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

COMPETÊNCIAS PARA O CARGO DE OFICIAL DE INTELIGÊNCIA: PROPOSTA DE MODELO BASEADO EM DESAFIOS ESTRATÉGICOS DA ATIVIDADE DE INTELIGÊNCIA NO BRASIL

Luiz Cláudio de Queiroz Rodrigues

Brasília, DF
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

COMPETÊNCIAS PARA O CARGO DE OFICIAL DE INTELIGÊNCIA: PROPOSTA DE MODELO BASEADO EM DESAFIOS ESTRATÉGICOS DA ATIVIDADE DE INTELIGÊNCIA NO BRASIL

Luiz Cláudio de Queiroz Rodrigues

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: Prof. Dr. Antônio Isidro da Silva Filho

Brasília, DF

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

Luiz Cláudio de Queiroz Rodrigues

COMPETÊNCIAS PARA O CARGO DE OFICIAL DE INTELIGÊNCIA: PROPOSTA DE MODELO BASEADO EM DESAFIOS ESTRATÉGICOS DA ATIVIDADE DE INTELIGÊNCIA NO BRASIL

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.

Local e data da defesa: Brasília/DF, em 29/07/2025.

Comissão Examinadora:

Prof. Dr. Antônio Isidro da Silva Filho – Orientador
MPA/PPGA/UnB

Prof. Dr. Francisco Antônio Coelho Junior – Examinador Interno
MPA/PPGA/UnB

Prof. Dra. Mariana Carolina Barbosa Rego – Examinadora Externa
Instituto Federal de Brasília

Prof. Dra. Marina Figueiredo Moreira – Examinadora Suplente
MPA/PPGA/UnB

DEDICATÓRIA

À Deus, sustentáculo em todo percalço.

À minha filha Laís, cuja doçura e alegria me lembram todos os dias do que realmente importa. Que este trabalho, fruto de esforço e perseverança, seja um testemunho de que o conhecimento transforma e de que os sonhos são sempre possíveis, sobretudo quando temos por quem e por que lutar.

Aos meus pais e irmãos, por me ensinarem a transformar estudo em propósito.

Aos amigos *Daniel Macedo*, *Daniel Monteiro*, *Gustavo Moraes*, *Pedro Paulo Simão da Rocha*, *Roniere Amaral* e *Wallace Dias*, pelas conversas, conselhos e incentivos diários – sem os quais não teria iniciado, persistido e concluído esta caminhada. Vocês foram os companheiros mais próximos nessa trajetória.

Aos Oficiais de Inteligência da ABIN, cujo trabalho silencioso, abnegado e longe dos holofotes protege o país. Sua dedicação é alicerce para um Brasil soberano.

À Universidade de Brasília, idealizada por Darcy Ribeiro e que há mais de seis décadas resiste no esforço de ser um centro de excelência educacional público, gratuito e a serviço do povo brasileiro. Que esta dissertação seja uma pequena contribuição à sua história de resistência.

AGRADECIMENTOS

A Deus, por conceder saúde, força e discernimento ao longo de toda esta jornada. Sua presença silenciosa e constante foi fundamental em cada etapa deste percurso.

À minha família, por ser fonte permanente de amor e inspiração. O apoio contínuo e a confiança depositada em mim foram pilares fundamentais para a realização deste trabalho.

Ao Prof. Antônio Isidro Filho, pela escuta, contribuições sempre lúcidas e acompanhamento ao longo da pesquisa. Sua atuação foi essencial para a maturação das ideias e para a consolidação desta dissertação.

À Universidade de Brasília (UnB), em especial ao Programa de Pós-Graduação em Administração Pública – Mestrado Profissional (MPA), pela excelência do curso e pela oportunidade de aprofundamento técnico e intelectual.

Aos professores do MPA/UnB, agradeço pelo conhecimento compartilhado e pelo compromisso com a formação de gestores públicos comprometidos com o bem comum.

Aos colegas de turma, pela parceria, incentivo e aprendizado coletivo ao longo dessa trajetória. A convivência e as trocas enriquecedoras tornaram o caminho mais leve e significativo.

Aos Oficiais de Inteligência que participaram desta pesquisa, meu profundo agradecimento pela disponibilidade, pela seriedade com que acolheram o convite e pelas valiosas contribuições oferecidas. Suas experiências foram essenciais para a construção dos achados desta dissertação.

Sejam fortes e corajosos, não tenham medo nem fiquem apavorados, pois o Senhor, o seu Deus, vai com vocês, nunca os deixará, nunca os abandonará.

Deuteronômio 31:6

Resumo

Este trabalho tem por objetivo desenvolver um *framework* de competências direcionado ao cargo de Oficial de Inteligência da Agência Brasileira de Inteligência (ABIN), a partir da identificação de desafios institucionais estratégicos. A pergunta central que orienta o estudo é: *quais competências devem compor um framework voltado à atuação do Oficial de Inteligência da ABIN, a partir da análise de desafios institucionais?* A pesquisa adota abordagem qualitativa, fundamentada em entrevistas com Oficiais de Inteligência com experiência em posições gerenciais e na análise do documento "Desafios de Inteligência – Edição 2025", de natureza pública. A partir dessa triangulação metodológica, foram identificados seis desafios estratégicos que sustentam a formulação de 26 competências essenciais ao desempenho da função. Cada competência foi estruturada com base no modelo CHA (conhecimentos, habilidades e atitudes), incluindo padrões de desempenho observáveis. O *framework* resultante busca suprir lacunas no modelo atual de gestão por competências, ainda incipiente e pouco sistematizado no contexto da ABIN, oferecendo um instrumento técnico que pode subsidiar ações de capacitação, recrutamento interno, avaliação de desempenho e planejamento estratégico da força de trabalho. A análise evidenciou a transversalidade das competências mapeadas, revelando forte interdependência entre os desafios enfrentados pela organização. Em razão das restrições impostas pelo sigilo institucional, o estudo fundamenta-se exclusivamente em fontes públicas e entrevistas previamente autorizadas. A proposta contribui para o amadurecimento da gestão por competências em ambientes de alta complexidade e sugere, como agenda de pesquisa futura, a realização de análises comparadas com modelos de países do Sul Global.

Palavras-chave: Gestão por Competências; Atividade de Inteligência; *Framework* de Competências.

Abstract

This study aims to develop a competency framework for the position of Intelligence Officer at the Brazilian Intelligence Agency (ABIN), based on the identification of strategic institutional challenges. The central research question that guides the study is: *which competencies should compose a framework directed at the performance of ABIN's Intelligence Officers, based on the analysis of institutional challenges?* The research adopts a qualitative approach, grounded in interviews with Intelligence Officers who have experience in managerial positions and in the analysis of the publicly available document "Desafios de Inteligência – Edição 2025". Through this methodological triangulation, six strategic challenges were identified, which support the formulation of 26 core competencies required for the role. Each competency was structured according to the CHA model (knowledge, skills, and attitudes), including observable performance standards. The resulting framework aims to address gaps in the current competency management model, which remains incipient and insufficiently systematized in the ABIN context, by offering a technical instrument to support training, internal recruitment, performance evaluation, and strategic workforce planning. The analysis highlighted the transversal nature of the identified competencies, revealing a strong interdependence between the challenges faced by the organization. Due to restrictions imposed by institutional confidentiality, the study is based exclusively on public sources and previously authorized interviews. The proposed framework contributes to the advancement of competency-based management in high-complexity environments and suggests, as a future research agenda, comparative analyses with models adopted in Global South countries.

Keywords: Competency-Based Management; Intelligence Activity; Competency Framework.

Sumário

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ABIN – Agência Brasileira de Inteligência

APT – *Advanced Persistent Threats*

CAPES – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CHA – Competências, Habilidades e Atitudes

DSR – *Design Science Research*

ESG – Escola Superior de Guerra

GPC – Gestão por Competências

HUMINT – *Human Intelligence*

ODNI – *Office of the Director of National Intelligence*

OSINT – *Open Source Intelligence*

PTT – Produto Técnico Tecnológico

SFICI – Serviço Federal de Informações e Contra-Informações

SOCMINT – *Social Media Intelligence*

SNI – Serviço Nacional de Informações

UFO – Ontologia Fundacional Unificada

UnB – Universidade de Brasilia

1. INTRODUÇÃO

O desempenho institucional de organizações públicas de caráter estratégico, como os Serviços de Inteligência, depende não apenas de estruturas organizacionais e recursos materiais, mas, sobretudo, de pessoas capacitadas e alinhadas às finalidades e desafios próprios dessas instituições. Em contextos de alta complexidade e exigência técnico-operacional, como o vivenciado pela Agência Brasileira de Inteligência (ABIN), a existência de padrões claros sobre as competências requeridas dos seus servidores torna-se condição fundamental para o fortalecimento da gestão e a elevação do desempenho organizacional. É nesse cenário que se insere a proposta de construção de um *framework* de competências voltado ao cargo de Oficial de Inteligência da ABIN.

No Brasil, o ingresso na carreira de Oficial de Inteligência ocorre por meio de concurso público de provas e títulos, com foco principal na aferição de conhecimentos teóricos. No entanto, o desempenho cotidiano dessa função exige competências que transcendem a dimensão cognitiva e incluem habilidades práticas e atitudes comportamentais que o modelo atual de seleção dificilmente consegue captar. Conforme Coelho e Menon (2018) a lógica tradicional dos concursos públicos, centrada na avaliação de conhecimentos teóricos, mostra-se anacrônica diante do paradigma da gestão por competências (GPC), que exige aferição integrada de conhecimentos, habilidades e atitudes. Isso impõe o desafio de repensar os mecanismos de ingresso no serviço público, buscando formas mais eficazes de selecionar profissionais alinhados às demandas reais dos cargos.

A atuação em ambientes de incerteza, pressão e alta responsabilidade demanda, por exemplo, controle emocional, discrição, capacidade de análise contextual e postura ética. A ausência de mecanismos específicos para aferição dessas dimensões no processo seletivo compromete a capacidade institucional de identificar perfis mais aderentes às complexidades reais da Atividade de Inteligência.

A GPC, nesse sentido, oferece uma abordagem estruturada para integrar planejamento estratégico e desenvolvimento de pessoas. Trata-se de um modelo amplamente adotado em diversas administrações públicas no Brasil e em experiências internacionais, como em agências das comunidades de Inteligência dos Estados Unidos e da França, que já incorporam *frameworks* de competências a seus processos de recrutamento, credenciamento e capacitação. Esses *frameworks* contribuem para o alinhamento entre metas institucionais e o desempenho individual, ampliando a racionalidade da alocação de recursos humanos e fortalecendo a cultura organizacional.

Embora a ABIN possa dispor de diretrizes internas voltadas à GPC, é provável que tais instrumentos sejam mantidos sob reserva, em conformidade com os princípios de proteção e discrição que regem a Atividade de Inteligência. Não foram encontrados, no escopo desta pesquisa, documentos públicos, sistematizados e técnicos que descrevam todas as competências essenciais ao exercício do cargo de Oficial de Inteligência. Essa lacuna configura uma oportunidade relevante de proposição técnica que auxilie a Agência no aperfeiçoamento de seus instrumentos de gestão de pessoas.

Nesse contexto, o problema central da presente pesquisa pode ser sintetizado na seguinte pergunta: quais competências devem compor um *framework* voltado à atuação do Oficial de Inteligência da ABIN, a partir da análise de desafios institucionais contemporâneos para a Atividade de Inteligência? A resposta a essa indagação orienta o esforço metodológico e fundamenta a construção do Produto Técnico-Tecnológico (PTT) proposto, buscando identificar e delinear um conjunto estruturado de competências para o cargo de Oficial de Inteligência, assegurando em última instância a eficiência e eficácia das operações realizadas pela Agência.

Derivados deste objetivo geral foram delineados os seguintes objetivos específicos:

a) localizar modelos ou *frameworks* de competências para Serviços de Inteligência;

b) identificar a percepção de Oficiais de Inteligência que ocuparam função gerencial na ABIN a respeito do tema gestão por competências na organização.

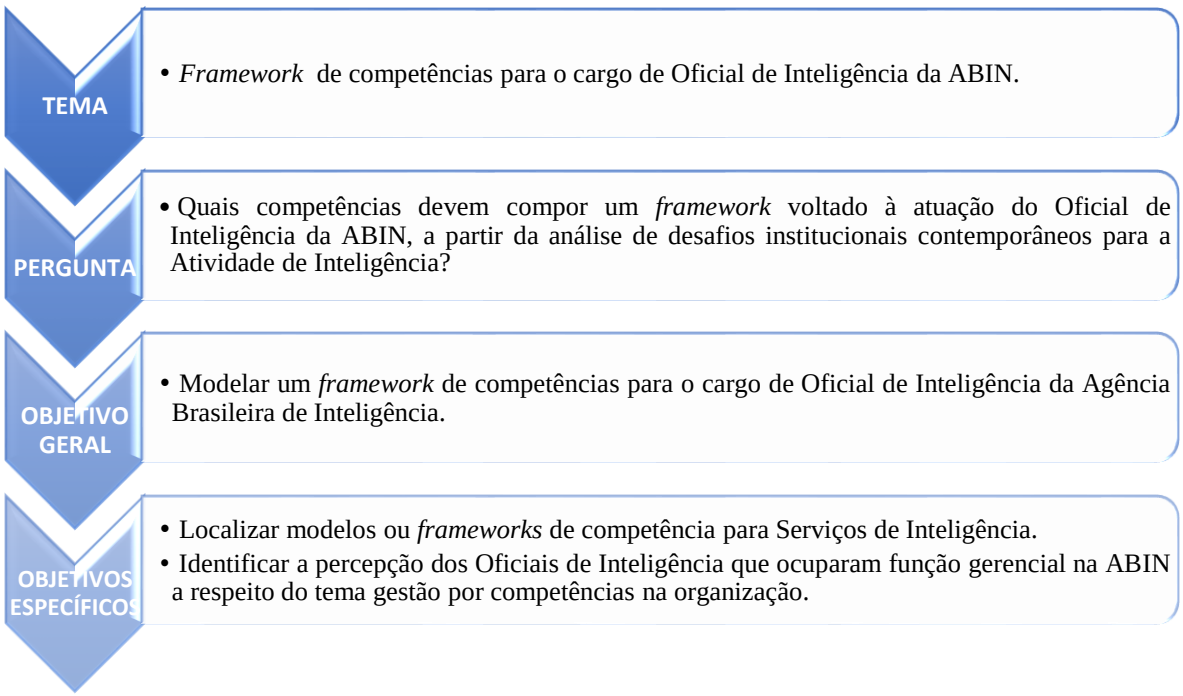


Figura 1 – Etapas de delineamento da pesquisa.

O *framework* de competências, caracterizado como um Produto Técnico-Tecnológico (CAPES, 2019) e desenvolvido especificamente nesta pesquisa para atender as particularidades do cargo de Oficial de Inteligência da ABIN traz vantagens ao alinhar as competências individuais desses profissionais com as necessidades institucionais, subsidiando a estruturação de processos de recrutamento, de desenvolvimento profissional e de avaliação de desempenho, além de promover uma cultura organizacional alinhada com os objetivos estratégicos da instituição. Isso inclui a adaptação de competências ao contexto local, considerando aspectos como a legislação nacional e as ameaças específicas enfrentadas pelo Brasil – elencadas, por exemplo, na Política Nacional de Inteligência (2016) e no documento Desafios de Inteligência – Edição 2025 (ABIN, 2024).

Esta dissertação está estruturada em seis capítulos, incluindo esta introdução. O capítulo seguinte apresenta a fundamentação teórica que sustenta a pesquisa, abordando a evolução histórica da institucionalização dos Serviços de Inteligência, referenciais internacionais de competências na Atividade de Inteligência bem como conceitos centrais relacionados ao construto modelagem de competências (*competency modelling*). No terceiro capítulo, é detalhado o método empregado para a construção do *framework* de competências voltado ao cargo de Oficial de Inteligência da ABIN. O quarto capítulo é destinado à apresentação e análise dos resultados obtidos com o estudo empírico realizado, com destaque para a identificação dos desafios institucionais e das competências necessárias para enfrentá-los, bem como a percepção dos Oficiais de Inteligência que ocuparam função gerencial na ABIN a respeito do tema gestão por competências na organização. O quinto capítulo sintetiza as conclusões alcançadas pelo estudo e sugere possibilidades para estudos futuros. Por fim, o sexto capítulo descreve o Produto Técnico-Tecnológico desenvolvido no âmbito desta pesquisa, apresentando suas principais características e aplicações práticas.

2. QUADRO TEÓRICO

Esse capítulo encontra-se segmentado em três seções. A primeira delineia as origens históricas e a evolução da Atividade de Inteligência, no mundo e no Brasil. A segunda seção aborda os referenciais de competências na Atividade de Inteligência dos Estados Unidos e da França. Por fim, a terceira seção esmiuça as bases teóricas, abordagens metodológicas e tendências referente ao construto modelagem de competências (*competency modeling*).

2.1. Institucionalização da Atividade de Inteligência: origens históricas e evolução.

Conforme Dulles, na obra *The Craft of Intelligence* (1963), a gênese dos Serviços de Inteligência remonta ao século XV, quando as cidades-estados italianas estabeleceram embaixadas no exterior, das quais os enviados obtinham informações estratégicas e em cujas bases fixaram redes regulares de espionagem. A partir do século XVI, no contexto da formação dos Estados nacionais, tais informações passaram a ser processadas em organizações permanentes e profissionais, inseridas na burocracia estatal, dando origem ao que se denomina Atividade de Inteligência (Brasil, 2016).

A Atividade de Inteligência como parte da burocracia do Estado originou-se de quatro matrizes institucionais e históricas: economia, guerra, diplomacia e polícia. As matrizes polícia e guerra, em especial, vincularam a Atividade de Inteligência ao aspecto coercitivo do Estado. No entanto, ao contrário dos demais aparatos coercitivos, não se fundamenta na força, e sim no conhecimento e no segredo, com o desempenho de função essencialmente informacional (Cepik, 2003). Na era moderna, a Atividade de Inteligência foi estabelecida como uma estrutura burocrática estatal, operando sob os princípios da razão de Estado. Essa lógica política era empregada para legitimar o uso de segredos de Estado e certas ações que apenas o Estado poderia legalmente executar (Brasil, 2016).

No século XIX, registrou-se de forma mais significativa a formalização dos Serviços de Inteligência, notadamente na Europa. Nesse período, países como Inglaterra e França estabeleceram unidades dedicadas à coleta de informações para fins militares e políticos, marcando o início da Atividade de Inteligência organizada como uma extensão do Estado moderno (Andrew, 2018).

Na primeira metade do século XX, a Segunda Guerra Mundial remodelou a Atividade de Inteligência, catalisando a burocratização de estruturas de Inteligência militar. Essas, que inicialmente focaram suas ações em espionagem e contraespionagem, expandiram seu escopo para incluir coleta de informações políticas, econômicas e de segurança. Ao término do conflito

armado, não houve desmobilização das estruturas militares de Inteligência, mas a elas foram adicionados novos organismos civis de Inteligência às estruturas estatais, que juntos passaram a atuar no período da Guerra Fria.

A participação brasileira na Segunda Guerra Mundial marcou um ponto crucial na evolução da Atividade de Inteligência no país. Em 1946, o presidente Eurico Gaspar Dutra instituiu o Serviço Federal de Informações e Contra-Informações (SFICI), o primeiro órgão brasileiro dedicado exclusivamente à Inteligência. Este órgão se tornou plenamente operacional apenas em 1956, durante o governo de Juscelino Kubitschek, ampliando suas operações para abranger áreas internas e externas, além de segurança interna e operações diversas (Brasil, 2016).

Em paralelo ao desenvolvimento do SFICI, a Escola Superior de Guerra (ESG), fundada em 1949 e inspirada pelo *National War College* dos Estados Unidos, começou a oferecer cursos destinados a formar especialistas para atuar no SFICI. A ESG tinha como objetivo preparar as elites militares e civis para o assessoramento das políticas governamentais de segurança e desenvolvimento, especialmente relevantes no contexto da Guerra Fria. A existência da ESG foi fundamental para o estabelecimento subsequente, em 1964, do Serviço Nacional de Informações (SNI), um órgão mais amplo e diretamente ligado ao Presidente da República, que se concentrou no monitoramento de ameaças internas.

O SNI foi instrumental na expansão da Atividade de Inteligência no Brasil, com agências em diversas capitais brasileiras e cobrindo todo o território nacional. Além disso, a estrutura de formação em Inteligência foi reforçada com a criação, em 1971, da Escola Nacional de Informações. No período compreendido entre 1972 e 1990, esta foi a única unidade de ensino no país voltada para essa finalidade.

Os processos de fim da Guerra Fria e da redemocratização do Brasil impuseram mudanças na Atividade de Inteligência. Com a Nova República e a promulgação da Constituição, houve a extinção do SNI em 1990, o que gerou reformulações estruturais na Atividade de Inteligência brasileira. Entre 1990 e 1999, esta foi reorganizada sob diferentes denominações e subordinações hierárquicas e também expandiu-se para abordar questões como crime organizado transnacional, terrorismo, entre outros desafios. Por fim, com a sanção da Lei n.º 9.883/99, a ABIN foi finalmente estabelecida como o órgão de Inteligência do Estado brasileiro.

Feito o delineamento histórico do processo de institucionalização dos Serviços de Inteligência, tanto no mundo quanto no Brasil, patente está que estas organizações integram a estrutura estatal e executam tarefa especializada, qual seja a de adquirir, analisar e repassar

informações importantes e essenciais para auxiliar o governo na tomada de decisões estratégicas nas áreas de política externa e interna e de manutenção da ordem pública (Cepik, 2003). Nesse sentido e para o bom desempenho de suas missões institucionais, os Serviços de Inteligência necessitam recrutar, selecionar, capacitar e manter profissionais em seus quadros que não sejam apenas academicamente preparados, mas providos de habilidades e atitudes para o exercício deste *múnus* público, que se posiciona em patamar estratégico na estrutura dos Estados modernos.

Como organizações, ou seja, definidas como entidades sociais com missão e visão clara, orientadas para metas e projetadas como sistemas de atividades coordenadas que interagem com o ambiente externo (Daft, 2016), os Serviços de Inteligência devem estruturar seus recursos humanos de forma adequada para alcançar seus objetivos e adaptar-se a mudanças externas. A GPC emerge como uma tecnologia que pode oferecer suporte para o desenvolvimento e a eficácia dos Serviços de Inteligência, auxiliando-os no cumprimento de suas missões.

2.2. Referenciais internacionais de competências na Atividade de Inteligência.

No cenário internacional, registra-se que distintos Serviços de Inteligência estruturam seus processos de recrutamento e desenvolvimento de Profissionais de Inteligência com base na modelagem de competências. Pesquisa efetuada no buscador Google, com a utilização articulada dos termos "*Competency framework*", "*US Intelligence workforce*", "*US Intelligence workforce skills framework*", "*Competency-Based Management and Intelligence Service*", "*Intelligence Community skills and competencies*" e "*France Renseignement competence*" permitiu a identificação de normativas que corroboram essa abordagem na Comunidade de Inteligência dos Estados Unidos e da França.

Nos Estados Unidos, o *Office of the Director of National Intelligence* (ODNI) – órgão responsável pela coordenação das 18 agências da Comunidade de Inteligência estadunidense, conforme apresentado na tabela 1 – publicou em 2008 a *Intelligence Community Directive 651***.** Esse documento estabelece diretrizes e políticas para a gestão dos profissionais que atuam nessas organizações.

NOMINATA DAS 18 AGÊNCIAS QUE COMPÕEM O ODNI	
01 – Air Force Intelligence	05 – Drug Enforcement Administration
02 – Army Intelligence	06 – Federal Bureau of Investigation
03 – Central Intelligence Agency	07 – Marine Corps Intelligence
04 – Coast Guard Intelligence	08 – National Geospatial Intelligence Agency
09 – Defense Intelligence Agency	14 – National Reconnaissance Office
10 – Department of Energy	15 – National Security Agency
11 – Department of Homeland Security	16 – Navy Intelligence
12 – Department of State	17 – Office of the Director National Intelligence
13 – Department of the Treasury	18 – Space Force Intelligence

Tabela 1 – Nominata das agências que compõem o ODNI.

Derivado desse primeiro documento, emergiram outros cinco que detalham o tema para a Comunidade de Inteligência estadunidense, conforme descrito na tabela 2:

DOCUMENTO	TRADUÇÃO	OBJETIVOS
Competency Library for the Intelligence Community Workforce (ICD 610)	Biblioteca de Competências para a Força de Trabalho da Comunidade de Inteligência	O documento estabelece uma nomenclatura padronizada de competências, fornecendo definições para caracterizar as habilidades da força de trabalho da Comunidade de Inteligência dos Estados Unidos. Ele institui uma biblioteca inicial de competências e determina que critérios como qualificação, treinamento, desenvolvimento de carreira, avaliação de desempenho, promoção e outros aspectos relacionados à gestão de pessoal civil da Comunidade de Inteligência sejam baseados nestas competências e na terminologia estabelecida.
Intelligence Community Competency Taxonomy (ICS 610.2)	Taxonomia de Competências da Comunidade de Inteligência	O documento estabelece a estrutura e a nomenclatura utilizadas para sistematizar as informações sobre as competências da força de trabalho da Comunidade de Inteligência dos Estados Unidos. Essa taxonomia possibilita que o ODNI implemente e administre um sistema padronizado que detalha as funções e habilidades da Comunidade de Inteligência, empregando definições uniformes.
Core competencies for non-supervisionary Intelligence Community employees at GS-15 and below (ICS 610.3)	Competências essenciais para funcionários da Comunidade de Inteligência não supervisionados nos níveis GS-15 e abaixo	O documento define rótulos e descrições para as competências fundamentais que se aplicam a todos os empregados do sistema *General Schedule*[1] até o nível GS-15, incluindo funcionários civis não executivos da Comunidade de Inteligência (IC), independentemente de categoria de missão ou grupo ocupacional. É importante destacar que estas competências essenciais formam a base para as competências e elementos de desempenho de supervisores e gerentes civis da Comunidade de Inteligência até o nível GS-15 ou equivalente, conforme estabelecido no ICS 610-4, assim como para os Oficiais Seniores do IC, conforme descrito no ICS 610-5.
Core competencies for supervisionary and managerial Intelligence Community employees at GS-15 and below (ICS 610.4)	Competências essenciais para funcionários da Comunidade de Inteligência de supervisão e gestão nos níveis GS-15 e abaixo	O documento estabelece rótulos e definições para competências fundamentais que se aplicam a todos os funcionários do sistema *General Schedule* até o nível GS-15, incluindo aqueles em posições de supervisão ou gestão da Comunidade de Inteligência, independentemente da categoria de missão ou grupo ocupacional. É importante ressaltar que as competências fundamentais delineadas para funcionários civis da Comunidade de Inteligência que não são supervisores no nível GS-15 ou equivalente (conforme descrito na ICS 610-3) são usadas como alicerce para as competências e os elementos de desempenho apresentados neste documento. Adicionalmente, as competências essenciais descritas no documento ICS 610.4 também formam a base para as competências e elementos de desempenho dos Oficiais Superiores da Comunidade de Inteligência, como detalhado na ICS 610-5.

[1] O sistema *General Schedule* (GS) é utilizado pelo governo federal estadunidense para fixar padrões remuneratórios e de progressão dos funcionários públicos civis, especialmente para posições técnicas e administrativas. Composto por 15 níveis – sendo o GS-1 o mais baixo e o GS-15 o mais alto – o sistema *General Schedule* revela-se crítico na gestão de recursos humanos daquele país, influenciando como posições de liderança e de especialistas são valorizadas e compensadas. Alcançar o GS-15 é visto como um marco na carreira de um funcionário público nos Estados Unidos, refletindo um nível de confiança e responsabilidade considerável.

Core competencies for Intelligence Community Senior Officers (ICS 610.5)	Competências essenciais para oficiais superiores da Comunidade de Inteligência	O documento apresenta rótulos e definições para competências essenciais de liderança destinadas a todos os executivos seniores, isto é, aqueles funcionários que ocupam posições acima do nível 15 no sistema *General Schedule* ou equivalente, ou com classificação pessoal comparável. É importante notar que as competências fundamentais estabelecidas para os funcionários civis não supervisores atuantes em organizações da Comunidade de Inteligência no nível GS-15 e inferiores, ou equivalente (descritas no documento ICS 610-3), bem como as destinadas a supervisores e gerentes civis da IC no nível GS-15 e abaixo ou equivalente (documento ICS 610-4), formam a base para os componentes e elementos de desempenho delineados no documento ICS 610.5.

Tabela 2 – Descrição dos documentos do ODNI que versam sobre competências.

Outro documento identificado na pesquisa refere-se ao *Répertoire des Métiers de la Fonction Publique* (*Diretório de Profissões do Serviço Público*, em tradução livre), publicado pelo Ministério da Transformação e Função Pública da França. Essa normativa classifica e descreve as diversas profissões e funções da administração pública francesa, incluindo um capítulo dedicado à Inteligência, no qual são catalogadas 23 ocupações dessa área.

O *Répertoire dés Métiers de la Fonction Publique* baliza processos de recrutamento de Profissionais de Inteligência na França. Seleção realizada no ano de 2024[2] pela *Direction du Renseignement et de la Sécurité de la Défense* – organização subordinada ao Ministério da Defesa e uma das seis agências de Inteligência especializadas que compõe o Primeiro Círculo de Inteligência – exigia dos candidatos os conhecimentos, habilidades e atitudes elencados para o cargo de Analista de Inteligência (*Analyste Renseignement*), mostradas na tabela 3:

CARGO	Analista de Inteligência
DEFINIÇÃO	Implementa processos de exploração e análise de Inteligência.
PRINCIPAIS ATIVIDADES	• Implementar o processo de exploração do ciclo de Inteligência; • Avaliar, analisar e perspectivar a Inteligência para antecipar riscos às instituições e aos interesses fundamentais da República Francesa; • Desenvolver notas resumidas e análises estratégicas e disseminar Inteligência.
ELEMENTOS DE COMPETÊNCIA	
CONHECIMENTOS	• Enquadramento administrativo, institucional e político; • Métodos e técnicas de controle; • Compreensão da organização e do ciclo de Inteligência; • Conhecimento geopolítico, geográfico, técnico, temático e/ou linguístico; • Enquadramento legal e jurídico da Inteligência (direito relativo à informação em particular).
HABILIDADES	• Coletar informações; • Analisar e produzir Inteligência; • Dominar sistemas de informação de Inteligência; • Saber como solicitar conhecimentos específicos de Inteligência; • Preservar a confidencialidade das informações;

[2] Link: https://choisirleservicepublic.gouv.fr/wp-content/uploads/pdf-offers/pdf-def_15-00034910/1725693348/analyste-renseignement-choisir-le-service-public.pdf. Último acesso em 13/03/2025.

	• Analisar um contexto/problema; • Demonstrar habilidades comprovadas de redação; • Saber produzir resumos; • Explorar técnicas de Inteligência; • Representar a organização de Inteligência na França ou mesmo no estrangeiro (dependendo dos serviços).
ATITUDES	• Ser organizado e metódico; • Trabalhar em equipe; • Sentido de análise; • Discrição; • Ser perseverante; • Espírito de síntese; • Curiosidade intelectual; • Rigor.
CONDIÇÕES ESPECIAIS DE EXERCÍCIO DO CARGO	
• Realizado na França e, dependendo dos serviços, em operações ou no estrangeiro; • Existência de riscos resultantes da natureza das missões (dependendo dos serviços); • Elevada disponibilidade; • Autorização do sigilo de defesa nacional; • Implementação possível de utilização de recursos linguísticos ou de gestão por competências (coordenação da atividade dos analistas juniores) em função dos serviços; • Transporte de armas (para determinados serviços).	
TENDÊNCIAS DA PROFISSÃO	
• Papel crescente da gestão de dados nos processos de processamento de informação, análise e produção de Inteligência; • Mudanças nas tecnologias de informação; • Massificação dos fluxos de informação (em particular em fontes abertas); e • Conhecimento de dialetos (dependendo dos serviços).	

Tabela 3 – Atributos exigidos para o cargo de Oficial de Inteligência na França.

Considerando o panorama internacional, que evidencia a consolidação de *framework* de competências em Serviços de Inteligência de referência global – como os modelos adotados pelas Comunidades de Inteligência dos Estados Unidos e da França –, a construção de um *framework* adaptado à realidade brasileira assume dupla relevância. Além de modernizar as práticas da ABIN, garantindo alinhamento estratégico com padrões internacionais de excelência, o artefato proposto pode servir de base comparativa para a estruturação de *frameworks* de competências em outras carreiras estratégicas no Brasil. Exemplos incluem ofícios como o de Delegado e Agente de Polícia e o de Perito Criminal, cujas atribuições demandam competências especializadas e integradas a políticas de Estado. Dessa forma, o estudo não apenas profissionaliza e fortalece a Atividade de Inteligência brasileira, mas também oferece um modelo metodológico replicável, capaz de orientar a profissionalização de setores críticos da estrutura estatal, como Segurança Pública.

2.3. Modelagem de competências: bases teóricas, abordagens metodológicas e tendências emergentes.

Para construção desta seção, foi efetuada pesquisa na base *Scopus*, via Portal de periódicos da CAPES, no período de novembro de 2024 a maio de 2025, com a utilização dos termos

"*Competency modeling*"; "*Competency framework*"; e "*Intelligence workforce*". Essa investigação permitiu identificar os artigos científicos que fundamentam teoricamente e proporcionam uma visão sobre o estado da arte da modelagem de competências (*competency modeling*).

A modelagem de competências tem sido amplamente reconhecida como um componente central na gestão estratégica de recursos humanos e no desenvolvimento das organizações. Seu principal propósito é integrar conhecimentos, habilidades e atitudes em uma abordagem sistemática que permita alinhar capacidades individuais aos objetivos institucionais, antecipar demandas emergentes e promover soluções inovadoras (Calhau et al., 2024; Levanaitė, 2025). A capacidade de estruturar e aprimorar competências tornou-se, portanto, um fator determinante para a adaptabilidade e o desempenho organizacional, sobretudo em contextos complexos, como os vivenciados pelos Serviços de Inteligência.

O conceito de competência é comumente ancorado no trinômio Conhecimentos, Habilidades e Atitudes, popularizado por Boyatzis (1982). Essa definição foi progressivamente aprofundada por autores como Campion et al. (2011), Jajoo e Deshmukh (2024) e Rothwell et al. (2025), os quais contribuíram para consolidar uma base teórica sobre os fundamentos, aplicações e limitações da modelagem de competências. Segundo essa perspectiva, competências são atributos integrados que permitem ao indivíduo desempenhar com eficácia funções específicas em determinados contextos de trabalho.

As bases teóricas da modelagem de competências abrangem distintas vertentes. Modelos de inspiração cognitivo-comportamental, como o *Cognitive Competency Development Model*, integram teorias como a hierarquia de necessidades de Maslow, o modelo ABC de atitude e a teoria da aprendizagem social, e defendem que as competências emergem da interação entre fatores individuais, sociais e ambientais (Jajoo & Deshmukh, 2024). O construtivismo e a teoria da carga cognitiva também são relevantes, ao enfatizar como os indivíduos constroem conhecimento e gerenciam recursos mentais durante a aprendizagem – aspectos críticos para o desenvolvimento de competências em ambientes de alta complexidade.

Outros autores, como Bradley (2015), adotam uma perspectiva sistêmica, argumentando que modelos de competências devem ser compreendidos como subsistemas dentro de sistemas organizacionais maiores. A teoria dos sistemas propõe que a modelagem de competências não seja tratada de forma isolada, mas integrada ao ecossistema institucional, considerando aspectos como cultura, estrutura, governança e fluxos decisórios. Essa visão também sustenta a necessidade de modelos adaptáveis e atualizados frente à volatilidade dos ambientes de trabalho.

Sob a ótica da gestão estratégica, Campion et al. (2020) demonstram que os modelos de competência podem funcionar como ferramentas de disseminação de metas institucionais, ao traduzirem objetivos estratégicos em comportamentos observáveis e mensuráveis. Modelos bem formulados permitem alinhar a performance dos servidores às diretrizes organizacionais, contribuindo para a consistência interna da cultura e para o alcance de metas organizacionais.

As contribuições metodológicas também merecem destaque. A literatura recente aponta a necessidade de métodos que assegurem a validade e aplicabilidade dos modelos propostos, destacando-se nesse cenário a abordagem da DSR. Como apontado por Sithole et al. (2023), enquanto a modelagem de competências define "o que" deve ser desenvolvido, a DSR se concentra em "como" construir e validar artefatos que sejam úteis e eficazes. Essa complementaridade metodológica é fundamental para garantir que os modelos resultantes estejam ancorados em evidências empíricas e sejam aplicáveis em contextos reais.

Além das teorias, a evolução tecnológica tem modificado significativamente a modelagem de competências. Cao e Zhang (2022) analisam o uso de algoritmos de *machine learning* e redes neurais para prever lacunas de competências, personalizar trilhas de capacitação e apoiar decisões de gestão de talentos. Tais recursos ampliam a precisão e a escalabilidade das análises, viabilizando modelos dinâmicos e responsivos às transformações digitais.

Do ponto de vista organizacional, modelos de competências bem definidos também favorecem a retenção de talentos e a construção de carreiras. Segundo Benayoune (2024), organizações que estabelecem trajetórias claras de desenvolvimento reduzem sua taxa de rotatividade, enquanto Jajoo e Deshmukh (2024) apontam que a clareza nas expectativas institucionais está associada à elevação da motivação e da satisfação profissional.

A revisão da literatura indica ainda um conjunto de tendências emergentes na modelagem de competências. Dentre elas, destacam-se: (i) a integração dos modelos à estratégia organizacional (Rothwell & Lindholm, 1999); (ii) a incorporação de competências digitais e orientadas para o futuro (Baek et al., 2024; Lee & Park, 2022); (iii) a adoção de modelos abrangentes e adaptáveis, particularmente em áreas como saúde global e educação (Hu et al., 2024); e (iv) o fortalecimento de competências comportamentais e socioemocionais como elementos críticos para o desempenho em contextos complexos (Dashko et al., 2020).

Nesse cenário, os principais autores que consolidaram o campo incluem Campion et al. (2011, 2020), Rothwell et al. (2025), Megahed (2018), Sliter (2015), Malachowski et al. (2011) e Gómez et al. (2014), cujos trabalhos oferecem uma síntese teórico-prática sobre métodos,

aplicações e limitações da modelagem de competências em diferentes contextos organizacionais. A literatura enfatiza que, apesar da robustez conceitual, a eficácia de um modelo depende fundamentalmente do seu alinhamento ao contexto institucional e de sua capacidade de adaptação contínua.

Em síntese, a modelagem de competências se apresenta como uma abordagem madura, multidisciplinar e em constante evolução, que articula fundamentos teóricos, métodos analíticos e aplicações práticas para fortalecer a capacidade das organizações de recrutar, desenvolver e reter talentos alinhados às suas finalidades estratégicas.

3. MÉTODOS E TÉCNICAS

Para atingir o objetivo da pesquisa – modelar um *framework* de competências para o cargo de Oficial de Inteligência da ABIN – foi adotada uma abordagem metodológica qualitativa, de natureza aplicada. Conforme Creswell e Creswell (2018), esse tipo de pesquisa é orientado por problemas concretos e visa oferecer soluções que resultem em impactos práticos, o que a torna especialmente adequada ao desenvolvimento de artefatos aplicáveis em contextos organizacionais complexos.

O percurso metodológico da pesquisa foi estruturado em quatro etapas sequenciais e interligadas: (i) delineamento dos desafios institucionais enfrentados pela ABIN; (ii) modelagem das competências com base na percepção dos Oficiais de Inteligência; (iii) categorização e vinculação das competências aos desafios identificados; e (iv) análise das transversalidades entre competências.

Figura 2 – Etapas de construção do *framework*de competências para o cargo de Oficial de Inteligência.

O método qualitativo permitiu captar as percepções dos participantes de maneira contextualizada e aprofundada. Complementarmente, adotou-se a abordagem da DSR, que orienta o desenvolvimento iterativo de soluções fundamentadas teoricamente e validadas empiricamente. A DSR agrega à modelagem de competências uma lógica de construção de artefatos úteis e rigorosamente avaliados, articulando teoria e prática de modo sistêmico.

O primeiro estágio consistiu no delineamento dos desafios a serem enfrentados pelo órgão de Inteligência do Estado brasileiro. Esses foram extraídos das seguintes fontes: (*i*) entrevistas semiestruturadas com Oficiais de Inteligência da ABIN; e (*ii*) análise documental.

As entrevistas foram realizadas presencialmente, no período de novembro de 2024 a janeiro de 2025, com 20 Oficiais de Inteligência da ABIN que nos últimos oito anos exerceram

funções gerenciais nas áreas de recursos humanos, ensino/capacitação, análise, operações e administrativa da Agência.

Esse quantitativo de entrevistas foi estabelecido com base na representatividade estatística e na relevância para o objetivo do estudo. Considerando que, de acordo com o Decreto n.º 11.816/2023 (Brasil, 2023), o total de funções em comissão disponibilizadas para Diretor, Coordenador-Geral, Coordenador, Superintendente e Assessor Técnico na ABIN é de 135, a amostra de 20 corresponderia a aproximadamente 15%. Esse percentual é considerado base sólida para obtenção de dados significativos, especialmente em estudos de natureza qualitativa e assegura a diversidade de perfis e a representatividade das diferentes áreas e níveis de gestão dentro da organização. Estudos na área de pesquisa qualitativa, como os de Creswell e Poth (2018), sugerem que uma amostra em torno de 10 a 30% é adequada para capturar as nuances e complexidades das percepções em contextos organizacionais específicos.

Dos 20 participantes da pesquisa, 13 (65%) se identificaram como do sexo masculino e 7 (35%) como do sexo feminino. A idade média dos entrevistados foi de 48,7 anos. Em relação à formação acadêmica, 5 (25%) possuem graduação, 11 (55%) especialização, 2 (10%) mestrado e 2 (10%) doutorado. O tempo médio de serviço na ABIN foi de 19,15 anos, enquanto a experiência média em funções comissionadas correspondeu a 6,55 anos.

O roteiro de entrevista continha 32 questões, incluindo perguntas abertas e fechadas e sua aplicação foi autorizada pela direção do órgão. Os entrevistados participaram de forma voluntária da pesquisa e assinaram Termo de Consentimento Livre e Esclarecido. Para atendimento do artigo 9º da Lei n.º 9.883/99 (Brasil, 1999) – que assegura o sigilo da identidade dos servidores da ABIN –, os entrevistados não foram nominalmente identificados, mas cognominados por pseudônimos de escritores brasileiros.

As entrevistas foram transcritas e a técnica empregada para análise qualitativa dos dados coletados seguiu as etapas propostas por Bardin (2021), começando pela pré-análise, seguida pela exploração detalhada do material, que compreendeu a codificação, categorização e identificação dos núcleos temáticos. Posteriormente, procedeu-se ao tratamento, inferência e interpretação dos resultados. Cabe destacar que esse processo ocorreu de forma iterativa, permitindo refinar continuamente as categorias e aprofundar progressivamente a interpretação dos dados obtidos. Adicionalmente, o uso do *software* Atlas.TI possibilitou maior eficiência na organização e análise dos dados.

No roteiro aplicado, uma das perguntas abertas visava justamente captar a percepção dos entrevistados sobre os principais desafios enfrentados no desempenho de suas funções dentro da

organização. A questão específica "Quais os principais desafios que o Oficial de Inteligência enfrenta ao trabalhar na ABIN?" proporcionou uma base empírica para a identificação de obstáculos estratégicos e procedimentais que impactam a prática laboral cotidiana no órgão de Inteligência do Estado brasileiro.

Em relação à pesquisa documental, a mesma permitiu identificar a publicação Desafios de Inteligência – Edição 2025 (ABIN, 2024), lançada pela ABIN em dezembro de 2024 e que se encontra disponibilizada no sítio eletrônico da Agência. Trata-se de documento prospectivo que aborda discussões sobre transições globais, situação internacional, América do Sul e ambiente estratégico brasileiro, além de apontaros desafios para a Atividade de Inteligência no Brasil.

A publicação foi examinada também com base na técnica de análise de conteúdo (Bardin, 2021) e a partir do exame do texto foram identificados e organizados desafios que abrangem questões afetas ao fortalecimento das capacidades da Contrainteligência; a implementação de uma cultura de resiliência dos setores estratégicos nacionais; e segurança cibernética e das instituições democráticas.

Dessa forma, a combinação dos dados qualitativos obtidos nas entrevistas com a análise da publicação Desafios de Inteligência – Edição 2025 (ABIN, 2024) permitiu o delineamento de seis desafios, proporcionando um panorama amplo e fundamentado sobre questões contemporâneas da Atividade de Inteligência no Brasil. Esse cruzamento metodológico reforça a validade dos achados e assegurou que a definição dos seis desafios estivesse respaldada em múltiplas fontes, conferindo robustez à construção teórica e aplicabilidade prática ao estudo.

A segunda etapa do desenvolvimento do *framework* de competências consistiu na modelagem de 26 competências que possibilitariam ao Oficial de Inteligência da ABIN suplantar os seis desafios delineados. Para garantir a validade e a aderência dessas competências à realidade institucional, as entrevistas novamente desempenharam papel central no levantamento dos conhecimentos, habilidades e atitudes considerados essenciais para o desempenho eficiente no contexto da organização e da Atividade de Inteligência.

Com esse objetivo, o questionário aplicado aos entrevistados incluiu três perguntas específicas voltadas à identificação dos elementos constitutivos das competências. Os Oficiais foram convidados a responder: (i) “Quais seriam os conhecimentos mais importantes que um Oficial de Inteligência deveria possuir para desempenhar suas funções na ABIN?”; (ii) “Quais seriam as habilidades mais importantes que um Oficial de Inteligência deveria possuir para desempenhar suas funções na ABIN?”; e (iii) “Quais seriam as atitudes mais importantes que um

Oficial de Inteligência deveria possuir para desempenhar suas funções na ABIN?". Essas questões possibilitaram captar percepções detalhadas e contextualizadas sobre os atributos considerados indispensáveis à prática laboral no órgão.

A partir das respostas obtidas, foi possível modelar cada competência abrangendo um título, uma descrição sintética e a identificação dos conhecimentos, habilidades e atitudes necessários ao seu adequado desenvolvimento. Esse procedimento garantiu não apenas a coerência interna do *framework*, mas também a aderência das competências ao contexto real de trabalho dos profissionais que atuam no órgão de Inteligência do Estado brasileiro.

A terceira etapa de elaboração do *framework* compreendeu o agrupamento das 26 competências modeladas, organizando-as em conjuntos que descrevem sua aplicabilidade no contexto da ABIN e da Atividade de Inteligência. Esse processo definiu a função das competências, permitindo que fossem integradas e vinculadas aos seis desafios delineados. O agrupamento partiu do princípio de que competências isoladas, quando analisadas conjuntamente, revelam padrões de complementaridade e interdependência, possibilitando a estruturação de um modelo mais robusto de gestão por competências.

Para realizar esse agrupamento, foram empregadas duas técnicas complementares: análise de conteúdo e categorização indutiva. A análise de conteúdo (Bardin, 2021) possibilitou a organização das competências a partir de suas características semânticas e funcionais, examinando seus componentes – conhecimentos, habilidades e atitudes – e sua relação com os desafios delineados. Em paralelo, a categorização indutiva (Miles, Huberman & Saldaña, 2019) permitiu que os agrupamentos emergissem diretamente dos dados analisados, sem a imposição de categorias predefinidas. Esse método baseia-se na identificação de padrões e conexões dentro do próprio conteúdo analisado, garantindo que as categorias sejam construídas a partir da própria realidade institucional, e não forçadas a se encaixar em um modelo preestabelecido.

Na etapa final, identificou-se que muitas das competências modeladas possuíam caráter transversal, contribuindo simultaneamente para a superação de mais de um desafio. Essa constatação reforça a natureza sistêmica da Atividade de Inteligência e a importância de *frameworks* de competências que reflitam a multifuncionalidade e a interdependência das atribuições institucionais (Halitsan, 2024; Moldabekova, 2023).

A adoção da DSR como referência metodológica conferiu à pesquisa um diferencial importante. Ao longo do processo, três princípios foram incorporados: foco na resolução de um problema real; desenvolvimento de um artefato conceitual aplicável (*framework* de competências);

e fundamentação teórica sólida. A DSR não apenas orientou a construção do *framework*, como também garantiu sua viabilidade prática no contexto específico da ABIN, onde a dinamicidade e o sigilo das atividades desempenhadas pelo órgão exigem ferramentas flexíveis, adaptativas e tecnicamente rigorosas (Maathuis, 2023; Holtkemper & Beecks, 2024).

A integração entre modelagem de competências e DSR, nesse caso, seguiu um fluxo lógico de três fases: (i) identificação do desalinhamento entre competências requeridas e práticas existentes; (ii) construção do *framework* com base nas percepções dos servidores e nos desafios institucionais; e (iii) avaliação qualitativa do artefato a partir do cruzamento entre dados empíricos e referenciais teóricos. Tal integração potencializou a construção de uma solução customizada para a realidade da ABIN.

A tabela 4 sintetiza as principais características metodológicas da pesquisa:

Etapas	**Pesquisa Qualitativa**
Tipo de Pesquisa	Aplicada
Objetivos	Modelar um *framework* de competências para o cargo de Oficial de Inteligência da ABIN. Identificar a percepção de gestores da ABIN sobre GPC.
Método	Qualitativo; *Design Science Research* (DSR)
Técnicas	Análise documental; Entrevista semiestruturada; Análise de conteúdo; Categorização indutiva
Instrumento	Roteiro de entrevista alinhado ao referencial teórico de GPC
Análise de dados	Análise de conteúdo (Bardin, 2021), com apoio do *software* Atlas.TI
Participantes da pesquisa	20 Oficiais de Inteligência que exerceram função gerencial nos últimos 8 anos
Resultados esperados	Construção de um *framework* de competências alinhado aos desafios institucionais da ABIN

Tabela 4 – Características metodológicas da pesquisa.

Essa combinação metodológica conferiu robustez à investigação e legitimidade à proposta apresentada, integrando conhecimento acadêmico, rigor técnico e aplicabilidade prática na estruturação de uma ferramenta de gestão alinhada às exigências da Agência.

No próximo capítulo são apresentados os achados desse processo, detalhando a relação entre os desafios, as competências estruturadas e sua articulação dentro do *framework*.

4. RESULTADOS E DISCUSSÃO

Este capítulo expõe os resultados da pesquisa, estruturados em quatro seções. A primeira detalha o delineamento dos seis desafios identificados para a ABIN e para a Atividade de Inteligência no Brasil, fundamentando sua relevância por meio de convergências entre dados empíricos (entrevistas) e projeções documentais, como a publicação Desafios de Inteligência – Edição 2025 (ABIN, 2024). A segunda seção descreve o processo de modelagem das 26 competências, articulando-as aos desafios por meio de critérios de criticidade e prioridade, com base na Ontologia Fundacional Unificada (UFO), que garantiu rigor conceitual e aderência à realidade institucional. A terceira seção explora as interconexões entre as competências, demonstrando como sua integração promove um modelo de gestão sistêmico, capaz de fortalecer sinergicamente a estrutura organizacional da ABIN. Por fim, a quarta seção busca identificar a percepção dos Oficiais de Inteligência que ocuparam função gerencial na ABIN a respeito do tema GPC na organização.

4.1. Delineamento dos desafios

Como destacado por Tarafdar e Bunker (2019), a eficácia de um *framework* de competências depende de sua ancoragem em problemas tangíveis, sob risco de se tornar um exercício teórico inconsequente. Nesse sentido, os seis desafios delineados emergiram de convergências entre as narrativas dos entrevistados e as projeções do documento Desafios de Inteligência – Edição 2025 (ABIN, 2024).

Os cinco primeiros desafios derivaram da análise de conteúdo aplicada ao documento Desafios de Inteligência – Edição 2025 (ABIN, 2024). A codificação sistemática do texto permitiu identificar não apenas padrões temáticos associados a ameaças estratégicas, mas também extrair as justificativas-chave que fundamentam cada desafio, alinhadas às vulnerabilidades e prioridades descritas na publicação. Por exemplo, a ênfase em *cooperação interinstitucional* (Desafio 1 e 5) e *proteção de infraestruturas críticas* (Desafio 5) emergiram como respostas diretas a lacunas identificadas no documento, enquanto questões como *instrumentalização de cidadãos* (Desafio 3) e *complexidade geopolítica* (Desafio 2) refletiram riscos sistêmicos mapeados na análise. Os desafios selecionados – (i) segurança das instituições democráticas; (ii) segurança cibernética; (iii) resiliência de setores estratégicos; (iv) mercados ilícitos e crime organizado; e (v) espionagem e interferência externa – consolidam-se, portanto, como eixos prioritários cujas justificativas foram validadas pela convergência entre dados qualitativos do texto e critérios de criticidade institucional, garantindo aderência tanto às demandas imediatas quanto a cenários prospectivos.

DESAFIO 1: Desenvolver e implementar estratégias de fortalecimento da cultura de resiliência, por meio de ações contínuas de sensibilização, capacitação e integração entre órgãos públicos, setor privado e sociedade civil, visando à proteção de conhecimentos sensíveis e à manutenção da continuidade operacional dos setores estratégicos brasileiros.	
JUSTIFICATIVAS PARA O DESAFIO	**Atuação proativa e estratégica:** O Oficial de Inteligência deve antecipar riscos e agir de modo a garantir que a organização esteja preparada para ameaças emergentes, em vez de apenas reagir a crises.
	Cooperação interinstitucional: A proteção e o uso de informações sensíveis, aliados à colaboração com diversos atores institucionais, são fundamentais para a eficácia das estratégias de fortalecimento da cultura de resiliência.
	Aprendizado contínuo e adaptação: O desenvolvimento das competências ocorre na prática cotidiana, exigindo adaptação constante a cenários dinâmicos e consolidando a resiliência estratégica como um pilar da atuação profissional.

Tabela 5 – Desafio 1

DESAFIO 2: Desenvolver e implementar estratégias para o monitoramento, análise e neutralização de organizações criminosas transnacionais, com foco na prevenção e no combate a mercados ilícitos, tráfico de pessoas e crimes ambientais, por meio da coordenação interinstitucional e do fortalecimento das capacidades operacionais nas áreas fronteiriças brasileiras.	
JUSTIFICATIVAS PARA O DESAFIO	**Expansão dos mercados ilícitos transnacionais:** A atuação crescente de organizações criminosas em mercados ilícitos, especialmente no tráfico de drogas, armas e pessoas, exige uma capacidade contínua de identificação e neutralização dessas atividades.
	Pressão externa e tensões geopolíticas: A atuação internacional de redes criminosas e a infiltração em estruturas estatais demandam ações coordenadas e proativas da Inteligência brasileira.
	Vulnerabilidades ambientais: A exploração ilegal de recursos naturais, notadamente na região amazônica, compromete a segurança nacional, os interesses ambientais globais e os direitos dos povos originários.
	Desafios nas fronteiras e integração internacional: A complexidade das fronteiras terrestres e marítimas do Brasil, aliada à presença crescente de atores criminosos internacionais, torna fundamental o fortalecimento da cooperação interinstitucional e internacional.

Tabela 6 – Desafio 2

DESAFIO 3: Fortalecer as capacidades de Contrainteligência para detectar, neutralizar e prevenir ações de espionagem e interferência externa, com foco na proteção de dados sensíveis, na integridade dos processos decisórios nacionais e na salvaguarda de recursos estratégicos, considerando o uso crescente de tecnologias avançadas e a instrumentalização de cidadãos e organizações privadas.	
JUSTIFICATIVAS PARA O DESAFIO	**Ameaças constantes de espionagem e interferência externa:** O Brasil tem sido historicamente alvo de Serviços de Inteligência estrangeiros interessados em dados sensíveis sobre recursos naturais, tecnologias estratégicas e processos decisórios.
	Instrumentalização de cidadãos e organizações privadas: O recrutamento de cidadãos brasileiros com acesso a informações sigilosas é uma prática crescente, exigindo protocolos rigorosos de conscientização, monitoramento e proteção.
	Adoção de novas tecnologias ofensivas por agentes adversos: O uso de robôs para raspagem de dados, engenharia social e operações de bandeira falsa demanda uma atualização constante das capacidades de defesa cibernética e da percepção situacional do Oficial de Inteligência.
	Complexidade do cenário geopolítico e tecnológico: O aumento da competição estratégica global gera uma multiplicidade de agentes e técnicas que dificultam a detecção e atribuição das ações adversas, exigindo análises criteriosas e coordenadas.
	Riscos ao processo decisório nacional: O sucesso de operações de influência externa pode comprometer a tomada de decisões estratégicas e a confiança na gestão pública nacional, o que reforça a necessidade de uma atuação preventiva e contínua.

Tabela 7 – Desafio 3

DESAFIO 4: Desenvolver e implementar estratégias para identificar, monitorar e neutralizar campanhas de desinformação e ações de influência externa que ameacem a confiança nas instituições democráticas, com foco no uso de tecnologias emergentes, análise sociopolítica e cooperação interinstitucional.	
JUSTIFICATIVAS PARA O DESAFIO	**Proteção da Democracia e da soberania nacional:** Campanhas de desinformação e interferências externas podem minar a confiança pública nas instituições democráticas, comprometendo a estabilidade política e a soberania do país.
	Adaptação às transições globais e tecnológicas: O avanço tecnológico e as mudanças no cenário global facilitam a disseminação rápida e ampla de informações falsas. Acompanhar essas transições é crucial para que os Serviços de Inteligência possam antecipar e neutralizar ameaças emergentes que exploram novas tecnologias para influenciar a opinião pública.
	Fortalecimento da Segurança Cibernética: A proliferação de ataques cibernéticos e o uso da internet para espalhar desinformação exigem uma postura proativa na defesa do espaço informacional brasileiro. A segurança cibernética é apontada como um dos principais desafios, reforçando a necessidade de se desenvolver estratégias para proteger o ambiente digital nacional.
	Promoção da cooperação interinstitucional: O combate eficaz à desinformação requer a colaboração entre diversas instituições governamentais e não governamentais. A cooperação interinstitucional revela-se essencial para enfrentar ameaças complexas que transcendem as capacidades de uma única entidade, promovendo uma resposta coordenada e abrangente.

Tabela 8 – Desafio 4

DESAFIO 5: Fortalecer a resiliência cibernética nacional por meio da implementação de estratégias integradas para identificar, mitigar e responder a ameaças cibernéticas, com foco na proteção de Infraestruturas Críticas, no uso seguro de tecnologias emergentes e na cooperação interinstitucional para combate a ataques patrocinados por atores estatais e não estatais.	
JUSTIFICATIVAS PARA O DESAFIO	**Proteção das Infraestruturas Críticas:** Setores essenciais como energia, telecomunicações e finanças dependem de sistemas digitais. A vulnerabilidade desses sistemas pode comprometer serviços básicos e a segurança nacional, tornando imperativo o desenvolvimento de estratégias robustas de cibersegurança.
	Ameaças de atacantes estatais e não estatais: O aumento do número de ataques cibernéticos patrocinados por diferentes atores exige uma resposta coordenada e eficaz para proteger os interesses nacionais e a integridade das informações sensíveis.
	Uso seguro de tecnologias emergentes: A rápida adoção de novas tecnologias, como Internet das Coisas (IoT) e Inteligência Artificial, amplia a superfície de ataque. Implementar medidas de segurança adequadas é essencial para mitigar riscos associados a essas inovações.
	Cooperação interinstitucional: A complexidade das ameaças cibernéticas requer colaboração entre órgãos governamentais, setor privado e instituições internacionais. A integração de esforços fortalece a capacidade de resposta e a resiliência frente a incidentes cibernéticos.

Tabela 9 – Desafio 5

A emergência do sexto desafio decorreu de padrões recorrentes identificados nas entrevistas com os Oficiais de Inteligência, cujos relatos expuseram lacunas na definição normativa-legislativa da Atividade de Inteligência. A análise de conteúdo aplicada às narrativas revelou uma convergência temática: a ausência de respaldo jurídico detalhado foi apontada como entrave central à segurança operacional e à eficácia institucional. Como destacou Machado de Assis, *"o Oficial de Inteligência tem uma carreira sem delimitação jurídica de sua missão [...] a*

Lei 9.883/99 [...] está completamente obsoleta", (comunicação pessoal, 19 de dezembro de 2024) crítica que ecoa a percepção de Cecília Meireles sobre a insegurança na atuação profissional: *"a gente às vezes fica inseguro com a nossa própria atividade [...] sente-se solitário e desamparado"* (comunicação pessoal, 18 de novembro de 2024). Essas fragilidades, somadas à observação de Tomás Antônio Gonzaga sobre o *"desalinhamento da Agência em relação à Administração Pública"*, (comunicação pessoal, 22 de novembro de 2024) evidenciaram a necessidade de formalizar atribuições para mitigar riscos de *"responsabilização individual indevida"* (Desafio 6) e assegurar alinhamento estratégico.

A codificação sistemática das entrevistas permitiu categorizar três eixos problemáticos: (i) ambiguidade funcional, que gera sobrecarga e ineficiência; (ii) exposição a questionamentos jurídicos devido à falta de respaldo normativo; e (iii) descompasso entre práticas operacionais e avanços tecnológicos pós-2000. Esses eixos não apenas validaram as justificativas do Desafio 6 – como a *"redução da proteção institucional"* e o *"desalinhamento entre funções e metas"* –, mas também reforçaram a premissa de Tarafdar e Bunker (2019) de que *frameworks* exigem ancoragem em problemas reais. A sobreposição entre discursos empíricos e demandas institucionais demonstrou que a segurança jurídica não é mera formalidade, mas condição essencial para operacionalizar a Inteligência como função estatal.

DESAFIO 6: Estabelecer de forma clara as atribuições dos Oficiais de Inteligência em atos normativos e legais para garantir segurança jurídica na atuação profissional e alinhamento estratégico com a organização.	
JUSTIFICATIVAS PARA O DESAFIO	**Risco de responsabilização individual indevida:** Sem atribuições formalizadas de suas atribuições, os Oficiais de Inteligência podem ser cobrados por ações que não estão claramente delimitadas.
	Dificuldade na tomada de decisão e no cumprimento de normas internas: A anomia compromete a eficiência operacional e gera incertezas sobre as responsabilidades funcionais.
	Redução da proteção institucional do Oficial de Inteligência: A ausência de regras claras aumenta o risco de que sua atuação seja questionada por órgãos de controle ou instâncias judiciais devido à falta de respaldo normativo.
	Desalinhamento entre funções e metas estratégicas da organização: Gera sobrecarga de alguns setores e ineficiência na distribuição das tarefas.

Tabela 10 – Desafio 6

Os seis desafios foram delineados conforme seu impacto para a ABIN e para a Atividade de Inteligência no Brasil, contemplando desde o fortalecimento da resiliência organizacional até o aprimoramento da segurança cibernética e da governança institucional. Essa estruturação não apenas sistematiza as necessidades institucionais, mas também orienta a modelagem de competências, promovendo um alinhamento entre os desafios identificados e as capacidades a serem desenvolvidas pelo Oficial de Inteligência.

4.2. Modelagem das competências e vinculação aos desafios

A modelagem das competências para o cargo de Oficial de Inteligência foi desenvolvida com o objetivo de estruturar, de maneira clara e coerente, os conhecimentos, habilidades e atitudes essenciais para o desempenho das funções na ABIN. Para garantir um modelo conceitualmente rigoroso e alinhado às necessidades institucionais, adotou-se a UFO como referencial teórico. Essa abordagem permitiu estabelecer definições precisas para cada competência e suas inter-relações, assegurando consistência conceitual e facilitando sua aplicação em processos organizacionais.

Como exemplo dessa aplicação, tem-se a Competência 5 (mostrada adiante), intitulada "Coordenação e cooperação interinstitucional no combate ao crime organizado transnacional". Sem o suporte conceitual da UFO, essa competência poderia ser interpretada de diversas maneiras quanto às ações específicas envolvidas. Com o emprego das categorias da UFO, tornou-se possível defini-la objetivamente, identificando ações concretas como "estabelecer parcerias com instituições nacionais e internacionais para troca de informações estratégicas" (evento), desempenhadas pelo Oficial de Inteligência (papel), visando "fortalecer a capacidade de resposta conjunta das instituições frente às ameaças de redes criminosas transnacionais" (relação). Desse modo, a UFO atuou como uma estrutura conceitual teórica que embasou o método adotado na pesquisa (*Design Science Research*), auxiliando a construção do *framework* de competências e mitigando o risco de polissemia no contexto institucional da ABIN.

Cada competência foi estruturada em título, descrição, padrões de desempenho, conhecimentos, habilidades e atitudes. Essa segmentação possibilitou detalhar os elementos essenciais que caracterizam o domínio da competência, garantindo que sua aplicação seja analisada de forma objetiva e alinhada às demandas institucionais. Os padrões de desempenho foram definidos a partir de comportamentos observáveis, permitindo uma avaliação concreta da aplicação das competências no contexto do Serviço de Inteligência.

A fim de assegurar que o *framework* estivesse diretamente ancorado às necessidades da ABIN, cada competência modelada foi vinculada a um dos seis desafios previamente delineados. Esse processo foi realizado por meio de uma análise qualitativa das competências e dos desafios organizacionais, estabelecendo uma correspondência entre as exigências operacionais e as capacidades requeridas do Oficial de Inteligência. A identificação dessas relações garantiu que a conexão entre competências e desafios refletisse a realidade institucional.

Para estruturar essa vinculação de maneira formal, novamente recorreu-se à UFO, que possibilitou representar essas conexões por meio de entidades e relações explícitas no modelo ontológico. No contexto desta modelagem, os desafios institucionais foram tratados como entidades organizacionais, enquanto as competências foram modeladas como relatores sociais, ou

seja, elementos que estabelecem uma relação entre o indivíduo (Oficial de Inteligência) e os requisitos organizacionais. Essa abordagem está alinhada à proposta da UFO, que estrutura conceitos e suas interdependências por meio de categorias ontológicas definidas, garantindo uma modelagem conceitual precisa e coerente (Guizzardi, 2005).

A aplicação da UFO na modelagem das competências possibilitou estruturar relações entre os desafios institucionais e as capacidades necessárias para enfrentá-los. Um exemplo dessa abordagem pode ser observado na relação entre a competência "Coordenação e cooperação interinstitucional no combate ao crime organizado transnacional" (Competência 5, mostrada adiante) e o Desafio 2, que consiste em "Desenvolver e implementar estratégias para o monitoramento, análise e neutralização de organizações criminosas transnacionais, com foco na prevenção e no combate a mercados ilícitos, tráfico de pessoas e crimes ambientais, por meio da coordenação interinstitucional e do fortalecimento das capacidades operacionais nas áreas fronteiriças brasileiras." A UFO permitiu modelar essa vinculação ao definir a competência como um relator social, ou seja, um elemento que estabelece uma relação formal entre o indivíduo (Oficial de Inteligência) e um requisito organizacional essencial para a superação do desafio. Dessa forma, o *framework* desenvolvido garante que essa competência não seja apenas um atributo individual do profissional, mas sim uma capacidade integrada ao funcionamento da instituição.

As tabelas de 11 a 36 detalham as 26 competências modeladas, apresentando seus respectivos título, descrição, padrões de desempenho, conhecimentos, habilidades e atitudes, compondo um referencial estruturado para orientar o desenvolvimento profissional e o fortalecimento das capacidades institucionais.

Para facilitar a compreensão da relação entre as competências modeladas e os desafios, o texto traz um esquema de cores que organiza visualmente essa conexão. As três primeiras competências, por exemplo, estão destacadas em amarelo e correspondem ao Desafio 1 (tabela 5), que aborda o fortalecimento da cultura de resiliência estratégica. Da mesma forma, as competências de 4 a 8, em cinza, vinculam-se ao Desafio 2 (tabela 6), focado no combate ao crime organizado transnacional. Essa padronização visual se repete para os demais desafios, permitindo que o leitor identifique quais competências estão associadas a cada desafio.

COMPETÊNCIA 1			
TÍTULO: Promoção da cultura de resiliência estratégica e proteção do conhecimento sensível.			
DESCRIÇÃO: Planejar e implementar ações de sensibilização para cultura de resiliência estratégica e proteção do conhecimento sensível.			
PADRÕES DE DESEMPENHO	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**

(COMPORTAMENTOS OBSERVÁVEIS)			
Mapear públicos-alvo em instituições parceiras e internas para ações de sensibilização sobre resiliência estratégica.	Conceitos fundamentais de resiliência estratégica e segurança de informações sensíveis	Desenvolver campanhas de sensibilização sobre resiliência estratégica.	Compromisso com a difusão da cultura de resiliência estratégica.
Planejar atividades de conscientização, como palestras, seminários e *workshops*, abordando a importância da proteção de conhecimentos sensíveis.	Princípios de gestão de riscos e análise de ameaças em setores estratégicos.	Planejar e conduzir treinamentos e eventos educativos.	Proatividade na criação e execução de ações de sensibilização.
Produzir materiais educativos para disseminar conceitos de segurança, proteção de informações e resiliência estratégica.	Métodos e técnicas de comunicação institucional e sensibilização de públicos.	Aplicar métodos de avaliação de impacto de iniciativas de conscientização.	Empatia e habilidade de comunicação com diversos públicos.
Avaliar o impacto das ações de sensibilização por meio de questionários, entrevistas e análise de indicadores.	Ferramentas para medição de impacto de ações educativas.	Comunicar informações técnicas de forma clara para diferentes públicos.	Perseverança na manutenção de uma agenda contínua de ações educativas.
Estabelecer parcerias interinstitucionais para ampliar o alcance das iniciativas de conscientização.	Estrutura e diretrizes do Programa Nacional de Proteção do Conhecimento Sensível (PNPC).	---	---

Tabela 11 – Competência 1

COMPETÊNCIA 2			
TÍTULO: Análise de Riscos e de vulnerabilidades em setores estratégicos.			
DESCRIÇÃO: Analisar riscos e vulnerabilidades em setores estratégicos.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Identificar ameaças e vulnerabilidades relacionadas a conhecimentos sensíveis em setores estratégicos.	Princípios de análise de risco, gestão de crises e resiliência organizacional.	Identificar e avaliar riscos em setores estratégicos.	Rigor metodológico na análise de riscos e vulnerabilidades.
Analisar riscos potenciais com base em dados históricos, indicadores de ameaças e cenários prospectivos.	Métodos de avaliação de vulnerabilidades em setores estratégicos (ex.: FMEA, *Bow-Tie Analysis*).	Correlacionar dados técnicos e contextuais para análise de ameaças.	Proatividade na busca de informações sobre ameaças emergentes.
Aplicar metodologias de análise de risco para avaliar impactos de ameaças e propor medidas mitigadoras.	Técnicas de simulação e modelagem de cenários prospectivos.	Elaborar relatórios com recomendações de medidas mitigadoras.	Compromisso com a antecipação e mitigação de riscos estratégicos.

Produzir relatórios técnicos com diagnósticos e recomendações para gestores institucionais.	Fundamentos de geopolítica aplicados à segurança de setores críticos.	Participar de simulações de crises e exercícios interinstitucionais.	Curiosidade analítica para compreender dinâmicas complexas de ameaça.
Participar de simulações e exercícios de resposta a incidentes para avaliar a resiliência institucional.	Regulamentações e normas aplicáveis à segurança de Infraestruturas Críticas.	---	---

Tabela 12 – Competência 2

COMPETÊNCIA 3			
TÍTULO: Coordenação interinstitucional para a proteção de conhecimentos sensíveis.			
DESCRIÇÃO: Coordenar a integração interinstitucional para proteção de conhecimentos sensíveis.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Estabelecer e manter canais de comunicação com instituições públicas e privadas de interesse estratégico.	Estrutura e funcionamento de setores estratégicos nacionais.	Estabelecer parcerias com instituições internas e externas.	Proatividade na busca de parcerias e oportunidades de cooperação.
Participar de fóruns e grupos de trabalho interinstitucionais para troca de informações sobre riscos e boas práticas de segurança.	Modelos de cooperação interinstitucional e de gestão de parcerias.	Participar de negociações para formalização de acordos de cooperação.	Compromisso com a segurança e proteção de conhecimentos sensíveis.
Coordenar ações conjuntas para a elaboração e revisão de protocolos de proteção de conhecimentos sensíveis.	Protocolos de segurança e proteção de informações sensíveis.	Gerenciar reuniões interinstitucionais com foco em segurança estratégica.	Habilidade de mediação e negociação interinstitucional.
Facilitar o compartilhamento seguro de informações entre os diversos atores envolvidos na proteção de ativos estratégicos.	Técnicas de gestão colaborativa de riscos e incidentes.	Propor e revisar protocolos de segurança conjuntos.	Foco na construção de soluções colaborativas e integradas
Propor acordos de cooperação entre a ABIN e instituições parceiras para fortalecimento da resiliência estratégica.	Estruturas regulatórias nacionais e internacionais sobre proteção de ativos críticos.	---	---

Tabela 13 – Competência 3

As competências de 1 a 3 foram modeladas a partir das demandas identificadas no desafio de fortalecimento da cultura de resiliência estratégica, consolidando a capacidade analítica e estratégica do Oficial de Inteligência para uma resposta rápida e coordenada diante de situações críticas. Ao integrar essas competências, há o desenvolvimento de um pensamento estratégico e analítico, essencial para a sensibilização de públicos internos e externos, a análise de riscos em

setores estratégicos e a coordenação de esforços interinstitucionais, garantindo a proteção de ativos sensíveis e a continuidade das operações dos setores estratégicos brasileiro em cenários de crise.

As próximas cinco competências vinculam-se ao desafio "Desenvolver e implementar estratégias para o monitoramento, análise e neutralização de organizações criminosas transnacionais, com foco na prevenção e no combate a mercados ilícitos, tráfico de pessoas e crimes ambientais, por meio da coordenação interinstitucional e do fortalecimento das capacidades operacionais nas áreas fronteiriças brasileiras".

COMPETÊNCIA 4			
TÍTULO: Monitoramento e análise da criminalidade organizada transnacional.			
DESCRIÇÃO: Monitorar e analisar atividades criminosas transnacionais, notadamenteemáreas fronteiriças.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Coletar dados de fontes abertas (OSINT) e fontes humanas (HUMINT) sobre organizações criminosas transnacionais.	Princípios de análise criminal.	Coletar, interpretar e correlacionar dados sobre organizações criminosas transnacionais.	Rigor analítico na avaliação de dados.
Analisar padrões de atuação criminosa em áreas fronteiriças, correlacionando informações de diferentes bases de dados.	Técnicas de *Open Source Intelligence* (OSINT) e *Human Intelligence* (HUMINT) aplicadas ao monitoramento de redes criminosas.	Operar ferramentas de geointeligência para mapeamento e análise de atividades ilícitas.	Discrição e sigilo ao lidar com informações sensíveis.
Identificar pontos críticos de movimentação de drogas, armas e pessoas nas fronteiras e áreas sensíveis.	Geopolítica regional, com foco nas relações do Brasil com os países vizinhos da América do Sul.	Produzir relatórios com recomendações para ações preventivas e repressivas à criminalidade organizada transnacional.	Proatividade na identificação de novas tendências e *modus operandi* de organizações criminosas.
Produzir relatórios analíticos com mapas de atuação e tendências de atividades criminosas.	Idiomas: Espanhol (preferencialmente avançado) e Inglês para análise de documentos internacionais.	Comunicar-se de forma eficaz com órgãos de segurança pública e Serviços de Inteligência estrangeiros.	Compromisso com a proteção da segurança nacional.
Sinalizar vulnerabilidades que possam ser exploradas por organizações criminosas.	Fundamentos de geointeligência e análise de fluxos migratórios	---	---

Tabela 14 – Competência 4

COMPETÊNCIA 5			
TÍTULO: Coordenação e cooperação interinstitucional no combate ao crime organizado transnacional.			
DESCRIÇÃO: Coordenar ações interinstitucionais para o combate ao crime organizado transnacional.			
PADRÕES DE DESEMPENHO	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**

(COMPORTAMENTOS OBSERVÁVEIS)			
Planejar e conduzir reuniões interinstitucionais com órgãos nacionais e internacionais de Segurança Pública e de Inteligência.	Estruturas e mecanismos de cooperação internacional em Segurança Pública e Inteligência.	Estabelecer e manter canais de comunicação com instituições nacionais e Serviços de Inteligência estrangeiros.	Proatividade na construção de parcerias estratégicas.
Elaborar protocolos de compartilhamento de informações para otimizar a cooperação interagências.	Protocolos de compartilhamento de dados entre instituições nacionais e entre Serviços de Inteligência estrangeiros.	Conduzir reuniões e negociações para alinhar estratégias e ações conjuntas.	Compromisso com a troca responsável de informações sensíveis.
Participar de fóruns e eventos internacionais para fortalecer parcerias e identificar boas práticas.	Legislação brasileira e internacional relacionada ao combate ao crime organizado.	Redigir acordos de cooperação interinstitucional.	Empatia e habilidade diplomática na interação com parceiros externos.
Implementar mecanismos de comunicação segura entre as instituições envolvidas em cooperação interagências.	Proficiência nos idiomas Inglês e Espanhol, dada a frequência de interações com parceiros da América Latina e de órgãos internacionais.	Participar de operações conjuntas.	Rigor no cumprimento de normas e protocolos estabelecidos.
Produzir relatórios de acompanhamento sobre os resultados das ações conjuntas realizadas.	Princípios de diplomacia e relações internacionais aplicados à cooperação em segurança.	---	---

Tabela 15 – Competência 5

COMPETÊNCIA 6			
TÍTULO: Análise financeira e investigação de fluxos ilícitos vinculados a Organizações Criminosas Transnacionais.			
DESCRIÇÃO: Identificar e analisar cadeias financeiras de Organizações Criminosas Transnacionais.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Mapear fluxos financeiros suspeitos associados a atividades ilícitas transnacionais.	Princípios de análise financeira e de combate à lavagem de dinheiro.	Utilizar ferramentas de análise financeira e de cruzamento de dados.	Perseverança diante de investigações complexas e extensas.
Analisar transações bancárias e movimentações de ativos que possam indicar práticas de lavagem de dinheiro.	Técnicas de análise financeira de redes criminosas.	Comunicar-se com instituições financeiras e órgãos de controle para troca de informações.	Comprometimento com a legalidade e ética nas análises realizadas.
Coletar e processar dados sobre empresas de fachada e redes de financiamento criminoso.	Legislação nacional e internacional sobre crimes financeiros (Lei n.º 9.613/1998 e suas alterações).	Elaborar relatórios técnicos com clareza e precisão.	Curiosidade investigativa para identificar novas estratégias de ocultação de recursos ilícitos.
Coordenar ações com órgãos de controle	Proficiência no idioma Inglês para leitura de	---	Discrição no tratamento de dados sensíveis.

financeiro nacional e internacional.	relatórios financeiros internacionais.		
---	Funcionamento de mecanismos de financiamento de atividades ilícitas transnacionais.	---	---

Tabela 16 – Competência 6

COMPETÊNCIA 7			
TÍTULO: Análise de dados e execução de operações de Inteligência para o combate a crimes ambientais.			
DESCRIÇÃO: Planejar e conduzir operações de Inteligência em áreas de risco ambiental.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Mapear regiões de atuação de organizações criminosas ambientais na Amazônia e outras áreas sensíveis.	Técnicas de geointeligência e sensoriamento remoto.	Operar *softwares* de análise geoespacial e de sensoriamento remoto.	Disposição para atuar em áreas de difícil acesso.
Planejar operações conjuntas com órgãos ambientais e de Segurança Pública.	Práticas de análise de crimes ambientais e suas implicações socioeconômicas.	Coletar e interpretar dados ambientais.	Atenção e zelo com os dados sensíveis coletados.
Utilizar tecnologias de sensoriamento remoto e de geointeligência para identificação de crimes ambientais.	Legislação ambiental brasileira (Lei n.º 9.605/1998 e regulamentações específicas).	Planejar, coordenar e participar de operações de campo em conjunto com outras instituições.	Rigor na análise e produção de Relatórios de Inteligência.
Participar de operações de campo em apoio a desintrusões e apreensões de recursos ilícitos.	Proficiência no idioma Inglês para análise de relatórios internacionais e uso de ferramentas estrangeiras de geointeligência.	---	---
Produzir relatórios sobre as dinâmicas criminosas observadas e suas implicações socioambientais.	Estruturas de organização e atuação de redes criminosas ambientais.	---	---

Tabela 17 – Competência 7

COMPETÊNCIA 8			
TÍTULO: Análise prospectiva e modelagem de tendências do fenômeno da criminalidade transnacional.			
DESCRIÇÃO: Produzir análises prospectivas sobre tendências criminais transnacionais.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Coletar e organizar dados sobre o histórico de	Métodos de análise preditiva e de modelagem de cenários.	Coletar, processar e analisar dados sobre organizações criminosas.	Curiosidade e interesse pela análise de tendências.

atuação de organizações criminosas transnacionais.			
Aplicar técnicas de análise prospectiva para antecipar tendências de atuação de organizações criminosas transnacionais.	Geopolítica internacional, com foco na América do Sul.	Aplicar métodos quantitativos de análise preditiva.	Disciplina na elaboração e validação dos cenários prospectivos.
Desenvolver cenários futuros com base na análise de dados disponíveis.	Proficiência nos idiomas Espanhol e Inglês para acesso a fontes abertas internacionais.	Desenvolver e apresentar cenários futuros para diferentes públicos.	Iniciativa para propor soluções com base nos cenários projetados.
Elaborar Relatórios de Inteligência que tragam projeções e possíveis implicações de novas dinâmicas criminosas.	Ferramentas de análise quantitativa e qualitativa de tendências (ex: Nvivo)	Utilizar *softwares* estatísticos e de análise de vínculos.	---

Tabela 18 – Competência 8

Importante destacar que as competências de 4 a 8, vinculadas ao Desafio 2, exigem proficiência nos idiomas Espanhol e Inglês, além da compreensão de fatos inerentes à geopolítica regional. Esses conhecimentos derivaram das evidências coletadas nas entrevistas com os Oficiais de Inteligência. Lima Barreto ressaltou a importância do domínio linguístico para análises precisas: *"tem a questão do conhecimento de idiomas, especialmente Inglês e Espanhol [...] entender alguns meandros de idiomas é muito importante para pesquisa e levantamento de dados"* (comunicação pessoal, 17 de dezembro de 2024), o que refoça que esses dois idiomas são essenciais para leitura e interpretação de documentos internacionais, bem como para propiciar a interação com órgãos de Inteligência de países lindeiros. Cecília Meireles complementou: *"ter conhecimento do que acontece nos países a nossa volta [...] e sua política externa"*, (comunicação pessoal, 18 de novembro de 2024) sublinhando a importância de acompanhar fatos e situações que ocorrem em nações que compartilham fronteiras com o Brasil, onde redes criminosas transnacionais atuam com frequência.

Além dos conhecimentos supramencionados, as cinco competências descritas abordam diferentes dimensões técnicas e operacionais necessárias para que o Oficial de Inteligência consiga superar o desafio de combater organizações criminosas transnacionais. O foco na coleta e análise de dados, no fortalecimento da cooperação interinstitucional, na análise financeira, na atuação em áreas ambientais e na construção de cenários prospectivos proporciona base sólida para atuação eficaz diante das ameaças contemporâneas à segurança nacional brasileira.

As competências de 9 a 13, abaixo descritas, se relacionam ao terceiro desafio que versa sobre fortalecer as capacidades da Contrainteligência brasileira para detectar e neutralizar ações de espionagem e de Interferência Externa.

COMPETÊNCIA 9

TÍTULO: Identificação e monitoramento de ameaças de espionagem e Interferência Externa.			
DESCRIÇÃO: Identificar e monitorar atividades de espionagem e Interferência Externa.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Coletar e analisar dados sobre possíveis ações de espionagem.	Princípios e técnicas de Contrainteligência.	Monitorar atividades suspeitas em ambientes físicos e digitais.	Proatividade na identificação de ameaças emergentes.
Empregar ferramentas de *Open Source Intelligence* (OSINT) para monitorar atividades suspeitas.	Técnicas de *Open Source Intelligence* (OSINT), *Human Intelligence* (HUMINT) e *Signals Intelligence* (SIGINT).	Analisar comportamentos de possíveis agentes de influência.	Discrição e sigilo na condução das atividades.
Aplicar técnicas de análise comportamental para identificar padrões de atuação.	Fundamentos de análise comportamental e de Engenharia Social.	Utilizar ferramentas de análise e de monitoramento de redes.	Comprometimento com a proteção dos interesses nacionais.
Produzir relatórios com avaliação de riscos e recomendações de mitigação.	Proficiência nos idiomas Inglês e Espanhol para análise de fontes abertas internacionais.	---	---

Tabela 19 – Competência 9

COMPETÊNCIA 10			
TÍTULO: Gestão de Riscos e proteção de Infraestruturas Críticas.			
DESCRIÇÃO: Aplicar técnicas de Análise de Risco e Vulnerabilidade em Infraestruturas Críticas.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Mapear vulnerabilidades em Infraestruturas Críticas.	Conceitos de análise de risco e de gestão de segurança informacional.	Aplicar metodologias de análise de risco e de simulação de incidentes.	Atenção a detalhes.
Desenvolver relatórios de análise de risco com recomendações práticas.	Protocolos internacionais de segurança de Infraestruturas Críticas.	Utilizar ferramentas de avaliação de vulnerabilidades.	Responsabilidade no manuseio de informações sensíveis.
Simular possíveis vetores de ataque para testar a resiliência das Infraestruturas Críticas.	Legislação nacional acerca de Infraestruturas Críticas (ex: Decretos n.º 9.573/2018; n.º 10.569/2020 e n.º 11.200/2022).	Comunicar achados técnicos de forma clara e precisa.	Iniciativa na proposição de melhorias nos processos de segurança.
---	Estruturas críticas nacionais e seus potenciais pontos de vulnerabilidade.	---	---

Tabela 20 – Competência 10

COMPETÊNCIA 11
TÍTULO: Prevenção e mitigação de ameaças de Engenharia Social por meio de protocolos de proteção.
DESCRIÇÃO: Desenvolver e implementar protocolos de proteção contra ações de Engenharia Social.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Criar e implementar campanhas de conscientização sobre riscos de Engenharia Social.	Técnicas e métodos de Engenharia Social.	Elaborar e ministrar treinamentos de conscientização de segurança contra ações de Engenharia Social.	Empatia ao lidar com diferentes perfis de colaboradores.
Realizar treinamentos periódicos para colaboradores de setores sensíveis.	Princípios de persuasão e de manipulação comportamental.	Aplicar testes simulados de Engenharia Social.	Dedicação ao ensino e à disseminação de boas práticas.
Estabelecer protocolos claros de comunicação segura.	Protocolos de segurança da informação e comunicação.	Desenvolver materiais didáticos sobre práticas seguras de comunicação.	Paciência e resiliência para mitigar comportamentos inseguros.
---	Técnicas de persuasão e manipulação psicológica.	---	---
---	Métodos de ataque e defesa contra Engenharia Social (*phishing*, *pretexting*, etc)	---	---

Tabela 21 – Competência 11

COMPETÊNCIA 12			
TÍTULO: Inteligência Cibernética na análise e mitigação de ameaças digitais e raspagem de dados sensíveis.			
DESCRIÇÃO: Analisar e mitigar ameaças digitais e raspagem de dados sensíveis.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Monitorar e analisar atividades suspeitas nos sistemas internos.	Segurança cibernética e protocolos de proteção de dados.	Operar ferramentas de detecção e de análise de intrusos.	Curiosidade investigativa.
Implementar ferramentas de segurança cibernética e detecção de intrusos.	Técnicas de raspagem de dados e como mitigá-las.	Desenvolver relatórios sobre atividades suspeitas.	Comprometimento com a segurança cibernética.
Desenvolver mecanismos para bloquear tentativas de coleta automatizada de dados.	Fundamentos de análise de *malware* e de Inteligência Cibernética.	Propor e implementar políticas de proteção contra raspagem de dados.	Paciência e persistência em análises cibernéticas.

Tabela 22 – Competência 12

COMPETÊNCIA 13			
TÍTULO: Planejamento e execução de operações de Contrainteligência em ambientes sensíveis.			
DESCRIÇÃO: Planejar e conduzir operações de Contrainteligência em ambientes sensíveis.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**

Planejar e coordenar operações para neutralização de agentes adversos.	Técnicas avançadas de despistamento e vigilância contraespionagem.	Executar operações de despistamento em campo.	Discrição.
Conduzir operações de despistamento e identificação de vulnerabilidades.	Técnicas de contraespionagem (e.g., *honeypots*, *Double agents*, *Whitelisting* e *Blacklisting*)	Monitorar atividades suspeitas em tempo real.	Capacidade de tomar decisões sob pressão.
Elaborar relatórios pós-operação com análise de resultados e aprendizados.	Protocolos de controle de danos em vazamentos (e.g., contenção midiática).	Produzir relatórios detalhados de avaliação operacional.	Iniciativa e controle emocional em situações críticas.
---	Técnicas de Inteligência humana (HUMINT) e sua aplicação na identificação de riscos de espionagem.	---	---

Tabela 23 – Competência 13

O conhecimento de técnicas de Contrainteligência, aliado a comportamentos como controle emocional em situações críticas foram assinaladas como atributos relevantes nas entrevistas com Oficiais de Inteligência. Graciliano Ramos destacou a necessidade de uma mentalidade estratégica: *"Conhecer técnicas analíticas e operacionais [...] e ter a noção de que existem outros interesses, outras ações de Inteligência adversa operando no Estado e não achar que é Teoria da Conspiração. Não, realmente outros países têm interesses aqui"* (comunicação pessoal, 14 de novembro de 2024), enfatizando que a Contrainteligência exige não apenas domínio metodológico, mas uma postura crítica ante riscos reais, como espionagem e interferência externa. Rachel de Queiroz complementou ao ressaltar a importância de uma atitude discreta e que priorize o controle emocional: *"Precisa ser alguém centrado emocionalmente e discreto[...] capaz de observar e não ser impulsivo"* (comunicação pessoal, 19 de novembro de 2024), atributo essencial para operações em ambientes sensíveis, onde decisões sob pressão demandam serenidade,concentração e discrição.

Esses elementos refletem-se diretamente nas competências modeladas: a análise de padrões de espionagem (Competência 9), a gestão de riscos em Infraestruturas Críticas (Competência 10) e a execução de operações de despistamento (Competência 13) exigem tanto *expertise* técnica quanto equilíbrio psicológico. As cinco competências apresentadas, articuladas às exigências contemporâneas de proteção de dados sensíveis e integridade institucional, abrangem dimensões essenciais para que o Oficial de Inteligência atue de forma proativa, técnica e segura contra ameaças como espionagem e Interferência Externa. A combinação entre habilidades técnicas e comportamentais – como serenidade, discrição e capacidade analítica – não apenas mitiga vulnerabilidades, mas constrói uma força de trabalho resiliente e preparada, apta a fortalecer a

resiliência institucional diante de desafios complexos e multifacetados da Contrainteligência brasileira.

O quarto desafio versa sobre o avanço da desinformação e a manipulação de narrativas que representam ameaças crescentes à segurança institucional e à estabilidade do Estado. Para enfrentar esse desafio, é necessário que o Oficial de Inteligência possua competências que permitam identificar, analisar e neutralizar campanhas de desinformação. Isso se torna fundamental porque tais campanhas podem comprometer a tomada de decisão estratégica, minar a confiança nas instituições e gerar instabilidade social. A atuação do Oficial de Inteligência na identificação e neutralização dessas ações contribui para a preservação da integridade informacional, assegurando que a formulação de políticas e a proteção dos interesses do Estado não sejam impactadas por narrativas manipuladas.

As competências de 14 a 17, relacionadas ao quarto desafio, incluem:

COMPETÊNCIA 14			
TÍTULO: Análise de dinâmicas sociopolíticas e de estratégias de desinformação.			
DESCRIÇÃO: Analisar dinâmicas sociopolíticas e discursos de desinformação.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Coletar e analisar discursos e narrativas que promovam desinformação e discursos antidemocráticos.	Fundamentos de Ciência Política e Teoria do Estado Democrático de Direito.	Analisar o impacto de discursos e narrativas de desinformação nas dinâmicas sociais e institucionais.	Compromisso com a imparcialidade e análise isenta.
Aplicar técnicas de Análise de Conteúdo e de Análise Crítica do Discurso para compreender o impacto social e político das campanhas de desinformação.	Conceitos de desinformação, *fakenews* e manipulação informacional.	Aplicar técnicas de Análise de Conteúdo, utilizando softwares de análise qualitativa.	Curiosidade investigativa para compreender fenômenos complexos.
Elaborar Relatórios de Inteligência detalhando e analisando as estratégias utilizadas por grupos que promovem a desinformação.	Princípios de Análise Crítica do Discurso e análise sociopolítica.	Produzir relatórios com análise isenta e desprovida de vieses ideológicos.	Discrição e responsabilidade no tratamento de dados sensíveis.
---	Proficiência nos idiomas Inglês e Espanhol para leitura de conteúdos e documentos internacionais.	---	---

Tabela 24 – Competência 14

COMPETÊNCIA 15			
TÍTULO: Análise de plataformas digitais, de algoritmos e de comportamentos em ambiente virtual.			
DESCRIÇÃO: Monitorar e analisar plataformas digitais e dinâmicas algorítmicas.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Monitorar atividades e tendências em redes sociais e aplicativos de mensagens.	Algoritmos de recomendação e funcionamento de mídias sociais.	Aplicar metodologias de análise de redes sociais.	Iniciativa para acompanhar as inovações tecnológicas.
Identificar padrões de comportamento e mecanismos de disseminação de desinformação.	Técnicas de *Open Source Intelligence* (OSINT) e *Social Media Intelligence* (SOCMINT).	Utilizar ferramentas específicas de monitoramento e análise de conteúdos digitais.	Disciplina e paciência na análise contínua de grandes volumes de dados.
Avaliar o impacto de campanhas de desinformação em diferentes segmentos populacionais.	Fundamentos de análise de redes sociais e comportamentos no ambiente virtual.	Correlacionar dados de diferentes fontes para compreender estratégias de desinformação.	Compromisso com a produção de análises imparciais e com valor estratégico.

Tabela 25 – Competência 15

COMPETÊNCIA 16			
TÍTULO: Modelagem prospectiva de narrativas associadas a ações antidemocráticas.			
DESCRIÇÃO: Produzir análises prospectivas sobre narrativas associadas a ações antidemocráticas.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Coletar e processar dados históricos sobre campanhas de desinformação e suas repercussões.	Métodos de análise preditiva e de modelagem de cenários.	Aplicar modelos estatísticos para análise de tendências.	Paciência e rigor analítico.
Aplicar técnicas de análise preditiva para identificar padrões e possíveis tendências.	Fundamentos de psicologia social aplicada à análise de comportamentos coletivos.	Integrar informações de múltiplas fontes para criar cenários futuros.	Curiosidade intelectual para compreender fenômenos complexos.
Produzir Relatórios de Inteligência com cenários prospectivos e recomendações para mitigação de riscos.	Teoria de jogos e análise de dinâmicas sociopolíticas.	Elaborar Relatórios de Inteligência com projeções e orientações estratégicas.	Disciplina na aplicação de métodos preditivos.

Tabela 26 – Competência 16

COMPETÊNCIA 17			
TÍTULO: Cooperação interinstitucional no combate à desinformação.			
DESCRIÇÃO: Estabelecer cooperação interinstitucional para o combate à desinformação.			
PADRÕES DE DESEMPENHO	**CONHECIMENTOS**	**HABILIDADES**	**ATITUDES**

(COMPORTAMENTOS OBSERVÁVEIS)	(SABER)	(SABER FAZER)	(QUERER FAZER)
Planejar e organizar reuniões com órgãos públicos e privados nacionais e internacionais.	Estruturas e práticas de cooperação internacional em Inteligência.	Conduzir reuniões e interagir com representantes de órgãos parceiros.	Proatividade na construção e manutenção de parcerias.
Estabelecer canais seguros para troca de informações sobre campanhas de desinformação.	Protocolos de segurança e compartilhamento de dados.	Estabelecer e manter redes de contato institucionais.	Empatia e diplomacia na interlocução com diferentes atores.
Participar de fóruns e grupos de trabalho relacionados ao tema.	Legislação nacional e internacional relacionada à desinformação.	Produzir relatórios e propostas de cooperação.	Manutenção do sigilo no compartilhamento de informações sensíveis.
---	Proficiência nos idiomas Inglês e Espanhol para articulação internacional.	Assinalar parceiros institucionais para cooperação.	---

Tabela 27 – Competência 17

As competências de 14 a 17, vinculadas ao Desafio 4 (combate à desinformação e influência externa), incorporam atitudes e comportamentos críticos identificados nas entrevistas com Oficiais de Inteligência. Jorge Amado destacou a importância do ceticismo analítico e do rigor metodológico: *"Desconfiar do que recebe [...] estar sempre validando as informações [...] como um trabalho científico, guiado por fatos e não por crenças"* (comunicação pessoal, 18 de novembro de 2024). Essa postura reflete-se diretamente nas competências que exigem análise imparcial de discursos (Competência 14) e modelagem prospectiva de narrativas (Competência 16), nas quais a desconfiança sistemática evita vieses ideológicos e garante conclusões embasadas em evidências. Zélia Gattai complementou ao enfatizar a ética profissional: *"Ser regido pela ética [...] entender que a informação serve à segurança do Estado e não ao ego individual"* (comunicação pessoal, 3 de janeiro de 2025), princípio fundamental para ações como a cooperação interinstitucional (Competência 17), onde o compartilhamento responsável de dados sensíveis exige transparência e alinhamento a valores democráticos.

As competências propostas – baseadas em comportamentos observáveis, conhecimentos técnicos e atitudes como imparcialidade e rigor científico – fortalece a capacidade de identificar e neutralizar campanhas de desinformação. Ao integrar ceticismo analítico e ética operacional, o *framework* de competências assegura que o Oficial de Inteligência atue equilibrando ação técnica e compromisso cívico em um cenário de ameaças complexas e desinformação globalizada.

As próximas seis competências – de 18 a 23 – foram modeladas para o enfrentamento ao quinto desafio, que visa fortalecer a resiliência cibernética nacional para identificar, mitigar e responder a ameaças cibernéticas, com foco na proteção de Infraestruturas Críticas, no uso seguro de tecnologias emergentes e na cooperação interinstitucional.

COMPETÊNCIA 18			
TÍTULO: Inteligência Cibernética e análise de ameaças de origem estatal e não estatal.			
DESCRIÇÃO: Monitorar e analisar ameaças cibernéticas de origem estatal e não estatal.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Coletar, processar e analisar indicadores de comprometimento (IoCs) e táticas, técnicas e procedimentos (TTPs) empregados em ataques cibernéticos.	Fundamentos de segurança cibernética, inteligência cibernética e análise de risco.	Operar ferramentas de cibersegurança (ex: scanners de vulnerabilidade, monitoramento de sistemas) e de *Threat Intelligence*.	Curiosidade investigativa para identificar padrões de ameaças emergentes.
Empregar ferramentas de *Threat Intelligence* para identificar padrões de ataque e possíveis agentes responsáveis.	Técnicas de *Open Source Intelligence* (OSINT) e análise comportamental de ameaças.	Analisar padrões de ataques cibernéticos.	Rigor analítico na análise de dados e evidências.
Produzir relatórios técnicos e estratégicos sobre o cenário atual e tendências emergentes.	Principais grupos APT (*Advanced Persistent Threats*) e seus métodos de ataque.	Produzir relatórios técnicos com linguagem clara e precisa.	Comprometimento com a produção de análises isentas e desprovidas de viés ideológico.
---	Proficiência no idioma Inglês para leitura de artigos técnicos e relatórios internacionais.	---	---

Tabela 28 – Competência 18

COMPETÊNCIA 19			
TÍTULO: Proteção cibernética e Gestão de Riscos para Infraestruturas Críticas.			
DESCRIÇÃO: Implementar protocolos de Segurança Cibernética para Infraestruturas Críticas.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Diagnosticar e mapear vulnerabilidades em sistemas críticos.	Princípios de segurança cibernética (CIA Triad: Confidencialidade, Integridade e Disponibilidade).	Realizar testes de intrusão e simulações de ataque (*redteaming*).	Proatividade na identificação e correção de vulnerabilidades.
Implementar e testar protocolos de segurança para proteção de dados sensíveis.	Normas internacionais de segurança, como ISO 27001 e *NIST Cybersecurity Framework*.	Configurar e administrar sistemas de detecção e prevenção de intrusos (IDS/IPS).	Atenção a detalhes e rigor na execução de protocolos.
Desenvolver planos de contingência para situações de ataque cibernético.	Conceitos de segurança em Infraestruturas Críticas e criptografia de dados.	Elaborar protocolos de segurança ajustados a diferentes cenários de risco.	Resiliência para lidar com cenários de crise e pressão.

Tabela 29 – Competência 19

COMPETÊNCIA 20

TÍTULO: Análise digital e extração de dados e evidências para produção de Conhecimento de Inteligência.			
DESCRIÇÃO: Coletar, analisar e interpretar dados digitais para identificar padrões, ameaças e tendências, subsidiando a produção de conhecimento de Inteligência.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Coletar, preservar e analisar evidências digitais seguindo padrões reconhecidos.	Fundamentos de forense digital e análise de artefatos de sistemas.	Analisar registros de log, artefatos de memória e fluxos de rede.	Zelo pela integridade e autenticidade das evidências.
Empregar ferramentas específicas para identificar a origem de ataques e métodos utilizados.	Técnicas de rastreamento de ameaças e identificação de padrões maliciosos.	Redigir laudos técnicos com clareza, detalhando metodologia e resultados.	Persistência na análise de dados complexos.
Produzir Relatórios de Inteligência para subsidiar investigações e processos decisórios.	Normativas legais sobre coleta, preservação e uso de evidências digitais.	---	Ética no tratamento de informações sensíveis.

Tabela 30 – Competência 20

COMPETÊNCIA 21			
TÍTULO: Operações de Contrainteligência no ambiente cibernético.			
DESCRIÇÃO: Planejar e executar operações de Contrainteligência cibernética.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Identificar e analisar tentativas de espionagem e infiltração em sistemas institucionais.	Princípios e técnicas de Contrainteligência cibernética.	Aplicar técnicas de rastreamento e atribuição de autoria de ataques.	Discrição e sigilo na condução de operações de Contrainteligência cibernéticas.
Planejar e conduzir operações de despistamento e engajamento com atores adversos.	Métodos de rastreamento e identificação de agentes hostis.	Executar operações de engajamento com segurança e discrição.	Iniciativa para antecipar ações de agentes adversos.
Produzir Relatórios de Inteligência para subsidiar decisões estratégicas de segurança organizacional.	Táticas de operações de despistamento e engajamento controlado.	Analisar comportamento de atacantes e padrões de ataque.	Compromisso com a proteção dos interesses institucionais.

Tabela 31 – Competência 21

COMPETÊNCIA 22			
TÍTULO: Cooperação para o fortalecimento da resiliência cibernética.			
DESCRIÇÃO: Estabelecer cooperação nacional e internacional para o fortalecimento da resiliência cibernética.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**

Identificar e estabelecer parcerias com instituições nacionais e internacionais.	Estruturas e mecanismos de cooperação internacional em segurança cibernética.	Conduzir reuniões e representar a organização em fóruns especializados.	Proatividade na construção de parcerias.
Participar de grupos de trabalho e fóruns relacionados à segurança cibernética.	Protocolos de comunicação e compartilhamento seguro de informações.	Negociar acordos de cooperação e articular iniciativas conjuntas.	Flexibilidade para lidar com interlocutores de diferentes culturas.
Produzir relatórios com análises compartilhadas e propostas de cooperação.	Proficiência nos idiomas Inglês e Espanhol para interação com parceiros internacionais.	Produzir documentos formais de cooperação e memorandos de entendimento.	Compromisso com a troca segura e responsável de informações.

Tabela 32 – Competência 22

COMPETÊNCIA 23			
TÍTULO: Aplicação de Inteligência Artificial e tecnologias emergentes para o fortalecimento da resiliência cibernética.			
DESCRIÇÃO: Desenvolver e implementar estratégias de resiliência cibernética com suporte de Inteligência Artificial.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Implementar modelos de Inteligência Artificial para detecção de padrões e anomalias em redes.	Fundamentos de aprendizado de máquina (*machine learning*) e de Inteligência Artificial aplicados à segurança cibernética.	Programar e ajustar modelos de Inteligência Artificial para análise de ameaças.	Interesse contínuo por inovações tecnológicas.
Analisar e validar dados fornecidos por sistemas de Inteligência Artificial em operações cibernéticas.	Princípios de análise comportamental baseada em Inteligência Artificial.	Integrar ferramentas de Inteligência Artificial com sistemas tradicionais de segurança.	Disciplina na validação e interpretação de dados automatizados.
Propor e desenvolver soluções automatizadas de resposta a incidentes.	Conhecimentos sobre ética e governança no uso de Inteligência Artificial.	Avaliar o desempenho e precisão de modelos preditivos.	Responsabilidade no uso ético de soluções baseadas em Inteligência Artificial.

Tabela 33 – Competência 23

As seis competências delineadas (18 a 23) envolvem amplo conhecimento e habilidade no uso de tecnologias emergentes, essenciais para responder às ameaças cibernéticas. Conforme destacado nas entrevistas com os Oficiais de Inteligência, essa demanda por *expertise* técnica é urgente. Castro Alves ressaltou que, diante das lacunas formativas em exatas, "*o próximo concurso poderia ser feito somente para a área de Tecnologia da Informação, Ciência da Computação e por aí vai*" (comunicação pessoal, 28 de novembro de 2024), enfatizando a necessidade de profissionais capazes de operar ferramentas como *big data* e Inteligência Artificial. Carlos Drummond de Andrade complementou: "*não dá pra pensar num profissional de informações [...] sem que ele tenha uma compreensão mínima [...] sobre ciência de dados, análise de dados, Inteligência Artificial, todo esse universo da informação no ambiente digital*" (comunicação

pessoal, 2 de dezembro de 2024), reforçando que mesmo conhecimentos básicos em estatística e ambiente digital são indispensáveis.

Essas percepções alinham-se diretamente às competências propostas. A Competência 23, por exemplo, que trata da aplicação de Inteligência Artificial para detecção de padrões em redes, exige domínio de *machine learning*, refletindo a ênfase dos entrevistados em habilidades técnicas avançadas. Já a Competência 18, voltada à análise de ameaças cibernéticas, demanda operação de ferramentas de *Threat Intelligence* e de *Open Source Intelligence* (OSINT), habilidades citadas por Castro Alves como críticas para suprir carências operacionais. Assim, a modelagem das competências não apenas atende ao Desafio 5 – fortalecer a resiliência cibernética –, mas também incorpora as críticas práticas dos profissionais, evidenciando que a superação de desafios contemporâneos exige que a organização detenha um corpo funcional com base sólida em ciências exatas e promova atualização constante de seu parque tecnológico.

O sexto desafio aborda a necessidade de uma definição mais clara e detalhada das atribuições do cargo de Oficial de Inteligência, aspecto essencial para garantir segurança jurídica no desempenho da função. Embora a Lei n.º 11.776/2008 (Brasil, 2008) estabeleça as atribuições do cargo, sua redação genérica gera lacunas que podem levar a questionamentos por órgãos de controle e expor os profissionais a riscos de responsabilização indevida.

Ainda que a superação desse cenário dependa, em grande parte, de medidas externas ao cotidiano do Oficial de Inteligência – como a aprovação de leis ou a expedição de decretos –, é possível mitigar esses riscos por meio da adoção de atitudes proativas, da busca contínua por conhecimentos jurídicos basilares e do desenvolvimento de habilidades que favoreçam a conformidade das ações com os princípios da legalidade e eficiência. Nesse sentido, foram delineadas três competências que orientam esses aspectos do comportamento profissional, proporcionando um referencial para que o Oficial de Inteligência atue com maior segurança jurídica, mesmo diante de um cenário normativo que ainda carece de refinamento.

COMPETÊNCIA 24			
TÍTULO: Segurança jurídica, governança e conformidade normativa na Atividade de Inteligência.			
DESCRIÇÃO: Interpretar e aplicar normativas da Atividade de Inteligência e da Administração Pública.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Consultar e aplicar normativas internas e externas que regem a Atividade de Inteligência e a Administração Pública.	Lei n.º 9.883/1999 (criação da ABIN e do Sistema Brasileiro de Inteligência).	Interpretar corretamente dispositivos normativos e administrativos.	Compromisso com a conformidade legal e administrativa.

Garantir que suas decisões e ações estejam embasadas na legislação vigente, reduzindo riscos jurídicos e institucionais.	Lei n.º 8.112/1990 (Regime Jurídico dos Servidores Públicos Federais).	Aplicar diretrizes legais em sua rotina de trabalho.	Proatividade na busca por segurança jurídica e clareza normativa.
Documentar suas atividades de maneira que demonstrem conformidade com as diretrizes normativas e regulatórias.	Direito Constitucional e Direito Administrativo	Redigir documentos administrativos e relatórios técnicos com respaldo normativo.	Responsabilidade ao interpretar e aplicar normativas.
Sugerir a atualização e a padronização das normativas internas sempre que identificar ambiguidades ou lacunas que possam comprometer a segurança jurídica dos servidores.	Normas internas da organização e sua relação com a legislação de Inteligência e da Administração Pública.	---	---

Tabela 34 – Competência 24

COMPETÊNCIA 25			
TÍTULO: Gestão da conformidade e eficiência institucional na Atividade de Inteligência.			
DESCRIÇÃO: Desenvolver e implementar estratégias que assegurem a conformidade jurídica e eficiência operacional na execução de atribuições.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Manter-se atualizado sobre a legislação que rege a Administração Pública e a Atividade de Inteligência.	Gestão pública e princípios da Administração Pública.	Monitorar o cumprimento de normas internas e regulamentos.	Compromisso com a integridade institucional.
Certificar-se de que sua atuação está alinhada às diretrizes institucionais e normativas, evitando riscos de responsabilização.	Mecanismos de responsabilização na Administração Pública.	Aplicar metodologias para garantir conformidade legal e eficiência operacional.	Responsabilidade na execução das atividades conforme as diretrizes normativas.
Formalizar ações estratégicas e operacionais por meio de relatórios e pareceres técnicos para garantir transparência e rastreabilidade das atividades.	Princípios de conformidade legal e governança institucional.	Propor melhorias nos processos administrativos com base na legislação vigente.	Iniciativa na busca por melhores práticas administrativas e jurídicas.
Sugerir melhorias nos normativos internos para mitigar riscos e fortalecer a governança organizacional.	---	---	---

Tabela 35 – Competência 25

COMPETÊNCIA 26			
TÍTULO: Articulação e alinhamento de atribuições no ambiente de trabalho.			
DESCRIÇÃO: Comunicar e alinhar atribuições funcionais com gestores e equipe.			
PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	**CONHECIMENTOS (SABER)**	**HABILIDADES (SABER FAZER)**	**ATITUDES (QUERER FAZER)**
Realizar reuniões periódicas para esclarecimento de atribuições e responsabilidades funcionais.	Princípios da comunicação organizacional.	Conduzir reuniões de alinhamento com equipes para esclarecimento institucional.	Interesse na promoção da integridade dos processos institucionais.
Contribuir para a padronização dos fluxos de trabalho e processos decisórios dentro da organização.	Estruturas organizacionais e Arquitetura Estratégica da organização.	Comunicar diretrizes estratégicas de forma assertiva e objetiva.	Compromisso com a transparência na comunicação de responsabilidades.
Monitorar a aderência das práticas internas às normativas institucionais e sugerir ajustes quando necessário.	Técnicas de mediação de conflitos e negociação.	---	Proatividade na mediação de conflitos organizacionais.

Tabela 36 – Competência 26

A padronização das atribuições do Oficial de Inteligência revela-se essencial para garantir segurança jurídica, prevenir responsabilizações individuais e fortalecer a execução da missão institucional da ABIN. A incorporação das competências mapeadas possibilita uma atuação mais precisa e alinhada aos princípios da legalidade e eficiência, mitigando riscos administrativos e assegurando que cada tarefa desempenhada esteja juridicamente respaldada. Além disso, esse modelo contribui para o aprimoramento da governança e da conformidade legal, garantindo que os esforços do Oficial de Inteligência estejam sincronizados com os objetivos estratégicos da organização.

A modelagem das 26 competências, fundamentada na Ontologia Fundacional Unificada, consolidou um *framework* de competências alinhado às demandas da ABIN, garantindo rigor conceitual e operacionalidade prática. Ao estruturar conhecimentos, habilidades e atitudes em padrões de desempenho observáveis, o modelo não apenas traduziu as exigências dos seis desafios em capacidades profissionais tangíveis, mas também estabeleceu relações ontológicas explícitas entre competências e necessidades institucionais. Essa articulação reflete a premissa de que a eficácia da Inteligência como função de Estado depende da convergência entre formação técnica e realidades organizacionais.

Com fins didáticos e para facilitar a compreensão e a aplicação prática do *framework*, as competências foram agrupadas em seis famílias temáticas, que representam agrupamentos

orientados por afinidade de propósito e por similaridade funcional. Essas famílias operam como eixos estruturantes do *framework*. A figura 3 ilustra as seis famílias.

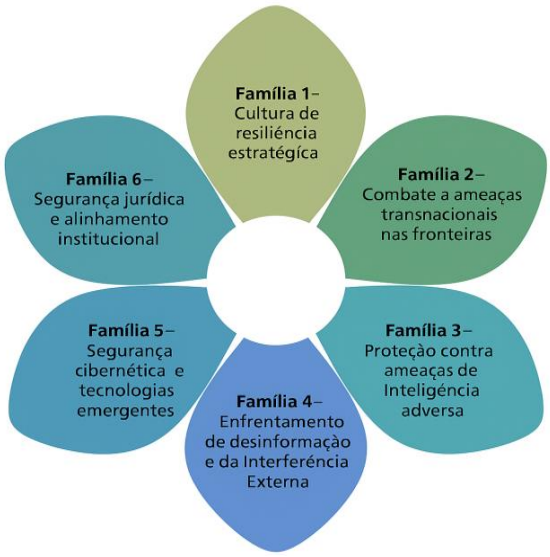


Figura 3 – Famílias de competências.

Contudo, as competências não se restringem a desafios isolados: sua natureza multifuncional e transversal será explorada na próxima seção, que analisa como a interdependência entre conhecimentos especializados e habilidades integradas amplifica a resiliência institucional, preparando a ABIN para responder a ameaças complexas e dinâmicas de forma sistêmica e sinérgica.

4.3. Interconexões entre competências e desafios

Esta seção analisa as interconexões das competências com os desafios delineados. À medida que se aprofundou a análise, identificou-se que diversas competências, mesmo agrupadas sob um desafio principal, possuem aplicabilidade ampliada, podendo contribuir simultaneamente para a superação de outros.

Essa interdependência ocorre porque os desafios enfrentados pela organização não são isolados, mas sim interligados por vulnerabilidades comuns, metodologias compartilhadas e exigências estratégicas semelhantes. Por exemplo, as competências associadas à Contrainteligência (Desafio 3) são fundamentais não apenas para a proteção contra espionagem, mas também para a identificação de ameaças cibernéticas (Desafio 5) e o enfrentamento de campanhas de desinformação (Desafio 4). Da mesma forma, as habilidades voltadas à análise de riscos e vulnerabilidades são essenciais para a resiliência institucional (Desafio 1), ao mesmo tempo em que são indispensáveis para o combate ao crime organizado transnacional (Desafio 2) e para a segurança cibernética (Desafio 5).

A identificação dessas inteconexões é fundamental para que o órgão de Inteligência do Estado brasileiro possa, por exemplo, desenvolver programas de capacitação mais integrados, garantindo que o Oficial de Inteligência adquira competências multifuncionais que o permita atuar de forma dinâmica e adaptável às demandas laborais. Estudos indicam que a capacidade de mobilizar competências transversais aumenta a eficiência e a resiliênciainstitucional diante de ameaças complexas e interconectadas (Ferraz, Melo-Silva, Coscioni & Rodrigues, 2023).

A seguir, apresenta-se uma tabela que ilustra as competências com aplicabilidade transversal, seu desafio principal e outros desafios organizacionais nos quais também desempenham papel crítico, juntamente com uma explicação dessas interconexões.

COMPETÊNCIA (NÚMERO)	DESAFIO PRINCIPAL	DESAFIO INTERCONECTADO	EXPLICAÇÃO DA RELAÇÃO COM OS DESAFIOS INTERCONECTADOS
Planejar e implementar ações para cultura de resiliência estratégica. (1)	Desafio 1	Desafio 3 Desafio 5	Contrainteligência exige resiliência institucional para lidar com ameaças persistentes. Resiliência cibernética é essencial para proteger Infraestruturas Críticas.
Analisar riscos e vulnerabilidades em setores estratégicos. (2)	Desafio 1	Desafio 2 Desafio 3 Desafio 5	A análise de riscos é essencial para operações contra redes criminosas transnacionais, proteção contra espionagem e mitigação de ataques cibernéticos.
Coordenar ações interinstitucionais contra o crime organizado transnacional. (5)	Desafio 2	Desafio 3 Desafio 4	A interinstitucionalidade fortalece operações de Contrainteligência e de combate à desinformação, pois redes criminosas utilizam influência digital para lavagem de reputação.
Monitorar e analisar atividades criminosas transnacionais nas fronteiras brasileiras. (4)	Desafio 2	Desafio 3 Desafio 4	Há registros de que ao redor do mundo o crime organizado transnacional cooperaria com Serviços de Inteligência estrangeiros, fornecendo logística,financiamento e redes de influência, ao mesmo tempo em que utilizaria desinformação e manipulação informacional para encobrir atividades ilícitas e desviar investigações, tornando essencial a atuação integrada da Contrainteligência e da Inteligência Estratégica.
Desenvolver e implementar protocolos de proteção contra ações de Engenharia Social. (11)	Desafio 3	Desafio 4 Desafio 5	A desinformação se apóia em técnicas de Engenharia Social para influenciar decisões. A proteção contra esses ataques também fortalece a segurança cibernética.
Monitorar e analisar plataformas digitais e dinâmicas algorítmicas.	Desafio 4	Desafio 3 Desafio 5	A espionagem digital frequentemente está ligada à coleta de dados para manipulação de

(15)			narrativas (Desinformação) e operações de Inteligência adversária.
Interpretar e aplicar normativas da Atividade de Inteligência e da Administração Pública. (24)	Desafio 6	Desafio 1 Desafio 3	A padronização normativa fortalece a governança institucional e a segurança jurídica na aplicação de protocolos de Contrainteligência.
Coordenação interinstitucional para a proteção de conhecimentos sensíveis. (3)	Desafio 1	Desafio 3 Desafio 5	A coordenação interinstitucional para proteger conhecimentos sensíveis (competência 3) contribui diretamente para neutralizar a espionagem (Desafio 3) ao reduzir brechas de informação entre órgãos. Ao mesmo tempo, essa proteção integrada dificulta a exploração de dados confidenciais em ataques cibernéticos (Desafio 5), fortalecendo a resiliência digital das instituições envolvidas.
Análise financeira e investigação de fluxos ilícitos vinculados a Organizações Criminosas Transnacionais. (6)	Desafio 2	Desafio 4 Desafio 5	O mapeamento de fluxos financeiros ilícitos associados ao crime organizado (competência 6) ajuda a desmantelar esquemas de financiamento de campanhas de desinformação (Desafio 4), pois muitas operações ilegais sustentam narrativas destinadas a desestabilizar instituições. Além disso, a análise financeira de redes criminosas apoia a identificação de grupos de cibercrime e ataques patrocinados por atores ocultos, reforçando a segurança cibernética nacional (Desafio 5).
Inteligência Cibernética na análise e mitigação de ameaças digitais e raspagem de dados sensíveis. (12)	Desafio 3	Desafio 1 Desafio 5	O monitoramento e a mitigação de ameaças digitais e da raspagem de dados sensíveis (competência 12), embora focados na Contrainteligência (Desafio 3), elevam a resiliência institucional (Desafio 1) ao evitar vazamentos de informações estratégicas que poderiam comprometer operações essenciais. Simultaneamente, essa competência aprimora a defesa cibernética (Desafio 5) ao detectar intrusões e tentativas de coleta ilegal de dados, agindo de forma preventiva contra ataques digitais sofisticados.
Cooperação interinstitucional no combate à desinformação. (17)	Desafio 4	Desafio 1 Desafio 3	Ao estabelecer cooperação interinstitucional contra a desinformação (competência 17), o Oficial de Inteligência ajuda a preservar a confiança nas instituições democráticas e a estabilidade organizacional (Desafio 1) por meio de ações coordenadas. Essa articulação também fortalece a

			proteção contra interferências externas maliciosas (Desafio 3), já que muitos esforços de espionagem ou influência adversária utilizam narrativas falsas – combatidas de forma mais eficaz quando há atuação conjunta entre órgãos diversos.
Proteção cibernética e Gestão de Riscos para Infraestruturas Críticas. (19)	Desafio 5	Desafio 1 Desafio 3	A implementação de protocolos robustos de segurança cibernética em Infraestruturas Críticas (competência 19), além de endereçar diretamente ameaças digitais (Desafio 5), assegura a continuidade de operações nos setores estratégicos (Desafio 1) mesmo diante de ataques, graças à pronta identificação e mitigação de vulnerabilidades. Adicionalmente, ao proteger esses sistemas vitais, a competência dificulta tentativas de espionagem (Desafio 3) que busquem explorar falhas nas infraestruturas nacionais, integrando a defesa cibernética com a Contrainteligência.
Análise digital e extração de dados e evidências para produção de Conhecimento de Inteligência. (20)	Desafio 3	Desafio 1 Desafio 5	A capacidade de identificação e neutralização de redes de influência externa (competência 20) não apenas mitiga ameaças diretas de espionagem e interferência estrangeira (Desafio 3), mas também fortalece a segurança institucional (Desafio 1) ao reduzir o impacto de atores externos que buscam desestabilizar políticas públicas e decisões estratégicas. Além disso, a atuação contra redes maliciosas que exploram vulnerabilidades digitais está diretamente ligada à proteção contra ataques cibernéticos (Desafio 5), uma vez que muitos vetores de influência adversária utilizam meios digitais para infiltração e coleta ilícita de dados.
Cooperação para o fortalecimento da resiliência cibernética. (22)	Desafio 4	Desafio 2 Desafio 5	A habilidade de monitoramento e análise de campanhas de desinformação (competência 22) tem impacto direto na segurança cibernética (Desafio 5), pois muitos desses ataques são estruturados a partir da manipulação digital de narrativas falsas. A atuação para mitigar esses impactos também se conecta à segurança de instituições democráticas (Desafio 2), pois campanhas desse tipo frequentemente visam deslegitimar processos eleitorais, decisões governamentais e órgãos

			institucionais, comprometendo a estabilidade do país.
Gestão da conformidade e eficiência institucional na Atividade de Inteligência. (25)	Desafio 6	Desafio 1 Desafio 3	A análise de ameaças emergentes no ambiente geopolítico internacional (competência 25) contribui para a resiliência de setores estratégicos (Desafio 6), antecipando riscos que podem impactar infraestruturas essenciais. Essa antecipação também reforça a segurança institucional (Desafio 1), permitindo que políticas preventivas sejam implementadas antes que as ameaças se concretizem. Simultaneamente, a inteligência sobre ameaças externas apoia a contraespionagem (Desafio 3), pois possibilita a identificação de vetores utilizados por adversários para obter vantagens estratégicas sobre o país.

Tabela 37 – Competências transversais e sua contribuição para enfrentamento aos desafios delineados.

A figura 4 ilustra, por meio de um diagrama de interseção, a natureza multifuncional das competências modeladas, destacando sua aplicabilidade simultânea a múltiplos desafios institucionais. As linhas contínuas em destaque representam a vinculação primária de cada competência a um desafio específico, conforme delineado na subseção anterior. Já as linhas pontilhadas demonstram as interconexões secundárias, nas quais uma mesma competência contribui para a superação de outros desafios organizacionais, reforçando a interdependência entre as demandas da ABIN.

Essa representação visual evidencia que as competências não atuam de forma isolada, mas sim de maneira sinérgica, ampliando sua eficácia ao abordar vulnerabilidades comuns, metodologias compartilhadas e contextos estratégicos sobrepostos. A transversalidade observada reflete a complexidade dinâmica do ambiente em que opera a Atividade de Inteligência, onde ameaças como a desinformação, a espionagem e o crime organizado transnacional estão intrinsecamente interligadas. Dessa forma, o diagrama reforça a necessidade de capacitação integrada, capaz de desenvolver profissionais aptos a mobilizar conhecimentos e habilidades de forma adaptável, assegurando respostas coordenadas e resilientes diante de desafios multifacetados.

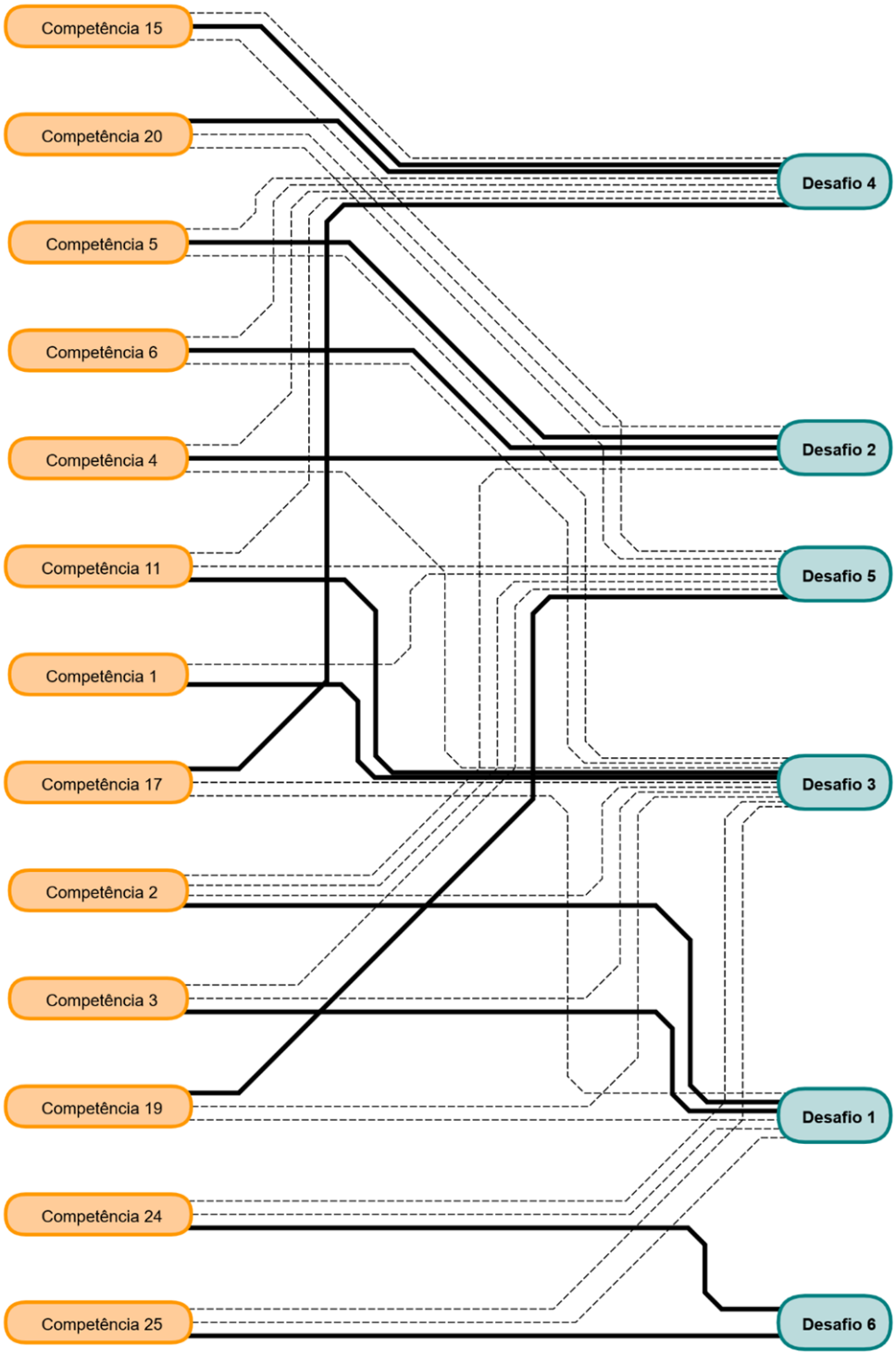


Figura 4 – Transversalidade das competências.

4.4. Percepção dos Oficiais de Inteligência quanto ao tratamento do tema gestão por competências na ABIN

Essa seção apresenta os resultados correspondentes ao objetivo específico de identificar e compreender a percepção de Oficiais de Inteligência que exerceram funções gerenciais na ABIN

sobre o tratamento conferido à GPC na organização. A partir da realização de 20 entrevistas semiestruturadas, analisaram-se qualitativamente as respostas oferecidas pelos participantes em torno de três eixos principais: (i) a percepção sobre a existência ou não da GPC na instituição; (ii) o grau de clareza dos gestores quanto às competências esperadas dos integrantes de suas equipes; e (iii) a avaliação sobre a capacidade da ABIN de operar com base nos pressupostos que caracterizam esse modelo de gestão.

A primeira questão investigada, de natureza fechada, buscou aferir a percepção dos entrevistados sobre a existência da GPC na ABIN, por meio da seguinte indagação: "O entrevistado acredita que há gestão por competências na ABIN?". As opções de resposta oferecidas foram: "não acredito", "acredito, mas parcialmente" e "acredito totalmente". Os dados revelaram uma percepção predominantemente negativa: 60% dos respondentes afirmaram não acreditar na existência de uma gestão estruturada por competências na organização, enquanto os 40% restantes indicaram acreditar parcialmente. Nenhum entrevistado assinalou a opção "acredito totalmente".

Entre os participantes que reconheceram alguma forma de aplicação da GPC, ainda que parcial, foram citadas como subáreas relacionadas à sua possível incidência: o processo de recrutamento (em especial para o concurso de ingresso ao cargo de Oficial de Inteligência), os processos seletivos internos e os procedimentos de cessões e requisições. A menção a essas áreas sugere que, embora não formalizadas sob uma abordagem sistêmica de competências, tais práticas estariam sendo conduzidas, ao menos em parte, com base em critérios compatíveis com a lógica desse modelo.

Dois depoimentos oriundos desse grupo que declarou acreditar parcialmente na existência da GPC fornecem elementos qualitativos relevantes para a análise. O primeiro, atribuído a Aluísio Azevedo, afirma: *"No subsistema de design de cursos e de capacitação, percebo iniciativas alinhadas com competências, mas sem uma diretriz clara e institucionalizada."* (comunicação pessoal, 19 de novembro de 2024). Esse relato sugere que há ações isoladas voltadas ao desenvolvimento de competências, particularmente no campo da capacitação, embora sem respaldo formal ou amparo em diretrizes estratégicas consistentes. O segundo depoimento, de Thomas Antônio Gonzaga, destaca: *"Tudo converge para não acreditar, porém existem alguns indícios."* (comunicação pessoal, 22 de novembro de 2024). Tal observação expressa uma percepção ambígua, em que são identificadas manifestações pontuais associadas à GPC, mas que não se consolidam em uma prática institucionalizada.

Esses elementos indicam que a GPC pode estar presente de maneira fragmentada e implícita, o que reforça a percepção de que a ausência de sistematização e de clareza

comunicacional dificulta seu reconhecimento por parte dos servidores. Nesse sentido, os entrevistados tendem a perceber uma desconexão entre a formulação conceitual da GPC e sua efetiva implementação na rotina institucional.

A análise integrada dos dados quantitativos e qualitativos corrobora essa interpretação: há, entre os entrevistados, um reconhecimento de que determinados processos apresentam aderência parcial aos princípios da GPC, mas também a constatação de que essas práticas não estão suficientemente consolidadas ou legitimadas em nível institucional. A ausência de uma política claramente comunicada e de mecanismos estruturantes pode explicar a dificuldade de identificação do modelo por parte dos profissionais.

Dessa forma, os resultados apontam para a necessidade de aprimorar a implementação e, sobretudo, a comunicação institucional da GPC na ABIN. Esse aprimoramento requer articulação entre diferentes níveis organizacionais. À alta gestão cabe assumir o compromisso estratégico com a GPC, promovendo diretrizes claras, alinhamento institucional e alocação adequada de recursos. À área de gestão de pessoas compete a tarefa de traduzir essas diretrizes em instrumentos operacionais concretos, como o mapeamento de competências, trilhas de desenvolvimento e avaliações compatíveis com esse modelo. Por sua vez, os gestores intermediários devem ser capacitados e responsabilizados pela aplicação prática da GPC no cotidiano das equipes, assegurando a coerência entre competências requeridas e resultados esperados.

A ausência de coordenação entre esses atores institucionais contribui, como evidenciado pelas respostas dos entrevistados, para a percepção de que a GPC inexiste – ainda que alguns de seus elementos possam estar presentes, de forma difusa, nas práticas organizacionais. Superar essa lacuna demanda não apenas ações técnicas, mas sobretudo um esforço institucional deliberado de integração, sensibilização e comunicação contínua sobre os fundamentos e os benefícios da GPC.

A segunda questão investigada procurou compreender a percepção dos entrevistados quanto à clareza dos gestores da ABIN em relação às competências esperadas de seus subordinados diretos. A pergunta formulada foi: “Os gestores da ABIN possuem clareza sobre as competências esperadas de cada colaborador em suas equipes?”. As opções de resposta disponibilizadas foram: “discordo totalmente”, “não concordo e nem discordo”, e “concordo totalmente”. Os resultados revelam uma percepção amplamente negativa: cerca de 60% dos entrevistados afirmaram “discordo totalmente”, enquanto os 40% restantes optaram por “não concordo e nem discordo”. Nenhum dos respondentes assinalou a opção que indicaria concordância com a proposição.

Essa distribuição indica que os gestores da ABIN não possuiriam clareza sobre as competências que cada membro de sua equipe detém, o que pode ser atribuído à inexistência de um processo estruturado de mapeamento de competências individuais. Em outras palavras, a ausência de um inventário formal de conhecimentos, habilidades e atitudes do corpo funcional dificulta qualquer tentativa, por parte dos gestores, de estabelecer relações objetivas entre os perfis dos servidores e as exigências das funções. Essa lacuna sistêmica foi mencionada de forma recorrente pelos entrevistados, muitos dos quais relataram que, em razão do déficit de pessoal, os gestores acabam alocando servidores com base na disponibilidade imediata, e não na adequação por competências.

O depoimento de Mário de Andrade ilustra essa realidade ao afirmar: *"O cotidiano de trabalho dos gestores é totalmente preenchido com questões diversas, restando-lhes pouco tempo para pensar nessa questão. Aliado a tal fato, a organização também não estimula ou cobra que isso seja feito."* (comunicação pessoal, 30 de dezembro de 2024). A ausência de estímulo institucional e de cobrança gerencial para que a GPC seja aplicada de forma sistemática revela um contexto em que a responsabilidade por esse modelo de gestão recai sobre indivíduos isoladamente, sem respaldo organizacional claro. Outro comentário qualitativo reforça essa perspectiva: Castro Alves menciona haver uma *"clareza limitada e genérica"* (comunicação pessoal, 28 de novembro de 2024) quanto às competências esperadas, sugerindo que, mesmo onde há alguma intuição gerencial sobre o tema, ela não está sustentada por processos institucionais robustos.

Esses relatos apontam para a inexistência de mecanismos normativos, técnicos ou operacionais que permitam aos gestores compreender, com precisão, o conjunto de competências disponíveis em suas equipes. A ausência de um sistema de mapeamento e de uma cultura organizacional voltada à valorização das competências, na percepção dos entrevistados, torna improvável a aplicação efetiva de uma gestão orientada por esse modelo.

A análise integrada dos dados sugere, portanto, que a clareza sobre as competências dos colaboradores, por parte dos gestores da ABIN, ainda não constitui uma prática institucionalizada. A falta de instrumentos adequados e a carência de formação continuada para os líderes contribuem para a fragilidade desse aspecto da gestão de pessoas.Dessa forma, os achados desta etapa da pesquisa reforçam a necessidade de fortalecer as ações de mapeamento, capacitação e instrumentalização dos gestores como condição indispensável para a consolidação da GPC na ABIN. A clareza dos gestores quanto às competências disponíveis em suas equipes é essencial para a alocação estratégica de pessoas, o planejamento de ações de desenvolvimento e a entrega

de resultados organizacionais. Sua inexistência compromete a articulação entre desempenho institucional e valorização do Oficial de Inteligência, demandando, por consequência, uma abordagem mais estruturada, coordenada e coerente com os princípios da GPC.

A terceira questão da pesquisa buscou explorar a percepção dos entrevistados quanto à capacidade institucional da ABIN para operar com base na lógica da GPC. A pergunta formulada foi: "Na opinião do entrevistado, a ABIN está estruturada para operar em uma lógica de gestão por competências?". As opções de resposta disponibilizadas foram: "discordo totalmente", "concordo parcialmente" e "concordo plenamente". Os dados revelaram uma percepção majoritariamente negativa: 14 dos 20 respondentes (70%) afirmaram "discordo totalmente", enquanto 5 respondentes (25%) indicaram "concordo parcialmente". Apenas um entrevistado (5%) optou por "concordo plenamente".

A predominância da resposta "discordo totalmente" sugere que, na percepção dos entrevistados, a ABIN ainda não está preparada – cultural, técnica e institucionalmente – para implementar um modelo de gestão baseado em competências. Essa prontidão institucional envolve não apenas a existência de estruturas formais, mas também uma cultura organizacional orientada à valorização das competências, o domínio técnico-conceitual por parte dos gestores e servidores, e a integração dos diversos subsistemas de gestão de pessoas.

Entre os respondentes que assinalaram "concordo parcialmente", as declarações indicam a percepção de que há determinados elementos institucionais que, embora ainda insuficientes, poderiam futuramente sustentar a consolidação da GPC. José de Alencar, por exemplo, menciona a existência de um Departamento de Gestão de Pessoas, o que, em sua visão, representaria um ponto de partida relevante. Contudo, ele destaca o descompasso entre a existência dessa estrutura e sua efetiva operacionalização: *"A estrutura existe, que permitiria o emprego de uma gestão adequada das capacidades de todos os servidores. Mas entre existir uma estrutura e colocar isso em prática no dia a dia, existe uma diferença."* (comunicação pessoal, 10 de janeiro de 2025). Em sua avaliação, a organização dispõe dos elementos formais básicos, mas não apresenta resultados que evidenciem sua utilização sistemática no contexto da GPC.

De modo complementar, Oswald de Andrade (comunicação pessoal, 2 de janeiro de 2025) recorda que, em momento anterior, foi realizada uma tentativa incipiente de mapeamento de competências na ABIN, embora essa iniciativa não tenha sido levada adiante. Ainda assim, ele entende que a experiência representou um vislumbre inicial de aproximação ao modelo: *"Chegou-se a tratar do assunto."*. Para o entrevistado, embora a instituição ainda não esteja alicerçada para operar integralmente sob a lógica da GPC, há gestores que demonstram conhecimento técnico e

preocupação com o tema. Em suas palavras: *"Essas pessoas têm conhecimento sobre a ferramenta, da técnica, do modelo de gestão. O que falta talvez é realmente fazer as fundações desses alicerces, que vai passar pelo mapeamento e tudo mais."*. Sua opção pela resposta "concordo parcialmente" traduz a percepção de que alguns passos preliminares foram dados, ainda que de forma isolada e sem institucionalização.

Esses relatos qualitativos indicam que a ausência de prontidão da ABIN para operar sob a lógica da GPC decorre de um conjunto de fatores interdependentes: lacunas formativas, inexistência de diretrizes normativas claras, ausência de instrumentos técnicos de mapeamento e avaliação de competências, e baixa articulação entre os subsistemas de gestão de pessoas. A ideia de estrutura organizacional, nesse contexto, deve ser compreendida de forma ampliada – abarcando não apenas a existência de departamentos ou unidades administrativas, mas sobretudo os processos, rotinas e práticas organizacionais que sustentariam uma abordagem baseada em competências.

A análise integrada dos dados quantitativos e qualitativos reforça, portanto, a interpretação de que a ABIN, segundo a percepção de seus Oficiais de Inteligência, não dispõe das condições necessárias – em termos de cultura, conhecimento técnico e práticas gerenciais – para operar de forma consistente com os fundamentos da GPC. As ações eventualmente associadas a esse modelo ocorrem de maneira fragmentada, empírica e desarticulada, carecendo de institucionalização.

Diante desse cenário, os achados indicam a necessidade de um esforço coordenado e gradual de construção dessa prontidão institucional. Tal esforço envolve a capacitação de gestores e servidores, o desenvolvimento de instrumentos técnicos apropriados, a integração dos subsistemas de gestão de pessoas e a internalização progressiva da lógica por competências na cultura da organização. A consolidação da GPC na ABIN depende, portanto, de uma abordagem sistêmica, estratégica e sustentada ao longo do tempo.

Em síntese, os dados revelam uma percepção predominantemente negativa dos Oficiais de Inteligência quanto ao grau de institucionalização da GPC na ABIN. Embora tenham sido mencionadas iniciativas pontuais ou elementos incipientes que tangenciam esse modelo – como processos seletivos internos, ações de capacitação e tentativas anteriores de mapeamento de competências –, o que prevalece é a avaliação de que tais práticas ocorrem de forma fragmentada, sem articulação sistêmica ou sustentação normativa. A ausência de diretrizes claras, a baixa integração entre os subsistemas de gestão de pessoas e a carência de formação gerencial em GPC foram identificadas como obstáculos centrais à sua consolidação. Dessa forma, os achados apontam para a necessidade de uma estratégia organizacional deliberada, capaz de promover não

apenas a implantação técnica da GPC, mas também sua internalização cultural, como condição para que esse modelo deixe de ser uma referência abstrata e se torne parte efetiva da prática institucional.

5. CONCLUSÕES

Esta dissertação partiu da premissa de que o fortalecimento da Atividade de Inteligência no Brasil requer, entre outras condições, o aperfeiçoamento dos instrumentos de gestão de pessoas, de modo a alinhá-los aos desafios organizacionais contemporâneos. A partir da abordagem da gestão por competências, buscou-se compreender a percepção de Oficiais de Inteligência que exerceram funções gerenciais sobre o tratamento conferido à GPC na Agência Brasileira de Inteligência, e propor um artefato técnico que contribua para a consolidação de uma cultura orientada ao desenvolvimento e valorização de competências.

Com base no percurso metodológico empreendido e nos resultados obtidos, é possível afirmar que os objetivos delineados na introdução desta dissertação foram alcançados. O objetivo geral – modelar um *framework* de competências para o cargo de Oficial de Inteligência da ABIN – foi concretizado por meio de uma metodologia combinada, que articulou revisão teórica, análise documental e consulta a especialistas da própria organização. Os objetivos específicos também foram atingidos: (i) localizou-se e analisou-se modelos e *frameworks* de competências adotados por Serviços de Inteligência internacionais, como nos Estados Unidos e na França; e (ii) investigou-se a percepção de Oficiais de Inteligência que ocuparam função gerencial na ABIN acerca do tratamento conferido à GPC na organização, revelando elementos qualitativos relevantes sobre suas potencialidades e lacunas. Por fim, a articulação entre essas etapas viabilizou a construção do Produto Técnico-Tecnológico proposto.

A partir dessas bases, a proposta apresentada nesta dissertação busca atender a um duplo propósito: oferecer um instrumento útil à gestão de pessoas na ABIN e estimular o debate acadêmico sobre modelos de competências em Serviços de Inteligência, ainda incipientes na literatura nacional. Nesse sentido, a proposta contribui tanto para a inovação institucional quanto para o amadurecimento do campo da Administração Pública aplicada à Segurança do Estado.

Importa reconhecer que, devido à natureza sensível da Atividade de Inteligência e às restrições legais, esta pesquisa enfrentou limitações quanto ao acesso e à divulgação de determinadas informações institucionais. Em razão do sigilo que rege alguns dos atos administrativos da ABIN, não foi possível consultar documentos internos restritos nem divulgar indicadores estratégicos ou operacionais que poderiam comprometer a segurança da organização. Por esse motivo, as análises e proposições aqui apresentadas baseiam-se exclusivamente em dados obtidos por meio de entrevistas com profissionais experientes e em fontes documentais de caráter público. Embora tais fontes tenham se revelado suficientes para sustentar a construção do

framework, reconhece-se que o escopo da pesquisa foi limitado pela necessidade de resguardar aspectos sigilosos da atuação institucional da Agência.

Importa destacar que as conclusões derivam exclusivamente da análise das entrevistas. Assim, quando os entrevistados mencionam a inexistência de diretrizes, instrumentos ou práticas de GPC, estão expressando uma percepção pessoal – o que não permite afirmar categoricamente que esses elementos não existam, mas apenas que não são reconhecidos ou apropriados por parte relevante dos servidores que atuaram em funções gerenciais.

Apesar das limitações apontadas, os dados coletados indicam que há, entre os entrevistados, uma percepção generalizada de que a GPC é um caminho viável e desejável para a profissionalização de processos no âmbito da organização. Vários depoimentos ressaltam a necessidade de adoção de critérios mais objetivos para recrutamento, alocação, desenvolvimento e avaliação de Oficiais de Inteligência. Trata-se de uma manifestação espontânea de abertura, não institucional, mas pessoal, por parte dos profissionais da carreira, em direção a modelos mais racionais e estratégicos de gestão de pessoas.

Com base nesse diagnóstico, a dissertação propôs a construção de um *framework* de competências para Oficiais de Inteligência. A proposta foi desenvolvida segundo os pressupostos metodológicos da DSR, que orienta a criação de artefatos a partir da interação entre problema prático, evidência empírica e fundamentação teórica. Essa abordagem permitiu articular os achados da pesquisa qualitativa com a construção de uma solução concreta voltada à realidade institucional analisada.

Além disso, o desenvolvimento do *framework* foi orientado por princípios da Ontologia Fundacional Unificada, o que garantiu coerência lógica, rigor conceitual e padronização terminológica ao modelo. O resultado foi um conjunto de 26 competências estruturadas em torno dos elementos de conhecimento, habilidade e atitude, cada uma associada a padrões de desempenho e aos desafios estratégicos da organização. Essa modelagem foi complementada pela utilização de entrevistas e pelo mapeamento de desafios institucionais como insumos centrais para a estruturação do artefato.

A integração de competências técnicas e comportamentais também foi aspecto central na construção do *framework*. Ao evidenciar que o desempenho na Atividade de Inteligência depende tanto do domínio de técnicas específicas quanto de atitudes como discrição, resiliência emocional e compromisso ético, o *framework* amplia a compreensão sobre o que significa “estar apto” a

exercer esse *múnus* público. Isso tem implicações diretas para o desenho de concursos públicos, programas de formação e instrumentos de avaliação funcional.

A efetiva implementação do *framework* dependerá de uma estratégia institucional progressiva. Recomenda-se sua introdução inicial em áreas prioritárias, como análise de riscos cibernéticos ou operações de Contrainteligência. Essa etapa-piloto permitiria validar a aplicabilidade do *framework* de competências, promover ajustes com base no uso real e construir as condições para sua posterior expansão para toda a organização. Além disso, a adoção do *framework* deve ser acompanhada de ações formativas voltadas à capacitação de gestores e servidores, com vistas à apropriação prática do modelo de competências e à incorporação dos princípios da GPC nas decisões cotidianas de gestão de pessoas. A consolidação da proposta dependerá da construção de uma cultura organizacional que valorize o desenvolvimento contínuo, o *feedback* estruturado e a objetividade na definição de critérios de desempenho.

Durante as entrevistas, 45% dos Oficiais de Inteligência relataram ter conhecimento, por meio de fontes abertas e interações profissionais, sobre a utilização da lógica da GPC por parte de Serviços de Inteligência estrangeiros. Essas menções referem-se, sobretudo, à adoção de critérios por competências em processos de ingresso em Serviços de Inteligência ou na assinalação de servidores para atividades específicas, como missões ou participação em cursos e treinamentos. Ainda que não tenham conhecimento pleno sobre a aplicação da GPC em sua dimensão estratégica, os entrevistados percebem que o modelo é compatível com a realidade de instituições similares no exterior.

Referências aos casos dos Estados Unidos e da França reforçam essa percepção. Em ambos os países, observam-se esforços para estruturar perfis por competência e alinhar processos seletivos, capacitações e avaliações de Profissionais de Inteligência aos objetivos estratégicos de seus Serviços de Inteligência. Ainda que sigam trajetórias distintas, esses exemplos demonstram que a lógica da GPC pode ser incorporada mesmo em instituições que operam sob rígidas condições de sigilo, compartimentação e pressão decisória – características também presentes na ABIN.

Finalmente, o processo de construção do *framework* mostrou-se relevante por si só como exercício institucional de escuta ativa e de síntese organizacional. Ao valorizar as vozes dos próprios servidores e cotejar suas experiências com os documentos oficiais da ABIN, a pesquisa contribui para uma visão mais integrada entre conhecimento tácito e orientação normativa. Trata-se de um esforço que vai além da descrição técnica: busca-se fomentar uma cultura de aprendizado

institucional, em que as competências são compreendidas como capacidades organizacionais compartilhadas e continuamente desenvolvidas.

Como agenda para estudos futuros, recomenda-se o aprofundamento de análises comparadas com modelos adotados por países do entorno estratégico brasileiro, a exemplo da Argentina e Colômbia, bem como do Sul Global, como Índia e África do Sul. Essas nações compartilham desafios estruturais semelhantes aos do Brasil – incluindo limitações de recursos, vulnerabilidades geopolíticas e sistemas administrativos complexos – o que as torna laboratórios relevantes para avaliação crítica da viabilidade e dos impactos da GPC em contextos de média potência. No entanto, deve-se reconhecer que o acesso a informações confiáveis sobre Serviços de Inteligência é limitado, tanto pela escassez de literatura científica quanto pelo caráter naturalmente reservado dessas instituições.

Deve-se reforçar, nesse ponto, que a proposta apresentada nesta dissertação não parte do pressuposto de que a ABIN atuou, ao longo de seus 25 anos de existência, sem parâmetros ou referenciais de desempenho. Ao contrário, a atuação exitosa da Agência em operações de grande complexidade – como aquelas vinculadas aos Jogos Pan-Americanos de 2007, à Copa do Mundo de 2014 e aos Jogos Olímpicos de 2016 – evidencia que a organização é composta por profissionais que detêm conhecimentos, habilidades e atitudes compatíveis com altos padrões de desempenho. O *framework* aqui apresentado não busca substituir essa experiência acumulada, mas sim contribuir para sua sistematização e fortalecimento.

Nesse sentido, o *framework* não deve ser interpretado como ponto de chegada, mas como instrumento de apoio para o amadurecimento da gestão de pessoas na ABIN. Ao proporcionar maior clareza conceitual e permitir o alinhamento entre desafios institucionais e competências profissionais, a proposta contribui para tornar a gestão de pessoas mais estratégica, transparente e orientada à missão, respeitando suas especificidades institucionais e os limites do contexto em que opera. Ao oferecer um modelo de gestão por competências tecnicamente fundamentado, alinhado aos desafios da Atividade de Inteligência e sensível às condições reais da organização, o trabalho busca fomentar o debate sobre profissionalização deste relevante serviço público e reforçar a capacidade do Estado brasileiro de enfrentar os desafios informacionais, operacionais e estratégicos que se impõem na atualidade. A lógica por competências, quando adequadamente adaptada, pode fortalecer a coerência interna das organizações públicas, aumentar sua capacidade adaptativa e promover maior racionalidade na alocação e desenvolvimento de servidores (Santos, 2022).

Por fim, a metodologia adotada nesta pesquisa – que combinou entrevistas qualitativas, modelagem conceitual e fundamentação ontológica – pode ser replicada em outros contextos da Administração Pública brasileira, especialmente em carreiras que exigem alto grau de especialização e atuação em ambientes sensíveis.

6. PRODUTO TÉCNICO-TECNOLÓGICO

O Produto Técnico-Tecnológico (PTT) desenvolvido nesta pesquisa consiste em um *framework* de competências voltado ao cargo de Oficial de Inteligência da Agência Brasileira de Inteligência. Seu objetivo é fornecer um referencial estruturado para a gestão institucional, abrangendo processos como recrutamento, seleção, capacitação profissional e avaliação de desempenho. A construção do *framework* baseou-se na identificação dos desafios organizacionais enfrentados pela ABIN e na modelagem das competências essenciais para enfrentá-los, permitindo um alinhamento entre as exigências institucionais e as capacidades dos profissionais da área.

Para a elaboração do *framework*, utilizou-se o método *Design Science Research*, que possibilitou a construção iterativa do artefato conceitual, garantindo que sua estrutura fosse aprimorada a partir da análise contínua dos dados coletados. O DSR permitiu que o desenvolvimento do *framework* ocorresse em ciclos sucessivos de refinamento, que consistiram na integração progressiva das informações extraídas das entrevistas, na sistematização das competências com base na literatura e na modelagem conceitual das competências utilizando a UFO. Cada ciclo envolveu a revisão dos achados empíricos, sua categorização e ajuste conforme a relação estabelecida entre competências e desafios institucionais.

A pesquisa empregou a técnica de análise de conteúdo (Bardin, 2021) para a identificação dos desafios institucionais, utilizando entrevistas com Oficiais de Inteligência e a análise do documento "Desafios de Inteligência – Edição 2025" (ABIN, 2024) como fontes primárias de informação. Para organizar e classificar os achados empíricos, empregou-se a técnica de categorização indutiva, que possibilitou a identificação de padrões e a construção de categorias emergentes associadas aos desafios institucionais.

A modelagem das competências foi realizada a partir das entrevistas com profissionais da ABIN. Para garantir precisão conceitual e eliminar ambiguidades na definição das competências, a pesquisa incorporou a Ontologia Fundacional Unificada como referencial conceitual. A UFO não é uma técnica de coleta ou análise, mas uma estrutura teórica que permitiu a organização das competências em categorias bem definidas – eventos, ações, papéis e relações –, assegurando clareza terminológica e coesão na relação entre as competências e os desafios institucionais.

O *framework* resultante desse processo conta com 26 competências que contêm descrição, padrão de desempenho, conhecimentos, habilidades e atitudes. Todas foram modeladas de forma a vincular-se aos desafios institucionais identificados na pesquisa e às ações concretas esperadas

dos Oficiais de Inteligência, permitindo que gestores tenham um referencial preciso para nortear o desenvolvimento de capacidades dentro da organização.

A complexidade do PTT reside na integração de diferentes abordagens metodológicas, que incluem análise qualitativa, modelagem conceitual e ciclos iterativos de refinamento. Sua elaboração exigiu um processo estruturado para garantir que as competências definidas refletissem fielmente as necessidades institucionais e estivessem alinhadas a um referencial conceitual sólido. Essa complexidade e seu alinhamento à modernização da gestão pública demonstram a aderência do PTT à linha de pesquisa Gestão de Organizações Públicas do Mestrado Profissional em Administração Pública da Universidade de Brasília, evidenciando sua contribuição para o aprimoramento da gestão de pessoas no setor público.

O potencial inovador do *framework* está na forma como ele estrutura a relação entre competências e desafios organizacionais. Diferentemente de modelos tradicionais que apenas listam competências, o PTT propõe um mapeamento que garante uma definição precisa e operacional das capacidades necessárias para o desempenho das funções na ABIN. Essa inovação reduz ambiguidades, favorece a padronização conceitual e possibilita a replicação do modelo em outras organizações que enfrentam desafios similares na gestão por competências.

Além disso, o *framework*, ao permitir um alinhamento sistemático entre competências individuais e desafios institucionais, se torna um instrumento para subsidiar políticas de gestão de pessoas e de desenvolvimento organizacional. A estrutura adotada possibilita que sua aplicação vá além dos processos de recrutamento e capacitação, sendo também útil para orientar avaliações de desempenho e definir trilhas de desenvolvimento profissional na ABIN.

Em termos de aplicabilidade, o *framework* apresenta duas dimensões relevantes: sua aplicabilidade potencial e sua aplicabilidade realizada. No primeiro caso, a estrutura conceitual desenvolvida pode ser adaptada para outras organizações do setor público que demandam um referencial metodológico para gestão de competências. A metodologia empregada na pesquisa permite ajustes conforme as particularidades de cada instituição, tornando o modelo escalável e replicável. Já a aplicabilidade realizada se manifesta no fato de que o *framework* foi construído com base em dados empíricos coletados diretamente da ABIN, garantindo que sua estrutura esteja alinhada às necessidades institucionais identificadas ao longo da pesquisa.

A adoção desse *framework* pode contribuir para o desenvolvimento de ferramentas complementares de gestão, como indicadores de maturidade organizacional e sistemas de monitoramento contínuo do desenvolvimento de competências. Sua metodologia estruturada pode

servir como base para a implementação de instrumentos mais avançados de avaliação de capacidades institucionais, potencializando sua aplicabilidade em longo prazo.

O impacto potencial do PTT transcende a ABIN, podendo servir de referência para outras organizações que necessitam estruturar suas competências institucionais. A possibilidade de adaptação do *framework* para diferentes contextos organizacionais amplia seu alcance, consolidando-o como um instrumento metodológico útil para a Administração Pública. Além disso, a integração entre análise qualitativa e modelagem conceitual confere ao PTT uma base sólida para futuras pesquisas sobre gestão estratégica de pessoas em órgãos públicos.

O impacto realizado pode ser mensurado pelos benefícios observados na estruturação do *framework*. Ao estabelecer um modelo padronizado para a gestão por competências, o PTT contribui para aprimorar a definição de perfis profissionais, otimizar processos seletivos e subsidiar estratégias de desenvolvimento profissional na ABIN. Esses benefícios reforçam a capacidade da organização de planejar e gerenciar talentos, promovendo um alinhamento mais eficiente entre recursos humanos e objetivos institucionais.

Concluindo, o *framework* de competências configura-se como um artefato técnico de alta aplicabilidade, que não apenas atende às demandas da Agência Brasileira de Inteligência, mas também oferece um referencial metodológico passível de adaptação por outras organizações públicas interessadas em estruturar seus processos de gestão por competências. Seu caráter inovador e sua fundamentação teórica consolidada garantem que o PTT contribua para o aprimoramento da Administração Pública e para a profissionalização da Atividade de Inteligência no Brasil.

7. REFERÊNCIAS

Andrew, C. (2018). *Secret World: a History of Intelligence*. New Haven, Ct Yale University Press.

Baek, Y., Han, A., Bailashivili, S., & Chung, J. (2024). Analysis of Trends in Teacher Competency Models Changes. *Yeollin Gyoyug Yeon´gu*, *32(5)*, 31–54. https://doi.org/10.18230/tjye.2024.32.5.31

Bardin, L. (2021). *Análise de conteúdo* (L. A. Reto & A. Pinheiro, Trads.). Edições 70. (Trabalho original publicado em 1977).

Benayoune, A. (2024). Competency-Based Framework Development and Implementation: Current and Future Perspectives. *Information Management and Business Review*, *16*(3(I)), 606–615. https://doi.org/10.22610/imbr.v16i3(i).4013

Boyatzis, R. E. (1982). *The competent manager: A model for effective performance*. John Wiley & Sons.

Bradley, J. M., Unal, R., Pinto, C. A., & Cavin, E. S. (2015). Competencies for governance of complex systems of systems. *International Journal of System of Systems Engineering*, *6*, 71–89. https://doi.org/10.1504/IJSSE.2015.068804

Brasil. (1999). Lei n.º 9.883, de 7 de dezembro de 1999. *Cria o Sistema Brasileiro de Inteligência, institui a Agência Brasileira de Inteligência - ABIN e dá outras providências*. Diário Oficial da União de 8 de dezembro de 1999, seção 1. Disponível em [https://www.planalto.gov.br/ccivil_03/leis/l9883.htm]

Brasil. (2008). Lei n.º 11.776, de 17 de setembro de 2008. *Dispõe sobre a estruturação do Plano de Carreiras e Cargos da Agência Brasileira de Inteligência - ABIN, cria as Carreiras de Oficial de Inteligência, Oficial Técnico de Inteligência, Agente de Inteligência e Agente Técnico de Inteligência e dá outras providências.* Diário Oficial da União de 18 de setembro de 2008, seção 1. Disponível em [https://www. planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11776.htm]

Brasil. (2016). Portaria n.º 244 – ABIN/GSI/PR, de 23 de agosto de 2016. *Aprova os Fundamentos Doutrinários da Doutrina Nacional da Atividade de Inteligência.* Disponível em [https://www.gov.br/abin/pt-br/centrais-de-conteudo/coletanea/36.pdf]

Brasil. (2016). Decreto n.º 8.793, de 29 de junho de 2016. *Institui a Política Nacional de Inteligência e dá outras providências*. Diário Oficial da União de 30 de junho de 2016, seção 1. Disponível em [https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm]

Brasil. (2023). Decreto n.º 11.816, de 28 de novembro de 2023. *Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência e da Agência Brasileira de Inteligência – ABIN*. Diário Oficial da União de 7 de dezembro de 2023, seção 1. Disponível em [https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11816.htm]

Brasil. Agência Brasileira de Inteligência. (2024). *Desafios de Inteligência – Edição 2025*. ABIN. Disponível em [https://www.gov.br/abin/pt-br/centrais-de-conteudo/desafios-de-inteligencia]

Campion, M. A., Fink, A., Ruggeberg, B. J., Carr, L., Phillips, G. M., & Odman, R. B. (2011). Doing competencies well: best practices in competency modeling. *Personnel Psychology*, *64*(1), 225–262. https://doi.org/10.1111/J.1744-6570.2010.01207.X

Campion, M. C., Schepker, D. J., Campion, M. A., & Sanchez, J. I. (2020). Competency modeling: A theoretical and empirical examination of the strategy dissemination process. *Human Resource Management*, 59(3), 291-306. https://doi.org/10.1002/HRM.21994

Cao, C., & Zhang, Z. (2022). Machine Learning-Assisted Competency Modeling for Human Resource Management Jobs. Mobile Information Systems, 2022, 1 – 15.https://doi.org/10.1155/2022/8380307

Calhau, R. F., Kokkula, S., & Guizzardi, G. (2024). Modeling competences in enterprise architecture: from knowledge, skills and attitudes to organizational capabilities. *Software and Systems Modeling*. https://doi.org/10.1007/s10270-024-01151-7

CAPES (2019). *Relatório do GT de Produção Técnica CAPES*, 2019.

Cepik, M. (2003). *Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de Serviços de Inteligência*. Rio de Janeiro: Fundação Getúlio Vargas.

Coelho, F. de S., & Menon, I. de O. (2018). A quantas anda a gestão de recursos humanos no setor público brasileiro? Um ensaio a partir das (dis)funções do processo de recrutamento e seleção – os concursos públicos. *Revista do Serviço Público*, 69, 151 – 180. https://doi.org/10.21874/rsp.v69i0.3497

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approaches*. Sage Publications.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.

Daft, R. L. (2016). *Organization theory and design* (12th ed.). Cengage Learning.

Dashko, Y., Vitchenko, O., & Kadomtsev, M. (2020). *Soft models of competence assessment in professional education*. 210, 18011. https://doi.org/10.1051/E3SCONF/202021018011

Director of National Intelligence. (2008). *Performance Management System Requirements for the Intelligence Community Civilian Workforce* (Intelligence Community Directive 651). Office of the Director of National Intelligence.

Dulles, A. (1963). *The craft of intelligence*. Westview Encore Edition.

Ferraz, R. A., Melo-Silva, L. L., Coscioni, V., & Rodrigues, J. P. O. (2023). Definições de competências transversais e transferíveis em estudantes universitários: Revisão de escopo. Revista Brasileira de Orientação Profissional, 24(1), 29–41. https://doi.org/10.26707/1984-7270/2023v24n0104

França. (2023). *Répertoire des Métiers de la Fonction Publique*. Direction Générale de l'Administration et de la Fonction Publique. Disponível em [https://www.fonction-

publique.gouv.fr/toutes-les-actualites/publication-du-premier-repertoire-commun-des-metiers-de-la-fonction-publique]. Último acesso em 24 de fevereiro de 2025.

Guizzardi**,** G. (2005). *Ontological foundations for structural conceptual models*. Enschede: University of Twente.

Halitsan, O. (2024). *Transversal competences of a specialist as a determinant of his professional development in the conditions of the university space*. 294–323. https://doi.org/10.24195/cm2024uuch6

Holtkemper, M., & Beecks, C. (2024). Empowering Data Science Teams: How Automation Frameworks Address Competency Gaps Across Project Lifecycles. 3134–3142. https://doi.org/10.1109/bigdata62323.2024.10825556

Hu, J. R., Wang, Z. Z., Wei, X. X., Gong, E. Y., & Shao, R. T. (2024). *Research progress on global health competency and its models*. *58*(1), 92–97. https://doi.org/10.3760/cma.j.cn112150-20230912-00179

Jajoo, A., & Deshmukh, P. (2024). Exploring competency: Corporate framework, learning theories, and a cognitive development model. *Multidisciplinary Reviews*, 7(8), 2024170. https://doi.org/10.31893/multirev.2024170

Lee, H.-K., & Park, S. J. (2022). Analysis of Learning Competency Research Trends and Direction of University Learning Support Using Topic Modeling Analysis. *Korean Association For Learner-Centered Curriculum And Instruction*, *22*(22), 847–863. https://doi.org/10.22251/jlcci.2022.22.22.847

Levanaitė, K. (2025). Competence Modelling From the Perspective of Complex Systems Theories: A Systematic Literature Review. *Pedagogika*, *156*(4), 166–187. https://doi.org/10.15823/p.2024.156.8

Maathuis, C. (2023). *Human Centered Explainable AI Framework for Military Cyber Operations*. 260–267. https://doi.org/10.1109/milcom58377.2023.10356338

Malachowski, B., Różewski, P., & Zaikin, O. (2011). Competence Modelling Tool for Enterprise Knowledge Management. *Management and Production Engineering Review*, *2*, 22–28. http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171572628

Megahed, N. (2018). A Critical Review of the Literature and Practice of Competency Modelling. *KnE Social Sciences, 3(10), 104-126*. https://doi.org/10.18502/KSS.V3I10.3106

Miles, M. B., Huberman, A. M., & Saldaña, J. (2019). *Qualitative data analysis: A methods sourcebook* (4ª ed.). Sage Publications.

Moldabekova, M. S. (2023). On the development of transversal competencies of students of physical and technical specialties. *Habaršysy - Ál-Farabi Atyndaġy Ḳazaḳ Memlekettik Ùltyḳ Universitetì. Fizika Seriâsy*. https://doi.org/10.26577/rcph.2023.v87.i4.05

Office of the Director of National Intelligence. (2015). *Intelligence Community Directive 610: Competency Library for the Intelligence Community Workforce*. https://www.dni.gov/files/documents/ICD/ICD_610.pdf

Office of the Director of National Intelligence. (2015). *Intelligence Community Standard Number 610-2: Intelligence Community Competency Taxonomy* (FOIA Case #DF-2015-00041). Aprovado para liberação em 25 de novembro de 2015. Washington, DC: ODNI.

Office of the Director of National Intelligence. (2015). *Intelligence Community Standard Number 610-3: Core Competencies for Non-Supervisory Intelligence Community Employees at GS-15 and Below*. Aprovado para liberação pelo ODNI em 25 de novembro de 2015, FOIA Case #DF-2015-00041. Washington, DC: ODNI.

Office of the Director of National Intelligence. (2015). *Intelligence Community Standard Number 610-4: Core Competencies for Supervisory and Managerial Intelligence Community Employees at GS-15 and Below*. https://www.dni.gov/files/documents/FOIA/DF-2015-00041.pdf

Office of the Director of National Intelligence. (2015). *Core Competencies for Intelligence Community Senior Officers*.

Pérez Gómez, Á., Romero Jaimes, P., & Torres Rincón, M. M. (2014). *Diseño de un modelo de competencias gerenciales a partir de la construcción de un diccionario genérico*. https://expeditiorepositorio.utadeo.edu.co/handle/20.500.12010/3428

Rothwell, W. J., & Lindholm, J. E. (1999). Competency Identification, Modelling and Assessment in the USA. *International Journal of Training and Development*, *3*(2), 90–105. https://doi.org/10.1111/1468-2419.00069

Rothwell, W. J., Mozaffari, F., & Al Hajri, A. (2025). A bibliometric overview of competency and capability modeling: research contributions and trends (2000–2024). *Performance Improvement Quarterly*. https://doi.org/10.56811/piq-24-0022

Santos, B. (org.). Caminhos da inovação no setor público. Brasília: Enap, 2022. 392 p. Disponível em: https://repositorio.enap.gov.br/bitstream/1/7420/1/caminhos_da_inovacao_no_setor_publico.pdf.

Sithole, T., du Toit, J., & Von Solms, S. H. (2023). *A Cyber Counterintelligence Competence Framework: Developing the Job Roles*. *22*(1), 450–457. https://doi.org/10.34190/eccws.22.1.1093

Sliter, K. A. (2015). Assessing 21st Century Skills: Competency Modeling to the Rescue.*Industrial and Organizational Psychology*, *8*(2), 284–289. https://doi.org/10.1017/IOP.2015.35

Tarafdar, M., & Bunker, D. (2019). Theorizing process dynamics with directed graphs: A study of sociotechnical change. *Journal of the Association for Information Systems*, 20(8), 1097-1136.

8. APÊNDICE

8.1. *Framework* de competências para o órgão de Inteligência do Estado brasileiro

FRAMEWORK DE COMPETÊNCIAS PARA O ÓRGÃO DE INTELIGÊNCIA DO ESTADO BRASILEIRO

1. INTRODUÇÃO

O *Framework de Competências* foi desenvolvido para sistematizar e descrever as competências essenciais ao cargo de Oficial de Inteligência da Agência Brasileira de Inteligência. Sua elaboração é resultado de trabalho de pesquisa conduzido no âmbito do Mestrado Profissional em Administração Pública da Universidade de Brasília (UnB), constituindo-se como Produto Técnico-Tecnológico da dissertação. O *Framework de Competências* propõe um referencial estruturado que visa subsidiar processos institucionais da ABIN, como recrutamento, seleção, capacitação profissional e avaliação de desempenho, garantindo que a atuação dos profissionais esteja alinhada às demandas organizacionais e aos desafios estratégicos enfrentados pela Agência.

A construção do *Framework de Competências* seguiu um processo estruturado composto por quatro etapas metodológicas, conforme ilustra a figura abaixo:

Figura 1 – Etapas de construção do *Framework de Competências*.

O primeiro estágio consistiu no delineamento dos desafios a serem enfrentados pelo órgão de Inteligência do Estado brasileiro. Esses foram extraídos das seguintes fontes: (*i*) entrevistas semiestruturadas com Oficiais de Inteligência da ABIN; e (*ii*) análise de conteúdo do documento "Desafios de Inteligência – Edição 2025", publicado em dezembro de 2024[3], a partir da qual emergiram seis desafios institucionais.

Posteriormente, foi realizada a modelagem das competências, empregando técnicas de categorização indutiva e análise de conteúdo para sistematizar as informações e definir as

[3] O documento *"Desafios de Inteligência – Edição 2025"* encontra-se disponível no sítio eletrônico da ABIN. *Link* para acesso: https://www.gov.br/abin/pt-br/centrais-de-conteudo/desafios-de-inteligencia

competências de forma clara e objetiva. A última etapa envolveu a organização e estruturação das 26 competências, cada uma delas vinculada a um dos desafios institucionais identificados.

O desenvolvimento das competências foi conduzidoa partir da análise de dados empíricos, coletados por meio de entrevistas com profissionais da ABIN. Além disso, a estruturação do *Framework de Competências* foi apoiada em técnicas como a análise de conteúdo e a categorização indutiva, permitindo a sistematização das informações e a definição clara das competências. Esse processo metodológico possibilitou não apenas a identificação dos desafios e a modelagem das competências, mas também a vinculação direta entre cada uma delas e os desafios institucionais.

O *framework* é composto por 26 competências, organizadas de forma a contemplar título, descrição, padrão de desempenho, conhecimentos, habilidades e atitudes associadas. Cada competência foi vinculada diretamente a um dos seis desafios institucionais identificados, garantindo que sua aplicação seja direcionada e compatível com as demandas específicas da Atividade de Inteligência no Brasil. Esse vínculo entre competências e desafios assegura que os Oficiais de Inteligência possam desenvolver capacidades alinhadas às necessidades estratégicas da organização.

A relevância do *Framework de Competências* está na sua capacidade de estruturar um referencial conceitual aplicável ao contexto da Inteligência de Estado, possibilitando sua utilização para múltiplos fins dentro da ABIN. Além de apoiar a formulação de políticas de gestão de pessoas, ele também pode ser empregado como base para a definição de trilhas de desenvolvimento profissional, avaliação de desempenho e estruturação de programas de formação continuada.

Outro aspecto relevante da estruturação do *Framework de Competências* é sua capacidade de subsidiar o desenvolvimento de ferramentas complementares para a gestão institucional. Entre as possibilidades de aplicação, destacam-se a construção de indicadores de maturidade organizacional e a implementação de sistemas de monitoramento do desenvolvimento de competências, permitindo o acompanhamento contínuo do aprimoramento profissional dos Oficiais de Inteligência.

A seguir, são apresentados os desafios organizacionais e as 26 competências modeladas que compõem o *Framework de Competências*.

Boa leitura!

2. DESAFIOS

DESENVOLVER E IMPLEMENTAR estratégias de fortalecimento da cultura de resiliência, por meio de ações contínuas de sensibilização, capacitação e integração entre órgãos públicos, setor privado e sociedade civil, visando à proteção de conhecimentos sensíveis e à manutenção da continuidade operacional dos setores estratégicos brasileiros.	
	JUSTIFICATIVAS
	**Atuação proativa e estratégica:** O Oficial de Inteligência deve antecipar riscos e agir de modo a garantir que a organização esteja preparada para ameaças emergentes, em vez de apenas reagir a crises.
	Cooperação interinstitucional: A proteção e o uso de informações sensíveis, aliados à colaboração com diversos atores institucionais, são fundamentais para a eficácia das estratégias de fortalecimento da cultura de resiliência.
	Aprendizado contínuo e adaptação: O desenvolvimento das competências ocorre na prática cotidiana, exigindo adaptação constante a cenários dinâmicos e consolidando a resiliência estratégica como um pilar da atuação profissional.

DESENVOLVER E IMPLEMENTAR estratégias para o monitoramento, análise e neutralização de organizações criminosas transnacionais, com foco na prevenção e no combate a mercados ilícitos, tráfico de pessoas e crimes ambientais, por meio da coordenação interinstitucional e do fortalecimento das capacidades operacionais nas áreas fronteiriças brasileiras.	
	JUSTIFICATIVAS
	**Expansão dos mercados ilícitos transnacionais:** A atuação crescente de organizações criminosas em mercados ilícitos, especialmente no tráfico de drogas, armas e pessoas, exige uma capacidade contínua de identificação e neutralização dessas atividades.
	Pressão externa e tensões geopolíticas: A atuação internacional de redes criminosas e a infiltração em estruturas estatais demandam ações coordenadas e proativas da Inteligência brasileira.
	Vulnerabilidades ambientais: A exploração ilegal de recursos naturais, notadamente na região amazônica, compromete a segurança nacional, os interesses ambientais globais e os direitos dos povos originários.
	Desafios nas fronteiras e integração internacional: A complexidade das fronteiras terrestres e marítimas do Brasil, aliada à presença crescente de atores criminosos internacionais, torna fundamental o fortalecimento da cooperação interinstitucional e internacional.

FORTALECER AS CAPACIDADES de Contrainteligência para detectar, neutralizar e prevenir ações de espionagem e interferência externa, com foco na proteção de dados sensíveis, na integridade dos processos decisórios nacionais e na salvaguarda de recursos estratégicos, considerando o uso crescente de tecnologias avançadas e a instrumentalização de cidadãos e organizações privadas.	
	JUSTIFICATIVAS
DESAFIO 3	**Ameaças constantes de espionagem e interferência externa:** O Brasil tem sido historicamente alvo de Serviços de Inteligência estrangeiros interessados em dados sensíveis sobre recursos naturais, tecnologias estratégicas e processos decisórios.
	Instrumentalização de cidadãos e organizações privadas: O recrutamento de cidadãos brasileiros com acesso a informações sigilosas é uma prática crescente, exigindo protocolos rigorosos de conscientização, monitoramento e proteção.
	Adoção de novas tecnologias ofensivas por agentes adversos: O uso de robôs para raspagem de dados, engenharia social e operações de bandeira falsa demanda uma atualização constante das capacidades de defesa cibernética e da percepção situacional do Oficial de Inteligência.
	Complexidade do cenário geopolítico e tecnológico: O aumento da competição estratégica global gera uma multiplicidade de agentes e técnicas que dificultam a detecção e atribuição das ações adversas, exigindo análises criteriosas e coordenadas.
	Riscos ao processo decisório nacional: O sucesso de operações de influência externa pode comprometer a tomada de decisões estratégicas e a confiança na gestão pública nacional, o que reforça a necessidade de uma atuação preventiva e contínua.

DESENVOLVER E IMPLEMENTAR estratégias para identificar, monitorar e neutralizar campanhas de desinformação e ações de influência externa que ameacem a confiança nas instituições democráticas, com foco no uso de tecnologias emergentes, análise sociopolítica e cooperação interinstitucional.	
	JUSTIFICATIVAS
DESAFIO 4	**Proteção da Democracia e da soberania nacional:** Campanhas de desinformação e interferências externas podem minar a confiança pública nas instituições democráticas, comprometendo a estabilidade política e a soberania do país.
	Adaptação às transições globais e tecnológicas: O avanço tecnológico e as mudanças no cenário global facilitam a disseminação rápida e ampla de informações falsas. Acompanhar essas transições é crucial para que os Serviços de Inteligência possam antecipar e neutralizar ameaças emergentes que exploram novas tecnologias para influenciar a opinião pública.
	Fortalecimento da Segurança Cibernética: A proliferação de ataques cibernéticos e o uso da internet para espalhar desinformação exigem uma postura proativa na defesa do espaço informacional brasileiro. A segurança cibernética é apontada como um dos principais desafios, reforçando a necessidade de se desenvolver estratégias para proteger o ambiente digital nacional.
	Promoção da cooperação interinstitucional: O combate eficaz à desinformação requer a colaboração entre diversas instituições governamentais e não governamentais. A cooperação interinstitucional revela-se essencial para enfrentar ameaças complexas que transcendem as capacidades de uma única entidade, promovendo uma resposta coordenada e abrangente.

FORTALECER a resiliência cibernética nacional por meio da implementação de estratégias integradas para identificar, mitigar e responder a ameaças cibernéticas, com foco na proteção de Infraestruturas Críticas, no uso seguro de tecnologias emergentes e na cooperação interinstitucional para combate a ataques patrocinados por atores estatais e não estatais.	
	JUSTIFICATIVAS
	**Proteção das Infraestruturas Críticas:** Setores essenciais como energia, telecomunicações e finanças dependem de sistemas digitais. A vulnerabilidade desses sistemas pode comprometer serviços básicos e a segurança nacional, tornando imperativo o desenvolvimento de estratégias robustas de cibersegurança.
	Ameaças de atacantes estatais e não estatais: O aumento do número de ataques cibernéticos patrocinados por diferentes atores exige uma resposta coordenada e eficaz para proteger os interesses nacionais e a integridade das informações sensíveis.
	Uso seguro de tecnologias emergentes: A rápida adoção de novas tecnologias, como Internet das Coisas (IoT) e Inteligência Artificial, amplia a superfície de ataque. Implementar medidas de segurança adequadas é essencial para mitigar riscos associados a essas inovações.
	Cooperação interinstitucional: A complexidade das ameaças cibernéticas requer colaboração entre órgãos governamentais, setor privado e instituições internacionais. A integração de esforços fortalece a capacidade de resposta e a resiliência frente a incidentes cibernéticos.

ESTABELECER de forma clara as atribuições dos Oficiais de Inteligência em atos normativos e legais para garantir segurança jurídica na atuação profissional e alinhamento estratégico com a organização.	
	JUSTIFICATIVAS
	**Risco de responsabilização individual indevida:** Sem atribuições formalizadas de suas atribuições, os Oficiais de Inteligência podem ser cobrados por ações que não estão claramente delimitadas.
	Dificuldade na tomada de decisão e no cumprimento de normas internas: A anomia compromete a eficiência operacional e gera incertezas sobre as responsabilidades funcionais.
	Redução da proteção institucional do Oficial de Inteligência: A ausência de regras claras aumenta o risco de que sua atuação seja questionada por órgãos de controle ou instâncias judiciais devido à falta de respaldo normativo.
	Desalinhamento entre funções e metas estratégicas da organização: Gera sobrecarga de alguns setores e ineficiência na distribuição das tarefas.

3. COMPETÊNCIAS

MOSAICO DE DESAFIOS
& COMPETÊNCIAS
6 DESAFIOS, 26 COMPETÊNCIAS

COMPETÊNCIA 1 **TÍTULO:** Promoção da cultura de resiliência estratégica e proteção do conhecimento sensível.			
DESCRIÇÃO: Planejar e implementar ações de sensibilização para cultura de resiliência estratégica e proteção do conhecimento sensível.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Mapear públicos-alvo em instituições parceiras e internas para ações de sensibilização sobre resiliência estratégica.	Conceitos fundamentais de resiliência estratégica e segurança de informações sensíveis	Desenvolver campanhas de sensibilização sobre resiliência estratégica.	Compromisso com a difusão da cultura de resiliência estratégica.
Planejar atividades de conscientização, como palestras, seminários e *workshops*, abordando a importância da proteção de conhecimentos sensíveis.	Princípios de gestão de riscos e análise de ameaças em setores estratégicos.	Planejar e conduzir treinamentos e eventos educativos.	Proatividade na criação e execução de ações de sensibilização.
Produzir materiais educativos para disseminar conceitos de segurança, proteção de informações e resiliência estratégica.	Métodos e técnicas de comunicação institucional e sensibilização de públicos.	Aplicar métodos de avaliação de impacto de iniciativas de conscientização.	Empatia e habilidade de comunicação com diversos públicos.
Avaliar o impacto das ações de sensibilização por meio de questionários, entrevistas e análise de indicadores.	Ferramentas para medição de impacto de ações educativas.	Comunicar informações técnicas de forma clara para diferentes públicos.	Perseverança na manutenção de uma agenda contínua de ações educativas.
Estabelecer parcerias interinstitucionais para ampliar o alcance das iniciativas de conscientização.	Estrutura e diretrizes do Programa Nacional de Proteção do Conhecimento Sensível (PNPC).	---	---

COMPETÊNCIA 2

TÍTULO: Análise de Riscos e de vulnerabilidades em setores estratégicos.

DESCRIÇÃO: Analisar riscos e vulnerabilidades em setores estratégicos.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Identificar ameaças e vulnerabilidades relacionadas a conhecimentos sensíveis em setores estratégicos.	Princípios de análise de risco, gestão de crises e resiliência organizacional.	Identificar e avaliar riscos em setores estratégicos.	Rigor metodológico na análise de riscos e vulnerabilidades.
Analisar riscos potenciais com base em dados históricos, indicadores de ameaças e cenários prospectivos.	Métodos de avaliação de vulnerabilidades em setores estratégicos (ex.: FMEA, *Bow-Tie Analysis*).	Correlacionar dados técnicos e contextuais para análise de ameaças.	Proatividade na busca de informações sobre ameaças emergentes.
Aplicar metodologias de análise de risco para avaliar impactos de ameaças e propor medidas mitigadoras.	Técnicas de simulação e modelagem de cenários prospectivos.	Elaborar relatórios com recomendações de medidas mitigadoras.	Compromisso com a antecipação e mitigação de riscos estratégicos.
Produzir relatórios técnicos com diagnósticos e recomendações para gestores institucionais.	Fundamentos de geopolítica aplicados à segurança de setores críticos.	Participar de simulações de crises e exercícios interinstitucionais.	Curiosidade analítica para compreender dinâmicas complexas de ameaça.
Participar de simulações e exercícios de resposta a incidentes para avaliar a resiliência institucional.	Regulamentações e normas aplicáveis à segurança de Infraestruturas Críticas.	---	---

COMPETÊNCIA 3

TÍTULO: Coordenação interinstitucional para a proteção de conhecimentos sensíveis.

DESCRIÇÃO: Coordenar a integração interinstitucional para proteção de conhecimentos sensíveis.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Estabelecer e manter canais de comunicação com instituições públicas e privadas de interesse estratégico.	Estrutura e funcionamento de setores estratégicos nacionais.	Estabelecer parcerias com instituições internas e externas.	Proatividade na busca de parcerias e oportunidades de cooperação.
Participar de fóruns e grupos de trabalho interinstitucionais para troca de informações sobre riscos e boas práticas de segurança.	Modelos de cooperação interinstitucional e de gestão de parcerias.	Participar de negociações para formalização de acordos de cooperação.	Compromisso com a segurança e proteção de conhecimentos sensíveis.

Coordenar ações conjuntas para a elaboração e revisão de protocolos de proteção de conhecimentos sensíveis.	Protocolos de segurança e proteção de informações sensíveis.	Gerenciar reuniões interinstitucionais com foco em segurança estratégica.	Habilidade de mediação e negociação interinstitucional.
Facilitar o compartilhamento seguro de informações entre os diversos atores envolvidos na proteção de ativos estratégicos.	Técnicas de gestão colaborativa de riscos e incidentes.	Propor e revisar protocolos de segurança conjuntos.	Foco na construção de soluções colaborativas e integradas
Propor acordos de cooperação entre a ABIN e instituições parceiras para fortalecimento da resiliência estratégica.	Estruturas regulatórias nacionais e internacionais sobre proteção de ativos críticos.	---	---

COMPETÊNCIA 4 **TÍTULO:** Monitoramento e análise da criminalidade organizada transnacional.			
DESCRIÇÃO: Monitorar e analisar atividades criminosas transnacionais, notadamenteemáreas fronteiriças.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Coletar dados de fontes abertas (OSINT) e fontes humanas (HUMINT) sobre organizações criminosas transnacionais.	Princípios de análise criminal.	Coletar, interpretar e correlacionar dados sobre organizações criminosas transnacionais.	Rigor analítico na avaliação de dados.
Analisar padrões de atuação criminosa em áreas fronteiriças, correlacionando informações de diferentes bases de dados.	Técnicas de *Open Source Intelligence* (OSINT) e *Human Intelligence* (HUMINT) aplicadas ao monitoramento de redes criminosas.	Operar ferramentas de geointeligência para mapeamento e análise de atividades ilícitas.	Discrição e sigilo ao lidar com informações sensíveis.
Identificar pontos críticos de movimentação de drogas, armas e pessoas nas fronteiras e áreas sensíveis.	Geopolítica regional, com foco nas relações do Brasil com os países vizinhos da América do Sul.	Produzir relatórios com recomendações para ações preventivas e repressivas à criminalidade organizada transnacional.	Proatividade na identificação de novas tendências e *modus operandi* de organizações criminosas.
Produzir relatórios analíticos com mapas de atuação e tendências de atividades criminosas.	Idiomas: Espanhol (preferencialmente avançado) e Inglês para análise de documentos internacionais.	Comunicar-se de forma eficaz com órgãos de segurança pública e Serviços de Inteligência estrangeiros.	Compromisso com a proteção da segurança nacional.
Sinalizar vulnerabilidades que possam ser exploradas por organizações criminosas.	Fundamentos de geointeligência e análise de fluxos migratórios	---	---

COMPETÊNCIA 5 **TÍTULO:** Coordenação e cooperação interinstitucional no combate ao crime organizado transnacional.			
DESCRIÇÃO: Coordenar ações interinstitucionais para o combate ao crime organizado transnacional.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Planejar e conduzir reuniões interinstitucionais com órgãos nacionais e internacionais de Segurança Pública e de Inteligência.	Estruturas e mecanismos de cooperação internacional em Segurança Pública e Inteligência.	Estabelecer e manter canais de comunicação com instituições nacionais e Serviços de Inteligência estrangeiros.	Proatividade na construção de parcerias estratégicas.
Elaborar protocolos de compartilhamento de informações para otimizar a cooperação interagências.	Protocolos de compartilhamento de dados entre instituições nacionais e entre Serviços de Inteligência estrangeiros.	Conduzir reuniões e negociações para alinhar estratégias e ações conjuntas.	Compromisso com a troca responsável de informações sensíveis.
Participar de fóruns e eventos internacionais para fortalecer parcerias e identificar boas práticas.	Legislação brasileira e internacional relacionada ao combate ao crime organizado.	Redigir acordos de cooperação interinstitucional.	Empatia e habilidade diplomática na interação com parceiros externos.
Implementar mecanismos de comunicação segura entre as instituições envolvidas em cooperação interagências.	Proficiência nos idiomas Inglês e Espanhol, dada a frequência de interações com parceiros da América Latina e de órgãos internacionais.	Participar de operações conjuntas.	Rigor no cumprimento de normas e protocolos estabelecidos.
Produzir relatórios de acompanhamento sobre os resultados das ações conjuntas realizadas.	Princípios de diplomacia e relações internacionais aplicados à cooperação em segurança.	---	---

COMPETÊNCIA 6 **TÍTULO:** Análise financeira e investigação de fluxos ilícitos vinculados a Organizações Criminosas Transnacionais.			
DESCRIÇÃO: Identificar e analisar cadeias financeiras de Organizações Criminosas Transnacionais.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Mapear fluxos financeiros suspeitos associados a atividades ilícitas transnacionais.	Princípios de análise financeira e de combate à lavagem de dinheiro.	Utilizar ferramentas de análise financeira e de cruzamento de dados.	Perseverança diante de investigações complexas e extensas.
Analisar transações bancárias e movimentações de ativos que possam indicar práticas de lavagem de dinheiro.	Técnicas de análise financeira de redes criminosas.	Comunicar-se com instituições financeiras e órgãos de controle para troca de informações.	Comprometimento com a legalidade e ética nas análises realizadas.
Coletar e processar dados sobre empresas de fachada e redes de financiamento criminoso.	Legislação nacional e internacional sobre crimes financeiros (Lei n.º 9.613/1998 e suas alterações).	Elaborar relatórios técnicos com clareza e precisão.	Curiosidade investigativa para identificar novas estratégias de ocultação de recursos ilícitos.

Coordenar ações com órgãos de controle financeiro nacional e internacional.	Proficiência no idioma Inglês para leitura de relatórios financeiros internacionais.	---	Discrição no tratamento de dados sensíveis.
---	Funcionamento de mecanismos de financiamento de atividades ilícitas transnacionais.	---	---

COMPETÊNCIA 7

TÍTULO: Análise de dados e execução de operações de Inteligência para o combate a crimes ambientais.

DESCRIÇÃO: Planejar e conduzir operações de Inteligência em áreas de risco ambiental.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Mapear regiões de atuação de organizações criminosas ambientais na Amazônia e outras áreas sensíveis.	Técnicas de geointeligência e sensoriamento remoto.	Operar *softwares* de análise geoespacial e de sensoriamento remoto.	Disposição para atuar em áreas de difícil acesso.
Planejar operações conjuntas com órgãos ambientais e de Segurança Pública.	Práticas de análise de crimes ambientais e suas implicações socioeconômicas.	Coletar e interpretar dados ambientais.	Atenção e zelo com os dados sensíveis coletados.
Utilizar tecnologias de sensoriamento remoto e de geointeligência para identificação de crimes ambientais.	Legislação ambiental brasileira (Lei n.º 9.605/1998 e regulamentações específicas).	Planejar, coordenar e participar de operações de campo em conjunto com outras instituições.	Rigor na análise e produção de Relatórios de Inteligência.
Participar de operações de campo em apoio a desintrusões e apreensões de recursos ilícitos.	Proficiência no idioma Inglês para análise de relatórios internacionais e uso de ferramentas estrangeiras de geointeligência.	---	---
Produzir relatórios sobre as dinâmicas criminosas observadas e suas implicações socioambientais.	Estruturas de organização e atuação de redes criminosas ambientais.	---	---

COMPETÊNCIA 8

TÍTULO: Análise prospectiva e modelagem de tendências do fenômeno da criminalidade transnacional.

DESCRIÇÃO: Produzir análises prospectivas sobre tendências criminais transnacionais.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Coletar e organizar dados sobre o histórico de atuação	Métodos de análise preditiva e de modelagem de cenários.	Coletar, processar e analisar dados sobre organizações criminosas.	Curiosidade e interesse pela análise de tendências.

de organizações criminosas transnacionais.			
Aplicar técnicas de análise prospectiva para antecipar tendências de atuação de organizações criminosas transnacionais.	Geopolítica internacional, com foco na América do Sul.	Aplicar métodos quantitativos de análise preditiva.	Disciplina na elaboração e validação dos cenários prospectivos.
Desenvolver cenários futuros com base na análise de dados disponíveis.	Proficiência nos idiomas Espanhol e Inglês para acesso a fontes abertas internacionais.	Desenvolver e apresentar cenários futuros para diferentes públicos.	Iniciativa para propor soluções com base nos cenários projetados.
Elaborar Relatórios de Inteligência que tragam projeções e possíveis implicações de novas dinâmicas criminosas.	Ferramentas de análise quantitativa e qualitativa de tendências (ex: Nvivo)	Utilizar *softwares* estatísticos e de análise de vínculos.	---

COMPETÊNCIA 9 **TÍTULO:** Identificação e monitoramento de ameaças de espionagem e Interferência Externa.			
DESCRIÇÃO: Identificar e monitorar atividades de espionagem e Interferência Externa.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Coletar e analisar dados sobre possíveis ações de espionagem.	Princípios e técnicas de Contrainteligência.	Monitorar atividades suspeitas em ambientes físicos e digitais.	Proatividade na identificação de ameaças emergentes.
Empregar ferramentas de *Open Source Intelligence* (OSINT) para monitorar atividades suspeitas.	Técnicas de *Open Source Intelligence* (OSINT), *Human Intelligence* (HUMINT) e *Signals Intelligence* (SIGINT).	Analisar comportamentos de possíveis agentes de influência.	Discrição e sigilo na condução das atividades.
Aplicar técnicas de análise comportamental para identificar padrões de atuação.	Fundamentos de análise comportamental e de Engenharia Social.	Utilizar ferramentas de análise e de monitoramento de redes.	Comprometimento com a proteção dos interesses nacionais.
Produzir relatórios com avaliação de riscos e recomendações de mitigação.	Proficiência nos idiomas Inglês e Espanhol para análise de fontes abertas internacionais.	---	---

COMPETÊNCIA 10 **TÍTULO:** Gestão de Riscos e proteção de Infraestruturas Críticas.			
DESCRIÇÃO: Aplicar técnicas de Análise de Risco e Vulnerabilidade em Infraestruturas Críticas.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Mapear vulnerabilidades em Infraestruturas Críticas.	Conceitos de análise de risco e de gestão de segurança informacional.	Aplicar metodologias de análise de risco e de simulação de incidentes.	Atenção a detalhes.

Desenvolver relatórios de análise de risco com recomendações práticas.	Protocolos internacionais de segurança de Infraestruturas Críticas.	Utilizar ferramentas de avaliação de vulnerabilidades.	Responsabilidade no manuseio de informações sensíveis.
Simular possíveis vetores de ataque para testar a resiliência das Infraestruturas Críticas.	Legislação nacional acerca de Infraestruturas Críticas (ex: Decretos n.º 9.573/2018; n.º 10.569/2020 e n.º 11.200/2022).	Comunicar achados técnicos de forma clara e precisa.	Iniciativa na proposição de melhorias nos processos de segurança.
---	Estruturas críticas nacionais e seus potenciais pontos de vulnerabilidade.	---	---

COMPETÊNCIA 11 **TÍTULO:** Prevenção e mitigação de ameaças de Engenharia Social por meio de protocolos de proteção.			
DESCRIÇÃO: Desenvolver e implementar protocolos de proteção contra ações de Engenharia Social.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Criar e implementar campanhas de conscientização sobre riscos de Engenharia Social.	Técnicas e métodos de Engenharia Social.	Elaborar e ministrar treinamentos de conscientização de segurança contra ações de Engenharia Social.	Empatia ao lidar com diferentes perfis de colaboradores.
Realizar treinamentos periódicos para colaboradores de setores sensíveis.	Princípios de persuasão e de manipulação comportamental.	Aplicar testes simulados de Engenharia Social.	Dedicação ao ensino e à disseminação de boas práticas.
Estabelecer protocolos claros de comunicação segura.	Protocolos de segurança da informação e comunicação.	Desenvolver materiais didáticos sobre práticas seguras de comunicação.	Paciência e resiliência para mitigar comportamentos inseguros.
---	Técnicas de persuasão e manipulação psicológica.	---	---
---	Métodos de ataque e defesa contra Engenharia Social (*phishing*, *pretexting*, etc)	---	---

COMPETÊNCIA 12 **TÍTULO:** Inteligência Cibernética na análise e mitigação de ameaças digitais e raspagem de dados sensíveis.			
DESCRIÇÃO: Analisar e mitigar ameaças digitais e raspagem de dados sensíveis.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**

Monitorar e analisar atividades suspeitas nos sistemas internos.	Segurança cibernética e protocolos de proteção de dados.	Operar ferramentas de detecção e de análise de intrusos.	Curiosidade investigativa.
Implementar ferramentas de segurança cibernética e detecção de intrusos.	Técnicas de raspagem de dados e como mitigá-las.	Desenvolver relatórios sobre atividades suspeitas.	Comprometimento com a segurança cibernética.
Desenvolver mecanismos para bloquear tentativas de coleta automatizada de dados.	Fundamentos de análise de *malware* e de Inteligência Cibernética.	Propor e implementar políticas de proteção contra raspagem de dados.	Paciência e persistência em análises cibernéticas.

COMPETÊNCIA 13

TÍTULO: Planejamento e execução de operações de Contrainteligência em ambientes sensíveis.

DESCRIÇÃO: Planejar e conduzir operações de Contrainteligência em ambientes sensíveis.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Planejar e coordenar operações para neutralização de agentes adversos.	Técnicas avançadas de despistamento e vigilância contraespionagem.	Executar operações de despistamento em campo.	Discrição.
Conduzir operações de despistamento e identificação de vulnerabilidades.	Técnicas de contraespionagem (e.g., *honeypots*, *Double agents*, *Whitelisting* e *Blacklisting*)	Monitorar atividades suspeitas em tempo real.	Capacidade de tomar decisões sob pressão.
Elaborar relatórios pós-operação com análise de resultados e aprendizados.	Protocolos de controle de danos em vazamentos (e.g., contenção midiática).	Produzir relatórios detalhados de avaliação operacional.	Iniciativa e controle emocional em situações críticas.
---	Técnicas de Inteligência humana (HUMINT) e sua aplicação na identificação de riscos de espionagem.	---	---

COMPETÊNCIA 14

TÍTULO: Análise de dinâmicas sociopolíticas e de estratégias de desinformação.

DESCRIÇÃO: Analisar dinâmicas sociopolíticas e discursos de desinformação.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Coletar e analisar discursos e narrativas que promovam desinformação e discursos antidemocráticos.	Fundamentos de Ciência Política e Teoria do Estado Democrático de Direito.	Analisar o impacto de discursos e narrativas de desinformação nas dinâmicas sociais e institucionais.	Compromisso com a imparcialidade e análise isenta.
Aplicar técnicas de Análise de Conteúdo e de Análise Crítica do Discurso para compreender o impacto social e político das campanhas de desinformação.	Conceitos de desinformação, *fakenews* e manipulação informacional.	Aplicar técnicas de Análise de Conteúdo, utilizando *softwares* de análise qualitativa.	Curiosidade investigativa para compreender fenômenos complexos.

Elaborar Relatórios de Inteligência detalhando e analisando as estratégias utilizadas por grupos que promovem a desinformação.	Princípios de Análise Crítica do Discurso e análise sociopolítica.	Produzir relatórios com análise isenta e desprovida de vieses ideológicos.	Discrição e responsabilidade no tratamento de dados sensíveis.
---	Proficiência nos idiomas Inglês e Espanhol para leitura de conteúdos e documentos internacionais.	---	---

COMPETÊNCIA 15 **TÍTULO:** Análise de plataformas digitais, de algoritmos e de comportamentos em ambiente virtual.			
DESCRIÇÃO: Monitorar e analisar plataformas digitais e dinâmicas algorítmicas.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Monitorar atividades e tendências em redes sociais e aplicativos de mensagens.	Algoritmos de recomendação e funcionamento de mídias sociais.	Aplicar metodologias de análise de redes sociais.	Iniciativa para acompanhar as inovações tecnológicas.
Identificar padrões de comportamento e mecanismos de disseminação de desinformação.	Técnicas de *Open Source Intelligence* (OSINT) e *Social Media Intelligence* (SOCMINT).	Utilizar ferramentas específicas de monitoramento e análise de conteúdos digitais.	Disciplina e paciência na análise contínua de grandes volumes de dados.
Avaliar o impacto de campanhas de desinformação em diferentes segmentos populacionais.	Fundamentos de análise de redes sociais e comportamentos no ambiente virtual.	Correlacionar dados de diferentes fontes para compreender estratégias de desinformação.	Compromisso com a produção de análises imparciais e com valor estratégico.

COMPETÊNCIA 16 **TÍTULO:** Modelagem prospectiva de narrativas associadas a ações antidemocráticas.			
DESCRIÇÃO: Produzir análises prospectivas sobre narrativas associadas a ações antidemocráticas.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Coletar e processar dados históricos sobre campanhas de desinformação e suas repercussões.	Métodos de análise preditiva e de modelagem de cenários.	Aplicar modelos estatísticos para análise de tendências.	Paciência e rigor analítico.
Aplicar técnicas de análise preditiva para identificar padrões e possíveis tendências.	Fundamentos de psicologia social aplicada à análise de comportamentos coletivos.	Integrar informações de múltiplas fontes para criar cenários futuros.	Curiosidade intelectual para compreender fenômenos complexos.
Produzir Relatórios de Inteligência com cenários prospectivos	Teoria de jogos e análise de dinâmicas sociopolíticas.	Elaborar Relatórios de Inteligência com projeções e orientações estratégicas.	Disciplina na aplicação de métodos preditivos.

erecomendações para mitigação de riscos.			

COMPETÊNCIA 17 **TÍTULO:** Cooperação interinstitucional no combate à desinformação.			
DESCRIÇÃO: Estabelecer cooperação interinstitucional para o combate à desinformação.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Planejar e organizar reuniões com órgãos públicos e privados nacionais e internacionais.	Estruturas e práticas de cooperação internacional em Inteligência.	Conduzir reuniões e interagir com representantes de órgãos parceiros.	Proatividade na construção e manutenção de parcerias.
Estabelecer canais seguros para troca de informações sobre campanhas de desinformação.	Protocolos de segurança e compartilhamento de dados.	Estabelecer e manter redes de contato institucionais.	Empatia e diplomacia na interlocução com diferentes atores.
Participar de fóruns e grupos de trabalho relacionados ao tema.	Legislação nacional e internacional relacionada à desinformação.	Produzir relatórios e propostas de cooperação.	Manutenção do sigilo no compartilhamento de informações sensíveis.
---	Proficiência nos idiomas Inglês e Espanhol para articulação internacional.	Assinalar parceiros institucionais para cooperação.	---

COMPETÊNCIA 18 **TÍTULO:** Inteligência Cibernética e análise de ameaças de origem estatal e não estatal.			
DESCRIÇÃO: Monitorar e analisar ameaças cibernéticas de origem estatal e não estatal.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Coletar, processar e analisar indicadores de comprometimento (IoCs) e táticas, técnicas e procedimentos (TTPs) empregados em ataques cibernéticos.	Fundamentos de segurança cibernética, inteligência cibernética e análise de risco.	Operar ferramentas de cibersegurança (ex: scanners de vulnerabilidade, monitoramento de sistemas) e de *Threat Intelligence*.	Curiosidade investigativa para identificar padrões de ameaças emergentes.
Empregar ferramentas de *Threat Intelligence* para identificar padrões de ataque e possíveis agentes responsáveis.	Técnicas de *Open Source Intelligence* (OSINT) e análise comportamental de ameaças.	Analisar padrões de ataques cibernéticos.	Rigor analítico na análise de dados e evidências.
Produzir relatórios técnicos e estratégicos sobre o cenário atual e tendências emergentes.	Principais grupos APT (*Advanced Persistent Threats*) e seus métodos de ataque.	Produzir relatórios técnicos com linguagem clara e precisa.	Comprometimento com a produção de análises isentas e desprovidas de viés ideológico.
---	Proficiência no idioma Inglês para leitura de artigos técnicos e relatórios internacionais.	---	---

COMPETÊNCIA 19 **TÍTULO:** Proteção cibernética e Gestão de Riscos para Infraestruturas Críticas.			
DESCRIÇÃO: Implementar protocolos de Segurança Cibernética para Infraestruturas Críticas.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Diagnosticar e mapear vulnerabilidades em sistemas críticos.	Princípios de segurança cibernética (CIA Triad: Confidencialidade, Integridade e Disponibilidade).	Realizar testes de intrusão e simulações de ataque (*redteaming*).	Proatividade na identificação e correção de vulnerabilidades.
Implementar e testar protocolos de segurança para proteção de dados sensíveis.	Normas internacionais de segurança, como ISO 27001 e *NIST Cybersecurity Framework*.	Configurar e administrar sistemas de detecção e prevenção de intrusos (IDS/IPS).	Atenção a detalhes e rigor na execução de protocolos.
Desenvolver planos de contingência para situações de ataque cibernético.	Conceitos de segurança em Infraestruturas Críticas e criptografia de dados.	Elaborar protocolos de segurança ajustados a diferentes cenários de risco.	Resiliência para lidar com cenários de crise e pressão.

COMPETÊNCIA 20 **TÍTULO:** Análise digital e extração de dados e evidências para produção de Conhecimento de Inteligência.			
DESCRIÇÃO: Coletar, analisar e interpretar dados digitais para identificar padrões, ameaças e tendências, subsidiando a produção de conhecimento de Inteligência.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Coletar, preservar e analisar evidências digitais seguindo padrões reconhecidos.	Fundamentos de forense digital e análise de artefatos de sistemas.	Analisar registros de log, artefatos de memória e fluxos de rede.	Zelo pela integridade e autenticidade das evidências.
Empregar ferramentas específicas para identificar a origem de ataques e métodos utilizados.	Técnicas de rastreamento de ameaças e identificação de padrões maliciosos.	Redigir laudos técnicos com clareza, detalhando metodologia e resultados.	Persistência na análise de dados complexos.
Produzir Relatórios de Inteligência para subsidiar investigações e processos decisórios.	Normativas legais sobre coleta, preservação e uso de evidências digitais.	---	Ética no tratamento de informações sensíveis.

COMPETÊNCIA 21 **TÍTULO:** Operações de Contrainteligência no ambiente cibernético.			
DESCRIÇÃO: Planejar e executar operações de Contrainteligência cibernética.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**

Identificar e analisar tentativas de espionagem e infiltração em sistemas institucionais.	Princípios e técnicas de Contrainteligência cibernética.	Aplicar técnicas de rastreamento e atribuição de autoria de ataques.	Discrição e sigilo na condução de operações de Contrainteligência cibernéticas.
Planejar e conduzir operações de despistamento e engajamento com atores adversos.	Métodos de rastreamento e identificação de agentes hostis.	Executar operações de engajamento com segurança e discrição.	Iniciativa para antecipar ações de agentes adversos.
Produzir Relatórios de Inteligência para subsidiar decisões estratégicas de segurança organizacional.	Táticas de operações de despistamento e engajamento controlado.	Analisar comportamento de atacantes e padrões de ataque.	Compromisso com a proteção dos interesses institucionais.

COMPETÊNCIA 22

TÍTULO: Cooperação para o fortalecimento da resiliência cibernética.

DESCRIÇÃO: Estabelecer cooperação nacional e internacional para o fortalecimento da resiliência cibernética.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Identificar e estabelecer parcerias com instituições nacionais e internacionais.	Estruturas e mecanismos de cooperação internacional em segurança cibernética.	Conduzir reuniões e representar a organização em fóruns especializados.	Proatividade na construção de parcerias.
Participar de grupos de trabalho e fóruns relacionados à segurança cibernética.	Protocolos de comunicação e compartilhamento seguro de informações.	Negociar acordos de cooperação e articular iniciativas conjuntas.	Flexibilidade para lidar com interlocutores de diferentes culturas.
Produzir relatórios com análises compartilhadas e propostas de cooperação.	Proficiência nos idiomas Inglês e Espanhol para interação com parceiros internacionais.	Produzir documentos formais de cooperação e memorandos de entendimento.	Compromisso com a troca segura e responsável de informações.

COMPETÊNCIA 23

TÍTULO: Aplicação de Inteligência Artificial e tecnologias emergentes para o fortalecimento da resiliência cibernética.

DESCRIÇÃO: Desenvolver e implementar estratégias de resiliência cibernética com suporte de Inteligência Artificial.

PADRÕES DE DESEMPENHO (COMPORTAMENTOS OBSERVÁVEIS)	CONHECIMENTOS (SABER)	HABILIDADES (SABER FAZER)	ATITUDES (QUERER FAZER)
Implementar modelos de Inteligência Artificial para detecção de padrões e anomalias em redes.	Fundamentos de aprendizado de máquina (*machine learning*) e de Inteligência Artificial aplicados à segurança cibernética.	Programar e ajustar modelos de Inteligência Artificial para análise de ameaças.	Interesse contínuo por inovações tecnológicas.
Analisar e validar dados fornecidos por sistemas de Inteligência Artificial em operações cibernéticas.	Princípios de análise comportamental baseada em Inteligência Artificial.	Integrar ferramentas de Inteligência Artificial com sistemas tradicionais de segurança.	Disciplina na validação e interpretação de dados automatizados.

Propor e desenvolver soluções automatizadas de resposta a incidentes.	Conhecimentos sobre ética e governança no uso de Inteligência Artificial.	Avaliar o desempenho e precisão de modelos preditivos.	Responsabilidade no uso ético de soluções baseadas em Inteligência Artificial.

COMPETÊNCIA 24 **TÍTULO:** Segurança jurídica, governança e conformidade normativa na Atividade de Inteligência.			
DESCRIÇÃO: Interpretar e aplicar normativas da Atividade de Inteligência e da Administração Pública.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Consultar e aplicar normativas internas e externas que regem a Atividade de Inteligência e a Administração Pública.	Lei n.º 9.883/1999 (criação da ABIN e do Sistema Brasileiro de Inteligência).	Interpretar corretamente dispositivos normativos e administrativos.	Compromisso com a conformidade legal e administrativa.
Garantir que suas decisões e ações estejam embasadas na legislação vigente, reduzindo riscos jurídicos e institucionais.	Lei n.º 8.112/1990 (Regime Jurídico dos Servidores Públicos Federais).	Aplicar diretrizes legais em sua rotina de trabalho.	Proatividade na busca por segurança jurídica e clareza normativa.
Documentar suas atividades de maneira que demonstrem conformidade com as diretrizes normativas e regulatórias.	Direito Constitucional e Direito Administrativo	Redigir documentos administrativos e relatórios técnicos com respaldo normativo.	Responsabilidade ao interpretar e aplicar normativas.
Sugerir a atualização e a padronização das normativas internas sempre que identificar ambiguidades ou lacunas que possam comprometer a segurança jurídica dos servidores.	Normas internas da organização e sua relação com a legislação de Inteligência e da Administração Pública.	---	---

COMPETÊNCIA 25 **TÍTULO:** Gestão da conformidade e eficiência institucional na Atividade de Inteligência.			
DESCRIÇÃO: Desenvolver e implementar estratégias que assegurem a conformidade jurídica e eficiência operacional na execução de atribuições.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Manter-se atualizado sobre a legislação que rege a Administração Pública e a Atividade de Inteligência.	Gestão pública e princípios da Administração Pública.	Monitorar o cumprimento de normas internas e regulamentos.	Compromisso com a integridade institucional.
Certificar-se de que sua atuação está alinhada às diretrizes institucionais e normativas, evitando riscos de responsabilização.	Mecanismos de responsabilização na Administração Pública.	Aplicar metodologias para garantir conformidade legal e eficiência operacional.	Responsabilidade na execução das atividades conforme as diretrizes normativas.

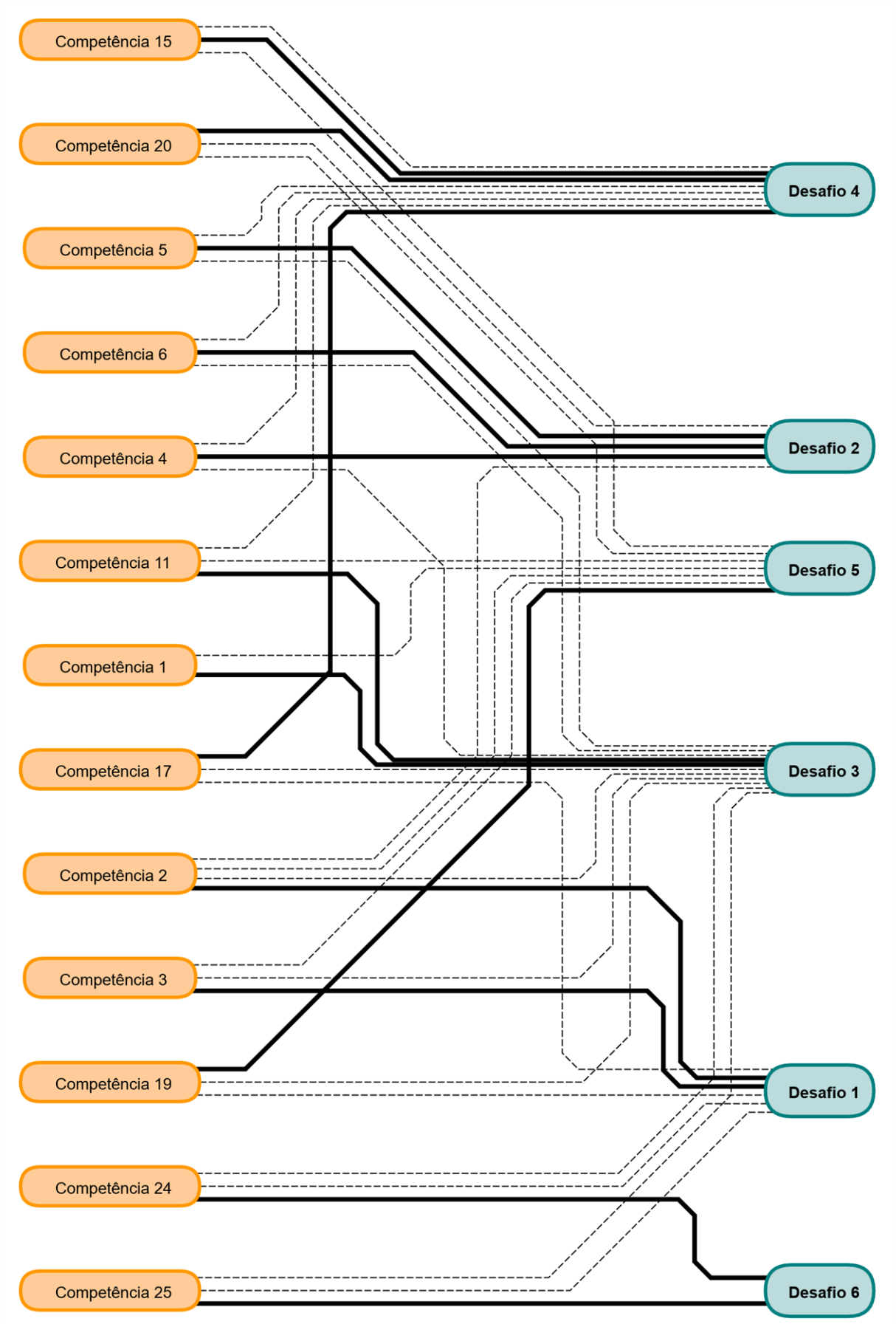
Formalizar ações estratégicas e operacionais por meio de relatórios e pareceres técnicos para garantir transparência e rastreabilidade das atividades.	Princípios de conformidade legal e governança institucional.	Propor melhorias nos processos administrativos com base na legislação vigente.	Iniciativa na busca por melhores práticas administrativas e jurídicas.
Sugerir melhorias nos normativos internos para mitigar riscos e fortalecer a governança organizacional.	---	---	---

COMPETÊNCIA 26 **TÍTULO:** Articulação e alinhamento de atribuições no ambiente de trabalho.			
DESCRIÇÃO: Comunicar e alinhar atribuições funcionais com gestores e equipe.			
PADRÕES DE DESEMPENHO **(COMPORTAMENTOS OBSERVÁVEIS)**	**CONHECIMENTOS** **(SABER)**	**HABILIDADES** **(SABER FAZER)**	**ATITUDES** **(QUERER FAZER)**
Realizar reuniões periódicas para esclarecimento de atribuições e responsabilidades funcionais.	Princípios da comunicação organizacional.	Conduzir reuniões de alinhamento com equipes para esclarecimento institucional.	Interesse na promoção da integridade dos processos institucionais.
Contribuir para a padronização dos fluxos de trabalho e processos decisórios dentro da organização.	Estruturas organizacionais e Arquitetura Estratégica da organização.	Comunicar diretrizes estratégicas de forma assertiva e objetiva.	Compromisso com a transparência na comunicação de responsabilidades.
Monitorar a aderência das práticas internas às normativas institucionais e sugerir ajustes quando necessário.	Técnicas de mediação de conflitos e negociação.	---	Proatividade na mediação de conflitos organizacionais.

4. TRANSVERSALIDADE DAS COMPETÊNCIAS

A figura abaixo ilustra, por meio de um diagrama de interseção, a natureza multifuncional das competências modeladas, destacando sua aplicabilidade simultânea a múltiplos desafios institucionais. As linhas contínuas em destaque representam a vinculação primária de cada competência a um desafio específico, conforme delineado na subseção anterior. Já as linhas pontilhadas demonstram as interconexões secundárias, nas quais uma mesma competência contribui para a superação de outros desafios organizacionais, reforçando a interdependência entre as demandas da ABIN.

Essa representação visual evidencia que as competências não atuam de forma isolada, mas sim de maneira sinérgica, ampliando sua eficácia ao abordar vulnerabilidades comuns, metodologias compartilhadas e contextos estratégicos sobrepostos. A transversalidade observada reflete a complexidade dinâmica do ambiente em que opera a Atividade de Inteligência, onde ameaças como a desinformação, a espionagem e o crime organizado transnacional estão intrinsecamente interligadas. Dessa forma, o diagrama reforça a necessidade de capacitação integrada, capaz de desenvolver profissionais aptos a mobilizar conhecimentos e habilidades de forma adaptável, assegurando respostas coordenadas e resilientes diante de desafios multifacetados.


Competência 15
Competência 20
Competência 5
Competência 6
Competência 4
Competência 11
Competência 1
Competência 17
Competência 2
Competência 3
Competência 19
Competência 24
Competência 25
Desafio 4
Desafio 2
Desafio 5
Desafio 3
Desafio 1
Desafio 6

5. CONSIDERAÇÕES FINAIS

O ponto de partida para a construção do *Framework de Competências* foi a identificação de seis desafios estratégicos que afetam diretamente a atuação dos Oficiais de Inteligência no contexto atual da ABIN. Esses desafios foram mapeados com base em duas fontes principais: entrevistas com Oficiais de Inteligência com experiência na carreira e a análise de conteúdo do documento institucional *Desafios de Inteligência – Edição 2025*. Eles refletem cenários como segurança cibernética, Contrainteligência, proteção de conhecimentos sensíveis, entre outros temas de alta complexidade.

O *Framework de Competências* apresentado reúne 26 competências que, em conjunto, oferecem uma visão estruturada das capacidades consideradas essenciais para que o Oficial de Inteligência cumpra com excelência suas atribuições. Cada competência foi detalhada com base nos elementos de conhecimento, habilidade e atitude (CHA), o que permite ao gestor entender não apenas *o que* se espera do servidor, *mas como* esse desempenho pode ser alcançado, desenvolvido ou aprimorado.

Mais do que uma lista, o *Framework de Competências* é um instrumento de gestão que pode ser utilizado como base para orientar processos de seleção interna, avaliação de desempenho, alocação de pessoal, desenho de ações formativas e planejamento de trilhas de desenvolvimento. A ideia é que os gestores da ABIN encontrem no documento um ponto de apoio para decisões mais estruturadas e alinhadas às necessidades reais da Agência.

É importante destacar que este material não tem a pretensão de esgotar o tema nem de substituir o julgamento gerencial, tão necessário em uma organização que opera em um ambiente dinâmico e complexo, como o vivenciado pela Atividade de Inteligência. Ao contrário: o *Framework de Competências* deve ser visto como uma referência flexível, que pode ser adaptada conforme o contexto e as especificidades de cada unidade/fração da Agência ou desafio, de acordo com suas demandas específicas.

Reconhece-se que a consolidação de uma lógica de gestão por competências é um processo gradual, que depende de mudança cultural, apoio institucional e uso racional e equilibrado dos instrumentos disponíveis. Neste sentido, o presente *Framework de Competências* pode ser um primeiro passo para ampliar o diálogo interno sobre como valorizar os saberes, as práticas e os comportamentos que fazem diferença para a Atividade de Inteligência.

O desenvolvimento deste material reflete um esforço de sistematização de práticas e saberes que já permeiam a atuação da ABIN, contribuindo para sua valorização e aprimoramento.

Na prática, o *Framework de Competências* pode ser utilizado por chefias para planejar ações formativas alinhadas às necessidades reais de suas equipes. Também pode servir de base para conversas sobre desenvolvimento de carreira, contribuindo para o engajamento, retenção de talentos e fortalecimento da cultura de desempenho, bem como apoiar a área de gestão de pessoas na formulação de critérios mais objetivos em processos internos.

Por fim, este material representa um convite à experimentação responsável. A proposta é que o *Framework de Competências* seja progressivamente testado, debatido e aprimorado a partir da experiência concreta dos gestores e Oficiais de Inteligência da ABIN. Com uso criterioso, contínuo e reflexivo, ele poderá se tornar uma ferramenta relevante para o fortalecimento da gestão estratégica de pessoas na Agência.

8.2. Roteiro de entrevista

Primeiro Bloco (Ambientação do Entrevistado eTrajetória Profissional)		
01	DATA DA ENTREVISTA	
02	NOME	GRACILIANO RAMOS
03	IDADE	
04	CARGO	OFICIAL DE INTELIGÊNCIA
05	GRAU DE INSTRUÇÃO	( ) GRADUAÇÃO EM QUAL ÁREA? _____ ( ) MESTRADO EM QUAL ÁREA? _____ ( ) DOUTORADO EM QUAL ÁREA? _____
06	DATA DE INGRESSO NA ABIN	
07	EM QUAIS ÁREAS DA ABIN O ENTREVISTADO LABOROU?	( ) RECURSOS HUMANOS ( ) CAPACITAÇÃO/ENSINO ( ) ANÁLISE ( ) OPERAÇÕES ( ) SUPERINTENDÊNCIA ( ) ADMINISTRATIVA
08	O ENTREVISTADO EXERCEU FUNÇÃO COMISSIONADA/CARGO EM COMISSÃO NAS ÁREAS MENCIONADAS NA QUESTÃO ANTERIOR? SE SIM, POR QUANTO TEMPO E QUAL(IS) FOI(RAM) ESTA(S) FUNÇÃO(ÕES)/CARGO(S)?	
Segundo Bloco (Contato ePercepções do Entrevistado com os ConstrutosMapeamento de Competências e Gestão Por Competências)		
09	NA SUA VISÃO, QUAIS SÃO OS MAIORES DESAFIOS QUE O OFICIAL DE INTELIGÊNCIA ENFRENTA AO TRABALHAR NA ABIN?	
10	QUAIS SERIAMOS **CONHECIMENTOS** MAIS IMPORTANTES QUE UM OFICIAL DE INTELIGÊNCIA DEVERIA POSSUIR PARA DESEMPENHAR SUAS FUNÇÕES NA ABIN?	
11	QUAIS SERIAM AS **HABILIDADES** MAIS IMPORTANTES QUE UM OFICIAL DE INTELIGÊNCIA DEVERIA POSSUIR PARA DESEMPENHAR SUAS FUNÇÕES NA ABIN?	
12	QUAIS SERIAM AS **ATITUDES** MAIS IMPORTANTES QUE UM OFICIAL DE INTELIGÊNCIA DEVERIA POSSUIR PARA DESEMPENHAR SUAS FUNÇÕES NA ABIN?	
13	O QUE O ENTREVISTADO ENTENDE POR *MAPEAMENTO DE COMPETÊNCIAS* E QUAL A SUA IMPORTÂNCIA PARA UMA ORGANIZAÇÃO?	
14	O QUE O ENTREVISTADO ENTENDE POR *GESTÃO POR COMPETÊNCIAS* E QUAL A SUA IMPORTÂNCIA PARA UMA ORGANIZAÇÃO?	
15	O ENTREVISTADO TEM CONHECIMENTO SE ALGUM SERVIÇO DE INTELIGÊNCIA NO EXTERIOR APLICA A *GESTÃO POR COMPETÊNCIAS* EM SEUS PROCESSOS? SE SIM, PODERIA INDICAR QUAL SERIA ESTE SERVIÇO?	

16	O ENTREVISTADO ACREDITA QUE HAVERIA ESPAÇO PARA A APLICAÇÃO DA *GESTÃO POR COMPETÊNCIAS* EM UM SERVIÇO DE INTELIGÊNCIA, DADA SUAS ESPECIFICIDADES?	(1) DISCORDO TOTALMENTE (2) CONCORDO PARCIALMENTE (3) CONCORDO PLENAMENTE
17	O ENTREVISTADO ACREDITA QUE HÁ *GESTÃO POR COMPETÊNCIAS* NA ABIN?	(1) NÃO ACREDITO (2) ACREDITO, MAS PARCIALMENTE (3) ACREDITO TOTALMENTE
18	CASO TENHA RESPONDIDO AS OPÇÕES (2) OU (3) DA PERGUNTA ANTERIOR, QUAL SUBSISTEMA DA *GESTÂO POR COMPETÊNCIAS* O ENTREVISTADO ACREDITA QUE ESTEJA DESENVOLVIDO NA ABIN?	( ) RECRUTAMENTO ( ) PROCESSOS SELETIVOS INTERNOS PARA PROVIMENTO DE CARGOS COMISSIONADOS ( ) CESSÕES E REQUISIÇÕES DE SERVIDORES ( ) DESENHO DE CARREIRAS ( ) *DESIGN* DE CURSOS E DE ATIVIDADES DE CAPACITAÇÃO
19	QUAIS COMPETENCIAS VOCE OBSERVA QUE SÃO MAIS DIFICEIS DE ENCONTRAR OU DESENVOLVER NOS OFICIAIS DE INTELIGÊNCIA DA ABIN?	
20	OS GESTORES DA ABIN POSSUEM CLAREZA SOBRE AS COMPETENCIAS ESPERADAS DE CADA COLABORADOR EM SUAS EQUIPES?	(1) DISCORDO TOTALMENTE (2) NÃO CONCORDO E NEM DISCORDO (3) CONCORDO TOTALMENTE
21	O ENTREVISTADO ACREDITA QUE A ORGANIZAÇÃO ALOCA OS OFICIAIS DE INTELIGÊNCIACOM BASE NA COMPARAÇÃO ENTRE AS COMPETÊNCIAS APRESENTADAS POR ELES E AS COMPETÊNCIAS ALMEJADAS PELAS UNIDADES?	(1) NÃO ACREDITO (2) ACREDITO EM PARTE (3) ACREDITO TOTALMENTE
22	O ENTREVISTADO ACREDITA QUE OS PERFIS PROFISSIONAIS ALMEJADOS PARA CADA FUNÇÃO/OCUPAÇÃO DA ABIN ESTÃO ALICERÇADOS EM UM MAPEAMENTO DE COMPETÊNCIAS E DEFINIDOS SOB O PRISMA DA *GESTÃO POR COMPETÊNCIAS*?	(1) NÃO ACREDITO (2) ACREDITO EM PARTE (3) ACREDITO TOTALMENTE
23	O ENTREVISTADO TEM CONHECIMENTO DE ALGUM DOCUMENTO QUE TRAGA O MAPEAMENTO DAS COMPETÊNCIAS DA ABIN?	( ) SIM, TENHO CONHECIMENTO E JA ME INTEIREI DO TEOR DO DOCUMENTO. ( ) SIM, SEI DA EXISTENCIA. CONTUDO, NÃO ME INTEIREI DO TEOR DO DOCUMENTO. ( ) NÃO, DESCONHEÇO QUALQUER DOCUMENTO NESTE SENTIDO.

24	O ENTREVISTADO TEM CONHECIMENTO DE ALGUM DOCUMENTO DA ABIN QUE VERSE SOBRE *GESTÃO POR COMPETÊNCIAS*?	( ) SIM, TENHO CONHECIMENTO E JA ME INTEIREI DO TEOR DO DOCUMENTO. ( ) SIM, SEI DA EXISTENCIA. CONTUDO, NÃO ME INTEIREI DO TEOR DO DOCUMENTO. ( ) NÃO, DESCONHEÇO QUALQUER DOCUMENTO NESTE SENTIDO.
25	O ENTREVISTADO TEM CONHECIMENTO SE A *GESTÃO POR COMPETÊNCIAS* ENCONTRA-SE CONTEMPLADA EM ALGUM DOS DOCUMENTOS QUE COMPÕEM A ARQUITETURA ESTRATÉGICA DA ABIN?	( ) SIM, TENHO CONHECIMENTO E JA ME INTEIREI DO TEOR DO DOCUMENTO. ( ) SIM, SEI DA EXISTENCIA. CONTUDO, NÃO ME INTEIREI DO TEOR DO DOCUMENTO. ( ) NÃO, DESCONHEÇO QUALQUER DOCUMENTO NESTE SENTIDO.
26	O ENTREVISTADO PORVENTURA TEM CONHECIMENTO ACERCA DA EXISTÊNCIA E DO TEOR DE ALGUM NORMATIVO FEDERAL (LEI, DECRETO, PORTARIA ETC) QUE VERSE SOBRE A APLICABILIDADE DA GESTÃO POR COMPETÊNCIAS PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL?	( ) SIM, TENHO CONHECIMENTO E JA ME INTEIREI DO TEOR DESTES DOCUEMENTOS. ( ) SIM, SEI DA EXISTENCIA. CONTUDO, NÃO ME INTEIREI DO TEOR DESTES DOCUMENTOS. ( ) NÃO, DESCONHEÇO QUAISQUER NORMATIVOS NESTE SENTIDO.
27	O ENTREVISTADO PODERIA DESCREVER UMA EXPERIÊNCIA PROFISSIONAL VIVENCIADA NA ABIN EM QUE TEVE OPORTUNIDADE DE APLICAR OU VIVENCIAR A *GESTÃO POR COMPETÊNCIAS*?	
28	NO PERÍODO EM QUE EXERCEU FUNÇÃO NA ABIN, O ENTREVISTADO EM ALGUMA OCASIÃO FOI CHAMADO PARA PARTICIPAR DE ALGUMA REUNIÃO/ENCONTRO OU CONVIDADO A PARTICIPAR DE ALGUM EVENTO QUE DISCORRESSE SOBRE *GESTÃO POR COMPETÊNCIAS*?	
29	NA OPINIÃO DO ENTREVISTADO, A ABIN ESTÁ ESTRUTURADA PARA OPERAR EM UMA LÓGICA DE *GESTÃO POR COMPETÊNCIAS*?	(1) DISCORDO TOTALMENTE (2) CONCORDO PARCIALMENTE (3) CONCORDO PLENAMENTE
30	ENTRE AS OPÇÕES APRESENTADAS, ORDENE OS PRINCIPAIS DESAFIOS QUE VOCÊ VISLUMBRA NA IMPLEMENTAÇÃO E/OU MANUTENÇÃO DE UM SISTEMA DE GESTÃO POR COMPETÊNCIAS NA ABIN	( ) ALINHAR A GESTÃO POR COMPETÊNCIAS COM A MISSÃO, A VISÃO E OS VALORES DA ORGANIZAÇÃO

		( ) APOIO/SUPORTE DO CORPO DIRETIVO DA ORGANIZAÇÃO ( ) APOIO/SUPORTE DOS SERVIDORES QUE TRABALHAM NA ORGANIZAÇÃO ( ) AUSÊNCIA DE PESSOAL QUALIFICADO PARA CONDUÇÃO DO PROCESSO ( ) AUSÊNCIA DE INFORMAÇÃO SOBRE O TEMA ( ) AUSÊNCIA DE RECURSOS FINANCEIROS ( ) OUTROS_____
31	DO ROL DE 26CONHECIMENTOS, HABILIDADES E ATITUDES APRESENTADOS A SEGUIR, ENUMERE EM ORDEM CRESCENTE – A DE MENOR NÚMERO SERIA A MAIS IMPORTANTE – QUAIS SERIAM NECESSARIAS/DESEJAVEIS PARA A ATUAÇÃO DE UM OFICIAL DE INTELIGENCIA DA ABIN.	**CONHECIMENTOS** ( ) CONHECIMENTO EM ANALISE DE DADOS: CAPACIDADE DE COMPREENDER E INTERPRETAR GRANDES VOLUMES DE DADOS QUANTITATIVOS E QUALITATIVOS, APLICANDO TECNICAS DE ANALISE ESTATISTICA E CONTEXTUAL PARA EXTRAIR INFORMAÇÕES ESTRATEGICAS. ( ) GEOPOLITICA E RELAÇÕES INTERNACIONAIS: ENTENDIMENTO DAS DINAMICAS INTERNACIONAIS, INCLUINDO A INTERAÇÃO ENTRE ESTADOS, ORGANIZAÇÕES E ATORES NÃO-ESTATAIS, BEM COMO OS FATORES POLITICOS, ECONOMICOS E CULTURAIS QUE AFETAM A SEGURANÇA GLOBAL. ( ) CIBERSEGURANÇA: CONHECIMENTO SOBRE AS AMEAÇAS NO AMBIENTE DIGITAL, INCLUINDO *HACKING*, ATAQUES CIBERNETICOS E MEDIDAS DE PROTEÇÃO DE DADOS, ALEM DE COMPREENDER AS

		TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO. ( ) LEGISLAÇÃO E NORMAS DE INTELIGENCIA: FAMILIARIDADE COM O ARCABOUÇO LEGAL QUE REGE AS ATIVIDADES DE INTELIGENCIA, TANTO NO AMBITO NACIONAL QUANTO INTERNACIONAL, GARANTINDO O CUMPRIMENTO DAS LEIS, ETICA E DIREITOS FUNDAMENTAIS. ( ) PSICOLOGIA SOCIAL E COMPORTAMENTAL: COMPREENSÃO DAS MOTIVAÇÕES E COMPORTAMENTOS INDIVIDUAIS E COLETIVOS, BEM COMO DAS DINAMICAS DE GRUPOS, O QUE E CRUCIAL PARA A INTERPRETAÇÃO DE AÇÕES DE ADVERSARIOS OU ALIADOS. ( ) TECNICAS DE INTELIGENCIA E CONTRAINTELIGENCIA: CONHECIMENTO DAS METODOLOGIAS UTILIZADAS PARA A COLETA, PROCESSAMENTO E ANALISE DE INFORMAÇÕES, ALEM DE AÇÕES NO CAMPO OPERACIONAL, VISANDO FORMULAR ESTRATEGIAS DE PROTEÇÃO CONTRA ATIVIDADES DE ESPIONAGEM. ( ) CONTRATERRORISMO: CONHECIMENTO DAS TÉCNICAS, TÁTICAS E POLÍTICAS RELACIONADAS AO COMBATE AO TERRRISMO. ( ) ECONOMIA E INTELIGÊNCIA FINANCEIRA: CONHECIMENTO DOS PRINCÍPIOS ECONÔMICOS E TÉCNICAS DE ANÁLISE FINANCEIRA APLICADAS AO

		RASTREAMENTO DE ATIVIDADES ILÍCITAS, COMO LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO. ( ) IDIOMAS: DOMÍNIO DE IDIOMA ESTRANGEIRO, NOTADAMENTE INGLÊS E ESPANHOL **HABILIDADES** ( ) ANALISE CRITICA: HABILIDADE DE AVALIAR DADOS E INFORMAÇÕES DE MANEIRA OBJETIVA E PROFUNDA, IDENTIFICANDO PADRÕES, ANOMALIAS E LACUNAS DE INFORMAÇÃO PARA TOMAR DECISÕES INFORMADAS. ( ) COMUNICAÇÃO EFICAZ: CAPACIDADE DE TRANSMITIR INFORMAÇÕES COMPLEXAS DE FORMA CLARA E PRECISA, TANTO POR MEIO DE RELATORIOS ESCRITOS QUANTO EM APRESENTAÇÕES ORAIS, ADAPTANDO-SE AO PUBLICO-ALVO. ( ) TOMADA DE DECISÃO SOB PRESSÃO: HABILIDADE DE AVALIAR CENARIOS DE ALTA COMPLEXIDADE E FAZER ESCOLHAS RAPIDAS E EFICAZES EM SITUAÇÕES DE CRISE, COM TEMPO LIMITADO E ALTO GRAU DE INCERTEZA. ( ) OPERAÇÃO DE TECNOLOGIAS AVANÇADAS: DOMINIO DE SISTEMAS E FERRAMENTAS TECNOLOGICAS UTILIZADAS EM INTELIGENCIA, COMO *SOFTWARES* DE ANALISE DE DADOS, FERRAMENTAS DE CRIPTOGRAFIA E

		PLATAFORMAS DE MONITORAMENTO DE INFORMAÇÕES. ( ) CAPACIDADE INVESTIGATIVA: HABILIDADE DE CONDUZIR INVESTIGAÇÕES DETALHADAS, IDENTIFICAR FONTES DE INFORMAÇÃO CONFIAVEIS, CORRELACIONAR DADOS APARENTEMENTE DESCONECTADOS E FORMULAR HIPOTESES PRECISAS. ( ) TRABALHO EM EQUIPE: CAPACIDADE DE COLABORAR DE FORMA EFICAZ COM COLEGAS DE DIFERENTES AREAS E ESPECIALIZAÇÕES, COMPARTILHANDO INFORMAÇÕES E CONSTRUINDO SOLUÇÕES CONJUNTAS PARA PROBLEMAS COMPLEXOS. ( ) LIDERANÇA EM SITUAÇÕES CRÍTICAS: COMPETÊNCIA PARA LIDERAREQUIPES EM AMBIENTES DE ALTA PRESSÃO, GERENCIANDO CRISES E COORDENANDO OPERAÇÕES DE INTELIGÊNCIA COMPLEXAS. ( ) GESTÃO DE RISCOS: HABILIDADE DE IDENTIFICAR, AVALIAR E MITIGAR RISCOS QUE POSSAM COMPROMETER A SEGURANÇA E A EFICIÊNCIA DASAÇÕES/OPERAÇÕES DE INTELIGÊNCIA. ( ) NEGOCIAÇÃO: CAPACIDADE DE NEGOCIAR COM *STAKEHOLDERS* INTERNOS E EXTERNOS. **ATITUDES**

		( ) DISCRIÇÃO E CONFIDENCIALIDADE: COMPROMETIMENTO EM PROTEGER INFORMAÇÕES SIGILOSAS E SENSIVEIS, RESPEITANDO OS PROTOCOLOS DE SEGURANÇA DA INFORMAÇÃO E AGINDO DE FORMA DISCRETA EM TODAS AS SITUAÇÕES. ( ) ÉTICA PROFISSIONAL: MANTER ELEVADOS PADRÕES ETICOS EM TODAS AS OPERAÇÕES DE INTELIGENCIA, RESPEITANDO OS DIREITOS HUMANOS E AS LEIS VIGENTES, ALEM DE EVITAR COMPORTAMENTOS IMPROPRIOS OU ANTIETICOS. ( ) RESILIENCIA: CAPACIDADE DE LIDAR COM SITUAÇÕES DE ESTRESSE ELEVADO, PRESSÕES CONTINUAS E ADVERSIDADES, MANTENDO O FOCO NO OBJETIVO E A CLAREZA MENTAL PARA TOMAR DECISÕES CRITICAS. ( ) CURIOSIDADE E APRENDIZADO CONTINUO: DISPOSIÇÃO PARA APRENDER CONSTANTEMENTE, ATUALIZANDO-SE COM AS NOVAS TENDENCIAS TECNOLOGICAS, POLITICAS E ESTRATEGICAS QUE AFETAM O CAMPO DA INTELIGENCIA. ( ) COMPROMETIMENTO COM A MISSÃO: DEDICAÇÃO PARA CUMPRIR AS RESPONSABILIDADES DE FORMA DILIGENTE E EFICAZ, DEMONSTRANDO UMA FORTE ORIENTAÇÃO PARA O CUMPRIMENTO DA MISSÃO DA ORGANIZAÇÃO DE INTELIGENCIA.

		( ) PENSAMENTO CRITICO E IMPARCIALIDADE: MANTER UMA POSTURA IMPARCIAL E OBJETIVA, AVALIANDO AS INFORMAÇÕES SEM PRECONCEITOS OU VIESES PESSOAIS, E QUESTIONANDO FONTES E DADOS DE MANEIRA CONSTRUTIVA. ( ) PROATIVIDADE: ATITUDE DE ANTECIPAR PROBLEMAS E OPORTUNIDADES, TOMANDO A INICIATIVA DE AGIR DE MANEIRA RÁPIDA E EFICAZ. ( ) ADAPTABILIDADE: FLEXIBILIDADE PARA SE AJUSTAR RAPIDAMENTE ÀS MUDANÇAS NO AMBIENTE OPERACIONAL OU A NOVOS DESAFIOS.
32	OUTRAS INFORMAÇÕES JULGADAS ÚTEIS PELO ENTREVISTADO	

8.3. Termo de Consentimento Livre e Esclarecido

Discente: Luiz Cláudio de Queiroz Rodrigues

Tema de Pesquisa: *Framework* de competências para o cargo de Oficial de Inteligência da ABIN.

Convidamos para participar de pesquisa que busca aferir a percepção e o tratamento do tema *Gestão por Competências* no âmbito da Agência Brasileira de Inteligência (ABIN), bem como coletar subsídios visando a elaboração de um *framework* de competências para o cargo de Oficial de Inteligência da instituição.

A pesquisa encontra-se sob responsabilidade do pesquisador *Luiz Cláudio de Queiroz Rodrigues*, no âmbito do Mestrado Profissional em Administração Pública da Universidade de Brasília. Sua realização foi autorizada pela Direção-Geral da ABIN.

A participação na pesquisa se dará por meio de entrevista semiestruturada, que será gravada, transcrita e submetida a análise de conteúdo. Ressalte-se que a participação do entrevistado é voluntária e visando atender aos preceitos do artigo 9º da Lei nº 9.883/99 – que assegura o sigilo da identidade dos servidores da ABIN –, o entrevistado não seránominalmente identificado, mas cognominadopelo pseudônimo de um escritor brasileiro.

O entrevistado poderá solicitar a interrupção da entrevista a qualquer momento. Ademais, é assegurado ao entrevistado o direito de retirar seu consentimento em qualquer fase da pesquisa, sem nenhuma restrição ou punição à pessoa ou à instituição.

Por fim e dado o caráter voluntário de participação do entrevistado, informa-se que não haverá nenhuma despesa ou remuneração referente a esta pesquisa.

8.4. Consentimento de participação

Eu,_____, fui informado(a) sobre o teor do Termo de Consentimento Livre e Esclarecido, bem como dos objetivos acerca da pesquisa. Desta forma, concordo em participar voluntariamente do presente estudo e confirmo que estou ciente de que me é assegurado o direito de retirar da pesquisa em qualquer fase.

Por oportuno, informo que nesta entrevista fui cognominado com o pseudônimo de _____.

Este documento é emitido em uma única via, que será assinada por mim e pelo pesquisador. O documento ficarána posse do pesquisador e será arquivada pelo prazo de um ano, a contar da presente data e após esse ínterim, será destruído.

_____

LOCAL E DATA

_____

PARTICIPANTE DA PESQUISA

_____

LUIZ CLÁUDIO DE QUEIROZ RODRIGUES