES INVESTIGATIVAS RELATIVAS A CRIMES CIBERNÉTICOS

As polícias, em cumprimento de suas atividades investigativas, atuam na busca pelo controle das ações criminosas no espaço cibernético. Para cumprir tal missão, é necessário que seus agentes estejam alinhados às tecnologias utilizadas e aos métodos de ação dos criminosos. A GC pode ser empregada para que o conhecimento necessário – bem como aquele gerado nas atuações investigativas relativas a crimes cibernéticos - seja devidamente armazenado e disponibilizado em outras investigações.

Contudo, nem todas as medidas de GC são aplicáveis, em razão da necessidade de serem sistêmicas e exigirem tanto o envolvimento individual dos servidores quanto ações institucionais. Este capítulo descreve produto técnico-tecnológico, contendo sugestões de melhorias em pontos indicados por policiais federais atuantes em investigações relativas a crimes cibernéticos e corroborados na literatura.

3.1. Descrição Geral Do Produto

O produto deste trabalho é apresentado em formato de cartilha, identificado como Material Didático (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior [CAPES], 2019) contendo conceitos sobre crimes cibernéticos, GC, e propondo sugestões de melhorias para a GC conforme os facilitadores e obstáculos identificados no artigo teórico-empírico, fruto de entrevistas com policiais federais atuantes na área de combate a crimes cibernéticos. O confronto dessas entrevistas com documentos e com a literatura permite propor um material didático para a elaboração de uma cartilha que pode tornar este produto aplicável às outras polícias ou mesmo outras organizações de segurança pública que lidem com crimes cibernéticos.

Para detalhar como este Produto Técnico-Tecnológico (PTT) foi elaborado – uma proposta de cartilha que se propõe como evidência – apresenta-se, na sequência, a base teórica utilizada para fundamentação dos conceitos usados neste capítulo. A pesquisa realizada no Capítulo 2 trouxe evidências sobre conceitos, facilitadores e obstáculos para a GC em atividades investigativas relativas a crimes cibernéticos, sendo então tais elementos confrontados com as percepções de policiais federais sobre o tema, capturadas

por meio de entrevistas executadas com base em roteiro semiestruturado, constante no Apêndice B desta dissertação.

3.2. Base Teórica Utilizada

Este produto possui base teórica amparada em autores citados em Quadro Teórico sobre GC, apresentado na Seção 2.2, trazendo conceitos de facilitadores e obstáculos e os fatores que os representam, em especial – mas não exclusivamente – no setor público. Além disso, conta com conceitos de segurança cibernética e crimes cibernéticos.

Os crimes cibernéticos demandam das forças policiais não apenas o combate inicial, mas também a gestão eficiente do conhecimento gerado nas investigações, exigindo especialização e estratégias para seu compartilhamento e aplicação. Esse desafio se agrava devido ao crescimento dessas atividades ilícitas, que são potencializadas por redes criminosas online e geram impactos significativos, sendo considerados um dos principais riscos globais em 2022 (Yarovenko et al., 2023). Em 2023, os danos financeiros decorrentes desses crimes superaram os do tráfico de drogas, afetando o desenvolvimento econômico mundial (Brici & Achim, 2023; Kassab et al., 2023).

A GC contribui para aprimorar a criação, a distribuição e a aplicação do conhecimento nas organizações, promovendo aprendizado contínuo e melhoria de resultados. A norma ISO 30401 (2018) enfatiza a relevância de facilitadores e obstáculos que podem tornar a implementação da GC um desafio complexo (Oliva, 2014; Oliva & Kotabe, 2019).

Facilitadores da GC são mecanismos organizacionais que promovem o desenvolvimento contínuo da GC, criando um ambiente favorável à circulação e transformação do conhecimento (Nonaka & Takeuchi, 1995; Lee & Choi, 2003; Joshi & Chawla, 2019). Em contrapartida, os obstáculos representam barreiras que dificultam a implementação da GC e o progresso organizacional (Kaldeen, 2019).

Os facilitadores e os obstáculos podem estar vinculados a aspectos relativos ao nível individual, organizacional ou ambiental. Essa divisão em níveis de análise de estudos em Administração Pública (Jilke et al., 2019) permite aprofundar estudos e pesquisas para auxiliar a organização a implementar medidas que potencializem os facilitadores ou mitiguem os obstáculos identificados.

Por fim, os facilitadores e os obstáculos identificados na percepção de policiais federais atuantes em atividades investigativas relativas a crimes cibernéticos encontram respaldo na literatura, conforme demonstrado na Seção 2.4 desta dissertação. Como exemplos de facilitadores identificados tem-se a existência de infraestrutura de tecnologia da informação e comunicação (Chong et al., 2011; Dhanhani & Naqbi, 2022; Syed-Ikhsan & Rowland, 2004) ou a evidência da participação ativa do servidor em redes sociais promovendo a circulação de informações que subsidiam suas atividades (Dhanhani & Naqbi, 2022; Kaldeen, 2019; Smith & Johnson, 2023).

Como exemplo de obstáculos cita-se a priorização da execução de tarefas em detrimento da aquisição do conhecimento (Alves et al., 2022; Abrahamson & Goodman-Delahunty, 2014; Kaldeen, 2019; Seba et al., 2012; Smith & Johnson, 2023) e liderança não comprometida com a GC (Abrahamson & Goodman-Delahunty, 2014; Xanthopoulou et al., 2023).

3.3. Relevância Do Produto

A cartilha desenvolvida visa indicar maneiras de melhorar a GC em organizações policiais – em especial em atividades relacionadas a crimes cibernéticos –, de forma a conscientizar investigadores e gestores sobre atitudes que contribuem para uma GC mais eficiente, além de indicar pontos de melhoria organizacional para eventual implantação de políticas por parte da gestão da organização. No que se refere à relevância da cartilha como PTT, na sequência, apresentam-se descrições sobre a complexidade e aderência, potencial inovador, aplicabilidade e impacto potencial.

a) Complexidade e aderência

O produto apresentado é fruto de análises na área de Administração Pública, especificamente em Gestão do Conhecimento, definido como "gestão no que diz respeito ao conhecimento", que envolve adotar "uma abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados, que incluem a otimização da identificação, criação, análise, representação, distribuição e aplicação do conhecimento para criar valor organizacional" (ISO, 2018).

O trabalho envolve a Administração Pública por tratar do tema Segurança Pública, definida como atividade estatal pela Constituição da República Federativa do Brasil (Brasil, 1988), e por estar entre as principais preocupações da população brasileira

(Menezes, 2020), que inclui os crimes cibernéticos em razão dos prejuízos econômicos gerados. Ocorre que as investigações de crimes cibernéticos exigem agilidade e conhecimento de como são executados, de forma que o investigador esteja capacitado com tais saberes para bem executar suas funções (Hunton, 2011; Kleve et al., 2011), o que está no escopo da Gestão do Conhecimento no Setor Público.

b) Potencial Inovador

Apesar de não ser um assunto novo, muitas organizações que precisam lidar com crimes cibernéticos possivelmente sofrem com a gestão do conhecimento envolvido nas investigações, tanto na aquisição quanto na documentação e compartilhamento. Ao apontar problemas já identificados na literatura, abre-se espaço para permitir que as equipes de investigadores e as próprias organizações busquem solucioná-los, na medida do possível, para melhoria de resultados

Outro ponto é a escassez de trabalhos que relacionem GC e crimes cibernéticos, temas que são apresentados de modo apertado na literatura. Dessa maneira, abre-se uma trilha para pesquisas futuras que abarquem o tema crimes cibernéticos com foco na gestão da organização para efetividade das investigações, não apenas no campo da segurança cibernética.

c) Aplicabilidade

A pesquisa tem foco específico nas investigações de crimes cibernéticos no âmbito da PF. No entanto, sua metodologia, ao incluir um comparativo com elementos mais amplos da GC no setor público, pode servir como referência para pesquisas semelhantes não apenas no contexto das investigações de crimes cibernéticos, mas também em outros setores da PF — relacionados ou não a investigações criminais —, bem como em outras organizações do setor público que desempenham atividades diversas. O produto desenvolvido – a cartilha ora apresentada – possibilita que organizações que adotem sua utilização possam rever suas políticas de gestão do conhecimento em busca de melhores resultados.

d) Impacto Potencial

A pesquisa tem foco específico nas investigações de crimes cibernéticos no âmbito da PF. No entanto, sua metodologia, ao incluir um comparativo com elementos mais amplos da GC no setor público, pode servir como referência para pesquisas

semelhantes não apenas no contexto das investigações de crimes cibernéticos, mas também em outros setores da PF — relacionados ou não às investigações criminais —, bem como em outras organizações do setor público que desempenham atividades diversas.

3.4. Documentos Comprobatórios e Evidências

Este produto foi elaborado com base na análise de entrevistas realizadas com policiais federais, confrontadas com documentos referentes à organização PF – como relatórios, portarias e instruções normativas – e com suporte da literatura sobre GC.

Como evidência, apresenta-se a sugestão de um material didático em forma de cartilha, para disponibilização a gestores e investigadores diretamente envolvidos com atividades investigativas relativas a crimes cibernéticos na PF. O material será apresentado à organização, a quem cabe a decisão de utilizar ou não o material, com ou sem alterações. Assim, apresenta-se o material didático em forma de cartilha a seguir.

GESTÃO DO CONHECIMENTO EM INVESTIGAÇÕES RELATIVAS A CRIMES CIBERNÉTICOS

2025

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE
Programa de Pós-Graduação Profissional em Administração Pública - PGAP
Mestrado Profissional em Administração Pública - MPA

GESTÃO DO CONHECIMENTO EM INVESTIGAÇÕES RELATIVAS A CRIMES CIBERNÉTICOS

Cartilha integrante de Dissertação de Mestrado Profissional em Administração Pública

André Luis Deccache Dias

Brasília
2025

SUMÁRIO

*** As imagens utilizadas foram criadas via chatgpt.com e leonardo.ai ***

APRESENTAÇÃO

Os crimes cibernéticos ganharam relevância a partir dos anos 2000 em virtude da incorporação massiva da tecnologia da informação e comunicação nas sociedades. Além de implicar na criação de novas modalidades criminosas, permitiu a amplificação dos danos de crimes preexistentes, chegando a quase 100 vítimas por hora em 2021, o que torna a modalidade criminosa mais rentável que o tráfico de entorpecentes e um dos dez maiores riscos globais, sendo considerado um entrave para o desenvolvimento econômico.

Em virtude do dinamismo existente no mundo cibernético, é imperativo que as organizações atuantes nas áreas de segurança cibernética e investigação de crimes cibernéticos adotem políticas de gestão do conhecimento robustas, que permitam processar informações de modo eficiente e gerenciar o conhecimento, o que traz vantagens competitivas – no caso, em relação aos malfeitores.

Para que o conhecimento siga seu fluxo e gere valor competitivo, são necessárias ações e posturas tanto das organizações quanto de seus trabalhadores. Estas ações que favorecem o fluxo do conhecimento são chamadas de facilitadores, e aquelas que dificultam o fluxo do conhecimento são denominados obstáculos.

Esta cartilha deriva de uma pesquisa de dissertação de mestrado realizada no âmbito da Universidade de Brasília, trazendo a oportunidade de apresentar facilitadores e obstáculos à gestão do conhecimento na organização.

Assim, este material visa apresentar as questões identificadas na pesquisa de modo a auxiliar policiais e gestores das polícias a compreenderem quais medidas vêm dificultando e quais medidas podem contribuir para a gestão do conhecimento em atividades investigativas no contexto das organizações de segurança pública em que atuam.

O QUE SÃO CRIMES CIBERNÉTICOS?

O crime cibernético pode ser compreendido de diversas maneiras. Uma das definições existentes é a atividade criminal em que serviços ou aplicativos no espaço cibernético são utilizados para cometer um crime, ou são eles próprios o alvo do crime. O espaço cibernético também pode ser a fonte, ferramenta, alvo ou local de um crime – definição apresentada pela norma NBR ISO/IEC 27032:2015. Outra abordagem define essas ações como tentativas de burlar a segurança de sistemas de informação para acessar dados sobre seus usuários, distinguindo-se de outros crimes pela inviabilidade de sua execução sem esses sistemas.

A criminalidade cibernética apresenta um crescimento alarmante, de seis vítimas por hora em 2001 para noventa e uma em 2021. Reconhecido pelo Fórum Econômico Mundial em 2022 como um dos dez maiores riscos globais, esses crimes são vistos como um entrave ao desenvolvimento econômico, causando prejuízos estimados em US$ 6 trilhões em 2023, ultrapassando os lucros do tráfico de drogas ilícitas.

ATENÇÃO!

Qualquer crime que envolva o uso de computadores pode ser considerado cibernético. Por essa razão, as técnicas de investigação de crimes cibernéticos devem ser conhecidas por todos os investigadores, de qualquer área, ao menos superficialmente.

DEFINIÇÃO DE ESPAÇO CIBERNÉTICO

É o ambiente complexo resultante da interação de pessoas, softwares ou serviços na internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe qualquer forma física – definição trazida pela NBR ISO/IEC 27032:2015.

A legislação brasileira já define uma série de crimes cibernéticos, sendo o Código Penal o principal veículo, além do Estatuto da Criança e do Adolescente (ECA), que trata de crimes envolvendo mídias de abuso sexual infantil.

A Lei n.º 12.737/2012, chamada Lei Carolina Dieckmann, que altera o Código Penal inserindo crimes ligados à invasão de dispositivos, obtenção, adulteração ou destruição de dados em sistemas de informação sem autorização, interrupções a serviços de comunicação, falsificação de documento particular, incluindo cartões de crédito ou débito.

Posteriormente, a Lei Nº 14.155, de 27 de maio de 2021, alterou-se o Código Penal para tratar de estelionato através de informações ou *links* falsos. As atividades de *phishing* , *ramsonware* e *malware* estão previstas nesta legislação. Crimes que envolvem

produção, armazenamento e distribuição de material de abuso infantil estão previstos nos artigos 241-A a 241-C da Lei nº 8.069/1990 – ECA.

O QUE É CONHECIMENTO?

Costumeiramente utilizamos a palavra conhecimento para uma série de saberes, como dados e informações. Apesar de comumente tratados como sinônimos, há diferenças significativas nos conceitos.

Como ponto de partida, tem-se o dado, definido como fatos sobre um objeto – podendo ser, por exemplo, a qualificação de uma pessoa, uma organização, um documento ou um equipamento. O dado possui um conteúdo absoluto, sendo observável por qualquer pessoa. Bancos de dados sobre veículos, armas, qualificações de pessoas e contatos de provedores de conexão ou serviço pertencem a essa categoria.

Já a informação envolve interpretação e valor: ela é o dado com significado, pois traz novos pontos de vista sobre eventos ou objetos que os dados descrevem, dando a eles um significado. Indicar que certa pessoa estava em determinado veículo em determinado local possui objetivo para a investigação, transformando então os dados em informação.

Por fim, tem-se o conhecimento, que pode ser definido como um processo humano dinâmico de justificar crenças pessoais através da "verdade" - um conceito ligado ao sistema de valores do indivíduo. O conhecimento consiste em uma coleção de experiências, valores,

informações contextualizadas e uma visão aprofundada que permite criar estruturas para avaliar e integrar novas experiências e informações, as quais são geradas e implementadas nas organizações. São as análises de indícios, as conclusões de laudos e os relatórios de inquérito, por exemplo, que dependem de processos técnicos e cognitivos individuais para gerar valor às informações que tratam.

O conhecimento é difícil de transmitir ou registrar por ser intrínseco ao indivíduo, fruto de suas análises e reflexões fundamentadas em suas experiências, o chamado *"know-how"*. Esse conhecimento pode estar ligado a habilidades físicas também, pois os processos que levam a pessoa a movimentar seu corpo de maneira específica para obter aquele resultado são únicos e dificilmente descritos, não apenas as atividades intelectuais e suas linhas de raciocínio. Um instrutor de armamento e tiro, de defesa pessoal ou o profissional que desenvolve retrato falado são exemplos.

Contudo, é possível a transmissão do conhecimento entre as pessoas. Observar atentamente alguém realizando determinada tarefa e conversas informais são bons exemplos. Mas, para que haja maior alcance na transmissão deste conhecimento, é necessário armazenamento e formalização, de modo que passe a fazer parte de um acervo a ser distribuído e disponibilizado para consultas futuras. Após estes movimentos, cabe ao indivíduo exposto a tais conhecimentos aplicá-los, de forma a permitir que se torne o seu conhecimento, que depende de prática para incorporá-los e lapidá-los.

As etapas descritas acima devem se repetir de forma contínua, garantindo a geração constante de novos conhecimentos documentados e aplicáveis, além de melhorias nos

existentes. Esse ciclo é chamado de espiral do conhecimento e permite a melhoria individual, que se traduz em ganho de produtividade para a organização. A espiral contém quatro etapas:

- Sociabilização: compartilhamento e criação de conhecimento tácito através de experiência direta (tácito para tácito);

- Externalização: articulação do conhecimento tácito através do diálogo e da reflexão (tácito para explícito);

- Combinação: sistematização e aplicação do conhecimento explícito e a informação (explícito para explícito);

- Internalização: aprendizado e aquisição do conhecimento novo na prática (explícito para tácito);

O conhecimento possui dois estágios: o conhecimento tácito – que é aquele pertencente ao indivíduo e suas capacidades técnicas e cognitivas – e o conhecimento explícito – aquele documentado, organizado e pronto para ser transmitido para outras pessoas - para que se torne conhecimento tácito novamente. A transformação de tácito para explícito constitui um grande desafio, pois depende de medidas da organização e do indivíduo, mas quando ocorre fecha a chamada espiral do conhecimento.

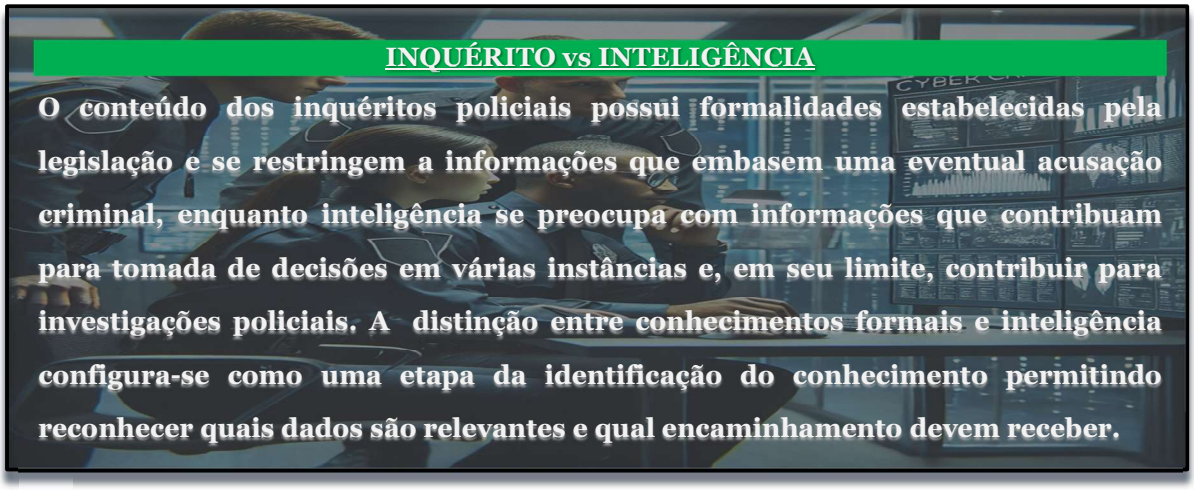
O conhecimento tácito é adquirido quando exercemos uma atividade e vamos repetindo para que cada vez se torne melhor. Não há como “ensinar” conhecimento tácito. Contudo, através da observação, da conversação e documentação – formas de conhecimento explícito – esta “maneira de fazer” algo pode ser traduzida em

linguagem e assim ser passada para outros, que precisarão aplicar o conhecimento que leram, viram ou ouviram para que se torne de fato conhecimento tácito.

O QUE É GESTÃO DO CONHECIMENTO?

A gestão do conhecimento envolve este processo de transformação de conhecimento tácito para explícito e de novo para tácito, pois cada vez que este ciclo se completa ocorrem avanços e melhorias nas atividades individuais e da organização.

O tema é de relevância reconhecida no meio acadêmico e corporativo. Apesar disso, seu conceito não é uniforme. Buscando esta unidade conceitual, foi editada a norma ISO 30401:2018, que firma ser gestão do conhecimento "gestão no que diz respeito ao conhecimento", que envolve adotar "uma abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados, que incluem a otimização da identificação, criação, análise, representação, distribuição e aplicação do conhecimento para criar valor organizacional".



A gestão do conhecimento, apesar de trazer muitos elementos em seu conceito, não precisa de todos para ser definida, bastando que alguns, ou até mesmo um elemento, seja percebido. Como exemplo, podemos tomar a identificação do conhecimento. Ele pode estar ligado à investigação ou à inteligência policial, e definir a qual esfera determinado saber pertence é gestão do conhecimento.

Para ser bem-sucedida, a gestão do conhecimento deve priorizar os fatores capital humano, processos, tecnologia e infraestrutura, governança, e cultura de gestão do conhecimento na organização. Em suma, consiste em aprender, utilizar, documentar e compartilhar saberes para maior produtividade e melhoria nos resultados.

O QUE SÃO FACILITADORES À GESTÃO DO CONHECIMENTO?

Os facilitadores são fatores que colocam os conceitos de gestão do conhecimento em prática de maneira a torná-la efetiva. Eles contribuem para formar um sistema capaz de estimular os membros da organização a ampliarem seus conhecimentos, a transporem as barreiras ao crescimento e a compartilharem esses saberes, estabelecendo um ambiente propício a iniciativas que promovam inovação e o desenvolvimento constante do conhecimento. Esses facilitadores são necessários para o sucesso da implementação dos processos de gestão do conhecimento.

Facilitadores referem-se a estruturas administrativas que permitem a gestão da aprendizagem organizacional e dos sistemas de gestão do conhecimento. No âmbito interno, compreendem a liderança, a cultura organizacional e os sistemas de recompensa — os quais desempenham papéis fundamentais, sendo a cultura organizacional emergindo como o fator mais influente.

Podemos citar o compartilhamento e a criação de conhecimento como elementos essenciais à gestão do conhecimento, e ambos são fortemente influenciados pela liderança, que se mostra um facilitador crítico desses processos. A cultura organizacional, fundamental para estabelecer valores necessários à inovação sustentável, é complementada pela tecnologia da informação; pelos canais de comunicação, sejam individuais ou coletivos, internos ou externos à organização; pela oferta de educação e treinamento; e pelo engajamento dos servidores na gestão do conhecimento.

A manifestação da habilidade e do interesse dos servidores em adquirir, compartilhar e utilizar conhecimentos é um comportamento relevante para a gestão do conhecimento na organização, assim como a participação ativa do servidor em redes sociais que promovam a circulação de informações, estejam os envolvidos próximos ou geograficamente distantes, usando ferramentas de tecnologia de informação e comunicação, como aplicativos de comunicação e e-mails.

A norma ISO 30401:2018 afirma que os facilitadores devem apoiar os objetivos do sistema de gestão do conhecimento, priorizando a cobertura dos fatores capital humano, processos, tecnologia e infraestrutura, governança e cultura de gestão do conhecimento.

O QUE SÃO OBSTÁCULOS À GESTÃO DO CONHECIMENTO?

Os obstáculos são fatores que bloqueiam a criação e o compartilhamento de conhecimento, variando de acordo com o contexto organizacional e não se restringem a uma lista definitiva,

evidenciando a complexidade e a extensão desses desafios na implementação eficaz da gestão do conhecimento.

Obstáculos à gestão do conhecimento incluem comportamentos dos servidores, como a ausência de vontade ou motivação para compartilhar informações ou conhecimento e de confiança em compartilhar o que se sabe, frequentemente ligados à ausência de recompensas e reconhecimento adequados. Outras barreiras envolvem a escassez de pessoal especializado e resistência ao uso de tecnologias percebidas como inseguras, como bancos de dados obsoletos.

Em uma perspectiva mais ligada à organização, podemos citar como obstáculos a ausência de políticas institucionais voltadas à gestão e ao compartilhamento do conhecimento; liderança não comprometida com a gestão do conhecimento.

A comunicação ineficiente sobre fontes de informação, conhecimento e iniciativas de capacitação obstáculo indica problemas no fluxo de informações na organização, que se torna barreira para o conhecimento. Sendo o conhecimento determinante para o sucesso nas atividades da organização, é relevante haver meios adequados para que o conhecimento flua e esteja disponível.

Também é visto como obstáculo a priorização da execução de tarefas em detrimento da aquisição do conhecimento, em geral justificada pela sobrecarga de trabalho que as polícias costumam ter, aliada à pressão por resultados, não permite que haja espaço para o indivíduo adquirir, gerar e compartilhar conhecimento.

Restrição de acesso a informações necessárias em razão do sigilo legal; falta de uniformidade nos procedimentos de compartilhamento de informações e conhecimento; escassez de recursos adequados para implementá-la; são outros exemplos de obstáculos à gestão do conhecimento.

FERRAMENTAS DE GESTÃO DO CONHECIMENTO

A gestão do conhecimento passa por adquirir, armazenar e compartilhar o que sabemos. Para nos auxiliar nessas tarefas, contamos com algumas ferramentas disponíveis nas redes de computadores:

- Páginas *wiki*: a criação de páginas *wiki*, local onde é possível obter conhecimentos e inserirmos novos para compartilhá-los, pode ser estruturada em uma rede interna ou ferramentas externas, gratuitas ou onerosas. As *wikis* permitem um uso descentralizado, mas d*eve* haver algum tipo de supervisão sobre a qualidade do conteúdo, pois a ferramenta permite que qualquer usuário insira, corrija ou atualize os conteúdos;

- Páginas de *intranet*: é importante que a organização possua estrutura de TIC que possibilite a criação de páginas temáticas para disponibilização de materiais diversos para consulta, como manuais, legislação, procedimentos, fluxos de processos, modelos de documentos ou mesmo dicas de ferramentas e instruções sobre como realizar determinadas tarefas, devendo ser criada e alimentada pelo setor responsável;

- Aplicativos de mensagens: o uso desse tipo de aplicativo permite o envio de mensagens privadas, a criação de grupos temáticos e realização de videoconferências, viabilizando não apenas reuniões de equipes em locais geograficamente distintos como a participação em aulas, palestras e *webinars* – relevantes fontes formais de conhecimento. São várias as opções, algumas gratuitas, outras assinadas.

- *E-mail* Corporativo: uma das principais ferramentas de comunicação, principalmente para anúncio de cursos e eventos relacionados a ferramentas e técnicas sobre crimes cibernéticos. Por isso deve ser acessado com frequência. A administração deve utilizar também este canal para informar a disponibilidade destes eventos;

- Armazenamento em nuvem: possibilita que documentos sejam compartilhados por equipes e permitindo acesso mesmo fora da rede organizacional, dando flexibilidade para obtenção e armazenamento de conhecimento. Existem múltiplas ferramentas, com alternativas gratuitas ou soluções corporativas.

ATENÇÃO!

Não armazene nem trafegue dados sigilosos, *malware*, vírus ou imagens de abuso sexual infantil fora dos servidores da organização ou dos canais específicos. NÃO ENVIAR POR *EMAIL*, CHAT, NEM COMPARTILHE NA NUVEM!

- Edição compartilhada de documentos: ferramentas de edição de textos, planilhas e apresentações *online* permitem a manipulação do conteúdo por vários usuários, desde que autorizados pelo criador do documento. Muitas dessas soluções interagem com armazenamento em nuvem. Também há variedade de serviços, tanto gratuitos quanto pagos.

CURSOS E TREINAMENTOS

No plano individual, a vontade de aprender e compartilhar é relevante para a gestão do conhecimento na organização. A realização de cursos, ou até mesmo ampliação do nível educacional do servidor, potencializam a utilização do conhecimento nas investigações de crimes cibernéticos. Ou seja: não parar de estudar traz benefícios para o servidor e para a organização! Busca por materiais em fontes abertas também contribuem enormemente, principalmente se isso é documentado e compartilhado. Por vezes, esse saber adquirido externamente pode levar o servidor a se tornar instrutor desse conteúdo dentro da corporação.

Contudo, é importante que as chefias compreendam a necessidade de constante atualização dos servidores, e que o tempo despendido com aquisição, armazenamento e compartilhamento de conhecimento – o que inclui cursos, treinamentos e missões em outras localidades – não deve ser visto como benefício pessoal para o servidor, mas sim como meio de estimular e aumentar a produtividade para a organização. As horas aplicadas em ampliar conhecimento se refletem em investigações mais céleres e de melhor qualidade.

Outro ponto relevante: cursos e treinamentos não devem ser ferramenta de punição. Devem participar de cursos e treinamentos em crimes cibernéticos aqueles que trabalham na área, e devem trabalhar na área de crimes cibernéticos aqueles que fizeram cursos e treinamentos na área. Ou farão. O não aproveitamento do conhecimento transmitido em tais cursos em virtude de o servidor não atuar na área após participar de cursos e treinamentos é desperdício de recursos.

CURSO É TRABALHO!

Cursos e capacitações fazem parte do bom andamento do serviço e não devem ser tratados como agrado, prêmio, obstáculo às atividades do setor ou punição. Estimule a participação.

PROXIMIDADE COM OUTRAS INSTITUIÇÕES

Muitos bancos de dados utilizados pelas polícias resultam de acordos firmados com outras organizações, públicas ou privadas. Além disso, é comum a existência de canais institucionais para a troca de informações. A proximidade com essas instituições possibilita a oferta de cursos e treinamentos em diversas áreas, permitindo que as organizações policiais absorvam conhecimentos externos sob diferentes perspectivas, o que contribui significativamente para a qualidade das investigações. Assim, recomenda-se que, sempre que houver oferta de cursos ou treinamentos promovidos por outras organizações, busque-se a participação, visando à ampliação e ao aprimoramento do conhecimento individual e, consequentemente, organizacional.

COMPARTILHAMENTO DE CONHECIMENTO NO COMBATE AOS CRIMES CIBERNÉTICOS

O principal recurso para qualquer investigação é o conhecimento - em especial sobre crimes cibernéticos. Acesso a banco de dados, a prospecção de informações de várias fontes e conhecimento sobre ferramentas e técnicas investigativas são exemplos. O conhecimento deve ser disponibilizado para o uso durante as investigações, mas precisa também ser atualizado e registrado para que haja tal disponibilidade.

Sendo o conhecimento algo intrínseco ao indivíduo, somente este pode buscar traduzi-lo para uma linguagem comum a outros de modo a transmiti-lo, seja por palavras, seja por exemplos. Assim, é de suma importância que sejam documentadas todas as informações que possam auxiliar outros colegas.

Lotações com alta rotatividade de pessoal, por exemplo, precisam desenvolver formas para que a pessoa que está saindo deixe um legado de conhecimento para quem chega. É muito importante para a continuidade do serviço, pois sem essa transmissão o conhecimento é perdido, devendo ser reconstruído, o que gera perda de tempo e eficiência. A elaboração de Procedimento Operacional Padrão (POP), ou mesmo uma lista de como fazer determinada atividade, onde se pode encontrar determinados dados ou ferramentas, são maneiras de compartilhar conhecimento. É importante compartilhar o que sabemos!

MAS... O QUE É "POP"?

O Procedimento Operacional Padrão (POP) é um passo-a-passo, devidamente publicado em normativo interno, que indica como determinada situação deve ser tratada, agilizando sua resolução.

COMO COMPARTILHAR CONHECIMENTO?

Como já mencionado, diversas organizações — públicas e privadas — dispõem de múltiplos bancos de dados acessíveis em razão de acordos interinstitucionais, além de sistemas voltados à pesquisa em perícias e inquéritos policiais. No entanto, o conhecimento aplicado à investigação de crimes cibernéticos vai além desses recursos tecnológicos.

É importante que as chefias divulguem os cursos disponíveis, assim como os demais servidores devem acompanhar os canais utilizados pela administração (*email* ou página da *intranet*), pois tais ações favorecem o fluxo do conhecimento na organização.

Sugestões de processos para a condução das investigações também são relevantes, assim como novidades em relação a aplicativos usados como instrumento de crime, páginas que ofereçam serviços ou sejam fonte de dados relevantes para investigação devem ser documentados e compartilhados.

A IMPORTÂNCIA DO "CAFEZINHO"

Não menos importante é a capacidade de comunicação com colegas – sejam de sua unidade, de outras unidades ou mesmo de outras instituições. Por vezes uma mensagem eletrônica, um café no corredor, uma visita na sala do colega ou um almoço podem ser

momentos importantes para compartilhar conhecimento. A participação em grupos nos aplicativos de mensagem também é um facilitador poderoso, pois não apenas é possível tirar dúvidas com um número maior de pessoas, como pode haver troca de materiais, como documentos ou manuais.

UNIÃO DE FORÇAS

Gestores, supervisores e operacionais devem buscar integração para o fluxo do conhecimento. Sem incentivos por parte da gestão, dificilmente haverá aquisição e compartilhamento de conhecimento no nível operacional.

CONSIDERAÇÕES

O conhecimento é essencial para que o trabalho seja realizado de maneira eficiente e traga os melhores resultados. E quanto mais se produz, mais conhecimento é gerado, o que resulta em melhorias nas atividades, completando a espiral do conhecimento. O contato com outras pessoas e outras fontes de conhecimentos documentados permite ampliar saberes e habilidades, que resultam em uma instituição mais produtiva e reconhecida pela sociedade por seu trabalho – algo de grande valor no serviço público.

Assim, é necessário o engajamento dos vários níveis administrativos da organização para que o conhecimento flua e possibilite tais ganhos de produtividade: a criação e a implantação de políticas de incentivo à gestão do conhecimento por parte da alta gestão; a participação e a motivação para a efetiva implementação dessas políticas por parte dos níveis de supervisão; e a disposição para adquirir e compartilhar conhecimento por parte dos níveis operacionais.

A dinâmica de novos dispositivos, tecnologias, aplicativos obriga os investigadores a estarem sempre atualizados. Assim, uma rede de contatos que permita a troca rápida de novos conhecimentos, a prática de documentar descobertas e inovações e a participação em cursos, treinamentos e eventos – que devem ser estimuladas e fomentadas pelos gestores – são essenciais para garantir eficiência e eficácia nas investigações relativas a crimes cibernéticos.

Os facilitadores e os obstáculos à gestão do conhecimento podem estar em diferentes níveis: individual ou organizacional. Apesar da imbricada relação entre ambos – afinal, um nível tem reflexos no outro – o individual envolve a vontade (ou sua falta) do indivíduo em agir para permitir o fluxo do conhecimento. Já o organizacional reflete as decisões da administração que trazem reflexos – positivos ou negativos – à gestão do conhecimento. Assim, tanto indivíduo como organização devem perceber os obstáculos que estão em seu escopo para buscar melhorias, assim como devem perceber os facilitadores existentes para que sejam melhorados e replicados.

Dessa forma, em um tópico tão dinâmico e complexo como os crimes cibernéticos, a gestão do conhecimento talvez seja a principal ferramenta para posicionar e manter as organizações que os investigam alinhadas àquelas que atuam em atividades criminosas no ambiente digital.

As imagens utilizadas foram criadas via chatgpt.com e leonardo.ai

MPA UnB
Mestrado Profissional em Administração Pública

PPGA UnB
Programa de Pós-graduação em
Administração Pública – UnB

4. CONSIDERAÇÕES FINAIS

Este capítulo apresenta as considerações finais deste estudo, cujo objetivo geral foi descrever os facilitadores e os obstáculos para gestão do conhecimento em atividades investigativas relativas a crimes cibernéticos, na percepção de policiais federais. Para alcançar este objetivo foi realizada uma pesquisa descritiva com abordagem qualitativa. Como fontes para coleta de dados foram realizadas entrevistas com policiais federais em Superintendências Regionais e nas coordenações subordinadas à DCIBER. Foram, também, coletados documentos públicos não sigilosos. O tratamento dos dados empregou análise documental e análise de conteúdo, considerando o teor do quadro teórico contendo facilitadores e obstáculos à GC, como também, a classificação dos facilitadores e dos obstáculos percebidos segundo os níveis individual, organizacional ou ambiental.

O primeiro objetivo específico buscou caracterizar o conceito de gestão do conhecimento, na percepção de policiais federais. Os principais resultados indicaram que os policiais percebem a definição de GC considerando oito elementos de conceito, na forma descrita na Figura 2 da Subseção 2.4.1 deste estudo. Tais elementos de conceito encontraram respaldo na literatura, especialmente nas normas ISO (complementar a descrição da norma).

O segundo objetivo específico foi identificar, a partir da percepção de policiais federais, os facilitadores e os obstáculos para a Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos. Foram identificados sete facilitadores na percepção dos policiais federais, conforme descrito na Tabela 5 da Seção 2.4.2 deste estudo. Os facilitadores encontraram respaldo na literatura, e foram confrontados com evidências documentais.

Em relação aos obstáculos, foram identificados dez obstáculos na percepção dos policiais federais, segundo apresentado na Tabela 6 da Seção 2.4.2 deste trabalho. Esses obstáculos encontraram respaldo em evidências documentais e na literatura pesquisada. À exceção de “Restrição do acesso a informações necessárias para a atividade investigativa em decorrência do sigilo legal”, os demais aparecem em diagnósticos realizados pela própria PF com todo o efetivo.

O terceiro objetivo específico foi classificar os facilitadores e os obstáculos previamente identificados segundo os níveis individual, organizacional e ambiental. Verificou-se que três facilitadores e dois obstáculos se vinculam ao nível individual; quatro facilitadores e sete obstáculos vinculam-se ao nível organizacional; e um obstáculo vincula-se ao nível ambiental,

sem evidências de facilitadores no nível ambiental, conforme evidenciado nas figuras 3 a 5 da Subseção 2.4.3 deste estudo.

O quarto objetivo específico foi alcançado com a produção de um PTT na forma de material didático, uma cartilha intitulada 'Gestão do Conhecimento em Investigações Sobre Crimes Cibernéticos', que apresenta os elementos de conceito para o entendimento da gestão do conhecimento exemplifica os facilitadores e os obstáculos à gestão do conhecimento, ilustra ferramentas e iniciativas para aquisição e compartilhamento do conhecimento e apresenta considerações sobre os conceitos apresentados, incluindo discussões segundo níveis organizacionais. O material didático proposto foi elaborado para livre distribuição entre policiais, em especial os que atuam na área investigativa de crimes cibernéticos. Apesar do propositalfoco na PF neste trabalho, entende-se que seu conteúdo pode ser aproveitado em outras organizações que atuem em atividade investigativas relativas a crimes cibernéticos.

Tendo sido alcançados os objetivos específicos, foi possível alcançar objetivo geral para este estudo. O estudo apresentou oito elementos de conceito para subsidiar o entendimento da GC, permitiu identificar sete facilitadores e dez obstáculos à GC, previamente citados no quadro teórico-conceitual. Esses facilitadores e esses obstáculos não se distribuíram uniformemente entre os níveis organizacionais. Verificou-se que três facilitadores e dois obstáculos se vinculam ao nível individual; quatro facilitadores e sete obstáculos vinculam-se ao nível organizacional; e um obstáculo vincula-se ao nível ambiental.

Depreende-se, com base nas evidências, que o órgão de segurança pública pode incentivar mudanças comportamentais em nível individual, tanto reforçando os facilitadores como mitigando os obstáculos através de políticas de incentivo e campanhas sobre GC. É possível, também, promover mudanças no nível organizacional pela gestão do próprio órgão de segurança pública. Já no nível ambiental, o que se refere à "Restrição do acesso a informações necessárias para a atividade investigativa em decorrência do sigilo legal", em virtude da questão do sigilo da investigação, não há margem para órgãos alterarem o estado de coisas ligada a tal obstáculo, especialmente se a atribuição desse sigilo for de origem externa ao referido órgão.

Isto posto, como resultado da pesquisa baseada nos facilitadores e obstáculos para a GC nas atividades investigativas relativas a crimes cibernéticos, o que permite propor recomendações à Gestão do Conhecimento em atividades investigativas relativas a crimes

cibernéticos no âmbito da Polícia Federal, com base nos facilitadores e obstáculos previamente identificados, alcançando o quarto objetivo específico:

- A inclusão do tema Gestão do Conhecimento na rotina dos policiais, seja através de comunicados, aplicativos de mensagens, cursos, *webinars* ou quaisquer outros meios efetivos de divulgação;
- A inclusão do tema Gestão do Conhecimento nos cursos de capacitação para gestores do órgão, demonstrando a importância do tema, a necessidade de tempo para a GC por parte de seus subordinados, o que inclui participação em cursos e treinamentos, que devem ser reservados àqueles que de fato trabalham com a matéria;
- A ampla divulgação da existência das páginas *Wiki* das áreas temáticas da DCIBER e incentivo para a inclusão de conhecimento também por parte dos burocratas de rua, com supervisão do órgão central sobre a qualidade do conteúdo postado;
- Centralização de informações sobre pessoas, procedimentos, modelos de documentos, fluxos, material didático e de suporte, além de informações sobre cursos de capacitação, de maneira a permitir o acesso de todos aqueles que atuem em ações investigativas relativas a crimes cibernéticos através de uma única página inicial a ser fortemente divulgada;
- Fomento do uso de aplicativos de rede social para troca de conhecimento de maneira ágil e remota; até mesmo com a participação de outras instituições;
- Realização frequente de encontros temáticos presenciais, com transmissão remota, de maneira a permitir a troca de experiências ao longo dos eventos;

Considera-se como limitação do trabalho a dificuldade em extrapolar resultados em virtude de a pesquisa tratar especificamente de uma organização, que pode sofrer influências das realidades específicas dos estados onde cada entrevistado trabalha. Outro ponto relevante de limitação foi o tempo disponível para as entrevistas e suas análises. Sem prejuízo dessas limitações, foi possível concluir todas as etapas desta dissertação, entregando o artigo teórico-empírico e propondo o PTT na forma descrita neste estudo.

Esse PTT, inclusive, como material didático em forma de cartilha, tem potencial de utilização por gestores e investigadores policiais que atuem na área de crimes cibernéticos de

outras organizações policiais. Porém, a GC não deve se limitar a materiais didáticos, devendo a organização buscar outros meios de incluir o tema em sua agenda.

Como sugestões para futuras pesquisas, recomendam-se:

- Incluir nas entrevistas policiais federais atuantes em atividades relativas a crimes cibernéticos que atuem nas delegacias de interior da PF, não apenas nas Superintendências Regionais.
- Capturar percepções considerando o Estado em que cada entrevistado atua. Tal abordagem pode revelar variações significativas devido à diversidade das realidades brasileiras.
- Replicar o estudo para que sejam ouvidos, também, os servidores atuantes em atividades investigativas relativas a crimes cibernéticos de outras organizações – em especial as polícias civis estaduais.

REFERÊNCIAS

Abrahamson, D. E., & Goodman-Delahunty, J. (2014). Impediments to information and knowledge sharing within policing: A study of three canadian policing organizations. *SAGE Open, 4*(1). https://doi.org/10.1177/2158244013519363

Academia Nacional de Polícia (ANP), Polícia Federal. (2021). *Plano Diretor Institucional (PDI) 2021–2025*. https://www.gov.br/pf/pt-br/assuntos/academia-nacional-de-policia-anp/cpa/outros-documentos/plano_pdi_versao_final.pdf

Adekannbi, J. O., & Bello, O. (2021). Factors Influencing Knowledge Sharing Behaviour of Police Officers in Ibadan Metropolis, Nigeria. *Journal of Information and Knowledge Management, 20*(2). https://doi.org/10.1142/S0219649221500179

Agrifoglio, R., Metallo, C., & di Nauta, P. (2021). Understanding Knowledge Management in Public Organizations through the Organizational Knowing Perspective: a Systematic Literature Review and Bibliometric Analysis. *Public Organization Review, 21*(1), 137–156. https://doi.org/10.1007/s11115-020-00480-7

Al Ahbabi, S. A., Singh, S. K., Balasubramanian, S., & Gaur, S. S. (2019). Employee perception of impact of knowledge management processes on public sector performance. *Journal of Knowledge Management, 23*(2), 351–373. https://doi.org/10.1108/JKM-08-2017-0348

Al-Ahbabi, S., Singh, S. K., Singh Gaur, S., & Balasubramanian, S. (2017). A knowledge management framework for enhancing public sector performance. *International Journal of Productivity and Performance Management and International Journal of Value Chain Management* (Vol. 8).

Alexandre, N. M. C., & Coluci, M. Z. O. (2011). Content validity in the development and adaptation processes of measurement instruments. *Cadernos de Saúde Pública, 27*(3), 523-537.

Almeida, D., Alves, C. A. de M., Mendes, F. F., & Nunes, R. R. (2024). Conscientização em segurança cibernética: Estudo baseado na percepção de trabalhadores de uma organização pública federal brasileira. *Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)*, *(E65)*, 67–81.

Alvarenga, A., Matos, F., Godina, R., & Matias, J. C. O. (2020). Digital transformation and knowledge management in the public sector. *Sustainability (Switzerland)*, 12(14). https://doi.org/10.3390/su12145824

Alves, J. L., Nadae, J. de, & Carvalho, M. M. de. (2022). Knowledge management enablers and barriers: exploring the moderating effect of communication barriers. *International Journal of Managing Projects in Business, 15*(7), 1091 – 1122. https://doi.org/10.1108/IJMPB-02-2022-0047

Amayah, A. T. (2013). Determinants of knowledge sharing in a public sector organization. *Journal of Knowledge Management, 17*(3), 454–471. https://doi.org/10.1108/JKM-11-2012-0369

Arpaci, I., & Ateş, E. (2023). Development of the cybercrime awareness scale (CAS): a validity and reliability study in a Turkish sample. *Online Information Review, 47*(4), 633–643. https://doi.org/10.1108/OIR-01-2022-0023

Ashok, M., Al Badi Al Dhaheri, M. S. M., Madan, R., & Dzandu, M. D. (2021). How to counter organisational inertia to enable knowledge management practices adoption in

public sector organisations. *Journal of Knowledge Management, 25*(9), 2245–2273. https://doi.org/10.1108/JKM-09-2020-0700

Asrar-ul-Haq, M., & Anwar, S. (2016). A systematic review of knowledge management and knowledge sharing: Trends, issues, and challenges. *Cogent Business & Management, 3*(1), 1127744. https://doi.org/10.1080/23311975.2015.1127744

Associação Brasileira de Normas Técnicas (ABNT). (2015). *NBR ISO/IEC 27032:2015 – Diretrizes para segurança cibernética*.

Bardin, L. (1977). *Análise de conteúdo*. Lisboa: Edições 70.

Barrett, M. (2018). *Framework for improving critical infrastructure cybersecurity: Version 1.1* (NIST Cybersecurity Framework No. 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Batista, F. F. (2012). *Modelo de gestão do conhecimento para a administração pública brasileira: Como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão*. Instituto de Pesquisa Econômica Aplicada (Ipea). https://repositorio.ipea.gov.br/bitstream/11058/754/1/Modelo%20de%20Gest%c3%a3o%20do%20Conhecimento%20para%20a%20Administra%c3%a7%c3%a3o%20P%c3%bablica%20Brasileira.%20Livro.pdf

Batista, F. F. (2015). *Gestão do conhecimento na administração pública: Resultados da Pesquisa Ipea 2014 – Níveis de maturidade*. Instituto de Pesquisa Econômica Aplicada (Ipea).

Birdi, K., Griffiths, K., Turgoose, C., et al. (2020). Factors influencing cross-border knowledge sharing by police organisations: An integration of ten European case studies. *Police Practice and Research*. https://doi.org/10.1080/15614263.2020.1789462

Brasil. (1940). *Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

Brasil. (1941). *Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm

Brasil. (1988). *Constituição da República Federativa do Brasil de 1988.* https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm

Brasil. (1990). *Lei no 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente.* https://www.planalto.gov.br/ccivil_03/leis/l8069.htm

Brasil. (1996). *Lei nº 9.266 de 15 de março de 1996. Reorganiza as classes da Carreira Policial Federal, fixa a remuneração dos cargos que as integram e dá outras providências.* https://www.planalto.gov.br/ccivil_03/leis/l9266.htm

Brasil. (2012). *Lei nº 12.737, de 30 de novembro de 2012 – Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar como crime a invasão de dispositivo informático alheio, com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular, ou instalar vulnerabilidades para obter vantagens ilícitas*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Brasil. (2023a). *Decreto 11.491 de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste.* https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm

Brasil. (2023b). *Decreto nº 11.348, de 30 de novembro de 2023 – Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão*

e funções de confiança. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11348.htm#:~:text=DECRETO%20N%C2%BA%2011.348%2C%20DE%201%C2%BA%20DE%20JANEIRO%20DE%202023&text=Aprova%20a%20Estrutura%20Regimental%20e,comiss%C3%A3o%20e%20fun%C3%A7%C3%B5es%20de%20confian%C3%A7a.

Brasil. (2023c). *Decreto no 11.856 de 26 de dezembro de 2023 - Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança*. Diário Oficial da União. https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-531482033

Brici, I., & Achim, M. V. (2023). Does the Digitalization of Public Services Influence Economic and Financial Crime? *Studies in Business and Economics, 18*(2), 67–85. https://doi.org/10.2478/sbe-2023-0025

CAPES. (2019). Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. Ficha de Avaliação - Área 27: Administração Pública e de Empresas, Ciências Contábeis e Turismo. 2020. Disponível em https://www.gov.br/capes/pt-br/centrais-de-conteudo/documentos/avaliacao/FICHA_ADMINISTRACAO_P_ATUALIZADA.pdf

Carvalho, A. A. da S., Ferneda, E., & Streit, R. E. (2020). A Gestão do Conhecimento e os desafios para a implementação de um modelo de excelência baseado na norma ISO 30401. *Perspectivas em Gestão & Conhecimento*, 19–46. https://doi.org/10.22478/ufpb.2236-417x.2020v10n3.57025

Castro, L., Santos-Corrada, M., Flecha-Ortiz, J. A., Lopez, E., Gomez, J., & Aponte, B. (2022). Knowledge management and innovative behavior: police reform efforts in Puerto

Rico. *Journal of Knowledge Management, 26*(5), 1262–1279. https://doi.org/10.1108/JKM-02-2021-0133

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). (2024). *Tipos de incidentes mensais*. https://stats.cert.br/incidentes/#tipos-incidente-mensal

Chong, S. C., Salleh, K., Ahmad, S. N. S., & Sharifuddin, S.-I. S. O. (2011). KM implementation in a public sector accounting organization: An empirical investigation. *Journal of Knowledge Management, 15(*3), 497–512. https://doi.org/10.1108/13673271111137457

Comissão Parlamentar de Inquérito – Pedofilia. (2010). *Relatório final nº 03/2010*. Senado Federal. https://www2.senado.leg.br/bdsf/bitstream/handle/id/194582/RF_CPI_pedofilia_2010.pdf?isAllowed=y&sequence=6

Conselho da União Europeia. (2022). *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e sistemas de informação em toda a União*. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022L2555

Conselho Monetário Nacional. (2021). *Resolução No 4.893 de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.*

https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893

Dean, G., Fahsing, I. A., & Gottschalk, P. (2006). Profiling police investigative thinking: A study of police officers in Norway. *International Journal of the Sociology of Law, 34*(4), 221–228. https://doi.org/10.1016/j.ijsl.2006.09.002

Departamento de Polícia Federal. (2015). *Portaria nº 5962-DG/DPF, de 8 de dezembro de 2015. Institui a política de gestão do conhecimento na Polícia Federal*

Departamento de Polícia Federal. (2016). *Portaria nº 6194-DG/DPF, de 16 de março de 2016: Institui a política de desenvolvimento de pessoal no âmbito da Polícia Federal.*

Dhanhani, M. A. Al, & Naqbi, S. Al. (2022). Identifying Enablers and Obstacles for Knowledge Management in a Police Organization: Case Study of Abu Dhabi Police. *Policing (Oxford), 16*(2), 270–281. https://doi.org/10.1093/police/paac019

Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. *Sensors, 23*(14). https://doi.org/10.3390/s23146302

Duan, C., Liu, X., Yang, X., & Deng, C. (2023). Knowledge complexity and team information processing: the mediating role of team learning goal orientation. *Journal of Knowledge Management, 27*(5), 1279–1298. https://doi.org/10.1108/JKM-11-2021-0858

Europol. (2022). *Cybercrime*. https://www.europol.europa.eu/crime-areas/cybercrime

Falqueto, J. maria zandonade, Hoffmann, V. E., & Farias, J. S. (2018). Saturação Teórica em Pesquisas Qualitativas: Relato de uma Experiência de Aplicação em Estudo na Área de

Administração. *Revista de Ciências da Administração*, 40–53. https://doi.org/10.5007/2175-8077.2018v20n52p40

Febraban. (2023, novembro 24). Febraban e Polícia Federal assinam mais um acordo para combater fraudes bancárias digitais. Febraban. https://portal.febraban.org.br/noticia/4031/pt-br/

Federal Bureau of Investigation. ([s.d.]). *What We Investigate.* https://www.fbi.gov/investigate/cyber

Fontanella, B. J. B., Luchesi, B. M., Saidel, M. G. B., Ricas, J., Turato, E. R., & Melo, D. G. (2011). Amostragem em pesquisas qualitativas: Proposta de procedimentos para constatar saturação teórica. *Cadernos de Saúde Pública, 27*(2), 389–394. https://doi.org/10.1590/S0102-311X2011000200020

Fórum Brasileiro de Segurança Pública. (2024). *18º Anuário Brasileiro de Segurança Pública: 2024*. https://publicacoes.forumseguranca.org.br/items/f62c4196-561d-452d-a2a8-9d33d1163af0

Ganapathy, S., Mansor, Z., & Ahmad, K. (2019). Investigating factors affecting knowledge management practices in public sectors. *International Journal of Advanced Computer Science and Applications, 10*(11), 205 – 212. https://doi.org/10.14569/IJACSA.2019.0101128

Gaur, A. S., Ma, H., & Ge, B. (2019). MNC strategy, knowledge transfer context, and knowledge flow in MNEs. *Journal of Knowledge Management, 23*(9), 1885–1900. https://doi.org/10.1108/JKM-08-2018-0476

Goswami, A. K., & Agrawal, R. K. (2023). It's a knowledge centric world! Does ethical leadership promote knowledge sharing and knowledge creation? Psychological capital as

mediator and shared goals as moderator. *Journal of Knowledge Management, 27*(3), 584 – 612. https://doi.org/10.1108/JKM-09-2021-0669

Gottschalk, P. (2006). Stages of knowledge management systems in police investigations. *Knowledge-Based Systems, 19*(6), 381–387. https://doi.org/10.1016/j.knosys.2006.04.002

Gottschalk, P., & Dean, G. (2010). Knowledge Management in Policing: The Case of Police Complaints and Police Crime. *Police Journal, 83*(2), 96–112. https://doi.org/10.1350/pojo.2010.83.2.473

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. Strategic Management Journal, 17(S2), 109–122. https://doi.org/10.1002/smj.4250171110

Heisig, P. (2009). Harmonisation of knowledge management – comparing 160 KM frameworks around the globe. *Journal of Knowledge Management, 13*(4), 4–31. https://doi.org/10.1108/13673270910971798

Hilbert, M. (2020). Digital technology and social change: The digital transformation of society from a historical perspective. *Dialogues in Clinical Neuroscience, 22*(2), 189–194. https://doi.org/10.31887/dcns.2020.22.2/mhilbert

Ho, C.-T. (2009). The relationship between knowledge management enablers and performance. *Industrial Management and Data Systems, 109*(1), 98–117. https://doi.org/10.1108/02635570910926618

Hoffman, C. J., Howell, C. J., Perkins, R. C., Maimon, D., & Antonaccio, O. (2024). Predicting new hackers' criminal careers: A group-based trajectory approach. *Computers and Security*, 137. https://doi.org/10.1016/j.cose.2023.103649

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law and Security Review, 27*(1), 61 – 67. https://doi.org/10.1016/j.clsr.2010.11.001

Hweidi, R. F. A., & Eleyan, D. (2023). Social Engineering Attack concepts, frameworks, and Awareness: A Systematic Literature Review. *International Journal of Computing and Digital Systems*, 20, 2210–142.

International Organization for Standardization. (2018). *ISO 30401:2018 – Knowledge management systems — Requirements*. https://www.iso.org/standard/68683.html

Interpol. (s.d.-a). *Brazil*. https://www.interpol.int/Who-we-are/Member-countries/Americas/BRAZIL

Interpol. (s.d.-b). *International child sexual exploitation database*. https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Interpol. (s.d.-c). *INTERPOL Innovation Centre*. https://www.interpol.int/How-we-work/Innovation/INTERPOL-Innovation-Centre

Jääskeläinen, A., Sillanpää, V., Helander, N., Leskelä, R.-L., Haavisto, I., Laasonen, V., & Torkki, P. (2022). Designing a maturity model for analyzing information and knowledge management in the public sector. *VINE Journal of Information and Knowledge Management Systems, 52*(1), 120–140. https://doi.org/10.1108/VJIKMS-01-2020-0017

Jilke, S., Olsen, A. L., Resh, W., & Siddiki, S. (2019). Microbrook, Mesobrook, Macrobrook. *Perspectives on Public Management and Governance, 2*(4), 245–253. https://doi.org/10.1093/ppmgov/gvz015

Jimoh, M. (2023). Critiquing the U.S. characterization, attribution and retaliation laws and policies for cyberattacks. *Computer Law and Security Review*, 50. https://doi.org/10.1016/j.clsr.2023.105847

Joshi, H., & Chawla, D. (2019). How knowledge management influences performance? *International Journal of Knowledge Management, 15*(4), 56–77. https://doi.org/10.4018/IJKM.2019100104

Kaldeen, M. (2019). Managing knowledge management: Identifying and evaluating enablers and hinders from the perspective of practicing managers from tourism sector in Sri lanka. *International Journal of Recent Technology and Engineering, 8*(2 Special Issue 11), 4167 – 4171. https://doi.org/10.35940/ijrte.B1602.0982S1119

Kalogiannidis, S., Paschalidou, M., Kalfas, D., & Chatzitheodoridis, F. (2023). Relationship between Cyber Security and Civil Protection in the Greek Reality. *Applied Sciences (Switzerland)*, 13(4). https://doi.org/10.3390/app13042607

Kassab, M., Amaba, B., Pound, E. S., & Fox, B. (2023). Is the Solution for Cybercrime Also a Path to Greater Productivity? *Computer, 56*(11), 91–94. https://doi.org/10.1109/MC.2023.3290263

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers and Security*, 127. https://doi.org/10.1016/j.cose.2022.103089

Kleve, P., De Mulder, R., & Van Noortwijk, K. (2011). The definition of ICT Crime. *Computer Law and Security Review, 27*(2), 162 – 167. https://doi.org/10.1016/j.clsr.2011.01.004

Laihonen, H., Kork, A.-A., & Sinervo, L.-M. (2023). Advancing public sector knowledge management: towards an understanding of knowledge formation in public administration. *Knowledge Management Research & Practice*, 1–11. https://doi.org/10.1080/14778238.2023.2187719

Lartey, P. Y., Kong, Y., Afriyie, S. O., Santosh, R. J., & Bah, F. B. M. (2021). Knowledge Management Issues in India: A Public Sector Perspective. *International Journal of Public Administration, 44*(3), 215 – 230. https://doi.org/10.1080/01900692.2019.1676778

Lee, H., & Choi, B. (2003). Knowledge management enablers, processes, and organizational performance: An integrative view and empirical examination. *Journal of Management Information Systems, 20*(1), 179 – 228. https://doi.org/10.1080/07421222.2003.11045756

Luen, T. W., & Al-Hawamdeh, S. (2001). Knowledge management in the public sector: Principles and practices in police work. *Journal of Information Science, 27*(5), 311–318. https://doi.org/10.1177/016555150102700502

Marques, J. M. R., La Falce, J. L., Marques, F. M. F. R., De Muylder, C. F., & Silva, J. T. M. (2019). The relationship between organizational commitment, knowledge transfer and knowledge management maturity. *Journal of Knowledge Management, 23*(3), 489 – 507. https://doi.org/10.1108/JKM-03-2018-0199

Massaro, M., Dumay, J., & Garlatti, A. (2015). Public sector knowledge management: A structured literature review. *Journal of Knowledge Management, 19*(3), 530 – 558. https://doi.org/10.1108/JKM-11-2014-0466

Mc Evoy, P. J., Ragab, M. A. F., & Arisha, A. (2019). The effectiveness of knowledge management in the public sector. *Knowledge Management Research and Practice, 17*(1), 39–51. https://doi.org/10.1080/14778238.2018.1538670

Mcadam, R., & Reid, R. (2000). A comparison of public and private sector perceptions and use of knowledge management. *Journal of European Industrial Training* (p. 317–329). http://www.mcbup.com/research_registers/tdev.asp

Menezes, R. F. de B. (2020). *Gestão do Conhecimento no Setor Público: o Aproveitamento da Atividade Investigativa da Polícia Federal Brasileira* [Dissertação de Mestrado Profissional, UNIVERSIDADE DE BRASÍLIA – UnB].

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences (Switzerland), 13*(10). https://doi.org/10.3390/app13105875

Nonaka, I. (2000). A Dynamic Theory of Organizational Knowledge Creation. *Knowledge, Groupware and the Internet* (p. 3–42). Elsevier. https://doi.org/10.1016/B978-0-7506-7111-8.50003-2

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

Nordin, M., Pauleen, D. J., & Gorman, G. E. (2009). Investigating KM antecedents: KM in the criminal justice system. *Journal of Knowledge Management, 13*(2), 4–20. https://doi.org/10.1108/13673270910942664

Ogar, J. A., Okpa, J. T., Abang, T. A., Opoh, F. A., Uyang, F. A., Ikpeme, B. B., Eneji, R. I., Bassey, A. E., Bisong, P. O., Ezikeudu, C. C., & Ebong, E. (2023). Malware victimisation and organisational survival: A multi-method exploration of emerging market. *Journal of Governance and Regulation*, *12*(3, Special Issue), 377–388. https://doi.org/10.22495/jgrv12i3siart19

Oliva, F. L. (2014). Knowledge management barriers, practices and maturity model. *Journal of Knowledge Management, 18*(6), 1053–1074. https://doi.org/10.1108/JKM-03-2014-0080

Oliva, F. L., & Kotabe, M. (2019). Barriers, practices, methods and knowledge management tools in startups. Journal of Knowledge Management, 23(9), 1838–1856. https://doi.org/10.1108/JKM-06-2018-0361

Oliveira, V. G. de, & Abib, G. (2024). Risco na administração pública: uma revisão sistemática focada em uma agenda de pesquisas futuras. *Revista de Administração Pública*. https://doi.org/10.1590/0034-761220220419

Özlen, M. K. (2021). Enablers and Outcomes of Knowledge Management Implementation in Supply Chains: Manufacturing Companies Perspective. *Journal of the Knowledge Economy, 12*(3), 1517 – 1532. https://doi.org/10.1007/s13132-020-00677-7

Pagon, M. (1996). Policing in Central and Eastern Europe: The role and importance of cooperation, training, education, and research. *Policing in Central and Eastern Europe: Comparing firsthand knowledge with experience from the West*. College of Police and Security Studies, Slovenia.

Parlamento Europeu, & Conselho da União Europeia. (2019). *Regulamento (UE) 2019/881 de 17 de abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação de cibersegurança das tecnologias da informação e da comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento sobre a Cibersegurança)*. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019R0881

Pee, L. G., & Kankanhalli, A. (2016). Interactions among factors influencing knowledge management in public-sector organizations: A resource-based view. *Government Information Quarterly, 33*(1), 188–199. https://doi.org/10.1016/j.giq.2015.06.002

Pellegrini, M. M., Ciampi, F., Marzi, G., & Orlando, B. (2020). The relationship between knowledge management and leadership: Mapping the field and providing future research avenues. *Journal of Knowledge Management, 24*(6), 1445–1492. https://doi.org/10.1108/JKM-01-2020-0034

Pepple, D., Makama, C., & Okeke, J.-P. (2022). Knowledge management practices: A public sector perspective. *Journal of Business Research, 153*, 509 – 516. https://doi.org/10.1016/j.jbusres.2022.08.041

Perkins, R. C., Ouellet, M., Howell, C. J., & Maimon, D. (2023). The Illicit Ecosystem of Hacking: A Longitudinal Network Analysis of Website Defacement Groups. *Social Science Computer Review, 41*(2), 390–409. https://doi.org/10.1177/08944393221097881

Pham, H.-H., Nguyen, T. T. H., Nguyen, V.-T., Nguyen, V.-M., The Cong, P., Vu, M.-C., Do, T.-N., Kim, M. H., & Tran, N.-M. (2023). The impacts of knowledge management enablers and knowledge management processes on university performance in Vietnam. *Knowledge Management Research and Practice, 21*(3), 512 – 524. https://doi.org/10.1080/14778238.2022.2105758

Polícia Civil do Distrito Federal. (2024). *Organograma da Polícia Civil do Distrito Federal. Polícia Civil do Distrito Federal.* https://www.pcdf.df.gov.br/institucional/organograma

Polícia Civil do Estado do Paraná. (2022). *Núcleo de Combate aos Cibercrimes - NUCIBER*. pr.gov.br. https://www.policiacivil.pr.gov.br/NUCIBER

Polícia Federal. (2021a). *Planejamento estratégico 2021-2023: Anexo II - Plano Estratégico 2021-2023*. https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/planejamento-estrategico-1/planejamento-estrategico-2021-2023/AnexoIIPlanoEstratgico20212023.pdf

Polícia Federal. (2021b). Requisitos e atribuições dos cargos da Carreira Policial Federal. *gov.br*. https://www.gov.br/pf/pt-br/acesso-a-informacao/servidores/concursos/caracteristicas-dos-cargos/carreira-policial/requisitos-e-atribuicoes-dos-cargos-da-carreira-policial-federal

Polícia Federal. (2022a). *Instrução Normativa nº 216-DG/PF, de 13 de janeiro de 2022. Regulamenta a atividade de inteligência Policial da Polícia Federal*

Polícia Federal. (2022b). *Projeto básico [PDF]. Diretoria de Tecnologia da Informação e Inovação.* https://www.gov.br/pf/pt-br/assuntos/licitacoes/2022/diretoria-de-tecnologia-da-informacao-e-inovacao-dti/contratos/contrato-08-2022-dti-pf/projeto-basico-sei_pf-25100540.pdf

Polícia Federal. (2022c) *Planot Estratégico da Polícia Federal -2022-2023.* https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/planejamento-estrategico-1/planejamento-estrategico-2022-2023/AnexoIIPlanoEstratgicodaPolciaFederal20222023.pdf

Polícia Federal. (2023a*). Instrução Normativa DG/PF Nº 270, de 15 de dezembro de 2023. Estabelece as competências específicas das unidades centrais e descentralizadas da Polícia Federal e as atribuições de seus dirigentes.*

Polícia Federal. (2023b). *Organograma Polícia Federal*. https://www.gov.br/pf/pt-br/acesso-a-informacao/institucional/estrutura

Polícia Federal. (2023c). PF passa a integrar o programa “No More Ransom”. *gov.br*. https://www.gov.br/pf/pt-br/assuntos/noticias/2023/04/pf-passa-a-integrar-o-programa-201cno-more-ransom201d

Polícia Federal. (2023d*). Projeto de Transformação Organizacional PF80 [PDF]*. https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/planejamento-estrategico-1/planejamento-estrategico-2024-2027/AnexoIVProjetodeTransformaoOrganizacionalPF80.pdf

Polícia Federal. (2024a*). Anexo III: Mapa dos Objetivos Estratégicos e Resultados-Chave Estratégicos da Polícia Federal 2024-2027*. Recuperado de https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/planejamento-estrategico-1/planejamento-estrategico-2024-2027/AnexoIIIMapadosObjetivosEstratgicoseResultadosChaveEstratgicosdaPolcia.pdf

Polícia Federal. (2024b). *Diretoria de Combate a Crimes Cibernéticos (DCIBER): Estatísticas*. Recuperado em 06 de fevereiro, de 2024 de https://www.gov.br/pf/pt-br/acesso-a-informacao/estatisticas/diretoria-de-combate-a-crimes-ciberneticos-dciber

Polícia Federal. (2024c). PF e Polícia Judiciária de Portugal trabalharão juntas no combate ao abuso sexual infantojuvenil. *gov.br*. https://www.gov.br/pf/pt-br/assuntos/noticias/2024/02/pf-e-policia-judiciaria-de-portugal-trabalharao-juntas-no-combate-ao-abuso-sexual-infantojuvenil

Polícia Federal. (2024d). *Plano Estratégico da Polícia Federal 2024-2027*. Recuperado de https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/planejamento-estrategico-1/planejamento-estrategico-2024-2027/AnexoIIPlanoEstratgicodaPolciaFederal20242027.pdf

Polícia Federal. (2024). *Planejamento estratégico da Polícia Federal 2024–2027*. https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/planejamento-estrategico-1/planejamento-estrategico-2024-2027

Polícia Federal. (2024f). Polícia Federal e National Crime Agency firmam acordo de cooperação policial em Londres. *gov.br*. https://www.gov.br/pf/pt-br/assuntos/noticias/2024/04/policia-federal-e-national-crime-agency-firmam-acordo-de-cooperacao-policial-em-londres

Poupart, J. (2014). A entrevista de tipo qualitativo: Considerações epistemológicas, teóricas e metodológicas. *Em* A. S. Turato, B. J. B. Fontanella, & M. G. B. Saidel (Orgs.), *A pesquisa qualitativa: Enfoques epistemológicos e metodológicos* (pp. 215–253). Vozes.

Razzaq, S., Shujahat, M., Hussain, S., Nawaz, F., Wang, M., Ali, M., & Tehseen, S. (2019). Knowledge management, organizational commitment and knowledge-worker performance: The neglected role of knowledge management in the public sector. *Business Process Management Journal, 25*(5), 923–947. https://doi.org/10.1108/BPMJ-03-2018-0079

Rego, A., Cunha, M. P., & Meyer, V. (2018). Quantos participantes são necessários para um estudo qualitativo? 17(2), 43–57.

Rios-Ballesteros, N., & Fuerst, S. (2022). Exploring the enablers and microfoundations of international knowledge transfer. *Journal of Knowledge Management, 26*(7), 1868–1898. https://doi.org/10.1108/JKM-04-2021-0344

Safernet. ([s.d.]). Delegacias Cibercrimes. Safernet. Recuperado 18 de maio de 2024, de https://new.safernet.org.br/content/delegacias-cibercrimes

Sahibzada, U. F., & Mumtaz, A. (2023). Knowledge management processes toward organizational performance – a knowledge-based view perspective: an analogy of emerging and developing economies. *Business Process Management Journal, 29*(4), 1057 – 1091. https://doi.org/10.1108/BPMJ-09-2022-0457

Salleh, K., Ahmad, S. N. S., Ikhsan, S. O. S. S., & Chong, S. C. (2011). Perceived KM benefits and obstacles: A survey on government institutions. *Electronic Government, 8*(4), 327 – 342. https://doi.org/10.1504/EG.2011.042810

Sampieri, R. H., Collado, C. F., & Lucio, M. P. B. (2013). Metodologia de pesquisa (5a). Penso.

Santos, M. (2022). *Delegacias virtuais: Veja como denunciar crimes cibernéticos no Brasil*. PSafe. https://www.psafe.com/blog/delegacias-virtuais-como-denunciar-crimes-ciberneticos/

Seba, I., & Rowley, J. (2010). Knowledge management in UK police forces. Journal of Knowledge Management, 14(4), 611–626. https://doi.org/10.1108/13673271011059554

Seba, I., Rowley, J., & Delbridge, R. (2012). Knowledge sharing in the Dubai Police Force. *Journal of Knowledge Management, 16*(1), 114–128. https://doi.org/10.1108/13673271211198972

Seba, I., Rowley, J., & Delbridge, R. (2013). Insights into knowledge sharing in the Dubai police force. *Proceedings of the European Conference on Knowledge Management, ECKM, 2*, 814–822. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84893778691&partnerID=40&md5=53f30c83a144d50e41b22a82e2beec5f

Sharma, A., Pandey, S. K., & Dubey, R. (2023). A timeline analysis of cybercrime and cyberattacks with reference to judicial pronouncements. *Revista Brasileira de Direito, 19*(3), e4986. https://doi.org/10.18256/2238-0604.2023.v19i3.4986

Shehzad, M. U., Zhang, J., Dost, M., Ahmad, M. S., & Alam, S. (2022). Knowledge management enablers and knowledge management processes: a direct and configurational approach to stimulate green innovation. *European Journal of Innovation Management*. https://doi.org/10.1108/EJIM-02-2022-0076

Smith, S., & Johnson, G. (2023). A systematic review of the barriers, enablers and strategies to embedding translational research within the public hospital system focusing on nursing and allied health professions. *PLoS ONE, 18*(2), e0281819. https://doi.org/10.1371/journal.pone.0281819

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. *ERA Forum, 23*(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

Syed-Ikhsan, S. O. S., & Rowland, F. (2004). Knowledge management in a public organization: A study on the relationship between organizational elements and the performance of knowledge transfer. *Journal of Knowledge Management, 8*(2), 95–111. https://doi.org/10.1108/13673270410529145

Tormin, R. V. (2022). Teletrabalho no Departamento Penitenciário Nacional e a Percepção dos Burocratas de Médio Escalão.

Tormin, R. V., & Alves, C. A. M. (2024). O teletrabalho e a percepção dos burocratas de médio escalão: Estudo no Departamento Penitenciário Nacional. *Revista de Direito da Administração Pública, 9*(1), 63-81.

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law and Security Review, 52*. https://doi.org/10.1016/j.clsr.2023.105890

Vergara, S. (2006). Métodos de Pesquisa em Administração (2a). Atlas.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Xanthopoulou, S., Kessopoulou, E., & Tsiotras, G. (2023). KM tools alignment with KM processes: the case study of the Greek public sector. *Knowledge Management Research & Practice,* 21(2), 361–371. https://doi.org/10.1080/14778238.2021.1882891

Yarovenko, H., Lyeonov, S., Wojcieszek, K. A., & Szira, Z. (2023). Do It Users Behave Responsibly in Terms of Cybercrime Protection? *Human Technology, 19*(2), 178–206. https://doi.org/10.14254/1795-6889.2023.19-2.3

Yeh, Y.-J., Lai, S.-Q., & Ho, C.-T. (2006). Knowledge management enablers: A case study. *Industrial Management and Data Systems, 106*(6), 793–810. https://doi.org/10.1108/02635570610671489

Yin, R. K. (2015). Estudo de caso: planejamento e métodos (5nd ed.). Bookman.

Zangirolami-Raimundo, J., Echeimberg, J. O., & Leone, C. (2018). Research methodology topics: Cross-sectional studies. *Journal of Human Growth and Development, 28*(3), 356–360. https://doi.org/10.7322/jhgd.152198

APÊNDICE A – SOLICITAÇÃO DE AUTORIZAÇÃO PARA COLETA DE DADOS

Com fulcro no artigo 5º, inciso XXXIII da Constituição Federal, regulamentado pela Lei nº 12.527, de 18 de novembro de 2011, solicito autorização de acesso a dados para a realização de pesquisa requisito para conclusão do Mestrado Profissional em Administração Pública, promovido pela Universidade de Brasília e patrocinado pela Polícia Federal, modalidade dissertação, com entrega de produto técnico-tecnológico de interesse deste órgão.

DISCENTE: ANDRE LUIS DECCACHE DIAS.

ORIENTADOR: Professor Doutor CARLOS ANDRÉ DE MELO ALVES.

PROGRAMA DE PESQUISA: Universidade de Brasília/Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas – FACE/Programa de Pós-Graduação em Administração – PPGA/Mestrado Profissional em Administração Pública – MPA.

TEMA: "FACILITADORES E OBSTÁCULOS PARA GESTÃO DO CONHECIMENTO EM ATIVIDADES INVESTIGATIVAS RELATIVAS A CRIMES CIBERNÉTICOS: ESTUDO NA PERCEPÇÃO DE POLICIAIS FEDERAIS ".

OBJETIVO: como objetivo geral buscar-se-á descrever os facilitadores e os obstáculos para Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos, na percepção de policiais federais.

DADOS SOLICITADOS: a coleta será feita por meio de **entrevistas, através da plataforma TEAMS ou de forma presencial, com policiais federais (Delegados, Peritos, Agentes, Escrivães, Papiloscopistas) que estejam diretamente envolvidos em investigações de crimes cibernéticos com objetivo de capturar suas percepções sobre facilitadores e obstáculos à Gestão do Conhecimento em suas atividades**; e por meio de pesquisa de **normativos internos não-sigilosos que tratem da Gestão do Conhecimento no âmbito da Polícia Federal**.

JUSTIFICATIVA: o projeto de dissertação objetiva identificar os facilitadores e obstáculos, **na percepção de policiais federais**, à Gestão do Conhecimento nas suas atividades investigativas em crimes cibernéticos em virtude da dinâmica de tais crimes, com muitas inovações técnicas e tecnológicas surgidas em curto prazo, exigindo conhecimento

frequentemente renovado por parte dos investigadores. Desta forma, se faz necessário compreender o que ajuda e o que impede que o conhecimento produzido seja armazenado, documentado e compartilhado, de maneira a aprimorar as investigações em que atuam, trazendo maior eficiência, eficácia e efetividade para suas rotinas, que podem se traduzir em investigações mais céleres e com maiores índices de identificação de autoria e confirmação de materialidade, tendo reflexos diretos na produtividade da Polícia Federal. Tais percepções serão apresentadas em um Relatório Técnico Conclusivo indicando sugestões para eventuais melhorias em conformidade com as entrevistas realizadas.

Cabe ressaltar que **os dados coletados e utilizados possuem propósito estritamente acadêmico, e que serão resguardados o anonimato dos servidores que aceitarem ser entrevistados e o sigilo das informações coletadas, sendo de responsabilidade do solicitante pela guarda das informações coletadas**, conforme preconizado pelo Ofício Circular nº 2/2021/CONEP/SECNS/MS, que dá orientações para a realização de procedimentos de pesquisas em qualquer etapa no ambiente virtual.

Certo da compreensão dessa Coordenação e sensibilidade com as necessidades da produção científica, aguardo deferimento ao tempo em que permaneço à disposição para os esclarecimentos pertinentes.

[redacted], na data da assinatura

ANDRÉ LUIS **DECCACHE** DIAS

[redacted]

[redacted]

APÊNDICE B – ROTEIRO DE ENTREVISTAS

Módulo I

1) Comente sobre a sua experiência em atividades investigativas relativas a crimes cibernéticos.
2) O que você entende por Gestão do Conhecimento?
3) Na sua visão, quais são os facilitadores à Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos?
4) Na sua visão, quais são os obstáculos à Gestão do Conhecimento em atividades investigativas relativas a crimes cibernéticos?
5) Você teria algo a acrescentar e que não foi abordado nas perguntas anteriores?

Módulo II (Demográficos)

6) CARGO:
   - Delegado
   - Perito Criminal
   - Agente
   - Escrivão
   - Papiloscopista
7) Tempo de Serviço na Polícia Federal (em anos):
8) Tempo de Atuação em atividades investigativas relativas a crimes cibernéticos (em anos):

Conceitos

- **Crimes Cibernéticos:** atividade criminal em que serviços ou aplicativos no espaço cibernético são usados para, ou são alvo de, um crime, ou em que o espaço cibernético é a fonte, ferramenta, alvo ou local de um crime (ABNT, 2015);
- **Espaço Cibernético:** ambiente complexo resultante da interação de pessoas, softwares ou serviços na internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe qualquer forma física (ABNT, 2015).
- **Facilitadores:** elementos que promovem ou apoiam os objetivos do sistema de Gestão do Conhecimento (GC), priorizando a cobertura dos fatores capital humano, processos, tecnologia e infraestrutura, governança, e cultura de GC (ISO, 2018);
- **Obstáculos:** barreiras que impedem o pleno aproveitamento do conhecimento por parte da organização, podendo ser de origem humana, organizacional e ambiental (Oliva, 2014; Oliva & Kotabe, 2019);

Referências

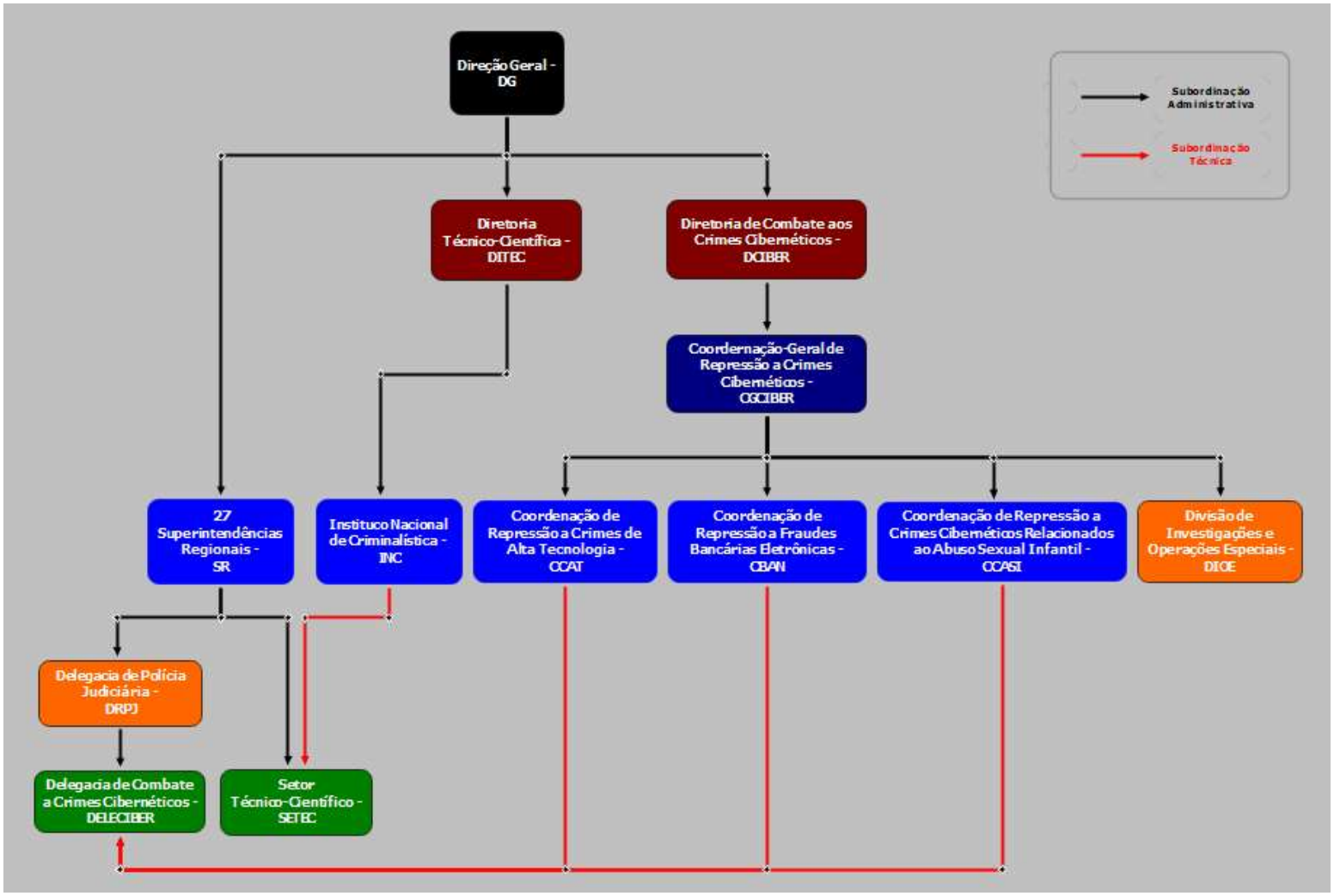
Associação Brasileira de Normas Técnicas (ABNT). (2015). *NBR ISO/IEC 27032/2015: Diretrizes para segurança cibernética*. www.abnt.org.br

International Organization for Standadization (ISO). (2018). *ISO 30.401:2018: Knowledge management systems-Requirements*. www.iso.org

Oliva, F. L. (2014). Knowledge management barriers, practices and maturity model. *Journal of Knowledge Management*, *18*(6), 1053–1074. https://doi.org/10.1108/JKM-03-2014-0080

Oliva, F. L., & Kotabe, M. (2019). Barriers, practices, methods and knowledge management tools in startups. *Journal of Knowledge Management*, *23*(9), 1838–1856. https://doi.org/10.1108/JKM-06-2018-0361

APÊNDICE C - ESTRUTURA DA PF PARA INVESTIGAÇÕES DE CRIMES CIBERNÉTICOS (SIMPLIFICADA E ADAPTADA)



APÊNDICE D – DOCUMENTOS SELECIONADOS PARA ANÁLISE DOS DADOS

Quadro 5 - Documentos da organização com alguma ligação com GC coletados na pesquisa

Documento / Norma	Breve Descrição
Portaria nº 5962-DG/DPF, de 8 de dezembro de 2015	Institui a política de gestão do conhecimento na Polícia Federal
Portaria nº 6194-DG/DPF, de 16 de março de 2016	Institui a política de desenvolvimento de pessoal no âmbito da Polícia Federal.
Plano Diretor Institucional da Academia Nacional de Polícia 2021/2025 (2020)	Identifica a filosofia de trabalho, a missão diretrizes pedagógicas, estrutura organizacional e atividades acadêmicas que desenvolve e que pretende desenvolver
Lici. Projeto Básico Nº 25100540/2022-SELIC/DAD/DTI/PF	Contratação de empresa para prestação de serviços e suporte para produtos Microsoft
Resolução CG/PF Nº 5, de 12 de agosto de 2021	Plano Estratégico da Polícia Federal 2021-2023 (2021)
Portaria DG/PF Nº 18.703, de 27 de outubro de 2023	Institui o Sistema de Governança da Polícia Federal.
Instrução Normativa DG/PF Nº 270, de 15 de dezembro de 2023	Estabelece as competências específicas das unidades centrais e descentralizadas da Polícia Federal e as atribuições de seus dirigentes
Projeto de Transformação Organizacional PF80 (2024)	apresentar os resultados obtidos com a Oficina de Planejamento Estratégico, primeira etapa prevista para a elaboração do Planejamento Estratégico 2024-2027
Resolução CG/PF Nº 007, de 27 de maio de 2024	Convalida o novo Sistema de Governança da Polícia Federal - SGPF e aprova o Plano Estratégico da Polícia Federal 2024/2027.

Fonte: dados da pesquisa

Apresenta-se no Apêndice D documentos selecionados para análise dos dados. Dos documentos mencionados, três são diretamente relevantes para este estudo devido à sua conexão com os resultados encontrados: a Portaria nº 5962-DG/DPF, de 8 de dezembro de 2015 (DPF, 2015), que discorre sobre a Gestão do Conhecimento na Polícia Federal; o Projeto de Transformação Estratégica Organizacional PF80 (PF, 2023d), que detalha diagnósticos de problemas identificados na instituição; em complemento, aponta-se o Projeto Básico Nº 25100540/2022-SELIC/DAD/DTI/PF (PF, 2022b), que versa sobre a contratação de suporte para serviços *Microsoft*, aponta para a existência dos sistemas de tecnologia da informação e comunicação citados por alguns entrevistados e traz informações sobre o uso de tais sistemas.

APÊNDICE E – ELEMENTOS CONFIRMADOS E INCLUÍDOS NAS ENTREVISTAS

Nº	Identificação dos primeiros elementos	Documentos relacionados
Categoria - Conceito de Gestão do Conhecimento		
1	Gestão no que diz respeito ao conhecimento, fazendo uso de uma abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados, que incluem a otimização da identificação, criação, análise, representação, distribuição e aplicação do conhecimento para criar valor organizacional.	DPF, 2015
EC	**Elementos do Conceito de Gestão do Conhecimento**	
1	Gestão voltada ao conhecimento	DPF, 2015
2	Abordagem holística e sistêmica em busca de aprendizado e melhoria de resultados	DPF, 2015
3	Identificação do conhecimento	DPF, 2015
4	Criação do Conhecimento	DPF, 2015
5	Análise do conhecimento	DPF, 2015 (implícito)
6	Representação do Conhecimento	DPF, 2015
7	Distribuição do Conhecimento	DPF, 2015
8	Aplicação do Conhecimento	DPF, 2015

Categoria - Facilitadores à Gestão do Conhecimento		Nível	Documentos relacionados
1	A existência de Infraestrutura de Tecnologia da Informação e Comunicação	Organizacional	PF, 2022b
2	Apoio da liderança à cultura de compartilhamento do conhecimento	Organizacional	PF, 2024e
3	A existência de cursos e treinamentos na área de atuação do servidor	Organizacional	ANP, 2021
4	A presença de canais formais de comunicação com outras instituições para permitir a troca de informações	Organizacional	PF, 2024e
5	O alto nível educacional e o conhecimento especializado dos empregados	Individual	Brasil, 1996; PF 2021c
6	Manifestação da habilidade e do Interesse dos servidores em Adquirir, Compartilhar e Utilizar Conhecimentos	Individual	PF, 2023d
7	Evidência da participação ativa do servidor em redes sociais promovendo a circulação de informações que subsidiam suas atividades	Individual	PF, 2022b

Categoria - Obstáculos à Gestão do Conhecimento		**Nível**	**Documentos relacionados**
1	Rotatividade de pessoal sem transmissão de conhecimento	Organizacional	PF, 2024d
2	Restrição do acesso à informações necessárias para a atividade investigativa em decorrência do sigilo legal	Ambiental	Brasil, 1941
3	Falta de uniformidade nos procedimentos de compartilhamento de informações e conhecimento	Organizacional	PF, 2023d
4	Priorização de execução de tarefas em detrimento da aquisição do conhecimento	Organizacional	PF, 2023d
5	Ausência de políticas para promover a gestão e compartilhamento de conhecimento	Organizacional	PF, 2023d
6	Comunicação ineficiente sobre fontes de informação e de conhecimento e sobre iniciativas de capacitação	Organizacional	PF, 2023d
7	Liderança não comprometida com GC	Organizacional	PF, 2023d
8	Falta de recursos adequados para Gestão do Conhecimento	Organizacional	PF, 2023d
9	Falta de confiança em relação aos outros na Gestão do Conhecimento	Individual	PF, 2023d
10	Falta de vontade ou motivação para compartilhar informações ou conhecimento	Individual	PF, 2023d