

COLEÇÃO ESTUDOS APLICADOS
Volume 1

GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO

ORGANIZAÇÃO
Escola Superior do Ministério Público da União





REPÚBLICA FEDERATIVA DO BRASIL

Ministério Público da União

Paulo Gustavo Gonet Branco
Procurador-Geral da República
Hindenburg Chateaubriand Pereira Diniz Filho
Vice-Procurador-Geral da República

Escola Superior do Ministério Público da União

Raquel Branquinho Pimenta Mamede Nascimento
Diretora-Geral

Manoel Jorge e Silva Neto
Diretor-Geral Adjunto

Renata Souza Mendes Salgueiro
Secretária de Ensino, Pesquisa e Extensão

Graziane Madureira
Secretária de Comunicação Social

Renata de Souza Rodrigues
Secretária de Administração

Vinícius dos Santos Moreira
Secretário de Tecnologia da Informação

Comitê Científico Consultivo

Clarissa Ribeiro Schinestsck
Procuradora do Trabalho
Coordenadora

Luiza Cristina Fonseca Frischeisen
Subprocuradora-Geral da República

Antonio do Passo Cabral
Procurador da República

Carlos Bruno Ferreira da Silva
Procurador da República

Gisele Santos Fernandes Góes
Procuradora Regional do Trabalho

Adriana Santos Imbrosio
Procuradora de Justiça Militar

André Vinícius Espírito Santo de Almeida
Procurador de Justiça

COLEÇÃO ESTUDOS APLICADOS
Volume 1

GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO

ORGANIZAÇÃO
Escola Superior do Ministério Público da União



ESMPU

Brasília-DF
2026

ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO

SGAS L2 Sul Quadra 603 Lote 22 · 70200-630 · Brasília-DF
www.escola.mpu.mp.br · coci@escola.mpu.mp.br

SECRETARIA DE ENSINO, PESQUISA E EXTENSÃO

Subsecretaria de Pesquisa, Pós-Graduação e Comunicação Científica

Allana de Albuquerque Sousa Silva

Coordenadoria de Comunicação Científica

Lizandra Nunes Marinho da Costa Barbosa

Divisão de Editoração

Sarah do Nascimento Araújo

Núcleo de Preparação e Revisão Textual

Sandra Maria Telles

Núcleo de Design Editorial

Sheylise Rhoden

Supervisão editorial

Allana de Albuquerque Sousa Silva

Produção editorial

Lizandra Nunes Marinho da Costa Barbosa

Preparação de originais e revisão de provas gráficas

Davi Silva do Carmo, Jennyfer Alves de Carvalho,

Mariana de Lima Georg e Sandra Maria Telles

Capa

Natali Andrea Gomez Valenzuela

Projeto gráfico

Sheylise Rhoden

Diagramação

Natali Andrea Gomez Valenzuela e Sheylise Rhoden

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP) ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO

E74g Escola Superior do Ministério Público da União (Brasil).

Governança da tecnologia da informação / Escola Superior do
Ministério Público da União. – Brasília, DF : ESMPU, 2026.

424 p. : il. ; 23 cm. – (Coleção Estudos Aplicados ; v. 1)

ISBN 978-65-88299-51-7 (coleção)

ISBN 978-65-88299-52-4 (volume 1)

DOI <https://doi.org/10.63601/978-65-88299-52-4>

1. Tecnologia da informação – Governança. 2. Tecnologia da
informação – Administração pública. 3. Governança corporativa.

I. Título. II. Série.

CDD 004.068

CDU 004:658

Elaborada por Artur Virginio dos Santos – CRB-1/1986

2026. Todos os direitos reservados.

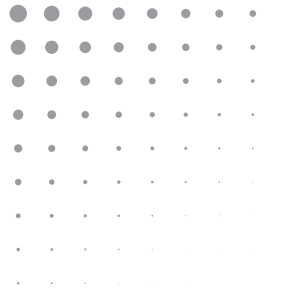
 **CC BY-NC 4.0**

Os textos estão sob Licença Creative Commons – Atribuição-Não Comercial 4.0.

É autorizada a reprodução total ou parcial para fins não comerciais,
desde que inserida a fonte e indicada a autoria do texto.

As opiniões expressas nesta obra são de exclusiva responsabilidade
dos autores. **Distribuição gratuita. Venda proibida.**





Esta obra é composta por artigos dos discentes que optaram por publicar na linha editorial de obras avulsas, na Coleção Estudos Aplicados.

A Escola Superior da Ministério Público da União para-
beniza todos os discentes do *Curso de Pós-Graduação Lato Sensu
em Governança da Tecnologia da Informação*, turma 2024-2025,
e estima sucesso em sua jornada profissional.

Alessandra Trindade dos Santos

Alessandro Glauber da Silva Evangelista

Alex da Silva Camara

Alexandre Saadi

Alinne Cristiane Aniceto Medeiros

André Kássio de Souza Lucena

Andrea dos Santos Publio

Angelo Stroligo Pecly

Antonio de Jesus da Silva Machado

Bernardo Heinz Pimentel Liedtke

Carolline Pereira Aca

César Medeiros Cupertino

Cleilson Sales Cassiano

Creuza Pereira Gama Gomes

Eduardo Reinert

Fabio Santos Pimenta

Fernando Henrique Nakashoji

Flávio Aparecido Angelo

George Antonio Ferreira de Araujo

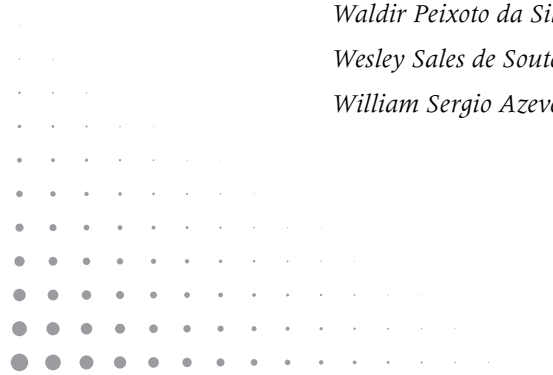
Gilberto Barbosa Lacerda Filho

Gilgleidson Vasconcelos de Souza





Glauce Picinini da Silva Millan
Henderson Rogers Melo da Silva
Italo Yure Braga Arruda
Leandro Engler Bocon
Leonardo Andrade Macedo
Leonardo Pereira Orrico
Luana da Silva Ferreira
Luis Marcos da Cruz de Amorim
Marcos Daniel Vaz Cavalcante Ramos
Maria Romilda da Silva Ventura
Maryane Maira Anchieta Santana
Patrícia Amancio do Prado Silva
Ricardo Lima Caio
Roberto D'Oliveira Vieira
Rodrigo Barreto da Silva
Rogério Postai
Ronnedy Santos de Carvalho
Sílvio Simplicio Pinheiro
Sostenes Pinto Leite Junior
Thiago Coelho Vieira
Thiago Duarte Mesquita
Thiago Russo Nantes
Wagner Pinheiro da Silva
Waldir Peixoto da Silva Júnior dos Santos
Wesley Sales de Souto
William Sergio Azevedo Guimaraes



9	APRESENTAÇÃO
11	MENSAGEM DO ORIENTADOR DO CURSO
15	Comunicação institucional nos Planos Diretores de Tecnologia da Informação (PDTIs): desigualdades no Ministério Público brasileiro Alessandra Trindade dos Santos Ronnedey Santos de Carvalho
43	Evolução estratégica da rede de dados de longa distância do MPF: os desafios decorrentes do atual modelo de contratação Alinne Cristiane Aniceto Medeiros Fernando Nakashoji
75	A inteligência artificial generativa no Ministério Público do Distrito Federal e Territórios: desafios à segurança da informação e conformidade com a Lei Geral de Proteção de Dados Pessoais André Kassio de Souza Lucena Thiago Duarte Mesquita
107	Governança de TI e IA como ferramentas para inclusão digital e melhoria do serviço digital prestado pelo MPF Andréa dos Santos Publio Fábio Santos Pimenta
143	Cibercrime e inteligência artificial: o papel dos modelos de linguagem no aperfeiçoamento de ataques de <i>phishing</i> Antônio de Jesus da Silva Machado Glauce Picinini da Silva Millan
175	Análise da oferta de serviços de TIC em unidades descentralizadas com foco na melhora da geração de valor institucional Cleilson Sales Cassiano Gilgleidson Vasconcelos de Souza

- 207 **Avaliação da maturidade digital do Ministério Público Federal:
cenário atual e estratégias para potencializar a transformação digital**
George Antônio Ferreira de Araújo
Sílvia Simplicio Pinheiro
Thiago Russo
- 245 **Governança de TI em escolas de governo: um estudo sobre diretrizes
estratégicas para tecnologias críticas**
Henderson Rogers Melo da Silva
- 273 **Da manutenção tradicional ao BIM: reformulação de contratos públicos
de operação e manutenção predial**
Italo Yure Braga Arruda
Wagner Pinheiro da Silva
- 309 **Governança de tecnologia da informação no Ministério Público Federal:
estratégias para resposta a incidentes de cibersegurança**
Leonardo Pereira Orrico
Marcos Daniel Vaz Cavalcante Ramos
- 337 **Desenvolvimento e avaliação de um chatbot agêntico multimodelo baseado
em RAG para facilitar o acesso do cidadão aos serviços do Ministério Público
da União e seus ramos**
Thiago Coelho Vieira
Luana da Silva Ferreira
- 367 ***Blockchain*, uma visão de futuro para o Ministério Público Federal**
Rodrigo Barreto da Silva
Sóstenes P. Leite Junior
- 393 **Cibercriminalidade e capacidade técnica e operacional dos órgãos de apoio
em tecnologia da informação e comunicação do Ministério Público Federal**
Rogério Postai
Waldir Peixoto da Silva Júnior dos Santos





A coleção “Estudos Aplicados”, que integra a linha editorial *Diálogos Científicos e Inovação*, contempla a publicação dos trabalhos de conclusão dos cursos do Programa de Pós-Graduação *Lato Sensu* (PPG) da Escola Superior do Ministério Público da União (ESMPU). Sua finalidade é difundir o conhecimento produzido pelos discentes da Escola durante sua jornada acadêmica.

O PPG da ESMPU busca fortalecer as competências profissionais e interdisciplinares de membros e servidores dos quatro ramos do Ministério Público da União (MPU) para uma atuação inovadora e eficaz, por meio do estímulo à reflexão crítica e aplicada às ciências jurídica e social e, também, à produção científica.

Nesse sentido, ao lado das pesquisas científicas e dos cursos de curta duração, o programa de pós-graduação da Escola traduz o compromisso institucional com a formação continuada e qualificada dos seus integrantes. Como é possível observar nesta obra coletiva, os temas selecionados para os cursos valorizam e impulsionam o conhecimento aplicado nas relevantes funções constitucionais do MPU.

Com esta publicação, que contempla o conhecimento produzido por discentes no percurso do PPG 2024-2025, a ESMPU posiciona-se estrategicamente diante do desafio de unir a atuação institucional de membros e servidores a projetos acadêmicos. Como agente de fomento, a Escola busca intermediar a discussão entre a ciência e a prática, visando entregas mais consistentes, sob a ótica da interdisciplinariedade e da integralidade das ações que envolvam a sua atividade-fim.

Neste volume, foram reunidos artigos que refletem estudos em Tecnologia da Informação, área do conhecimento cada vez mais relevante para a sociedade no cenário mundial e que se tornou imprescindível para a entrega de serviços públicos e um eficaz exercício da cidadania.

Sob a orientação pedagógica de Mauro Sobrinho, analista do MPU e mestre em Ciência da Computação pela Universidade de Brasília (UnB), o curso de especialização “Governança da Tecnologia da Informação”

proporcionou o desenvolvimento e a consolidação de habilidades e competências específicas dos discentes, servidores do MPU, por meio de mecanismos de governança e gestão direcionados ao melhor uso da tecnologia da informação.

Ao entregar a coleção “Estudos Aplicados” à comunidade acadêmica e ao público em geral, a ESMPU contribui para o acesso à informação qualificada e interdisciplinar destinada à melhoria dos serviços prestados pelo Ministério Público da União à sociedade.

Boa leitura!

Raquel Branquinho Pimenta Mamede Nascimento
Diretora-Geral



Como orientador pedagógico do curso de especialização em “Governança de Tecnologia da Informação”, promovido pela Escola Superior do Ministério Público da União (ESMPU), é com imenso orgulho que apresento esta coletânea de artigos que compõe a coleção “Estudos Aplicados”.

Mais que celebrar a entrega desta publicação, o meu intuito é convidá-lo a olhar para a jornada que nos trouxe até aqui. Quando iniciamos o projeto dessa pós-graduação, nosso objetivo não era apenas certificar especialistas, mas promover uma verdadeira formação de discentes pesquisadores. Queríamos instigar nossos membros e servidores a irem além da execução técnica diária, desenvolvendo uma capacidade de análise crítica, interpretação e resolução de problemas complexos na realidade do MPU.

É essencial ressaltar que o mais importante dessa pós-graduação não foram as entregas finais – os excelentes artigos científicos inéditos que vocês lerão a seguir, submetidos ao rigor do método científico. O nosso maior triunfo foi todo o processo de aprendizagem e de colaboração vivenciados no curso. A evolução em cada fórum de discussão, a troca de vivências nos encontros síncronos, o esforço nas leituras críticas e a resolução colaborativa de problemas moldaram uma nova consciência multidimensional nos participantes.

Essa jornada de transformação só foi possível graças à arquitetura do curso e à dedicação ímpar de nosso corpo docente, que conduziu e orientou os alunos por uma trilha interdisciplinar e progressiva.

O alicerce foi estabelecido pelo Prof. Dr. Wagner Silva de Araújo, na disciplina de *Estratégia e Governança*, que nos fez compreender o alinhamento indispensável entre o uso da tecnologia e os objetivos estratégicos institucionais.

Em seguida, a Prof^a. Me. Diana Leite Nunes dos Santos aprofundou esses conceitos na disciplina de *Governança de TIC*, capacitando

os alunos a avaliar, dirigir e monitorar a TI com base nas melhores práticas corporativas.

Como a tecnologia não opera no vácuo, o Prof. Me. Cleber de Araujo, em *Gestão de TIC, Processos e Pessoas*, trouxe a dimensão humana e operacional, fundamental para garantir a entrega de serviços contínuos e o desenvolvimento por competências.

A capacidade de tirar as ideias do papel e transformá-las em realidade foi lapidada pelo Prof. Esp. Weslei Gomes de Sousa, com a disciplina de *Gestão de Portfólio, Programas e Projetos*, vital para a priorização e gestão ágil no ambiente público.

A proteção do nosso maior ativo foi tratada com a máxima seriedade pelo Prof. Me. Marcelo Beltrão Caiado em *Gestão da Segurança da Informação*, despertando nos discentes o pensamento crítico sobre a gestão de riscos e a resiliência institucional.

Com os olhos voltados para o futuro, o Prof. Dr. Vinicius Maia Pacheco instigou a turma em *Novas Tecnologias e a Governança de TIC*, explorando desde a inteligência artificial e o governo digital até a inovação no serviço público.

Por fim, coroando o processo de formação de pesquisadores, a Prof^a. Me. Larissa Melo Bezerra de Oliveira conduziu a *Metodologia de Pesquisa Científica*. Foi ela quem instrumentalizou os alunos para organizar o conhecimento adquirido e transformarem suas reflexões e inquietações do cotidiano funcional em produção científica estruturada, incluindo um inédito *pitch* científico.

Ao longo desses meses, vimos profissionais se tornarem investidores de suas próprias rotinas, utilizando a teoria para questionar e aperfeiçoar a prática.

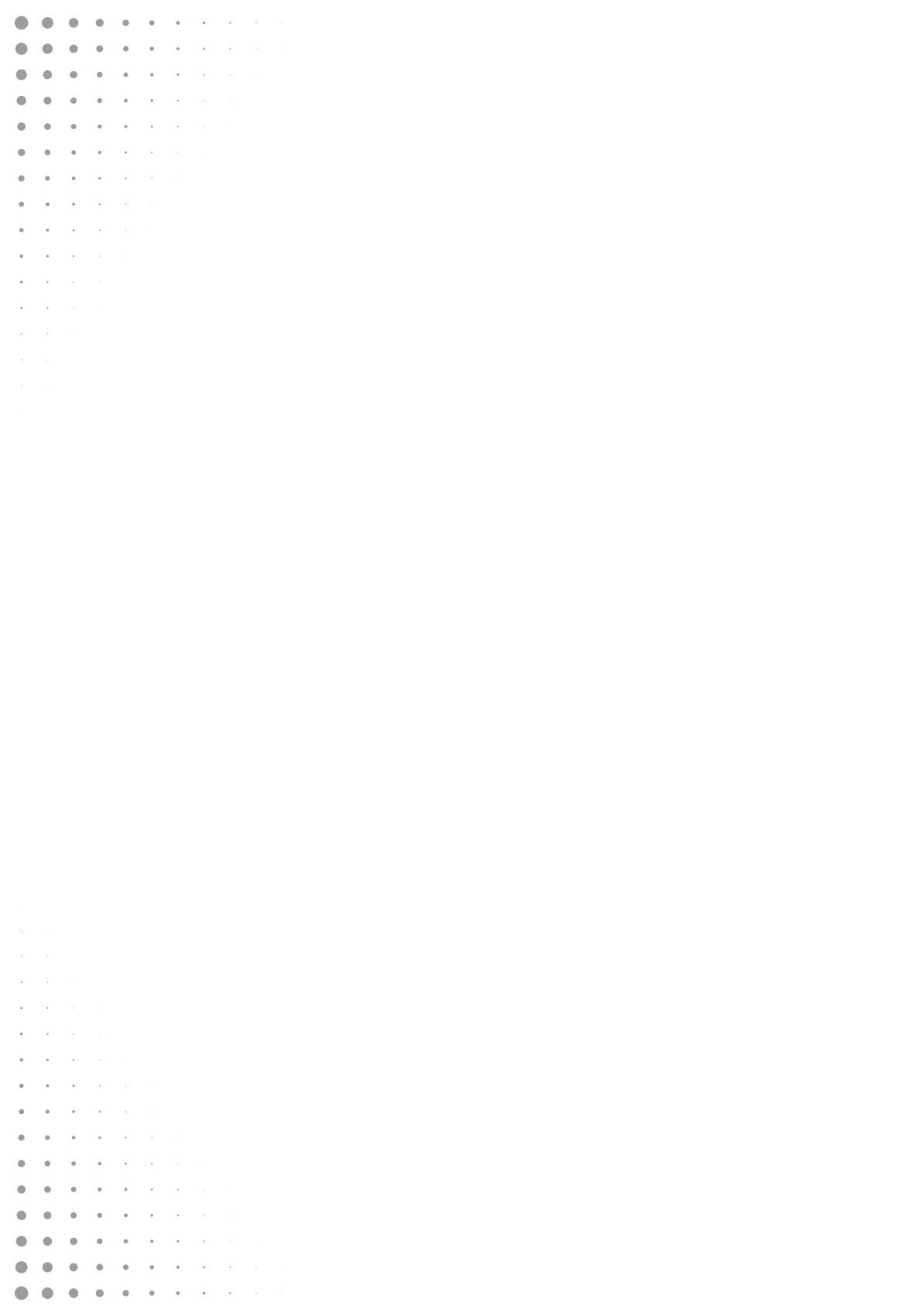
Os artigos apresentados nesta obra são o reflexo desse amadurecimento e versam sobre desafios reais das nossas instituições. No entanto, o legado duradouro deste curso é o grupo de servidores agora capacitados a pensar a tecnologia de forma estratégica, inovadora e interdisciplinar. O processo educacional que vivenciamos construiu alicerces que continuarão a gerar valor para o Ministério Público e para a sociedade muito além destas páginas.

Desejo a você uma excelente leitura e que estes trabalhos inspirem novas pesquisas e transformações no nosso MPU.

Mauro Cesar Sobrinho

Orientador Pedagógico do Curso de Especialização em
Governança de Tecnologia da Informação – Turma 2024-2025





Comunicação institucional nos Planos Diretores de Tecnologia da Informação (PDTIs): desigualdades no Ministério Público brasileiro

Institutional communication in Information Technology Master Plans (PDTIs): inequalities in the Brazilian Prosecution Service

DOI: https://doi.org/10.63601/978-65-88299-52-4_1

Alessandra Trindade dos Santos

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). MBA em Inteligência Artificial para Negócios pela Faculdade Exame. Graduada em Processos Gerenciais. Servidora do Ministério Público Federal (MPF).

Ronneddy Santos de Carvalho

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Gestão Pública pelo Instituto Federal do Maranhão (IFMA) e em Gestão de Pessoas na Era Digital pela Universidade Federal do Maranhão (UFMA). Bacharel em Direito e Administração de Empresas. Licenciado em História e Música. Servidor do Ministério Público do Estado do Maranhão (MPMA).

Resumo: Este estudo analisa como os Planos Diretores de Tecnologia da Informação (PDTIs) são comunicados pelos Ministérios Públicos no Brasil, com foco em linguagem, transparência e estratégias de divulgação. Foram convidadas 30 unidades – quatro ramos do MPU e 26 MPs estaduais. Houve nove respostas completas, e esses nove planos foram incluídos e analisados. Os resultados revelam forte desigualdade na forma de comunicação e acesso público, com documentos claros e bem estruturados em alguns casos e, em outros, linguagem técnica ou ausência de divulgação. A pesquisa classificou os planos em quatro níveis de maturidade comunicacional: Comunicacionais-Estratégicos, Informativos-Abertos,

Técnico-Operacionais e Omissos. Conclui-se que a comunicação não é um aspecto acessório, mas parte essencial da governança. Melhorar a clareza e a transparência fortalece a legitimidade institucional, amplia a confiança social e qualifica o controle público sobre decisões tecnológicas.

Palavras-chave: PDTI; comunicação institucional; transparência; governança; Ministério Público; acesso à informação.

Abstract: *This study analyzes how IT Master Plans (PDTIs) are communicated by Brazilian Prosecution Services, focusing on language, transparency, and dissemination strategies. Thirty units were invited, four federal branches and 26 state offices. There were nine complete answers, these nine plans were included and analyzed. The results show strong inequalities in communication and public access, with some plans being clear and well structured, while others are overly technical or not publicly available. The research classified the plans into four levels of communication maturity: Strategic-Communicational, Informative-Open, Technical-Operational, and Omissive. It concludes that communication is not accessory but a key part of governance. Improving clarity and transparency strengthens institutional legitimacy, increases public trust, and enhances social oversight of technological decisions.*

Keywords: *PDTI; institutional communication; transparency; governance; Public Prosecution Service; access to information.*

1 Introdução

A comunicação estratégica consolidou-se como prática indispensável na era digital, contexto em que instituições públicas precisam alinhar sua missão e cultura organizacional a um ambiente caracterizado pela hiperconectividade e pela velocidade dos fluxos informacionais. A chamada Quarta Revolução Industrial introduziu novas dinâmicas sociotécnicas, ampliando a complexidade da relação entre Estado e sociedade (Toledo, 2020). Nesse cenário, a comunicação institucional deixou de ocupar posição meramente instrumental e assumiu papel estratégico, contribuindo diretamente para a construção de legitimidade, transparência e confiança pública.

A literatura contemporânea entende a comunicação organizacional como fluxo intencional (Ruão, 2020) e projeto institucional orientado a necessidades sociais (Pérez, 2020), reforçando seu caráter estratégico. No setor público, isso se traduz na necessidade de integrar políticas tecnológicas aos objetivos constitucionais das organizações. Esse alinhamento não se restringe ao plano técnico: ele depende da forma como decisões e diretrizes são comunicadas, interpretadas e legitimadas socialmente.

É nesse contexto que os Planos Diretores de Tecnologia da Informação (PDTIs) ganham centralidade. Além de orientarem investimentos, priorizarem projetos e estabelecerem diretrizes de uso da tecnologia, os PDTIs materializam escolhas estratégicas que moldam a capacidade de inovação institucional e a qualidade do relacionamento com a sociedade. Mais do que documentos técnicos, são instrumentos de governança que expressam a vontade política e institucional – e, por isso, dependem diretamente de como são comunicados.

A interface entre governança e gestão de TI é apontada por diversos autores como um elo ainda frágil, embora fundamental para a efetividade organizacional. Juiz e Gomez (2021) destacam que essa interface permanece amplamente subexplorada, representando uma lacuna relevante na literatura sobre governança de TI. Segundo os autores, a comunicação eficaz atua como elo entre níveis estratégicos e operacionais, possibilitando que objetivos de governança sejam traduzidos em ações de gestão. Quando essa dimensão é negligenciada, surgem desalinhamentos institucionais, falhas de execução e perda de eficiência.

Dias, Silva e Dias (2021) reforçam essa fragilidade ao evidenciar que 47,7 % das organizações públicas brasileiras apresentam níveis incipientes de maturidade em governança de TI. No cenário internacional, Lnenicka *et al.* (2024) destacam que práticas de *benchmarking* em dados abertos favorecem a identificação de padrões e o aprendizado institucional coletivo, fortalecendo a transparência e a confiança pública. Considerando que os Ministérios Públicos estaduais e o MPU integram uma mesma estrutura institucional, a adoção de estratégias semelhantes de comparação e compartilhamento de práticas poderia reduzir assimetrias, gerar ganhos de escala e ampliar a legitimidade pública da instituição.

No caso brasileiro, a análise ganha contornos particulares no âmbito do Ministério Público, composto pelo MPU e pelos Ministérios Públicos estaduais. Trata-se de uma estrutura institucional descentralizada, autônoma e sem hierarquia entre eles, o que exige parâmetros comuns de transparência e linguagem para que os PDTIs cumpram seu papel estratégico. A forma como esses documentos são comunicados – sua clareza, acessibilidade, aderência normativa e visibilidade pública – revela diferentes níveis de maturidade comunicacional.

A literatura da área de comunicação organizacional contribui de maneira decisiva para compreender esse fenômeno. A comunicação

organizacional integrada (Kunsch, 2020) oferece uma perspectiva sistêmica, articulando dimensões estratégicas, culturais e administrativas. O modelo de alinhamento estratégico (Duarte, 2020) destaca a importância da coerência entre discurso institucional e práticas efetivas. Carrillo-Durán (2020) diferencia comunicação estratégica de marketing institucional, ressaltando que, no setor público, a primeira está ancorada em valores éticos e na responsabilidade com o interesse coletivo, enquanto o marketing busca fins promocionais e reputacionais. Nesse sentido, a elaboração de PDTIs acessíveis e visualmente claros deve ser entendida como *estratégia de comunicação institucional* – voltada à transparência e à construção de confiança –, e não como ação de marketing. Sob uma *perspectiva hermenêutica*, a comunicação estratégica é compreendida como um espaço de interpretação e co-construção de sentidos (Echenique; Untiveros, 2020), no qual linguagem, valores e práticas dialogam com seus públicos. Assim, mais do que transmitir informações, trata-se de promover entendimento mútuo e legitimidade institucional.

Esses fundamentos teóricos se conectam ao arcabouço normativo brasileiro, notadamente às Resoluções CNMP n. 102/2013 e n. 171/2017, que estabelecem diretrizes estruturantes para a atuação institucional dos Ministérios Públicos. Essas normas tratam de temas amplos, que envolvem planejamento estratégico, racionalização administrativa, uso de tecnologia da informação, transparência e controle social, constituindo pilares para a modernização e o fortalecimento da governança pública no âmbito ministerial.

A Resolução n. 102/2013 disciplina a gestão administrativa, orçamentária e financeira, promovendo a publicidade ativa de informações e o fortalecimento do planejamento institucional. Ao estabelecer regras sobre a divulgação de dados e atos administrativos, reforça a obrigação dos MPs de assegurar acesso à informação e mecanismos de controle social. Desse modo, a transparência deixa de ser uma ação isolada e assume caráter transversal, estruturando a gestão institucional e conectando comunicação, prestação de contas e legitimidade pública.

De forma complementar, a Resolução n. 171/2017 institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP), estabelecendo diretrizes para a governança e gestão de TI em todas as unidades, orientando práticas de planejamento, gestão de

riscos, segurança da informação, interoperabilidade e padronização institucional. Além disso, reforça a comunicação como instrumento de transparência, participação dos usuários e responsabilização institucional – aproximando a dimensão tecnológica da estratégia organizacional. Ao integrar planejamento, TI e comunicação institucional, ambas as resoluções criam condições normativas para a consolidação de práticas de governança pública, fortalecendo *accountability* e participação social. Nesse contexto, a dimensão comunicacional deixa de ser periférica e passa a se afirmar como vetor de integração entre estratégia, tecnologia e legitimidade institucional, alinhando-se também a referenciais internacionais amplamente adotados, como COBIT 2019, ITIL 4 e ISO/IEC 38500.

A pesquisa parte, assim, da seguinte questão: “De que modo a comunicação institucional dos Planos Diretores de Tecnologia da Informação, no âmbito do Ministério Público brasileiro, reflete critérios de linguagem, transparência e estratégias de divulgação?”

O objetivo geral é analisar a comunicação institucional dos PDTIs, com foco nesses três critérios centrais: linguagem, transparência e estratégias de divulgação. Os objetivos específicos consistem em: (I) mapear a disponibilidade pública dos documentos; (II) identificar padrões de linguagem; (III) avaliar a clareza e a acessibilidade das informações; e (IV) propor uma tipologia para classificar níveis de maturidade comunicacional nos Ministérios Públicos.

Ao articular governança de TI, comunicação institucional e *accountability* pública, este estudo contribui para preencher lacunas na literatura – tradicionalmente focada em aspectos técnicos – e oferecer subsídios práticos para fortalecer a transparência, a legitimidade e a efetividade do planejamento tecnológico no Ministério Público brasileiro.

2 Metodologia

A pesquisa adota uma abordagem descritivo-analítica, fundamentada em métodos qualitativos e quantitativos complementares, com foco na análise comunicacional e institucional dos Planos Diretores de Tecnologia da Informação do Ministério Público brasileiro. A estratégia metodológica foi concebida para permitir a observação comparativa entre diferentes unidades, integrando coleta empírica estruturada,

análise assistida por IA e interpretação crítica humana. Tal combinação metodológica alinha-se à recomendação de Juiz e Gomez (2021), que defendem a adoção de abordagens exploratórias para lidar com lacunas comunicacionais entre governança e gestão de TI.

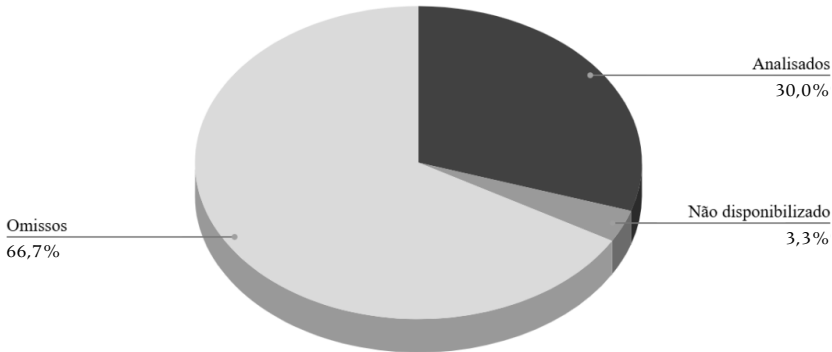
Para análise assistida, este estudo contou com o uso da ferramenta de IA generativa ChatGPT – versão GPT-5 – como apoio para tarefas de análise textual e revisão linguística, com validação crítica pelos autores.

2.1 Universo e amostragem

O universo da pesquisa compreende as 30 unidades que compõem o Ministério Público brasileiro – quatro ramos do Ministério Público da União e 26 Ministérios Públicos estaduais. O levantamento foi realizado entre 21 e 29 de agosto de 2025, por meio de buscas públicas em portais institucionais e canais de contato oficiais. Nesse período, foi confirmada a existência de 10 PDTIs, dos quais apenas 9 foram efetivamente analisados. O Ministério Público de Goiás (MP/GO) informou possuir o plano, acessível exclusivamente em ambiente de intranet, sem disponibilizar o arquivo, o que impossibilitou sua análise. Assim, o documento foi considerado no universo identificado, mas excluído da amostra efetivamente analisada.

Gráfico 1 – Distribuição dos PDTIs identificados no levantamento (n=30)

Figura 1 – Distribuição dos PDTIs Identificados no Levantamento (n=30)



Fonte: elaborado pelos autores com base na coleta de dados da pesquisa.

No MPU, todos os quatro ramos possuem PDTI vigente e acessível, tendo o Ministério Público Militar (MPM), o Ministério Público do Trabalho (MPT) e o Ministério Público do Distrito Federal e Territórios (MPDFT) disponibilizado os documentos em ambiente público. No caso do Ministério Público Federal (MPF), o acesso ao PDTI ocorreu por meio de ambiente interno (intranet), viabilizado pela condição de um dos autores como servidor do ramo, o que permitiu a análise integral do documento.

Entre os estados, Ministério Público do Acre (MP/AC), Ministério Público do Amapá (MP/AP), Ministério Público do Rio Grande do Norte (MP/RN) e Ministério Público de Santa Catarina (MP/SC) apresentaram versões publicamente acessíveis. Já o Ministério Público de Minas Gerais (MP/MG) teve seu PDTI obtido mediante contato por e-mail institucional, sem informação explícita sobre disponibilidade em ambiente público ou interno.

2.2 Procedimentos de coleta

A coleta ocorreu em três etapas principais: 1) busca ativa em portais institucionais, priorizando seções de transparência, tecnologia da informação e publicações oficiais; 2) verificações complementares em páginas setoriais e canais alternativos para localizar documentos não indexados em áreas principais; 3) contato direto via telefone e e-mail institucional, a fim de confirmar a existência de PDTIs ou obter endereços não disponíveis publicamente.

Foram enviados 22 e-mails às unidades sem referência pública aos PDTIs. Até o término da coleta, três haviam respondido. Além disso, 19 ouvidorias receberam comunicações formais informando o encerramento da fase de levantamento público, com solicitação para confirmação da existência de PDTI vigente ou previsão de elaboração. A Ouvidoria do MP/GO encaminhou a resposta com informação da existência do PDTI, disponível na intranet, sem enviar o arquivo, enquanto o MP/MT respondeu não dispor de plano, nem previsão de elaboração.

2.3 Estratégia de análise

A análise foi organizada em duas fases complementares, combinando agilidade técnica e profundidade interpretativa:

- FASE I – análise assistida por IA: aplicação de *prompts* padronizados para leitura sistemática dos PDTIs, identificação de padrões de linguagem, mapeamento de aderência normativa e avaliação preliminar da transparência. Essa etapa buscou padronizar a coleta de evidências e reduzir vieses, criando uma base metodológica comum que permita comparar, de forma consistente, tanto as práticas comunicacionais entre diferentes Ministérios Públicos quanto as características estruturais e comunicacionais dos próprios documentos analisados. Essa estratégia está alinhada à recomendação de Juiz e Gomez (2021), que destacam o valor da padronização para fortalecer a comparabilidade institucional e apoiar análises mais robustas.
- FASE II – revisão crítica humana: avaliação por dois perfis de análise – administrativo e jurídico – para refinar as notas e incluir interpretação contextual, considerando esforço de manutenção, clareza, conformidade normativa e horizonte temporal dos planos. Essa etapa dialoga com a proposta de integração metodológica de Juiz e Gomez (2021), segundo a qual a combinação de abordagens técnicas e interpretativas fortalece a governança.

Essa lógica metodológica também se apoia no estudo de Dias, Silva e Dias (2021), que associa níveis de maturidade em governança de TI ao desempenho institucional, recomendando métricas objetivas articuladas à análise interpretativa.

2.4 Critérios de avaliação

Com base no arcabouço normativo e nos referenciais conceituais, foram definidos quatro eixos de avaliação. Esses eixos articulam, de forma integrada, os critérios de linguagem, transparência e estratégias de divulgação, permitindo observar não apenas a aderência formal dos documentos, mas também a forma como comunicam e tornam públicas suas informações.

- Eixo 1 – Conformidade mínima: identifica elementos básicos de validade e estrutura documental (versão vigente, portaria de designação, vigência mínima e artefatos obrigatórios). Ao assegurar a existência desses elementos, este eixo cria as condições mínimas

para que as informações sejam divulgadas de forma clara e verificável (*transparência básica*).

- Eixo 2 – Aderência normativa: verifica o alinhamento aos instrumentos legais e normativos aplicáveis, incluindo Constituição Federal, Decreto-Lei n. 200/1967, Instrução Normativa SGD/ME n. 1/2019 e Resoluções CNMP n. 102/2013 e n. 171/2017, além da aprovação em instâncias de governança. Este eixo reforça a confiabilidade da informação divulgada, fortalecendo a transparência institucional.
- Eixo 3 – Clareza e transparência: examina diretamente os critérios de linguagem (clareza e inteligibilidade), acessibilidade da publicação e indicadores de acompanhamento, permitindo avaliar o potencial comunicacional dos PDTIs.
- Eixo 4 – Gestão e governança: observa o alinhamento ao planejamento estratégico institucional (PEI e PEN-MP), definição de metas, previsão de riscos, orçamento, infraestrutura e menções à sustentabilidade e inovação. Ao evidenciar a integração da comunicação com os mecanismos de governança, este eixo permite avaliar a estratégia de divulgação e articulação institucional.

Os critérios dialogam com conceitos de comunicação organizacional integrada (Kunsch, 2020), estratégia comunicacional (Duarte, 2020) e ética e transparência comunicacional (Carrillo-Durán, 2020), reforçando que a clareza de linguagem e a acessibilidade dos planos não são atributos acessórios, e sim condições essenciais de governança pública.

Além disso, autores como Félix (2020) e Bueno (2020) defendem a adoção de mapas estratégicos de comunicação, mecanismos de distinção entre informação institucional e publicidade e práticas sistemáticas de verificação – elementos que contribuíram para a definição dos parâmetros de análise. Também foi considerada a orientação do CNMP (2024) para excelência e transparência, bem como padrões internacionais como COBIT 2019, ITIL 4 e ISO/IEC 38500.

Importa salientar que, embora nem todos os normativos fossem citados expressamente nos documentos, a aderência foi avaliada de forma substantiva, ou seja, considerando evidências de alinhamento mesmo quando implícitas.

3 Resultados

A análise empreendida demonstra que os PDTIs cumprem papel essencial como instrumentos de governança e comunicação institucional no Ministério Público brasileiro. No entanto, também evidencia profunda heterogeneidade na forma como essas estratégias são estruturadas, comunicadas e disponibilizadas ao público, refletindo distintos níveis de maturidade comunicacional e institucional.

Durante o levantamento, foi confirmada a existência de dez PDTIs, distribuídos entre ramos do MPU e Ministérios Públicos estaduais. Entretanto, apenas nove foram efetivamente analisados, uma vez que o Ministério Público de Goiás (MP/GO) informou possuir PDTI exclusivamente em intranet, sem acesso público externo, inviabilizando sua análise.

Os Ministérios Públicos do Rio Grande do Sul (MP/RS), do Ceará (MP/CE) e de Mato Grosso (MP/MT) informaram formalmente não possuir PDTI elaborado – os dois primeiros por e-mail institucional e o último por meio da Ouvidoria. Outros dezessete Ministérios Públicos estaduais não apresentaram documentos localizados nem forneceram respostas aos contatos para o levantamento. Assim, os vinte órgãos foram classificados, para efeito desta pesquisa, como “omissos”, categoria que não avalia o conteúdo técnico ou a qualidade do planejamento, mas indica exclusivamente a ausência de disponibilização pública ou direta – condição que inviabilizou a aplicação dos eixos de análise.

A análise foi organizada em duas etapas complementares: fase I, com aplicação de *prompts* padronizados com apoio de inteligência artificial, e fase II, realizada por avaliadores humanos com vieses administrativo e jurídico. Essa combinação metodológica assegurou comparabilidade entre documentos distintos e ampliou a leitura sobre linguagem, esforço administrativo de manutenção, aderência normativa e horizonte temporal.

Os resultados apresentados a seguir foram consolidados com base nos quatro eixos de análise definidos no Plano de Avaliação: Conformidade Mínima, Aderência Normativa, Clareza e Transparência, e Gestão e Governança.

Ademais, a dificuldade de acesso e a ausência de repositórios centralizados indicam padrões comunicacionais pouco uniformes entre as unidades, evidenciando lacunas de transparência e assimetria institucional.

3.1 Conformidade Mínima

De forma geral, os documentos analisados atendem aos requisitos mínimos de conformidade previstos na Resolução CNMP n. 171/2017: vigência mínima de dois anos, portaria de designação de equipe e contemplação dos principais artefatos (diagnóstico, metas, ações, orçamento e riscos).

Destacam-se nesse aspecto os PDTIs do Ministério Público Federal, Ministério Público Militar, Ministério Público do Trabalho e Ministério Público de Minas Gerais, que apresentam estruturas robustas e maior formalização processual.

Em contraponto, documentos como os do Ministério Público de Santa Catarina e do Ministério Público do Distrito Federal e Territórios estabelecem vigência inferior ao horizonte temporal mínimo estabelecido na Resolução n. 171/2017. Essa escolha fragiliza a previsibilidade administrativa e reduz a estabilidade das políticas de tecnologia da informação, dificultando a gestão de contratos e projetos de médio prazo.

Outro ponto que merece atenção diz respeito ao detalhamento da gestão de pessoas, frequentemente mencionado de forma superficial ou secundária. Apesar de estar presente na maioria dos documentos, a dimensão de pessoal raramente aparece como eixo estruturante do planejamento, excetuando-se casos como MPM e MP/MG, em que há mapeamento consistente de força de trabalho, necessidades futuras e estratégias de capacitação.

3.2 Aderência Normativa

Os resultados mostram que todos os PDTIs analisados possuem algum grau de alinhamento às normas vigentes, ainda que com níveis diferentes de explicitação. A Resolução CNMP n. 171/2017 aparece de forma expressa na maioria dos documentos e orienta a estrutura de governança e planejamento estratégico de TI. Já a Resolução CNMP n. 102/2013, que trata das contratações de TI, recebe menos destaque – sendo muitas vezes incorporada de forma implícita ou indireta.

Os documentos com maior densidade normativa – MPF, MPM, MPT e MP/MG – articulam claramente os dispositivos normativos

ao planejamento estratégico e ao portfólio de ações, estabelecendo vínculos diretos com o Plano Estratégico Institucional (PEI) e o Plano Estratégico Nacional do MP (PEN-MP). Já os planos do MP/SC e do MPDFT apresentam menor profundidade normativa, com menções superficiais ou ausência de vinculação explícita a normativos estruturantes, o que limita a rastreabilidade jurídica e reduz a robustez institucional desses instrumentos.

Outro ponto relevante diz respeito à referência a marcos legais e *frameworks* complementares. Documentos como os do MP/AP e MPF incorporam menções a legislações contemporâneas, como a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação, bem como a *frameworks* internacionais como COBIT 2019, ITIL 4 e ISO/IEC 38500, ampliando sua base normativa e reforçando sua aderência a padrões de governança consolidados.

3.3 Clareza e Transparência

Em termos comunicacionais, observou-se que todos os PDTIs analisados estão disponíveis publicamente, atendendo ao princípio da publicidade previsto na Resolução CNMP n. 171/2017. No entanto, a forma como essas informações são apresentadas varia consideravelmente entre os Ministérios Públicos, refletindo diferentes níveis de maturidade comunicacional. De modo geral, prevalece uma linguagem técnica, direcionada a públicos internos especializados, o que assegura precisão, mas limita a inteligibilidade para públicos externos – dimensão essencial para a transparência ativa.

Os planos com maior investimento em recursos gráficos e estruturais – como os do MPF, MPM, MPT e MP/SC – apresentaram mapas estratégicos, quadros, indicadores e tabelas que tornam a leitura mais fluida para públicos administrativos e de governança. Essas estratégias visuais ampliam a transparência e reforçam a legitimidade institucional, ainda que impliquem maior esforço de manutenção ao longo dos ciclos de revisão.

Em um segundo grupo, formado por MP/MG, MP/RN, MP/AC e MP/AP, identificou-se um equilíbrio entre estrutura técnica e clareza administrativa: apesar da predominância de texto corrido, há

organização lógica e elementos que favorecem compreensão interna e operacionalização. Essa escolha tende a reduzir o esforço de atualização, mas limita o potencial de engajamento externo.

Por fim, no caso do MPDFT, verificou-se uma linguagem mais densa e tecnicista, com menor investimento em recursos de apoio à leitura. Embora o plano apresente boa rastreabilidade formal, seu alcance comunicacional é restrito, reforçando a percepção de que a publicação cumpre mais uma função normativa do que estratégica.

Nenhum dos nove documentos, entretanto, alcança plenamente o padrão de linguagem cidadã proposto por Kunsch (2020) e Duarte (2020), nem a dimensão ética e estratégica destacada por Carrillo-Durán (2020). A comunicação institucional ainda é tratada predominantemente como etapa instrumental de publicação, e não como elemento estruturante de governança, o que limita a inteligibilidade, a aproximação com públicos diversos e o potencial de *accountability*.

3.4 Gestão e Governança

A análise revelou diferenças significativas no grau de maturidade em gestão e governança entre os PDTIs. Documentos como os do MPF, MPM, MPT e MP/MG apresentam maior sofisticação estratégica, com metas mensuráveis, integração com PEI e PEN, portfólios detalhados, indicadores de execução e planos de acompanhamento institucional. Essa estrutura dialoga com práticas recomendadas por *frameworks* internacionais como COBIT 2019, ITIL 4 e ISO/IEC 38500, além de atender a dispositivos normativos nacionais.

Já planos como os do MP/AC e do MP/AP, embora tecnicamente adequados, apresentam menor detalhamento de riscos e de gestão de pessoas, permanecendo mais próximos de uma lógica operacional. Por sua vez, os documentos do MP/SC e do MPDFT mostram fragilidades tanto na temporalidade quanto na articulação estratégica, apesar de cumprirem formalmente requisitos mínimos.

Um aspecto transversal observado é a ausência quase total de referências à sustentabilidade, seja ambiental ou digital. No contexto deste estudo, a sustentabilidade digital é compreendida como a capacidade de planejar, operar e evoluir ecossistemas digitais de forma responsável,

contínua e resiliente, equilibrando eficiência tecnológica, responsabilidade social e impacto ambiental. Trata-se de uma visão que associa planejamento tecnológico a estratégias de longo prazo, interoperabilidade, redução de riscos, transparência ativa e criação de valor público (Lnenicka *et al.*, 2024; Juiz; Gomez, 2021).

Essa dimensão tem ganhado destaque em agendas internacionais de governança digital por seu papel estratégico em garantir continuidade institucional, reduzir assimetrias tecnológicas e evitar a obsolescência acelerada de sistemas e dados. A ausência dessa perspectiva nos PDTIs analisados indica que, embora a governança de TI esteja formalmente institucionalizada, práticas associadas à perenidade, interoperabilidade e impacto social ainda não foram plenamente incorporadas aos instrumentos de planejamento.

3.5 Tipologia de maturidade comunicacional

Com base nos critérios definidos nesta pesquisa – linguagem, transparência e estratégias de divulgação –, foi possível classificar os PDTIs analisados em quatro níveis de maturidade comunicacional: Comunicacionais-Estratégicos, Informativos-Abertos, Técnico-Operacionais e Omissos.

Tabela 1 – Distribuição dos PDTIs por tipologia de maturidade comunicacional

TIPOLOGIA DE MATURIDADE COMUNICACIONAL	Nº DE MPs	UNIDADES IDENTIFICADAS
Comunicacionais-Estratégicos	4	MPF, MPM, MPT, MP/MG
Informativos-Abertos	3	MP/AC, MP/AP, MP/RN
Técnico-Operacionais	2	MP/SC, MPDFT
Omissos	21	MP/GO, MP/CE, MP/RS, MP/MT + 17 MPs estaduais sem resposta

Fonte: elaborada pelos autores.

Essa tipologia foi construída no âmbito desta pesquisa, a partir da análise empírica dos documentos, e ancorada em referenciais teóricos consolidados sobre comunicação estratégica, integração institucional e

maturidade em governança de TI. Félix (2020) e Duarte (2020) destacam a importância da clareza de propósitos e da coerência entre discurso e ação institucional como elementos centrais da maturidade comunicacional. Juiz e Gomez (2021) ressaltam que a integração entre governança e comunicação fortalece padrões comparáveis entre organizações públicas, enquanto Dias, Silva e Dias (2021) discutem agrupamentos de maturidade em governança de TI como instrumento para análises comparativas.

Assim, a classificação proposta não é uma reprodução de modelos existentes, mas uma formulação original inspirada nesses referenciais, voltada a capturar como diferentes Ministérios Públicos estruturam – ou não estruturam – a comunicação institucional de seus PDTIs. Cada nível representa um conjunto de práticas e padrões comunicacionais que permitem compreender a posição relativa das instituições no espectro de maturidade comunicacional.

Comunicacionais-Estratégicos

- Ministério Público Federal (MPF)
- Ministério Público Militar (MPM)
- Ministério Público do Trabalho (MPT)
- Ministério Público de Minas Gerais (MP/MG)

Caracterizam-se por forte aderência normativa, uso consistente de referências estratégicas, presença de mapas, tabelas e indicadores claros, além de publicação acessível e estrutura comunicacional mais madura.

Informativos-Abertos

- Ministério Público do Acre (MP/AC)
- Ministério Público do Amapá (MP/AP)
- Ministério Público do Rio Grande do Norte (MP/RN)

Apresentam estrutura técnica consistente e disponibilização pública dos documentos, com linguagem relativamente clara. Ainda assim, há limitações na dimensão estratégica e na comunicação voltada à sociedade, mantendo-se mais próximos de um modelo técnico do que comunicacional.

Técnico-Operacionais

- Ministério Público de Santa Catarina (MP/SC)
- Ministério Público do Distrito Federal e Territórios (MPDFT)

Correspondem a planos tecnicamente corretos e formalmente publicados, mas com linguagem excessivamente especializada, temporalidade reduzida e baixa integração estratégica, dificultando a inteligibilidade para públicos não técnicos.

Omissos

- Ministério Público de Goiás (MP/GO) – informou possuir PDTI, porém restrito à intranet, impossibilitando acesso e análise externa. Não disponibilizou o arquivo na resposta à Ouvidoria.
- Ministério Público do Ceará (MP/CE) – informou possuir PDTI em atualização.
- Ministério Público do Rio Grande do Sul (MP/RS) – informou não possuir PDTI, com previsão de elaboração.
- Ministério Público do Mato Grosso (MP/MT) – informou não possuir PDTI, nem previsão de elaboração.
- Demais dezesseis Ministérios Públicos estaduais que não apresentaram resposta nem disponibilização pública ou direta no período da coleta:
 - Ministério Público do Amazonas (MP/AM)
 - Ministério Público da Bahia (MP/BA)
 - Ministério Público do Espírito Santo (MP/ES)
 - Ministério Público do Maranhão (MP/MA)
 - Ministério Público do Mato Grosso do Sul (MP/MS)
 - Ministério Público do Pará (MP/PA)
 - Ministério Público da Paraíba (MP/PB)
 - Ministério Público do Paraná (MP/PR)
 - Ministério Público de Pernambuco (MP/PE)

- Ministério Público do Piauí (MP/PI)
- Ministério Público do Rio de Janeiro (MP/RJ)
- Ministério Público de Rondônia (MP/RO)
- Ministério Público de Roraima (MP/RR)
- Ministério Público de São Paulo (MP/SP)
- Ministério Público de Sergipe (MP/SE)
- Ministério Público do Tocantins (MP/TO)

Essa classificação não implica qualquer juízo de valor sobre a existência ou a qualidade dos processos de governança e gestão de TI nessas instituições, mas reflete exclusivamente a ausência de disponibilização pública dos PDTIs, objeto de análise desta pesquisa. Essa condição impediu a aplicação dos eixos de análise e inviabilizou qualquer classificação de maturidade comunicacional além da constatação da omissão.

Cabe destacar que, embora o MPF esteja classificado como Comunicacional-Estratégico, o acesso ao seu PDTI também se deu por meio de ambiente de intranet institucional, viabilizado pelo fato de um dos autores pertencer ao quadro funcional do ramo. Isso reforça que, mesmo entre instituições com alto nível de maturidade comunicacional, ainda há barreiras de acesso público que impactam a transparência plena.

Essa particularidade não altera a classificação do MPF, pois o conteúdo foi efetivamente analisado, mas ilustra com clareza que a disponibilidade pública ainda não é uniforme no ecossistema do Ministério Público, inclusive nos órgãos com estruturas mais consolidadas.

Em números absolutos, 20 dos 26 Ministérios Públicos estaduais (76,9%) não disponibilizaram PDTI público ou não responderam ao levantamento, sendo classificados como omissos. Em contraste, os quatro ramos do MPU (100%) tiveram seus PDTIs identificados e analisados. Esse dado evidencia uma assimetria comunicacional significativa entre as esferas federais e estaduais do Ministério Público brasileiro. A falta de acesso público aos PDTIs limita não apenas a transparência e o controle social, mas também a comparabilidade técnica e a indução de boas práticas entre unidades.

4 Discussão e implicações

Os resultados obtidos evidenciam forte heterogeneidade nas práticas comunicacionais dos PDTIs do Ministério Público brasileiro, tanto na forma de disponibilização quanto no conteúdo, linguagem e horizonte temporal. Essa diversidade reflete diferentes níveis de maturidade comunicacional e institucional, confirmando tendências já observadas na literatura especializada sobre governança de TI no setor público.

Além da variação estrutural e comunicacional entre os documentos analisados, também se observam assimetrias significativas no acesso público aos planos. Todos os quatro ramos do MPU possuem PDTI vigente, mas apenas três deles – MPM, MPT e MPDFT – disponibilizam os documentos em ambiente público. O PDTI do MPF foi acessado por meio de intranet, pelo motivo já mencionado.

No caso dos MPs estaduais, MP/AC, MP/AP, MP/RN e MP/SC apresentaram versões publicamente acessíveis, enquanto o PDTI do MP/MG foi obtido diretamente, via contato por e-mail institucional, sem informação explícita sobre sua disponibilização.

Essa diferença na forma de acesso aos documentos já constitui, por si só, um marcador de maturidade comunicacional, pois impacta diretamente a transparência ativa e a *accountability* institucional.

4.1 Assimetria comunicacional e governança de TI

As diferenças entre planos densos e normativamente aderentes – como os do MPM, MP/MG e MPF – e planos mais enxutos e operacionais – como os do MP/AC, MP/AP e MP/SC – refletem padrões assimétricos de capacidade institucional e estratégias comunicacionais. Além da densidade técnica e da estrutura normativa, a própria forma de acesso aos documentos revela camadas distintas de transparência: enquanto alguns ramos oferecem acesso direto e público, outros dependem de caminhos internos ou solicitações formais.

Esse fenômeno dialoga diretamente com Juiz e Gomez (2021), que apontam a interface comunicação-governança de TI como um dos elos mais frágeis nos mecanismos de governança organizacional. A ausência

de padrões consolidados de linguagem, estrutura e transparência compromete a comparabilidade entre planos e, sobretudo, a capacidade de engajamento com públicos internos e externos.

Dias, Silva e Dias (2021) reforçam que a baixa maturidade em governança de TI afeta a qualidade da gestão pública, gerando desigualdades de desempenho. Essas assimetrias ficam evidentes, por exemplo, quando planos tecnicamente robustos apresentam linguagem excessivamente técnica e de difícil compreensão (casos do MPF e MPT), enquanto outros oferecem acesso facilitado, mas com fragilidades estruturais e normativas (como MP/SC).

4.2 Comunicação instrumental vs. estratégica

A análise dos padrões de divulgação dos PDTIs também evidencia a prevalência de práticas comunicacionais instrumentais. Em muitas unidades, a publicação ocorre apenas para cumprimento formal de obrigações legais ou normativas, sem preocupação com clareza, atratividade ou inteligibilidade para diferentes públicos.

Echenique e Untiveros (2020) descrevem essa postura como comunicação instrumental – centrada na transmissão unilateral de informações –, contrastando com a comunicação estratégica, que pressupõe diálogo, interpretação e construção compartilhada de sentidos.

Portales e Sousa (2020) destacam que a confiança institucional é construída justamente nesses espaços de relação comunicativa e transparência ativa. Juiz e Gomez (2021) complementam que barreiras comunicacionais reduzem *accountability* e transparência, enfraquecendo a legitimidade institucional.

4.3 Maturidade comunicacional e legitimidade institucional

A tipologia proposta – Omissos, Técnico-Operacionais, Informativos-Abertos e Comunicacionais-Estratégicos – ajuda a diferenciar graus de maturidade comunicacional. Essa classificação não apenas reflete o estágio técnico-normativo dos documentos, mas indica a capacidade das instituições de transformar planos em instrumentos efetivos de governança estratégica.

Félix (2020) e Duarte (2020) reforçam que a clareza de propósitos, a adoção de mapas estratégicos e a coerência entre discurso e ação institucional são determinantes para elevar o grau de maturidade comunicacional. Juiz e Gomez (2021) complementam que a integração entre governança e comunicação reduz assimetrias e amplia a efetividade organizacional.

Essa leitura se alinha também ao diagnóstico de Dias, Silva e Dias (2021), segundo o qual a maturidade em governança de TI apresenta *clusters* de desempenho institucional, permitindo agrupar organizações com comportamentos semelhantes. No caso dos PDTIs do MP brasileiro, a presença desses padrões híbridos – documentos com pontos fortes e fragilidades simultâneas – confirma a coexistência de estágios desiguais de desenvolvimento institucional.

4.4 Comunicação e *accountability*

No setor público, a comunicação institucional tem papel decisivo para garantir *accountability*, transparência e legitimidade democrática. Quando tratada apenas como etapa de publicação ou formalização, essa dimensão perde sua capacidade de gerar confiança e permitir controle social.

Kerche, Oliveira e Couto (2020) mostram que, mesmo em estruturas com forte autonomia, como o Ministério Público, os mecanismos de *accountability* são tensionados pela assimetria entre autonomia e responsabilização, tornando a comunicação estratégica ainda mais relevante.

A literatura reforça que comunicação estratégica não é apenas transmissão de dados, mas mediação política e institucional. Echenique e Untiveros (2020) e Portales e Sousa (2020) indicam que a legitimidade decorre da construção de confiança por meio de mensagens claras, compreensíveis e abertas ao escrutínio público. No caso dos PDTIs, planos com linguagem acessível, boa navegabilidade e horizonte temporal consistente tendem a reforçar a credibilidade institucional.

4.5 Implicações para a governança

Ao articular esses achados, torna-se evidente que a maturidade comunicacional dos PDTIs não depende apenas de aderência normativa,

mas também da capacidade das instituições de dialogar com públicos diversos. Planos com alta densidade técnica, mas baixa clareza, limitam a apropriação interna e externa dos conteúdos. Já planos comunicacionais-estratégicos combinam consistência técnica, transparência e linguagem acessível, ampliando a legitimidade e fortalecendo a governança de TI.

Esse entendimento converge com Juiz e Gomez (2021), que destacam a comunicação como elo estrutural entre gestão e governança, e com Echenique e Untiveros (2020), que ressaltam a necessidade de práticas comunicacionais orientadas à interpretação coletiva.

Assim, a comunicação deixa de ser mero suporte e passa a ser componente estruturante da governança pública.

4.6 Síntese dos principais resultados

A análise empreendida demonstra que os Planos Diretores de Tecnologia da Informação cumprem papel essencial como instrumentos de governança e comunicação institucional no Ministério Público brasileiro. No entanto, também evidencia profunda heterogeneidade na forma como essas estratégias são estruturadas, comunicadas e disponibilizadas ao público, refletindo distintos níveis de maturidade comunicacional e institucional.

A pesquisa analisou a comunicação institucional dos PDTIs a partir dos critérios de linguagem, transparência e estratégias de divulgação, permitindo mapear a disponibilidade pública dos documentos, identificar padrões de linguagem, avaliar a clareza comunicacional e propor uma tipologia de maturidade comunicacional nos Ministérios Públicos. Cada uma das etapas da investigação foi desenhada para atender a esses propósitos – e os resultados demonstram que todos foram integralmente cumpridos ao longo da análise.

Os achados confirmam que a comunicação não pode ser tratada apenas como etapa instrumental de publicação: ela condiciona a legitimidade, a transparência e a efetividade dos planos. Quando bem estruturada – com linguagem clara, estratégias de divulgação consistentes e aderência normativa –, a comunicação institucional amplia a confiança pública e reforça a governança de TI (Juiz; Gomez, 2021; Echenique; Untiveros, 2020). O estudo revelou quatro padrões

distintos de maturidade comunicacional nos PDTIs – Omissos, Técnico-Operacionais, Informativos-Abertos e Comunicacionais-Estratégicos – que refletem diferentes capacidades institucionais de integrar governança e comunicação. Enquanto alguns planos apresentam completude normativa, mas barreiras linguísticas e técnicas (como MPF e MPT), outros oferecem linguagem acessível e estrutura simplificada, porém com lacunas estratégicas (como MP/SC e MP/AP). A Tabela 2 sintetiza os principais achados da pesquisa, organizando-os por tipologia de maturidade comunicacional, número de MPs, características observadas e forma de acesso aos PDTIs.

Tabela 2 – Síntese dos resultados por tipologia de maturidade comunicacional

TIPOLOGIA	Nº DE MPs	PRINCIPAIS CARACTERÍSTICAS	EXEMPLOS DE MPs	FORMA DE ACESSO PREDOMINANTE
Comunicacionais-Estratégicos	4	Alta aderência normativa, linguagem estruturada, presença de mapas/tabelas, comunicação estratégica madura	MPF MPM MPT MP/MG	Público (3) / Intranet (1)
Informativos-Abertos	3	Disponibilização pública, linguagem clara, estrutura técnica consistente, menor densidade estratégica	MP/AC MP/AP MP/RN	Público
Técnico-Operacionais	2	Linguagem técnica, pouca integração estratégica, temporalidade reduzida, acesso restrito ou parcial	MP/SC MPDFT	Público
Omissos	21	Ausência de disponibilização pública, impossibilidade de análise pelos eixos propostos	MP/GO MP/CE MP/RS MP/MT + 17 outros	Inexistente

Fonte: elaborada pelos autores.

A identificação dessas tipologias e dos padrões de linguagem e transparência corresponde diretamente aos objetivos II e IV da pesquisa, evidenciando como as práticas comunicacionais se distribuem entre os diferentes Ministérios Públicos.

Essa coexistência de forças e fragilidades também foi observada por Balbinot, Araújo e Luft (2021), que identificaram avanços e deficiências estruturais no PETI do MPF. O fenômeno reforça as análises de Juiz e Gomez (2021) e de Dias, Silva e Dias (2021), que associam maturidade comunicacional e desempenho institucional.

Além disso, o mapeamento realizado – contemplando trinta unidades e nove documentos efetivamente analisados – cumpre o primeiro objetivo específico (I), ao revelar fortes assimetrias no acesso público aos PDTIs e distintos graus de transparência ativa.

4.7 Implicações para a governança pública

No campo da governança de TI, os resultados reforçam que a maturidade institucional depende tanto da aderência normativa quanto da clareza comunicacional. Como destacam Félix (2020) e Duarte (2020), a adoção de mapas estratégicos de comunicação, indicadores objetivos e coerência entre discurso e ação são determinantes para consolidar práticas de governança mais consistentes.

Planos comunicacionais-estratégicos – como os do MPM e do MP/MG – confirmam esse potencial: combinaram completude normativa com transparência ativa, obtendo melhor desempenho no ranking consolidado. Por outro lado, planos tecnicamente densos, mas pouco acessíveis, como os do MPF e do MPT, ilustram os limites de uma comunicação restrita a públicos especializados. Essa assimetria reforça a tese de Juiz e Gomez (2021): a comunicação desempenha papel estruturante, na interface entre gestão e governança, e não meramente complementar.

Esse quadro se articula com a literatura sobre *accountability* no Ministério Público. Como argumentam Kerche, Oliveira e Couto (2020), a autonomia institucional ampliada do MP exige contrapesos baseados em transparência ativa. Em um ambiente em que os mecanismos de controle externo são limitados, a comunicação institucional se torna peça-chave para legitimar a autonomia e sustentar a confiança pública.

Ao evidenciar a importância da inteligibilidade e da acessibilidade da linguagem, esta seção responde diretamente ao objetivo III da pesquisa, reforçando que comunicação clara e estratégica é vetor de governança.

4.8 Recomendações práticas

Com base nos achados empíricos e no referencial teórico, recomenda-se:

- Institucionalizar mapas estratégicos de comunicação, com indicadores claros de acompanhamento e alinhamento à estratégia organizacional (Félix, 2020). O PDTI do MPM destaca-se como exemplo de estrutura comunicacional consistente, articulada a objetivos estratégicos.
- Reforçar propósitos éticos e de responsabilidade pública, fortalecendo a legitimidade institucional (Dantas; Abreu, 2020). O MP/MG apresentou boas práticas nesse sentido, conciliando clareza e robustez normativa.
- Adotar mecanismos sistemáticos de verificação contra desinformação, ampliando a confiança pública e a confiabilidade institucional (Moreira, 2020).
- Aprimorar padrões de transparência e divulgação, tomando como referência as diretrizes da publicação “Governança para Líderes” do Conselho Nacional do Ministério Público (CNMP, 2024), que enfatiza transparência ativa, linguagem acessível e responsabilização institucional. Casos como os PDTIs do MP/AC, MP/AP e MP/RN demonstram que a disponibilização pública clara e objetiva é factível mesmo em planos mais enxutos.
- Integrar boas práticas nacionais e internacionais de governança, alinhando-se a frameworks consolidados como COBIT 2019, ITIL 4 e ISO/IEC 38500, ampliando a maturidade institucional.

Essas recomendações associam fundamentos teóricos, diretrizes normativas e boas práticas já observadas nos PDTIs analisados, permitindo que outras unidades tenham referências concretas e adaptáveis ao seu contexto institucional.

4.9 Limitações e perspectivas futuras

O recorte empírico incluiu trinta unidades, mas apenas nove PDTIs foram efetivamente analisados – o que limita a generalização dos achados, embora revele padrões consistentes de heterogeneidade institucional. Além disso, como os PDTIs são documentos formais, não refletem integralmente processos internos de decisão ou dificuldades de implementação, restringindo a análise à dimensão comunicacional e normativa.

Outra limitação refere-se ao uso combinado de inteligência artificial e avaliação humana: embora a metodologia híbrida tenha garantido padronização e profundidade, não elimina nuances interpretativas. Ainda assim, ao conjugar agilidade técnica e análise crítica, permitiu identificar padrões comunicacionais comparáveis entre as unidades.

Como perspectivas futuras, recomenda-se ampliar a base empírica, investigar a relação entre comunicação e execução prática e acompanhar a evolução dos PDTIs ao longo de diferentes ciclos de planejamento – permitindo medir, inclusive, impactos em transparência e *accountability*.

5 Conclusão

Ao integrar governança de TI, comunicação institucional e *accountability* pública, este estudo reafirma que a maturidade comunicacional é elemento estruturante da governança contemporânea. A clareza, a transparência e a coerência entre discurso e prática fortalecem não apenas os PDTIs, mas também a credibilidade e a legitimidade das instituições públicas.

Conclui-se que a comunicação institucional dos PDTIs reflete níveis desiguais de maturidade comunicacional no Ministério Público brasileiro, variando desde modelos estratégicos e transparentes até práticas predominantemente instrumentais e pouco acessíveis. Os objetivos da pesquisa foram alcançados ao permitir o mapeamento sistemático da disponibilidade dos documentos, a identificação de padrões de linguagem, a avaliação da clareza comunicacional e da transparência ativa, bem como a proposição de uma tipologia original de maturidade comunicacional.

Os resultados oferecem uma leitura diagnóstica do cenário atual e contribuem metodologicamente para futuras pesquisas sobre governança de TI, comunicação institucional e *accountability* pública.

No Ministério Público, a assimetria comunicacional observada nos PDTIs reflete e reforça desigualdades institucionais mais amplas. Em um cenário de elevada autonomia institucional, a comunicação e a transparência ativa assumem papel relevante como mecanismos de equilíbrio democrático. PDTIs acessíveis, inteligíveis e bem estruturados tornam-se instrumentos de *accountability* substantiva, permitindo que sociedade e órgãos de controle compreendam, acompanhem e questionem as decisões tecnológicas e estratégicas.

Assim, a comunicação estratégica deixa de ser mero suporte e se torna vetor de legitimidade democrática. Elevar a maturidade comunicacional dos PDTIs significa também elevar a maturidade democrática das instituições: não apenas informando, mas permitindo participação, escrutínio e responsabilização. Desse modo, o estudo contribui para ampliar a compreensão sobre como governança de TI, comunicação institucional e *accountability* se entrelaçam, e para sinalizar caminhos concretos para fortalecer a transparência e a confiança pública no Ministério Público brasileiro.

Referências

BALBINOT, Jeysonn Isaac; ARAÚJO, Cleber de; LUFT, Renato. Análise dos resultados estratégicos de Tecnologia da Informação e Comunicação no Ministério Público Federal decorrentes do Projeto de Modernização da Gestão Administrativa no período 2011-2020. *In: ENCONTRO DOS PROGRAMAS DE PÓS-GRADUAÇÃO PROFISSIONAIS EM ADMINISTRAÇÃO – EMPRAD*, 2021, São Paulo. **Anais [...]**. São Paulo: FEA/USP, 22-23 nov. 2021. Disponível em: <https://tinyurl.com/caam6yaz>. Acesso em: 29 ago. 2025.

BUENO, Wilson da Costa. O jornalismo patrocinado como estratégia nos negócios: rupturas e tensões no processo de comunicação de marca. *In: FÉLIX, Joana d’Arc Bicalho (org.). Comunicação estratégica e integrada: a visão de 23 renomados autores em 5 países*. Brasília: Rede Integrada, 2020. p. 366-389.

CARRILLO-DURÁN, María-Victoria. La comunicación estratégica ¿qué es y para qué sirve? *In: FÉLIX, Joana d’Arc Bicalho (org.). Comunicação*

estratégica e integrada: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 67-83.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Governança para líderes dos Ministérios Públicos:** um referencial para a excelência, transparência de resultados e construção de confiança. Brasília: CNMP, 2024.

DANTAS, Edmundo Brandão; ABREU, Maria Fernanda Dangelo Valentim. As estratégias de comunicação de marcas que apoiam causas e possuem um propósito. *In:* FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada:** a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 437-479.

DIAS, Claudia Marcia Vasconcelos e Mello; SILVA, Jorge Ferreira da; DIAS, Augusto Cesar Arenaro e Mello. Impacto da governança e gestão de TI nos resultados das organizações brasileiras. **Iberoamerican Journal of Strategic Management (IJSM)**, [s. l.], v. 20, p. 1-30, 2021. DOI: <https://doi.org/10.5585/riac.v20i1.17117>.

DUARTE, Jorge Antonio Menna. Estratégia em comunicação. *In:* FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada:** a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 219-289.

ECHENIQUE, Raúl Herrera; UNTIVEROS, Raúl Bendezú. De la comunicación instrumental a la estratégica. *In:* FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada:** a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 105-139.

FÉLIX, Joana d’Arc Bicalho. El flujo de la comunicación estratégica: integrada y en el entorno online y offline. *In:* FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada:** a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada., 2020. p. 141-188.

JUIZ, Carlos; GOMEZ, Beatriz. Delving into the IT governance-management communication interface: a scoping review. **International Journal of Digital Strategy, Governance, and Business Transformation**, [s. l.], v. 11, n. 1, p. 1-24, 2021. DOI: <https://doi.org/10.4018/IJDGBT.291542>.

KERCHE, Fábio; OLIVEIRA, Vanessa Elias de; COUTO, Cláudio Gonçalves. Os Conselhos Nacionais de Justiça e do Ministério Público no Brasil: instrumentos de *accountability*? **Revista de Administração Pública**, Rio de Janeiro, v. 54, n. 5, p. 1334-1360, set./out. 2020. DOI: <https://doi.org/10.1590/0034-7612201900212>.

KUNSCH, Margarida Maria Krohling. Comunicação organizacional integrada na perspectiva estratégica. *In*: FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada**: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 85-103.

LNENICKA, Martin *et al.* Identifying patterns and recommendations of and for sustainable open data initiatives: a benchmarking-driven analysis of open government data initiatives among European countries. **Government Information Quarterly**, [s. l.], v. 41, n. 1, p. 101898, 2024. DOI: <https://doi.org/10.1016/j.giq.2023.101898>.

MOREIRA, Manoel Henrique Tavares. O impacto das fake news nas estratégias de comunicação das organizações públicas brasileiras. *In*: FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada**: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 309-331.

PÉREZ, Rafael Alberto. El proyecto corporativo como lugar de encuentro. *In*: FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada**: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 43-65.

PORTALES ECHEVERRÍA, Juan Cristóbal; SOUSA AMUNÁTEGUI, Rafael. Lo que está en juego: consecuencias de la desconfianza pública hacia las empresas. *In*: FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada**: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 417-437.

RUÃO, Teresa. A comunicação enquanto estratégica. *In*: FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada**: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 27-42.

TOLEDO, Jorge Alberto Hidalgo. Comunicación estratégica en la era digital: retos y desafíos ante la 4ª revolución industrial. *In*: FÉLIX, Joana d’Arc Bicalho (org.). **Comunicação estratégica e integrada**: a visão de 23 renomados autores em 5 países. Brasília: Rede Integrada, 2020. p. 291-317.

Evolução estratégica da rede de dados de longa distância do MPF: os desafios decorrentes do atual modelo de contratação

Strategic evolution of FPS's long-distance data network: challenges of the current contracting model

DOI: https://doi.org/10.63601/978-65-88299-52-4_2

Alinne Cristiane Aniceto Medeiros

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Engenheira eletricista pela Universidade Federal da Paraíba (UFPB). Servidora do Ministério Público Federal (MPF), com atuação na área de licitações e contratos, com foco em planejamento, condução de processos licitatórios e gestão contratual.

Fernando Nakashoji

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Gestão e Segurança de Redes de Computadores pela Unieuro Brasília. Tecnólogo em processamento de dados pela Universidade Católica de Brasília (UCB). Servidor do Ministério Público Federal (MPF). Titular da Subsecretaria de Infraestrutura de Tecnologia da Informação, onde coordena a prospecção, o planejamento e a fiscalização técnica de contratos de soluções e serviços de infraestrutura de tecnologia da informação.

Resumo: Esta pesquisa analisa o esforço do Ministério Público Federal (MPF) em obter maior eficiência, padronização, transparência e controle de custos na entrega de soluções de Tecnologia da Informação e Comunicação (TIC). O objetivo geral do estudo é apresentar o cenário atual de contratações centralizadas sob a ótica da Governança de TIC e propor melhorias. Para isso, examina os requisitos técnicos e a execução do Contrato n. 13/2023, que provê serviços de conectividade à internet e segurança de perímetro, e que implementa a tecnologia SDWAN (*Software Defined Wide-Area Network*)

para maior resiliência de rede. Os resultados demonstram que a contratação centralizada ainda é a melhor opção para o serviço em estudo. No entanto, em futuras contratações, torna-se imprescindível que haja maior envolvimento de representantes das demais unidades, a fim de garantir que as peculiaridades locais sejam atendidas, sem prejudicar a uniformidade e a qualidade do serviço nacional.

Palavras-chave: padronização; contratações centralizadas; governança de TIC.

Abstract: *This research analyzes the effort of the Federal Prosecution Service (MPF) to achieve greater efficiency, standardization, transparency, and cost control in the delivery of Information and Communication Technology (ICT) solutions. The general objective of the study is to present the current scenario of centralized procurement from the perspective of ICT Governance and propose improvements. Therefore, it examines the technical requirements and execution of Contract No. 13/2023, which provides internet connectivity and perimeter security services, and implements SDWAN (Software Defined Wide-Area Network) technology for better network resilience. The results show that centralized procurement remains the best option for the service under review. However, in future procurements, it will be critical to ensure broader involvement from representatives of the other units to make sure local needs are met without compromising the service's nationwide uniformity and quality.*

Keywords: *standardization; centralized procurement; IT governance.*

1 Introdução

A Constituição Federal (CF) de 1988 outorgou ao Ministério Público brasileiro, como função essencial à justiça, a defesa dos direitos sociais e individuais indisponíveis, a defesa da ordem jurídica e a defesa do regime democrático.

O Ministério Público brasileiro é composto pelos Ministérios Públicos estaduais e pelo Ministério Público da União (MPU), que, por sua vez, possui quatro ramos: o Ministério Público Federal (MPF), o Ministério Público do Trabalho (MPT), o Ministério Público Militar (MPM) e o Ministério Público do Distrito Federal e Territórios (MPDFT).

O MPF, um dos maiores ramos do MPU, atua junto à Justiça Federal, como fiscal da lei e também nas áreas cível, criminal e eleitoral, em causas nas quais a Constituição considera haver interesse federal, perante o Supremo Tribunal Federal, o Superior Tribunal de Justiça, o Tribunal Superior Eleitoral, os tribunais regionais federais, os juízes federais e os juízes eleitorais, nos casos regulamentados pela Constituição e pelas leis federais.

A atuação do MPF perante a Justiça brasileira exige que tenha representações em todo o território nacional. Além das capitais das unidades da Federação, conta com unidades (Procuradorias da República nos Municípios) em centenas de cidades brasileiras.

A dispersão geográfica, aliada à dependência de soluções tecnológicas para a execução de suas atividades, levou à adoção de um modelo centralizado de contratações de Tecnologia da Informação e Comunicação como forma de fortalecer a governança, promover eficiência administrativa e garantir maior uniformidade nas aquisições.

A experiência do MPF fornece uma oportunidade concreta para examinar os efeitos práticos da centralização, especialmente em termos de governança de Tecnologia da Informação e Comunicação (TIC), eficiência operacional e entrega de valor aos seus usuários e, conseqüentemente, à sociedade.

O modelo centralizado de contratações visa, em essência, a reunir demandas comuns das diferentes unidades organizacionais sob uma gestão única, e pode proporcionar vantagens como alcançar ganhos de escala, padronização de processos e redução de redundâncias (Alves *et al.*, 2019; Góis; Ouro; Mendonça, 2024).

Apesar dos benefícios esperados, outros estudos demonstram algumas desvantagens do modelo, como maior complexidade na gestão contratual, riscos de inflexibilidade e dificuldades na adaptação às especificidades locais ou técnicas de determinados serviços (Góis; Ouro; Mendonça, 2024; Lima, 2024).

A prestação de serviços ao MPF traz desafios para o mercado, principalmente em serviços que exigem boa logística, de infraestrutura de comunicações ou os de alta complexidade. O contrato n. 13/2023, analisado neste artigo, apresenta objeto complexo, uma vez que as especificações técnicas são inovadoras em relação aos contratos anteriores e requer, para a sua boa execução, condições adequadas de infraestrutura e logística.

A pouca competitividade observada já na etapa do certame licitatório, decorrente de um número limitado de fornecedores aptos a prestar os serviços, indica que o modelo centralizado é também desafiador para o mercado. Outras dificuldades que ocorreram na implantação, como

demora no desembaraço aduaneiro de equipamentos importados pela contratada, logística de envio e instalação desses equipamentos, e até mesmo condições geográficas e climáticas adversas, que acarretaram atrasos nos trabalhos, evidenciaram o desafio em utilizar o modelo centralizado em escala nacional.

Nesse contexto, esta pesquisa tem como tema: “Evolução estratégica da rede de dados de longa distância do MPF: os desafios decorrentes do atual modelo de contratação”. O estudo busca responder as seguintes perguntas: “Quais as motivações encontradas na literatura que justificaram a centralização de contratações públicas, em especial contratações de TIC? Quais resultados puderam ser observados no MPF após a aplicação dessa medida? Quais elementos ainda carecem de atenção e podem ser melhorados no modelo? Os modelos misto e descentralizado podem ser alternativas para aprimorar o processo de contratação de soluções complexas e que devam atender a todas as unidades do MPF?”

O objetivo da pesquisa é apresentar o cenário atual de contratação de TIC de média e alta complexidade, capazes de atender a todas as unidades do Ministério Público Federal, sob a ótica da governança de TIC, e propor melhorias para os problemas atualmente enfrentados, tomando como base os dados de elaboração dos requisitos técnicos e da execução de um dos maiores contratos vigentes de serviço com estas características, o qual provê os serviços de conectividade à internet e segurança de perímetro¹. Para atingir esse propósito, serão examinados os fundamentos legais da centralização, as diretrizes de governança de TIC aplicáveis e os impactos observados no contexto institucional do MPF.

A justificativa para esta pesquisa reside na relevância do tema para o aprimoramento da gestão de TIC no MPF, uma vez que a instituição passa por processo constante de transformação digital e faz uso intensivo de soluções tecnológicas no desempenho de suas atividades. Além disso, a experiência do MPF evidenciou a necessidade de ajustes na implantação do modelo centralizado de contratações, dada a sua

¹ Conjunto de soluções tecnológicas que protegem individualmente os pontos de acesso à internet das unidades do MPF contra acessos não autorizados e outras ameaças. Este serviço objetiva monitorar, detectar e impedir tentativas de invasão ou movimentação suspeita, e, no caso de incidentes, pode evitar a disseminação de uma unidade afetada para as demais, minimizando eventuais prejuízos.

abrangência nacional e as características do mercado fornecedor de soluções de TIC brasileiro.

2 Revisão de literatura

A Constituição Federal de 1988 estabelece que a Administração Pública, em todos os seus atos, deverá obedecer aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Especificamente quanto às contratações públicas, determina que estas deverão ser realizadas mediante processo de licitação pública, de modo a assegurar a igualdade de condições a todos os concorrentes.

A Lei n. 14.133, de 1º de abril de 2021, comumente referenciada como a Nova Lei de Licitações e Contratos (NLLC), regulamenta as contratações públicas no âmbito das Administrações Públicas diretas, autárquicas e fundacionais. Ao analisar o referido normativo, observa-se que a centralização das contratações é incentivada, conforme depreende-se do art. 19:

Art. 19. Os órgãos da Administração com competências regulamentares relativas às atividades de administração de materiais, de obras e serviços e de licitações e contratos deverão:

I - instituir instrumentos que *permitam, preferencialmente, a centralização* dos procedimentos de aquisição e contratação de bens e serviços; [...]. (Grifo nosso).

Apesar de na Lei n. 8.666, de 21 de junho de 1993, não haver, explicitamente, dispositivo que determine a preferência pelas contratações centralizadas, como no art. 19 da NLLC, tal prática já era observada em algumas contratações da Administração Pública Federal. O contrato n. 13/2023, por exemplo, foi celebrado observando o disposto na Lei n. 8.666, mas já se configurava como um instrumento com a maior parte de sua fiscalização centralizada no órgão central do MPF – a Procuradoria-Geral da República. Importa informar que o referido instrumento também era regido com base no disposto na Resolução CNMP n. 102, de 23 de setembro de 2013, vigente à época e que disciplinava os procedimentos relativos à contratação de soluções de tecnologia da informação.

A Lei Complementar n. 75, de 20 de maio de 1993, dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União, do qual o Ministério Público Federal é um dos ramos, e estabelece que são princípios institucionais a unidade, a indivisibilidade e a independência funcional.

A observância desses princípios orientava a adoção de serviços e soluções de TIC uniformes no Ministério Público Federal, antes mesmo da formalização das estruturas de governança na instituição. Consequentemente, muitos processos de contratação de soluções já vinham sendo conduzidos de forma centralizada, como os de aquisição de soluções de colaboração corporativa, infraestrutura de datacenter, micro-computadores, serviços de impressão e de rede de dados de longa distância.

A primeira versão do Planejamento Estratégico Institucional (PEI) do Ministério Público Federal, com vigência de 2011 a 2020 (MPF, 2011), além de observar os princípios institucionais, teve como principais objetivos a implementação de um novo modelo de gestão, alinhando os recursos – orçamentários, físicos, humanos – à estratégia da instituição.

O Planejamento Estratégico definiu e implementou um novo modelo de gestão, tornando o MPF mais ágil e eficiente. O mapa estratégico do MPF estabeleceu vinte objetivos estratégicos para processos internos, aprendizado e crescimento, e cinco objetivos voltados à sociedade, visando aprimorar a excelência da atuação institucional.

O Plano Diretor de Tecnologia da Informação (PDTIC), biênio 2013/2014, desdobramento do PEI de 2011, propôs um novo modelo de atuação orientado pela concepção de uma “TI Nacional”, que visava à padronização de soluções, racionalização de recursos e integração de serviços. A ideia principal foi propiciar uma atuação uniforme dos profissionais de TI em todo o país, com base em políticas definidas pela Gestão Nacional. As unidades permaneceram com uma parcela de autonomia, mas em consonância com o definido em âmbito nacional.

O estabelecimento da Comissão Estratégica de Tecnologia da Informação (Ceti), inicialmente designada Subcomitê Estratégico de Tecnologia da Informação (Seti), foi fundamental na estratégia de atuação unificada. Formalizada em atendimento à Resolução n. 102 do CNMP, de 23 de setembro de 2013, atualmente a Ceti tem papel preponderante na definição da estratégia de TIC do MPF, sendo responsável pelo acompanhamento da execução do PDTIC, análise de diretrizes e políticas, além de ser instância consultiva na priorização de demandas e de contratações.

As contratações, aquisições e o orçamento de TIC passaram a ser acompanhados no Plano de Contratações e Orçamento de Tecnologia da Informação e Comunicação (PCTIC) a partir de setembro de 2020, com

a participação de todas as unidades do MPF e gestão da Subsecretaria de Orçamento e Gestão de Contratações (Sogec) e da Assessoria Técnica da Secretaria de Tecnologia da Informação e Comunicação (STIC) do MPF.

Houve períodos de significativas restrições orçamentárias, que chegaram a dificultar a aquisição de infraestrutura e a nomeação de novos profissionais de TI, evidenciando ainda mais a importância de uma gestão alinhada à estratégia, com a definição clara das prioridades e o direcionamento correto dos esforços e recursos.

A centralização busca economia de escala, padronização e maior controle (Alves *et al.*, 2019; Góis; Ouro; Mendonça, 2024; Silva, 2024), mas se depara com desafios como morosidade, perda de competitividade para micro e pequenas empresas, dificuldade com as particularidades locais, aumento de custos de informação e monitoramento, resistência das equipes locais que irão realizar a fiscalização contratual e necessidade de um planejamento robusto (Góis; Ouro; Mendonça, 2024; Lima, 2024).

Dessa forma, embora o modelo de contratações centralizado traga benefícios, também apresenta deficiências e desvantagens, como demonstraram diversos estudos e experiências. A escolha do modelo de contratação deve ser embasada por uma análise crítica, caso a caso, pois não existe um modelo universalmente “certo” (Góis; Ouro; Mendonça, 2024; Góis, 2024).

Em Fernandes (2015), observa-se que a ideia de centralização das contratações públicas remonta à década de 1930. Inicialmente, a centralização foi concebida como estratégia para ampliar a eficiência administrativa e aplicar métodos de racionalização inspirados em modelos internacionais. No entanto, seu trabalho demonstra que a iniciativa enfrentou limitações operacionais e resistências que prejudicaram sua consolidação.

Os recursos de tecnologia da informação, todavia, foram meios que facilitaram o fortalecimento de um órgão central de contratações. A partir de Fernandes (2016), pode-se entender que a criação do Sistema Integrado de Administração de Serviços Gerais (Siasg), do Comprasnet, e das demais soluções tecnológicas relacionadas à padronização das contratações, fortaleceu a atuação da Administração Federal na uniformização dos procedimentos relacionados às contratações públicas.

Em Góis, Ouro e Mendonça (2024), foi realizada uma pesquisa a fim de identificar os benefícios e limitações da centralização das compras públicas na Administração Federal, considerando os critérios de sustentabilidade. O estudo identificou que, embora as compras centralizadas promovam economia de escala, padronização, eficiência contratual e adoção mais robusta de critérios de sustentabilidade, também apresentam desvantagens como morosidade, riscos de desabastecimento, enfraquecimento da autonomia local e exclusão de micro e pequenas empresas. Portanto, a centralização não deve ser adotada como regra geral, mas analisada caso a caso, com base em estudos técnicos preliminares que considerem as peculiaridades do objeto, do mercado e das políticas públicas envolvidas.

Outros estudos tiveram a finalidade de analisar o processo de centralização em órgãos públicos específicos. Em Silva (2024), a pesquisa objetivou demonstrar a economia proporcionada pela adoção do pregão eletrônico nas aquisições centralizadas da Rede Ebserh em 2022. Os resultados evidenciaram que as compras centralizadas favorecem a economicidade e promovem maior eficiência nas contratações públicas.

A abordagem baseada exclusivamente na redução de custos, todavia, pode não ser adequada quando se trata de contratos de TIC, tendo em vista a demanda crescente na contratação desse tipo de serviço que, por si só, pode provocar aumento de custos.

No estudo de Lima (2024), a análise não se baseou na redução de custos, mas sim na percepção dos gestores de licitações e contratações após a centralização das contratações de serviços essenciais nas Superintendências Regionais do Instituto Nacional do Seguro Social (INSS). Os resultados se assemelham aos apresentados em Góis, Ouro e Mendonça (2024): se, por um lado, a centralização permite economia de escala, padronização e aumento de eficiência, por outro, pode resultar em atrasos e menor flexibilidade para atendimento às demandas particulares de cada unidade local.

Já o estudo de Góis (2024) analisou especificamente o cenário de contratações do MPF, propondo a criação das chamadas “Contratações Estratégicas” e discorreu também sobre os aspectos da centralização das contratações. A pesquisa reforçou que as compras centralizadas promovem aumento do desempenho organizacional por meio da

melhoria da eficiência, redução de custos, rapidez na entrega e melhor preço no mercado, objetivos da Lei n. 14.133/2021; entretanto, também corroboram as desvantagens esperadas do modelo centralizado, como a morosidade e a potencial redução de fornecedores capacitados.

Diante da análise normativa e da literatura especializada, verifica-se que a centralização das contratações públicas, especialmente de soluções de TIC, tem sido adotada como instrumento de racionalização administrativa, busca por eficiência, padronização de processos e economia de escala. No entanto, estudos apontam que o modelo não está isento de limitações, sendo necessário um planejamento criterioso que considere as peculiaridades locais, a maturidade institucional e os riscos associados à uniformização excessiva.

A experiência do MPF, bem como os dados extraídos de estudos de caso e análises históricas, revelam que o sucesso da centralização depende de uma governança sólida, do uso estratégico de instrumentos como o PDTIC e o PCTIC, e da constante avaliação dos impactos gerados.

3 Metodologia

Este estudo adotou o paradigma interpretativo, com abordagem metodológica mista, combinando técnicas qualitativas e quantitativas para investigar as contratações centralizadas de TIC no MPF, com foco no Termo de Contrato MPF/PGR n. 13/2023, que tem como objeto a contratação de serviço de “solução integrada de rede corporativa de comunicação, por meio de tecnologia SDWAN² como serviço, com capacidade para prover tráfego de dados, voz e vídeo entre as unidades do MPF em todo o território nacional, de serviços de segurança em *data-center*”. A finalidade é descritiva e explicativa, buscando compreender o cenário atual, identificar as discrepâncias regionais e explicar as causas das falhas no fornecimento de serviços, sobretudo em relação ao acesso à internet com tecnologia SDWAN, objeto do contrato supracitado. Por fim, buscou-se explicar os fatores que levaram a essas deficiências, com o objetivo de subsidiar propostas de melhoria.

Os métodos utilizados foram:

² *Software-Defined Wide Area Network*, ou rede de longa distância definida por software.

- a. análise documental, com foco nos seguintes tópicos:
 - Planos Diretores de TI: revisão do Planejamento Estratégico Institucional 2011-2020 e dos planos estratégicos de TI do MPF para identificar tendências, desafios históricos e o alinhamento das contratações com as demandas da instituição.
 - Registros de Falhas e SLAs: coleta e análise de dados do sistema de chamados, relatórios de SLA, registros de descumprimento contratual e solicitações formais das unidades para a contratação excepcional de canais de contingência, todos referentes ao instrumento PGR n. 13/2023, para quantificar e qualificar os problemas de desempenho dos serviços.
- b. *survey*, na forma de questionário aplicado aos atuais fiscais setoriais do contrato n. 13/2023, objetivando coletar a percepção destes quanto à qualidade dos serviços prestados e alternativas de contratação.

Neste artigo, o uso de inteligência artificial baseou-se nas diretrizes apresentadas em Sampaio, Sabbatini e Limongi (2024). Importa informar que nenhum texto gerado foi incorporado sem edição e que dados sensíveis não foram compartilhados.

As ferramentas Litmaps e NotebookLM foram utilizadas na etapa de revisão de literatura, a fim de auxiliar no fichamento bibliográfico. A ferramenta NotebookLM também foi utilizada na revisão final do artigo, e foram incorporadas ao texto algumas sugestões dessa ferramenta, com as devidas adequações. Nenhuma outra ferramenta de inteligência artificial foi utilizada.

4 Contextualização

A interconectividade das unidades do MPF iniciou-se a partir dos anos 1990. Todos os sistemas institucionais eram hospedados em equipamentos localizados na sede da Procuradoria-Geral da República (PGR), em Brasília (DF), nas Procuradorias Regionais da República (PRRs) e nas Procuradorias da República (PRs) sediadas nas capitais do Rio Grande do Sul, Paraná, São Paulo, Rio de Janeiro, Minas Gerais e Pernambuco. Eram empregados minicomputadores da Cobra Computadores, com acesso multiusuário e conexões locais multiponto. Não havia interligação do MPF com outras instituições. A conectividade

entre unidades do MPF ocorria sob demanda, uma vez que a internet ainda não estava difundida no país.

As comunicações e os fluxos de demandas entre as unidades eram feitos por meio de malotes ou fax. No entanto, já se utilizava tecnologia de acesso discado para o suporte da área de TI, prestado pela PGR às demais unidades da federação onde estavam instalados os minicomputadores. As implantações de sistemas pela equipe de desenvolvimento eram realizadas presencialmente, o que gerava custos significativos com viagens e estadias.

Em 1994, iniciaram-se as implantações de redes locais nas unidades do MPF, que possibilitaram o início do desenvolvimento das primeiras aplicações cliente-servidor, além dos serviços de compartilhamento de arquivos e impressão em rede.

Em 1995, a PGR conectou-se pela primeira vez à internet, mediante convênio celebrado com a Rede Nacional de Ensino e Pesquisa (RNP), entidade que provia os acessos à internet para entidades de pesquisa, educacionais e governamentais. Iniciaram-se os estudos para o provimento do serviço de acesso à internet às demais unidades do MPF, que culminaram no primeiro contrato de prestação de serviço de acesso à internet e conectividade das unidades, celebrado com a Embratel.

Os novos serviços possibilitaram o acesso à internet, a publicação de sítios e serviços do MPF e a interconexão entre as unidades nas capitais das unidades federativas e a PGR, em Brasília. Até o final dos anos 1990, o acesso à internet, bem como os principais serviços que foram possibilitados, como o correio eletrônico, mensageria instantânea e compartilhamento de arquivos, já faziam parte da cultura dos usuários de todo o MPF.

Durante a primeira década dos anos 2000, a oferta dos serviços de tecnologia da informação no MPF permaneceu basicamente a mesma. Cada unidade mantinha sua infraestrutura local, adotando, em boa medida, a padronização estabelecida. Além disso, cada unidade mantinha recursos para armazenamento, banco de dados, ambientes de desenvolvimento de sistemas e demais serviços, de forma independente e descentralizada.

Apesar de buscar a adoção de soluções uniformes, como forma de garantir uma cultura técnica de suas equipes e consequente facilitação

da prestação do suporte técnico, até a definição das diretrizes de modernização, cada unidade nas capitais se comportava como uma entidade independente, necessitando de meios para a publicação de seus sítios de internet, sistemas de correio eletrônico, videoconferência, telefonia IP, entre outros.

O PEI (MPF, 2011) estabeleceu as diretrizes da boa governança e, como desdobramento, a Secretaria de Tecnologia da Informação e Comunicação, em seu Planejamento Estratégico de Tecnologia da Informação, iniciou o planejamento para o desenho da nova infraestrutura de tecnologia da informação do MPF.

O desenvolvimento centralizado de soluções e a unificação dos ambientes dos serviços de correio eletrônico, armazenamento de arquivos e sítios *web* foram ações iniciadas a seguir, e possibilitaram o estabelecimento do que viria a se tornar a “nuvem privada do MPF”, ambiente centralizado que hospeda a maioria dos recursos institucionais.

As opções técnicas de conectividade disponíveis no mercado à época eram limitadas, e, entre estas, a que se mostrava mais adequada era o *Multi-Protocol Label Switching* (MPLS)³. Na topologia utilizada no MPF, os túneis virtuais conectavam todas as unidades entre si, e a um único ponto de saída para a internet, localizado nas dependências da empresa contratada, protegido por mecanismos de segurança da informação.

Com os recursos de garantia de qualidade de serviço, ou *Quality of Service* (QoS), e a convergência de entrada e saída para a internet em um único ponto, o MPLS possibilita a realização de videoconferências, a implementação de telefonia IP e a publicação de sítios internet e sistemas de correio eletrônico localizados em cada uma das Procuradorias da República nas capitais, Procuradorias Regionais da República e na PGR.

Outra camada de segurança foi posteriormente adicionada, mediante os serviços de segurança de perímetro, que consistem na inclusão de equipamentos de segurança em cada uma dessas unidades, primeiramente *firewalls* e sistemas de prevenção de intrusão e, posteriormente, os *Unified Threat Management* (UTM), que consolidam várias funções de segurança em um único dispositivo ou serviço.

³ Tecnologia que possibilita o estabelecimento de uma rede privativa de longa distância, utilizando rótulos em pacotes de rede e estabelecendo canais VPN (*Virtual Private Networks*) entre as localidades.

Embora robusta e confiável, a topologia trazia grandes desafios técnicos e de fiscalização contratual. Para a interconexão dos equipamentos das contratadas nas redes locais das unidades, eram necessárias configurações complexas e, na sua implementação final, durante uma das migrações contratuais, o MPF chegou a ter quatro grandes contratos, celebrados com três empresas diferentes.

Em 2018, adotou-se uma topologia de rede de dupla abordagem, ou seja, o serviço de conectividade de longa distância utilizaria dois circuitos diferentes objetivando a otimização do tráfego, mediante a implementação de segmentação e redundância. Foram celebrados os contratos n. 51/2018 e n. 60/2018 com a empresa Claro, que passou a prover os dois circuitos: um circuito IP, para o tráfego destinado à internet, e um circuito *Business Link Direct* (BLD), utilizando a tecnologia MPLS, interligando as unidades do MPF entre si e ao *datacenter* da contratada, onde eram providas diversas soluções de conectividade externa, como a publicação de sítios e conectividades externas específicas.

A topologia de dupla abordagem possibilitou a adoção de soluções típicas de uma rede SDWAN, como segregação e desvio de tráfego automático de um circuito para outro por meio de políticas ou em caso de falhas. Entretanto, a necessidade de atuação conjunta de duas, ou até três empresas contratadas, como foi o caso do período de migração contratual dos serviços de segurança de perímetro, ocorrido em 2019, sempre foi um desafio. Eram comuns os erros de configuração e consequente perda de conectividade, e a depuração do erro e sua resolução geralmente demandavam esforço e tempo consideráveis.

A partir de 2021, iniciou-se a fase final de centralização de recursos, com a análise e classificação dos sistemas locais, desenvolvidos nas unidades do MPF, que seriam descontinuados, hospedados na infraestrutura centralizada ou mantidos até sua substituição por solução nacional.

Com a “Nuvem privada do MPF” operacional e a maioria dos sistemas centralizados e já adequados, puderam ser iniciados os estudos para o aprimoramento da topologia de rede de longa distância no MPF, mais simples e flexível. Os estudos culminaram com as especificações que dariam origem ao Contrato n. 13/2023.

Um resumo sobre as soluções de TI adotadas pelo MPF ao longo do tempo encontra-se consolidado na Figura 1 abaixo.

Figura 1 – Linha do tempo com os principais marcos da conectividade no MPF



Fonte: elaborada pelos próprios autores.

As dificuldades operacionais e técnicas na implantação do Contrato n. 13/2023 trouxeram instabilidades e, muitas vezes, indisponibilidades de acesso por períodos consideráveis. Esses problemas ensejaram alguns pedidos de contratação de canais de comunicação de contingência, e, embora poucas unidades fossem afetadas, o número de incidentes e o impacto decorrente das instabilidades chegaram a níveis críticos.

Foram então adotados critérios para que esses pedidos fossem autorizados, consistindo na análise de disponibilidade dos últimos seis meses para cada unidade. As localidades que apresentam três ou mais eventos intercalados (mensais) ou dois seguidos de não cumprimento de disponibilidade contratada têm a contratação do circuito de contingência autorizada, por um período inicial de doze meses. Após este período, a análise é realizada novamente para avaliar a eventual necessidade de manutenção do circuito de contingência.

O correlacionamento do resultado da pesquisa com os pedidos de contratação de canais de contingência autorizados para o Rio Grande do Sul, Bahia, Minas Gerais e Espírito Santo reside na investigação das falhas operacionais e se o impacto negativo nas atividades institucionais pode ser mitigado caso se adote um modelo misto de contratação para determinados serviços e soluções de TIC no MPF.

5 Apresentação e discussão de resultados

O estudo utilizou a coleta e análise de dados relativos a solicitações formais das unidades para a contratação excepcional de canais de contingência, restringindo a análise aos que tiveram a contratação autorizada, como um meio de quantificar e qualificar os problemas de desempenho dos serviços do Contrato n. 13/2023.

Esse correlacionamento possibilita identificar se pedidos de contingência servem como evidência prática de que o contrato centralizado está enfrentando dificuldades em garantir a qualidade do serviço devido a dificuldades de adaptação às especificidades locais, fatores geográficos ou de logística.

Para a realização do *survey* e acesso aos procedimentos administrativos relativos à contratação, foi solicitada autorização mediante requerimento endereçado às Secretarias de Administração e de Tecnologia da Informação e Comunicação do MPF, apresentando o projeto de pesquisa aprovado e informando que tanto os dados obtidos no *survey* quanto os acessados nos procedimentos administrativos seriam utilizados exclusivamente para fins de elaboração da presente pesquisa acadêmica.

O requerimento, acompanhado do Termo de Confidencialidade e Não Divulgação dos dados utilizados, foi encaminhado à Secretaria de Tecnologia da Informação e Comunicação do MPF e analisado pela Unidade de Proteção de Dados Pessoais (UPDP) quanto ao alinhamento à Lei Geral de Proteção de Dados, que emitiu parecer favorável à realização da pesquisa.

O *survey*, composto por sete questões, seis de múltipla escolha e uma opcional em texto livre, objetivou obter a percepção dos fiscais setoriais quanto à qualidade do serviço contratado atualmente e traçar um comparativo entre a contratação centralizada, modelo atual, e uma eventual contratação em modelo misto, com parte dos serviços sendo contratada nacionalmente e parte contratada de forma local, por cada Procuradoria da República e Procuradoria Regional da República.

Pode-se dividir o *survey* em dois blocos lógicos de questões. O primeiro bloco, composto pelas duas primeiras questões, buscou avaliar a percepção dos fiscais quanto à qualidade dos serviços prestados, do

ponto de vista técnico/operacional e de fiscalização. O segundo bloco, composto pelas quatro questões restantes, buscou avaliar a percepção dos fiscais quanto à viabilidade de adoção de modelo misto de contratação, a capacidade de realizar a fiscalização contratual no caso de adoção desse modelo e a capacidade de fornecimento de canais de comunicação nos mercados locais.

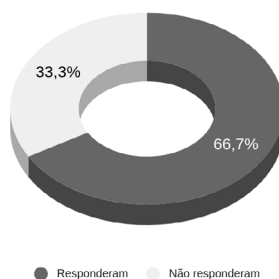
A análise comparativa do Contrato n. 13/2023 baseou-se no modelo até então utilizado nos contratos anteriores, no qual sempre se adotou a premissa de que a contratação centralizada se justifica pela uniformização da solução, considerando-se aí os requisitos técnicos e a definição de parâmetros de SLA que levem à boa prestação do serviço em todo o território nacional, bem como a uniformização dos procedimentos relativos à fiscalização contratual.

A listagem dos participantes da pesquisa foi obtida na portaria de nomeação dos fiscais técnicos setoriais. O universo da pesquisa, obtido na citada portaria, era composto por 64 pessoas, um fiscal setorial titular e um substituto para cada Procuradoria da República e Procuradoria Regional da República, à exceção da Procuradoria Regional da República da 6ª Região (Minas Gerais), que compartilha as instalações físicas com a Procuradoria da República em Minas Gerais (PR/MG).

A amostragem, embora pareça pequena em uma primeira análise, para os pesquisadores foi considerada adequada, uma vez que os fiscais técnicos setoriais acompanham detalhadamente a situação dos canais de comunicação de suas próprias unidades e das Procuradorias da República nos Municípios da respectiva unidade federativa, quando for o caso.

A sua atuação permite que realizem um acompanhamento histórico da qualidade das conexões, o registro e acompanhamento dos chamados técnicos, a consolidação do Instrumento de Medição de Resultado e a interação com os fiscais técnicos globais do contrato, reportando dificuldades e obtendo orientações para a correta fiscalização.

Ao término do prazo, foram colhidas 27 respostas. Durante a análise dos resultados, constatou-se que havia quatro respostas para uma mesma unidade da Federação. Para este caso, foram suprimidas as duas respostas mais antigas do levantamento. No Gráfico 1, é apresentado o percentual geral de unidades que participaram da pesquisa.

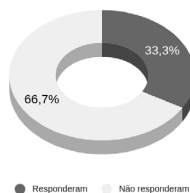
Gráfico 1 – Representatividade das unidades da Federação na pesquisa

Fonte: elaborado pelos próprios autores com base nos dados coletados.

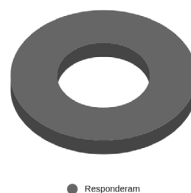
As 25 respostas válidas possibilitaram uma análise de 66,67% do cenário nacional, uma vez que representam 18 unidades da Federação. A distribuição das respostas por região configurou-se da forma apresentada no Gráfico 2, a seguir:

Gráfico 2 – Representatividade por região

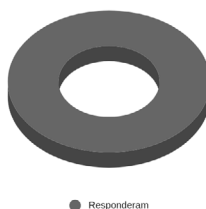
Sul



Sudeste



Centro-Oeste

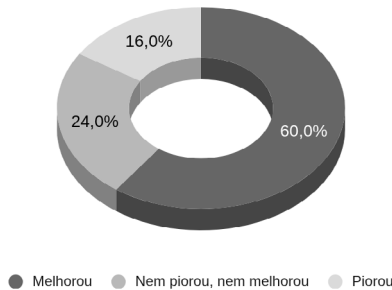


Fonte: elaborado pelos próprios autores com base nos dados coletados.

A participação dos fiscais setoriais no *survey* possibilitou uma boa análise da percepção da qualidade dos serviços nas respectivas regiões do Brasil representadas na pesquisa: 42,85% da Região Norte (3 estados), 66,67% da Região Nordeste (6 estados), 100% da Região Centro-Oeste (3 estados mais o Distrito Federal), 33,33% da Região Sul (1 estado) e 100% da Região Sudeste (4 estados).

A primeira pergunta teve como enunciado: “O serviço SDWAN contratado atualmente buscou aprimorar a qualidade e simplificar tecnicamente a configuração e operação dos *links* de acesso à internet nas unidades do MPF. Considerando os contratos anteriores, em que eram fornecidos *links* redundantes MPLS/BLD, e o período entre o recebimento definitivo e o início desta pesquisa (30/out/2024 a 30/abr/2025), o acesso à internet em sua unidade (e nas PRMs respectivas):”, e com as opções de resposta “Melhorou”, “Nem piorou, nem melhorou”, “Piorou” e “Não sei”. Os resultados obtidos são apresentados no Gráfico 3.

Gráfico 3 – Percepção quanto à qualidade dos serviços prestados em relação aos contratos anteriores

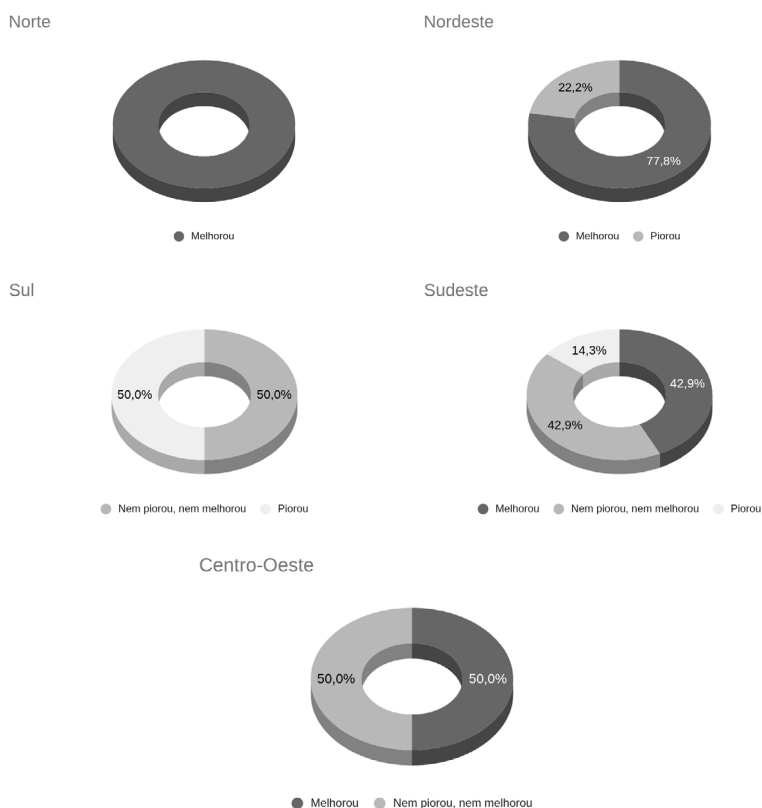


Fonte: elaborado pelos próprios autores com base nos dados coletados.

Considerando que os contratos anteriores, no geral, sempre obtiveram resultados satisfatórios para as necessidades do MPF, uma vez que o mesmo modelo foi se aprimorando ao longo dos anos e a cada nova contratação, podem-se considerar positivas as respostas “Nem piorou, nem melhorou”. Desta forma, para 84% dos entrevistados, o contrato n. 13/2023 vem sendo conduzido de forma satisfatória.

A distribuição das respostas por região configurou-se da forma apresentada no Gráfico 4, e, à exceção da Região Sul, onde houve um equilíbrio entre percepções negativas e positivas, as respostas das demais regiões corroborou a percepção de aprimoramento na qualidade dos serviços contratados.

Gráfico 4 – Percepção quanto à qualidade dos serviços prestados, por região



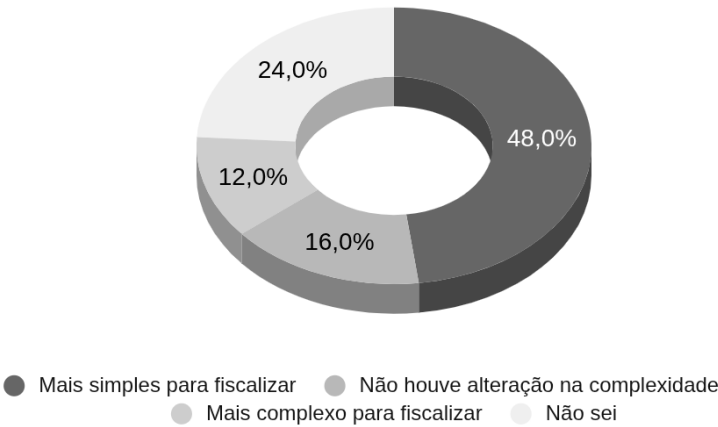
Fonte: elaborado pelos próprios autores com base nos dados coletados.

Correlacionando as respostas desta pergunta com os pedidos de ativação de canais de comunicação de contingência, duas unidades da Federação, Bahia e Minas Gerais, cada uma com duas participações no

questionário, responderam que a qualidade dos serviços melhorou em relação aos contratos anteriores. Espírito Santo e Rio Grande do Sul, também com duas participações cada, informaram ou que o serviço havia piorado, ou que o serviço não havia nem piorado, nem melhorado.

A segunda pergunta, cujo enunciado foi “Outro objetivo buscado no contrato n. 13/2023 foi a simplificação dos itens a serem avaliados para a análise de conformidade do IMR – Instrumento de Medição de Resultados (anteriormente denominado SLA). Desta forma, o contrato n. 13/2023, em relação aos anteriores está:” e com as opções “Mais simples para fiscalizar”, “Não houve alteração na complexidade da fiscalização”, “Mais complexo para fiscalizar” e “Não sei”, apresentou a distribuição de respostas apresentada no Gráfico 5.

Gráfico 5 – Percepção quanto à dificuldade de fiscalização contratual



Fonte: elaborado pelos próprios autores com base nos dados coletados.

Ao contrário da pergunta anterior, as respostas “Não houve alteração na complexidade da fiscalização” foram consideradas negativas, uma vez que um dos objetivos com o estabelecimento dos parâmetros do Instrumento de Medição de Resultados do Contrato n. 13/2023 foi a simplificação da fiscalização contratual. Desta forma, 28% dos entrevistados apontaram falhas no objetivo de simplificação.

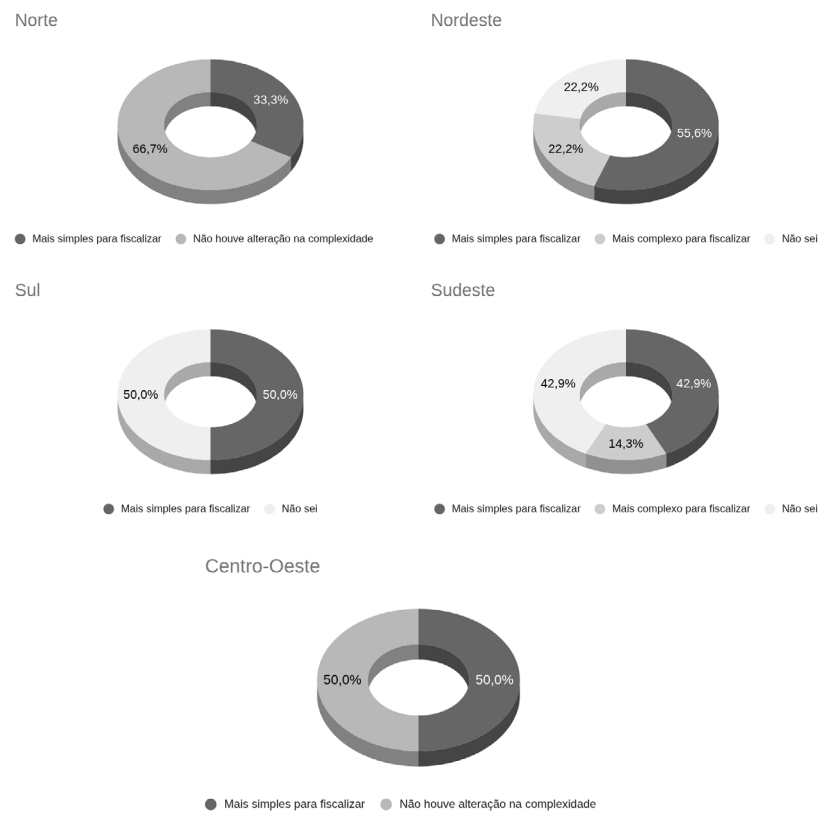
Acredita-se que o número expressivo de respostas “Não sei” (24%) deve-se ao fato de que o estabelecimento da fiscalização setorial ocorreu apenas em contratos recentes, sendo o de n. 13/2023 o primeiro contrato de comunicação de dados de longa distância a contar com este agente. Anteriormente, as equipes locais aferiam o IMR e apenas repassavam as informações para a fiscalização do contrato, que era realizada de forma centralizada, sendo responsável por toda a consolidação e conferência das informações.

Este alto percentual sugere que os fiscais setoriais perceberam falhas de comunicação ou capacitação e, conseqüentemente, a eles faltou a real compreensão dos objetivos, responsabilidades e impacto de suas atuações nos procedimentos técnicos e de aferição contratual.

Uma parcela dos 12% que informaram que o contrato ficou mais complexo de fiscalizar também pode ser explicada pelo mesmo motivo, uma vez que as atribuições dos fiscais setoriais se tornaram ligeiramente mais complexas.

A distribuição das respostas por região configurou-se conforme apresentado no Gráfico 6, a seguir.

Gráfico 6 – Percepção quanto à dificuldade de fiscalização contratual, por região



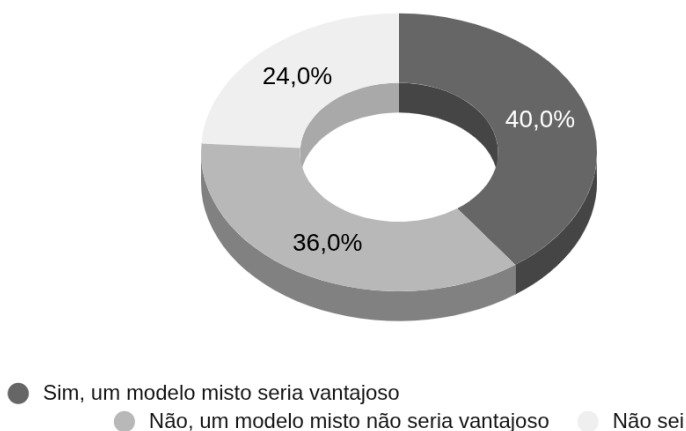
Fonte: elaborado pelos próprios autores com base nos dados coletados.

A percepção dos fiscais quanto à viabilidade de adoção de modelo misto de contratação, à capacidade de realizar a fiscalização contratual no caso de adoção deste modelo e à capacidade de fornecimento de canais de comunicação nos mercados locais foi levantada no segundo bloco de perguntas.

A primeira pergunta do bloco, terceira do questionário, teve como enunciado: “Considerando o custo, a oferta do mercado local, a

complexidade técnica e a capacidade de fiscalização contratual setorial e local, você acredita que o contrato poderia ser desmembrado, com parte da contratação sendo realizada de forma centralizada (serviços SDWAN e segurança de perímetro), e parte sendo realizada de forma descentralizada (os links de acesso propriamente ditos)?” e as opções “Sim, um modelo misto seria vantajoso”, “Não, um modelo misto não seria vantajoso” e “Não sei”. A distribuição das respostas está representada no Gráfico 7.

Gráfico 7 – Percepção quanto à vantajosidade de adoção de um modelo misto na contratação

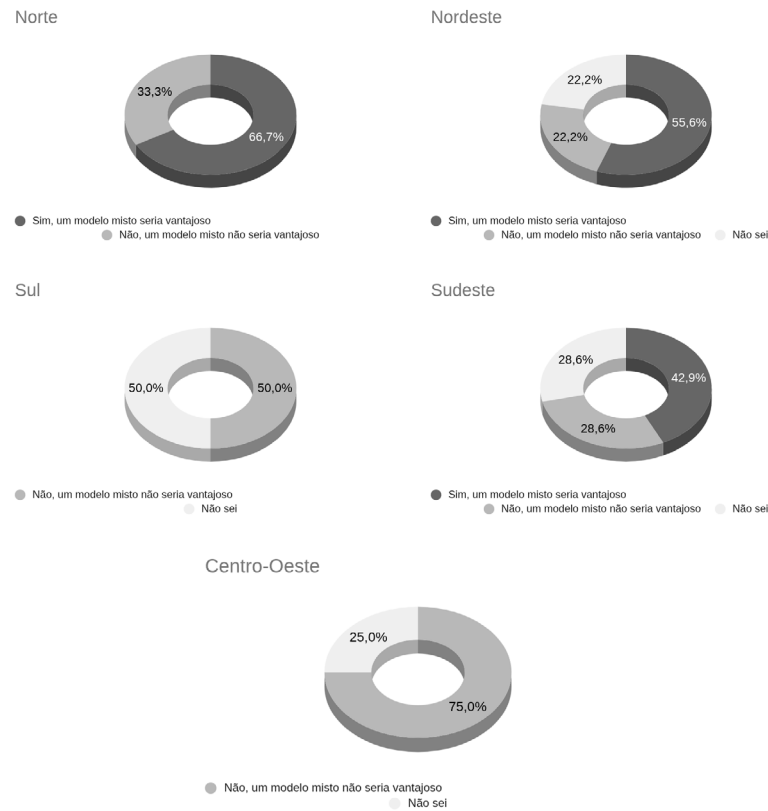


Fonte: elaborado pelos próprios autores com base nos dados coletados.

Um número expressivo de respostas “Não sei”, 24% dos participantes, indica que há dúvidas quanto ao modelo de contratação, embora a opção pelo modelo misto tenha sido preponderante nas Regiões Norte, Nordeste e Sudeste.

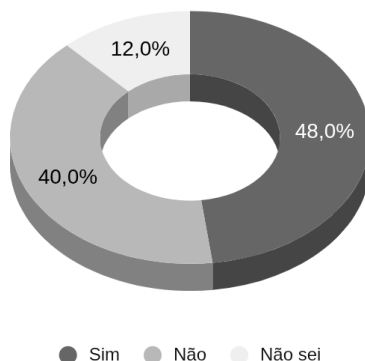
Este alto índice também pode ter sido devido ao desconhecimento dos modelos de contratação, suas vantagens e desvantagens.

Gráfico 8 – Percepção quanto à vantajosidade de adoção de um modelo misto na contratação, por região



Fonte: elaborado pelos próprios autores com base nos dados coletados.

A segunda pergunta do bloco procurou avaliar a percepção dos fiscais setoriais quanto à capacidade de fiscalização de contratos locais e nacionais, no caso de adoção do modelo misto de contratação. O Gráfico 9 apresenta o resultado geral obtido.

Gráfico 9 – Percepção quanto à capacidade local para a fiscalização

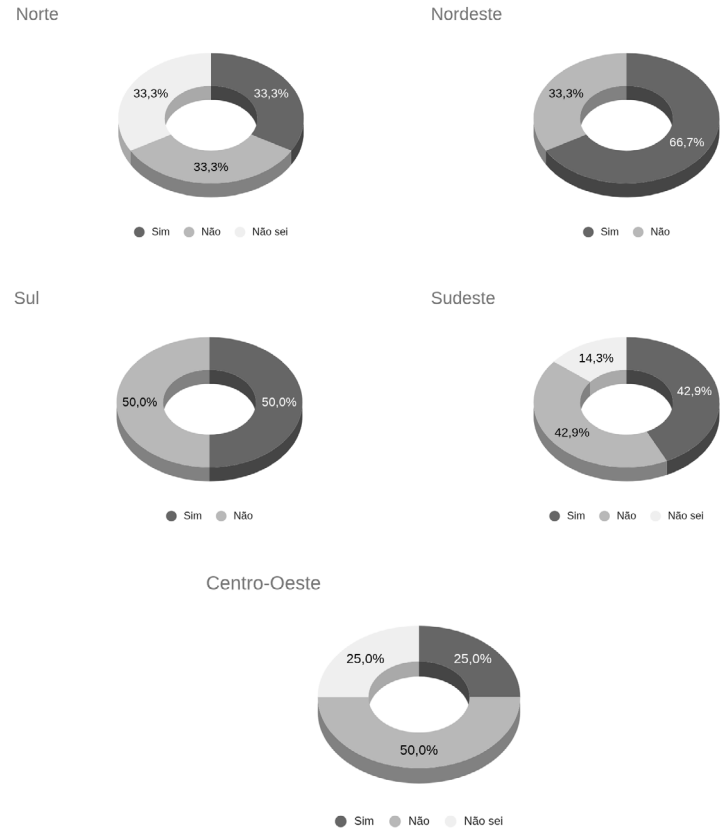
Fonte: elaborado pelos próprios autores com base nos dados coletados.

Observa-se uma certa incongruência entre a percepção quanto à vantajosidade de adoção de um modelo de contratação misto – pergunta anterior, e a percepção quanto à capacidade local para fiscalização contratual. Deveria haver um alinhamento entre as respostas que apontam para o modelo de contratação misto e a capacidade de fiscalização dos contratos, uma vez que, em tese, dois contratos exigem mais dedicação à fiscalização do que apenas um.

Observando a distribuição geográfica apresentada no Gráfico 10, apenas as Regiões Nordeste e Sudeste apresentam alinhamento com a resposta anterior, indicando a possibilidade de contratação mista com a percepção da capacidade local para a fiscalização. As Regiões Sul e Centro-Oeste também se alinham, porém no espectro oposto: manutenção do modelo centralizado aliado à incapacidade local de fiscalização contratual. A Região Norte apresentou resultados discrepantes entre uma e outra questão.

Das unidades que tiveram os canais de contingência aprovados, Bahia e Minas Gerais informaram que as equipes são suficientes para a realização das atividades de fiscalização contratual. Espírito Santo, com uma resposta “Não” e uma “Não sei”, e Rio Grande do Sul, com uma resposta “Não” e uma “Sim”, demonstraram, assim como outras unidades, percepções divididas.

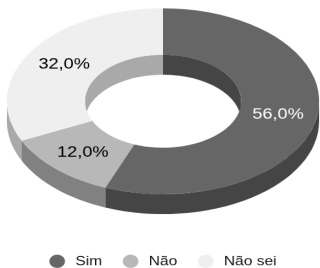
Gráfico 10 – Percepção quanto à capacidade local para a fiscalização, por região



Fonte: elaborado pelos próprios autores com base nos dados coletados.

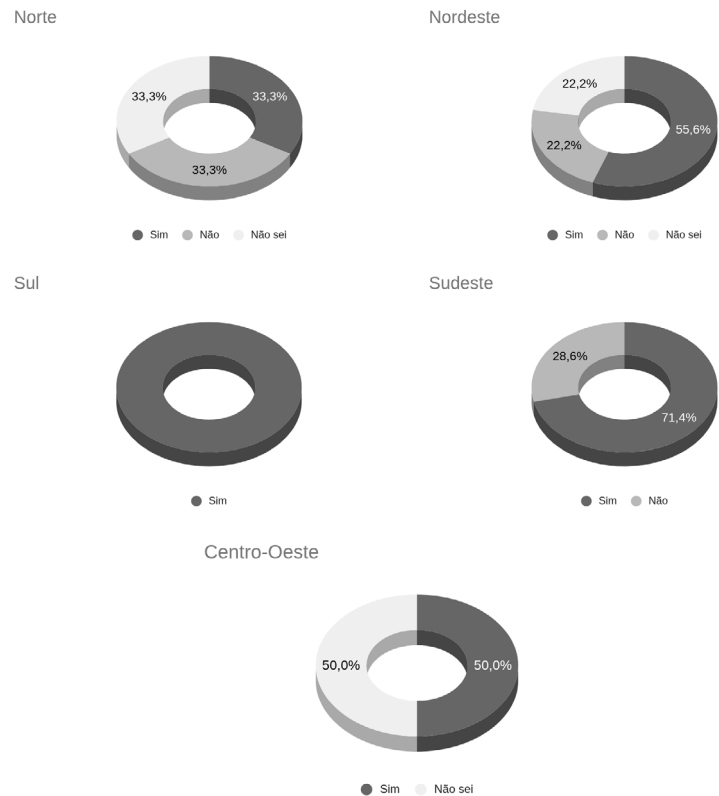
A terceira pergunta do bloco procurou avaliar se os mercados locais possuem capacidade de fornecimento dos canais de comunicação para as unidades do MPF. As respostas estão representadas nos Gráficos 11 e 12.

Gráfico 11 – Percepção quanto à capacidade de fornecedores locais



Fonte: elaborado pelos próprios autores com base nos dados coletados.

Gráfico 12 – Percepção quanto à capacidade de fornecedores locais, por região



Fonte: elaborado pelos próprios autores com base nos dados coletados.

Por fim, uma pergunta em texto livre solicitou que os fiscais informassem um valor médio de contratação de um canal de comunicação junto a fornecedores locais. A resposta a esta pergunta foi opcional e deverá ser reavaliada em futura contratação.

Entre os critérios estabelecidos para a autorização de contratação de canais de comunicação de contingência, estava o de que o custo mensal não excedesse a 15% do valor do canal equivalente no contrato n. 13/2023. Esta pergunta pretendia complementar a anterior, com a análise do critério custo mensal de uma eventual contratação.

As unidades que obtiveram autorização para a contratação de canais de contingência tiveram dificuldades em adequar os custos ao critério estabelecido. Em futuras contratações, para uma melhor análise quanto à economicidade e governança da rede, este critério deverá ser revisto.

Ao examinar as respostas da *survey* especificamente para as unidades que necessitaram de contingência, observa-se que as percepções variam, mas confirmam a existência de problemas ou a busca por modelos alternativos:

- Rio Grande do Sul e Espírito Santo: Pelo menos um respondente em cada um desses estados indicou que a percepção da qualidade do serviço prestado piorou em relação aos contratos anteriores. Outro respondente do Rio Grande do Sul classificou a qualidade como “Nem piorou, nem melhorou”, e outro do Espírito Santo deu a mesma avaliação, indicando que a implementação do SDWAN, que buscava aprimorar a qualidade, não foi universalmente bem-sucedida nessas regiões que demandaram contingência.
- Minas Gerais e Bahia: Embora os respondentes dessas unidades tenham relatado que o serviço melhorou, os resultados ainda se correlacionam com a necessidade de contingência. O fato de que pedidos de contingência existiram (conforme o contexto da consulta e o referencial metodológico do artigo) sugere que, mesmo onde a percepção geral de qualidade melhorou, a resiliência ou a adequação do serviço nacional pode ter sido insuficiente em determinados momentos.
- Modelo misto: Os estados de Bahia e Minas Gerais apresentaram respostas favoráveis à adoção de um modelo misto de contratação

(parte centralizada para serviços SDWAN/segurança e parte descentralizada para os links de acesso). Essa preferência pelo modelo misto sugere uma busca por maior adaptabilidade local e melhorias na conectividade, validando a preocupação do artigo com a dificuldade em lidar com particularidades locais sob o regime centralizado.

6 Considerações finais

O *survey* demonstrou que o contrato n. 13/2023 manteve ou aprimorou a qualidade dos serviços de conectividade do MPF, e, considerando a distribuição geográfica, a complexidade da solução contratada e a percepção dos entrevistados, o modelo de contratação centralizado permanece como a melhor opção para serviços como o analisado.

Destaca-se que a percepção geral é de que a qualidade do serviço é adequada à instituição, uma vez que 84% das respostas consideraram o contrato satisfatório, mesmo nas unidades que obtiveram autorização para contratação de canais redundantes. Apesar de não ter obtido a percepção de todas as unidades da Federação, a amostra possibilitou a representatividade do cenário nacional. Assim, novos levantamentos poderão obter resultados diferentes dos ora apresentados.

A percepção de um percentual significativo dos fiscais setoriais foi que as equipes locais são insuficientes ou não possuem qualificação para a fiscalização contratual, corroborando para a manutenção do modelo centralizado de contratação, para objetos complexos e de abrangência nacional.

Os pedidos de canais de contingência validam a necessidade de examinar os impactos práticos da centralização, principalmente quanto às especificidades locais. Mesmo com a adoção do modelo centralizado, as equipes de contratação devem se atentar às peculiaridades locais e garantir a resiliência dos serviços em todas as unidades do país.

Todas as unidades do MPF que tiveram os pedidos de canais de contingência autorizados passaram, em maior ou menor grau, por algum tipo de problema ocasionado por questões climáticas ou de logística, o que pode ter influenciado diretamente tanto a percepção da qualidade quanto a real necessidade de contratação de canais redundantes.

Como melhoria identificada, considera-se imprescindível o envolvimento de representantes das unidades dispersas pelo território nacional, preferencialmente que representem todos os estados da Federação, como forma de garantir que as peculiaridades locais sejam observadas e novas contratações possibilitem a devida flexibilização, sem prejudicar a uniformidade e a qualidade dos serviços.

O alto percentual de respostas “Não sei” em questões cruciais, como as relativas à simplificação contratual e à vantajosidade de adoção do modelo misto de contratações, deve ser avaliado. A capacitação inadequada, o desconhecimento da legislação relativa a contratações e as falhas na divulgação dos procedimentos e parâmetros a serem observados são fatores a serem aprimorados para melhor atuação dos fiscais setoriais. Além da potencial falha na capacitação dos fiscais setoriais, nova análise do Instrumento de Medição de Resultados deve ser realizada, uma vez que a percepção geral é de que o objetivo de simplificação na fiscalização não foi atingido.

Grandes fornecedores ainda enfrentam dificuldades, decorrentes principalmente de questões de distribuição, infraestrutura e logística. Essa dificuldade, que pode sugerir que a adoção do modelo de contratação misto seja a solução, pode também ser interpretada de forma oposta, pois, se um fornecedor de atuação nacional enfrenta dificuldades, não há garantia de que pequenas empresas regionais, que em tese não possuem recursos técnicos e capacidade operacional aprimorados, ofereçam serviços com qualidade.

A análise da vantajosidade e da resiliência deve ser um esforço contínuo e estratégico, e um processo de contratação bem elaborado, com a consequente fiscalização contratual eficiente, promove diretamente a melhoria na prestação de serviços.

Em última análise, o sucesso das contratações centralizadas no MPF, especialmente em contratos de alta complexidade como o de n. 13/2023, depende da capacidade da Gestão Nacional de integrar as variáveis operacionais e as especificidades locais. O caminho apontado por esta pesquisa – que sugere o envolvimento imprescindível de representantes dispersos, a capacitação contínua dos fiscais setoriais e a consulta criteriosa ao mercado – fortalece o modelo centralizado, porém com olhar atento da Governança de TIC para

que a contratação tenha flexibilidade e possibilite adaptatividade à realidade institucional.

Referências

ALVES, Jamille Soares Moreira *et al.* Impacto econômico entre dois modelos de compras públicas: centralizado e descentralizado. **Revista Eletrônica Gestão & Saúde**, Brasília, v. 10, n. 3, p. 278-297, 2019. Disponível em: <https://tinyurl.com/32emm5uf>. Acesso em: 31 ago. 2025.

BRASIL. **Lei Complementar n. 75, de 20 de maio de 1993**. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União. Brasília: Congresso Nacional, 1993a. Disponível em: <https://tinyurl.com/mryeexke>. Acesso em: 8 out. 2025.

BRASIL. **Lei n. 8.666, de 21 de junho de 1993**. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Brasília: Congresso Nacional, 1993b. Disponível em: <https://tinyurl.com/5n6uj7ze>. Acesso em: 9 out. 2025.

BRASIL. **Lei n. 14.133, de 1º de abril de 2021**. Lei de Licitações e Contratos Administrativos. Brasília: Congresso Nacional, 2021. Disponível em: <https://tinyurl.com/4tv6j3en>. Acesso em: 2 maio 2025.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução n. 102, de 23 de setembro de 2013**. Disciplina no âmbito do Ministério Público Brasileiro, procedimentos relativos à contratação de soluções de Tecnologia da Informação. Brasília: CNMP, 2013. Disponível em: <https://tinyurl.com/32kn8daz>. Acesso em: 12 maio 2025.

FERNANDES, Ciro Campos Christo. A centralização das compras na administração federal: lições da história. In: CONGRESSO CONSAD DE GESTÃO PÚBLICA, 8., 2015, Brasília. **Anais [...]**. Brasília: ENAP, 2015. Disponível em: <https://tinyurl.com/38rbtvwh>. Acesso em: 24 jun. 2025.

FERNANDES, Ciro Campos Christo. A organização da área de compras e contratações públicas na administração pública federal brasileira: o elo frágil. **Revista do Serviço Público**, Brasília, v. 67, n. 3, p. 407-432, 2016. DOI: <https://doi.org/10.21874/rsp.v67i3.672>. Acesso em: 2 maio 2025.

GÓIS, Lúcio. **Proposta de governança para as contratações estratégicas do Ministério Público Federal**. 2024. Dissertação (Mestrado em

Administração Pública) – Universidade Federal de Sergipe, São Cristóvão, 2024. 249 f. il. Disponível em: <https://tinyurl.com/2apuytmy>. Acesso em: 18 jun. 2025.

GÓIS, Lúcio; OURO, Abimael; MENDONÇA, Cláudio. Compras públicas centralizadas: vantagens e desvantagens à luz dos critérios de sustentabilidade. **Revista do Serviço Público**, Brasília, v. 75, n. 1, p. 161-180, 2024. DOI: <https://doi.org/10.21874/rsp.v75i1.10150>. Acesso em: 2 maio 2025.

LIMA, Bárbara Macena de. **Repercussões da centralização em contratações de serviços essenciais**: um estudo sobre o Instituto Nacional do Seguro Social. 2024. Dissertação (Mestrado em Administração Pública) – Escola Brasileira de Administração Pública e Empresas, Fundação Getúlio Vargas, Rio de Janeiro, 2024.

MPF – MINISTÉRIO PÚBLICO FEDERAL. **Portaria PGR/MPF n. 687, de 20 de dezembro de 2011**. Institui o planejamento estratégico do Ministério Público Federal para o decênio 2011-2020. Brasília: MPF, 2011. Disponível em: <https://tinyurl.com/5bxxrje4>. Acesso em: 10 maio 2025.

SAMPAIO, Rafael Cardoso; SABBATINI, Marcelo; LIMONGI, Ricardo. **Diretrizes para o uso ético e responsável da Inteligência Artificial Generativa**: um guia prático para pesquisadores. São Paulo: Sociedade Brasileira de Estudos Interdisciplinares da Comunicação – Intercom, 2024. Disponível em: <https://tinyurl.com/csasyuze>. Acesso em: 13 abr. 2025.

SILVA, Lucas Brito da. A utilização do modelo de compras centralizadas como estratégia de economicidade na Rede Ebserh. **Observatorio de la Economía Latinoamericana**, [s. l.], v. 22, n. 3, p. e3834, 2024. DOI: <https://doi.org/10.55905/oelv22n3-159>. Acesso em: 2 maio 2025.

A inteligência artificial generativa no Ministério Público do Distrito Federal e Territórios: desafios à segurança da informação e conformidade com a Lei Geral de Proteção de Dados Pessoais

Generative artificial intelligence in the Public Prosecutor's Office of the Federal District and Territories: challenges to information security and compliance with the General Data Protection Law

DOI: https://doi.org/10.63601/978-65-88299-52-4_3

André Kassio de Souza Lucena

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Servidor do Ministério Público Federal (MPF) na área de Tecnologia da Informação.

Thiago Duarte Mesquita

Mestre em Direito pela Universidade Católica de Brasília (UCB). Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Servidor do Ministério Público do Distrito Federal e Territórios (MPDFT). Assessor Jurídico na Unidade Especial de Proteção de Dados Pessoais no Conselho Nacional do Ministério Público (CNMP).

Resumo: Este estudo investiga os desafios impostos pela implementação da inteligência artificial generativa (*GenAI*) no Ministério Público do Distrito Federal e Territórios (MPDFT), com foco nos riscos à Segurança da Informação e na conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). A rápida adoção da *GenAI*, frequentemente sob a forma de *Shadow AI*, exige uma análise sobre a adequação dos mecanismos institucionais de controle. Adotou-se um estudo de caso qualitativo e exploratório, utilizando a estratégia de informantes-chave (N=8), cujos

dados foram submetidos à Análise de Conteúdo de Bardin. Os achados revelam um Paradoxo Produtividade-Vulnerabilidade, em que o entusiasmo pela eficiência coexiste com o temor de vazamento de dados sigilosos (75% consideram o risco crítico). Verificou-se que 50% dos especialistas consideram a governança de tecnologia da informação insuficiente, o que se estabelece como o principal impulsionador das práticas de *Shadow AI*. A conclusão central aponta que o desafio do MPDFT reside no déficit de governança habilitadora; não se trata de insubordinação, mas da carência de ferramentas oficiais e da necessidade de capacitação constante. O trabalho defende a urgência de a instituição transitar de um modelo meramente proibitivo para uma postura adaptativa, integrando o investimento em competências de TI e a garantia da conformidade ética para alcançar a maturidade em governança tecnológica da informação.

Palavras-chave: inteligência artificial generativa; segurança da informação; LGPD; governança de TI; *shadow AI*; MPDFT.

Abstract: *This study investigates the challenges posed by the implementation of Generative Artificial Intelligence (GenAI) within the Public Prosecutor's Office of the Federal District and Territories (MPDFT), focusing on Information Security risks and compliance with the General Data Protection Law (LGPD). The rapid adoption of GenAI, frequently in the form of Shadow AI, demands an analysis of the institutional control mechanisms' adequacy. A qualitative and exploratory case study was conducted, employing the key-informant strategy (N=8), with data analyzed via Bardin's Content Analysis. The findings reveal a Productivity-Vulnerability Paradox, where enthusiasm for efficiency coexists with the fear of classified data leaks (75% consider the risk critical). We found that 50% of specialists deem institutional governance insufficient, establishing this deficit as the primary driver of Shadow AI practices. The central conclusion indicates that the MPDFT's challenge lies in the lack of enabling governance; this is not insubordination, but a gap in official tools and the need for constant training. The research advocates for the urgent transition from a merely prohibitive model to an adaptive stance, integrating investment in IT competencies and ensuring ethical compliance to achieve technological governance maturity.*

Keywords: *generative artificial intelligence; information security; LGPD; IT governance; shadow AI; MPDFT.*

1 Introdução

A inteligência artificial generativa apresenta um dos principais desafios atuais para a Administração Pública, especialmente em instituições que lidam com dados sensíveis, como o Ministério Público. Embora essas tecnologias ofereçam ganhos em eficiência, inovação e

suporte à decisão, também introduzem riscos inéditos de segurança da informação, dependência tecnológica e violações à privacidade.

O Ministério Público do Distrito Federal e Territórios (MPDFT), em sua missão constitucional de defesa da ordem jurídica e dos direitos fundamentais, encontra-se diante de um dilema: aproveitar o potencial da *GenAI* ou expor-se a riscos significativos de *Shadow IT* e *Shadow AI*. Esses fenômenos descrevem o uso de tecnologias fora da governança institucional (Silic; Back, 2014), frequentemente sem controles adequados de segurança ou alinhamento às normativas legais (Haag; Eckhardt, 2017; Kopper; Westner; Strahringer, 2020).

Diante disso, este estudo investiga como a utilização da *GenAI* no MPDFT pode comprometer o princípio da segurança, previsto no art. 6º, VII, da Lei Geral de Proteção de Dados Pessoais (LGPD), e de que forma membros e servidores – gestores ou não – percebem riscos, benefícios e dilemas éticos associados.

A pesquisa combina pesquisa de campo via questionário online com análise de conteúdo qualitativa (Bardin, 2015), articulando os dados levantados com o referencial teórico e o arcabouço normativo vigente. Busca-se, assim, contribuir para a reflexão crítica sobre os limites e possibilidades do uso da *GenAI* no setor público, oferecendo subsídios para a gestão de riscos, a governança de TI e a conformidade regulatória.

2 Referencial teórico

O cenário organizacional contemporâneo é profundamente redefinido pelo avanço das tecnologias digitais, promovendo novas formas de interação, automação e processamento de dados, pessoais ou não. Contudo, a adoção acelerada da *GenAI*, e o seu uso incipiente e muitas vezes informal por servidores públicos, expõe uma tensão fundamental entre o ímpeto pela inovação e produtividade e a rigorosa necessidade de conformidade legal e segurança (Aragão; Streit, 2023). Para investigar essa dicotomia no contexto do MPDFT, o presente artigo articula quatro eixos teóricos e práticos interligados, os quais fornecem o arcabouço para a análise das percepções e dos riscos: *Shadow IT/Shadow AI* (Chin *et al.*, 2025), compreendido como o sintoma de falhas de governança que leva à adoção de tecnologias de *GenAI* não homologadas (Puthal *et al.*, 2025).

2.1 Inteligência artificial generativa: conceitos e usos

A *GenAI* representa um salto paradigmático no campo da inteligência artificial. É caracterizada, principalmente, pela capacidade de criar conteúdos originais – como textos, imagens, áudios e códigos – a partir do aprendizado obtido em extensos conjuntos de dados (OpenAI, 2025). Diferentemente dos sistemas tradicionais de IA, que focam em análise e classificação, a *GenAI* gera novas informações, simulando criatividade e raciocínio contextual (Duque-Pereira; Moura, 2023).

No contexto organizacional, essa capacidade traduz-se em ganhos substantivos de eficiência operacional, abrangendo desde a automação de tarefas repetitivas até o suporte a processos decisórios complexos, sendo um motor de produtividade (Chen *et al.*, 2021; Puthal *et al.*, 2025). Entretanto, essa mesma característica inovadora introduz uma série de questões sensíveis. O uso desregulado de ferramentas de *GenAI* levanta desafios críticos relacionados à confiabilidade, responsabilidade, transparência e ética (Chen *et al.*, 2021), que são exacerbados em ambientes que lidam com informações críticas.

A inteligência artificial generativa abrange diversos modelos, que podem ser categorizados de acordo com o tipo de conteúdo que produzem:

- **Large Language Models (LLMs):** modelos como GPT, Gemini e Llama, essenciais para a redação automatizada de documentos, sumarização de textos e apoio à pesquisa jurídica.
- **Modelos de Geração de Imagens e Multimídia:** a exemplo de DALL-E e Midjourney, aplicados em materiais de comunicação e visualização de dados (Ramesh *et al.*, 2021).
- **Modelos Especializados em Geração de Código:** modelos que auxiliam no desenvolvimento e na manutenção de sistemas institucionais (Chen *et al.*, 2021).

No âmbito do Ministério Público brasileiro, a exemplo do que foi identificado nos dados coletados no MPDFT, a *GenAI* tem sido rapidamente incorporada em atividades como elaboração de minutas e síntese de documentos complexos. No entanto, o entusiasmo pela produtividade esbarra na realidade da *Shadow AI*. Esse cenário eleva os riscos de segurança, como o vazamento de dados sigilosos e o descumprimento

de normas como a LGPD, um desafio já mapeado na literatura sobre *Shadow IT* em organizações públicas brasileiras (Aragão; Streit, 2023).

Portanto, a adoção da *GenAI* no serviço público não exige apenas a compreensão de seu potencial transformador, mas fundamentalmente a implementação de estruturas de Governança de TI capazes de definir de forma clara a transparência e a prestação de contas (*accountability*) sobre o tratamento de dados (Pinheiro, 2020; Weill; Ross, 2004). Essa forma de gestão procedimental é indispensável para assegurar a conformidade regulatória e o uso ético e responsável da tecnologia.

2.2 *Shadow IT* e *Shadow AI*

O conceito de *Shadow IT* refere-se ao uso paralelo de soluções e ferramentas de Tecnologia da Informação sem o conhecimento ou a aprovação formal do departamento de TI da organização (Behrens, 2009). Conforme argumentam Silic e Back (2014), esse fenômeno não deve ser visto meramente como uma violação de política, mas como um sintoma de falhas de governança. A *Shadow IT* emerge quando o departamento de TI não apresenta soluções que os usuários necessitam para lidar com as demandas, levando os colaboradores a buscarem formas mais funcionais de realizar suas tarefas (Behrens, 2009). Tal procedimento, embora motivado por demandas de produtividade, acarreta riscos de segurança e conformidade (Haag; Eckhardt, 2017).

Com a ascensão exponencial da inteligência artificial generativa, o conceito evoluiu para a *Shadow AI* (Krantz; MCgrath; Jonker, 2025), definido como o uso de aplicações de IA não homologadas para atividades corporativas (Chen *et al.*, 2021; Puthal *et al.*, 2025). Essa prática é impulsionada pela busca por produtividade e agilidade – conforme identificado nos resultados desta pesquisa –, mas cria um dilema crítico (Chin *et al.*, 2025) tanto no setor privado quanto no setor público.

Estudos demonstram que a *Shadow AI* tende a emergir em situações de alta pressão por inovação, em que servidores utilizam aplicações públicas para acelerar tarefas de apoio, como produção de relatórios ou análises preliminares (Klotz *et al.*, 2019). No setor público, o risco é potencializado pela natureza sensível dos dados tratados.

No contexto do MPDFT, a *Shadow AI* manifesta-se quando membros e servidores utilizam ferramentas de *GenAI* para tarefas institucionais sem supervisão ou homologação. Essa prática, embora potencialmente eficiente para ganhos de produtividade imediatos, cria vulnerabilidades críticas de segurança e conformidade regulatória.

2.3 A LGPD e o princípio da segurança

A Lei Geral de Proteção de Dados Pessoais estabelece princípios fundamentais que orientam o tratamento de dados pessoais, dentre os quais se destaca o princípio da segurança. Previsto no art. 6º, inciso VII, esse princípio impõe aos controladores – públicos e privados – o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas que possam comprometer sua integridade, disponibilidade ou confidencialidade.

Nesse contexto, a inserção de dados pessoais em aplicações de *GenAI* configura, inequivocamente, uma operação de tratamento de dados, nos termos do art. 5º, inciso X, da LGPD. Todavia, em grande parte dessas situações, o tratamento não seria necessário à finalidade pretendida, o que pode acarretar ausência de base legal legítima, conforme dispõem os arts. 7º, 11, 14 e 23 da referida lei. Com efeito, evidencia-se violação à norma e exposição do titular.

Assim, o princípio da segurança, além de exigir a implementação de controles técnicos e organizacionais que garantam a proteção sistêmica dos ambientes de tecnologia da informação, também orienta condutas prudentes e preventivas por parte dos usuários institucionais. No âmbito do MPDFT, essa diretriz consiste, de forma prática e efetiva, em evitar a inserção de dados pessoais em aplicações de *GenAI*, salvo quando houver necessidade comprovada e respaldo jurídico. Essa postura representa não apenas uma medida de conformidade com a LGPD, mas também uma expressão concreta da segurança da informação enquanto valor institucional, reforçando a cultura de proteção de dados no ambiente organizacional.

No entanto, estudos têm evidenciado um déficit de compreensão prática da LGPD entre profissionais de tecnologia da informação, o que se reflete em vulnerabilidades na implementação de políticas e controles

de segurança (Fernandes *et al.*, 2021). No contexto de ferramentas baseadas em *GenAI*, essa limitação torna-se ainda mais evidente, uma vez que o uso de plataformas públicas para o processamento de informações pode expor dados institucionais sensíveis ou mesmo violar obrigações legais de sigilo e de proteção de dados.

Essas dificuldades revelam um descompasso entre o arcabouço normativo e as práticas tecnológicas emergentes, indicando a necessidade de novas abordagens de governança e de conformidade que conciliem o avanço tecnológico com a proteção efetiva dos direitos fundamentais à privacidade e à proteção de dados pessoais. Assim, a adoção de soluções inovadoras deve estar intrinsecamente vinculada à consolidação de uma cultura institucional de segurança da informação e à capacitação contínua dos profissionais envolvidos na gestão e no tratamento de dados.

2.4 Governança de TI e governança de IA

A governança de TI, segundo Weill e Ross (2004), consiste em mecanismos que definem direitos de decisão e responsabilidades para garantir o uso eficiente e seguro da tecnologia em prol dos objetivos organizacionais. No entanto, a *GenAI* demanda novas formas de governança adaptativa, considerando a velocidade de mudanças tecnológicas e a ausência de padrões regulatórios consolidados (Teixeira; Magro, 2020).

Isso implica na criação de políticas específicas para IA, comitês multidisciplinares de acompanhamento e estratégias de capacitação contínua. A ausência de tais mecanismos abre espaço para práticas de *Shadow AI*, ampliando os riscos de inconformidade.

2.5 Governança de TI na era da IA: do controle à adaptação

Em sua essência, a governança de Tecnologia da Informação consiste na definição clara dos direitos de decisão e das responsabilidades organizacionais (Weill; Ross 2004). No âmbito do Ministério Público do Distrito Federal e Territórios, verifica-se que o modelo tradicional de governança, baseado em estruturas hierarquizadas e em mecanismos de controle estrito, tem se mostrado insuficiente para lidar com a natureza distribuída e o ritmo acelerado de evolução da *GenAI*.

Diante desse contexto, impõe-se a adoção de um modelo de governança adaptativa e descentralizada, com a instituição de pontos focais de governança em cada unidade ou área estratégica (Teixeira; Magro, 2020). Tal configuração promove maior agilidade decisória, responsabilidade compartilhada e capilaridade na gestão de riscos e na conformidade institucional, acompanhando a própria descentralização dos serviços e fluxos informacionais do MPDFT. Assim, a governança passa a operar de modo coordenado, responsivo e alinhado aos objetivos institucionais, sem comprometer a autonomia operacional necessária à inovação tecnológica.

Impõe ressaltar que a ausência de diretrizes claras e de mecanismos eficazes de controle sobre o uso da *GenAI* suscita questões relevantes de *accountability* e de transparência, pilares estruturantes da Lei Geral de Proteção de Dados Pessoais. Essa lei estabelece, em seu art. 6º, inciso VI, o princípio da transparência, que impõe aos agentes de tratamento o dever de garantir aos titulares informações acessíveis e compreensíveis sobre a utilização de seus dados pessoais. O emprego de sistemas de *GenAI* sem supervisão humana ou governança adequada viola esse princípio, na medida em que inviabiliza a prestação de contas sobre quais dados foram utilizados, em que contexto e de que forma se chegou a determinada resposta algorítmica (Teixeira; Armelin, 2020). Tal cenário compromete o dever institucional de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais, conforme preconizado pela LGPD.

2.6 Arcabouço normativo no Ministério Público

Dentro desse cenário, o Conselho Nacional do Ministério Público (CNMP) já sinaliza preocupações com tecnologia e inovação. A Resolução n. 281/2023 (CNMP, 2023) estabelece diretrizes para o tratamento de dados pessoais, empregando medidas de governança de TI.

2.6.1 Resolução CNMP n. 281/2023

No plano nacional, destaca-se a Resolução CNMP n. 281/2023, que institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público. A norma prevê que cada ramo e unidade do Ministério Público implemente um Programa de Privacidade, baseado em princípios de segurança e prevenção,

com processos internos que assegurem conformidade com a LGPD. A resolução aproxima-se do conceito de *compliance*, entendido como conjunto de medidas de prevenção, monitoramento e resposta a riscos legais e éticos.

Em complemento, o MPDFT dispõe de um conjunto de instrumentos normativos e organizacionais, compreendidos como medidas técnicas e administrativas, que buscam assegurar governança, segurança da informação e conformidade com a legislação vigente. Esse arcabouço estabelece diretrizes para a gestão da tecnologia, da inovação e da proteção de dados pessoais, configurando-se como base essencial para disciplinar a adoção de novas tecnologias, como a *GenAI*, conforme se passa a expor.

2.6.2 Comitê Estratégico de Inovação e Governança de Dados (CEID)

O CEID, instituído pela Portaria Normativa PGJ n. 842/2022, tem como finalidade fomentar e priorizar projetos voltados à inovação e à gestão de dados no MPDFT. Entre suas competências, estão o apoio ao Programa de Governança de Dados Pessoais, a promoção do diálogo interinstitucional, a coordenação de políticas do Programa Prodados e a aproximação da instituição ao ecossistema tecnológico. O CEID pauta-se por princípios, como inovação, integração, transparência, segurança da informação e foco no usuário (MPDFT, 2022).

2.6.3 Comitê Estratégico de Tecnologia da Informação (CETI)

Criado pela Portaria Normativa n. 32/PGJ, de 26.12.2009, o Comitê Estratégico de Tecnologia da Informação (CETI) é responsável pela definição das diretrizes estratégicas de TI no MPDFT. Compete-lhe aprovar o Plano Diretor de TI, estabelecer prioridades de investimento, definir padrões de qualidade e segurança, avaliar indicadores de desempenho e emitir pareceres sobre estratégias de capacitação em TI. Dessa forma, o comitê atua como instância central de governança tecnológica da instituição.

2.6.4 Política de Segurança da Informação (PSI)

A Política de Segurança da Informação (PSI), instituída pela Portaria Normativa n. 177/2011, estabelece diretrizes voltadas à proteção da confidencialidade, integridade e disponibilidade das informações

sob responsabilidade do MPDFT. Além disso, a norma criou o Comitê Gestor de Segurança da Informação, responsável por supervisionar a implementação dessas diretrizes. A PSI constitui um dos principais marcos normativos capazes de disciplinar diretamente o uso da *GenAI*, ao vincular inovação tecnológica a requisitos de segurança (MPDFT, 2011).

2.6.5 Plano Diretor de Tecnologia da Informação (PDTI) 2021-2026

O Plano de Desenvolvimento de Tecnologia da Informação (PDTI) 2021-2026 é o principal instrumento de planejamento tático-operacional da TI no MPDFT. O documento define objetivos estratégicos, metas e iniciativas para garantir eficiência e conformidade. Embora não mencione explicitamente a *GenAI*, o PDTI contempla ações voltadas à gestão de riscos de TI, adequação à legislação de proteção de dados, tratamento de incidentes e fortalecimento da governança (MPDFT, 2021a). Essas medidas são compatíveis com a prevenção da *Shadow AI*, visto que disciplinam a adoção de novas tecnologias em alinhamento com a segurança institucional.

2.6.6 Plano Estratégico de Tecnologia da Informação (PETI) 2021–2026

O Plano Estratégico de Tecnologia da Informação (PETI) 2021-2026 orienta a atuação de TI em médio e longo prazos, alinhando tecnologia à missão e aos objetivos institucionais. O documento prevê indicadores de conformidade normativa, como o índice de aderência à Política Nacional de TI, e inclui iniciativas de adoção planejada de inteligência artificial e ciência de dados. Destacam-se objetivos relacionados ao fortalecimento da governança e à garantia de infraestrutura segura, elementos centrais para disciplinar o uso de *GenAI* de forma oficial e controlada (MPDFT, 2021b).

Em conjunto, CEID, CETI, Resolução CNMP n. 281/2023, PSI, PDTI e PETI constituem um arcabouço normativo robusto que sustenta a governança digital do MPDFT. Embora a *GenAI* ainda não seja tratada de forma explícita nesses documentos, os mecanismos já existentes oferecem instrumentos para regular seu uso, prevenir riscos associados a *Shadow AI* e assegurar conformidade com a LGPD.

3 Procedimentos metodológicos

A presente pesquisa foi concebida sob um desenho metodológico robusto, que articula a coleta e a análise de dados de natureza quantitativa e qualitativa, buscando não apenas descrever o fenômeno da *GenAI* no MPDFT, mas também interpretá-lo em seu contexto organizacional e legal (Creswell, 2014; Minayo, 2017).

3.1 Tipo e natureza da pesquisa

O estudo adota o paradigma quali-quantitativo misto, combinando técnicas para uma compreensão aprofundada do objeto. Classifica-se como pesquisa aplicada (Gil, 2002), visando gerar conhecimento de utilidade prática imediata para subsidiar a tomada de decisão em governança, segurança da informação e conformidade legal (LGPD) no MPDFT. O estudo possui ainda natureza exploratória, dada a incipiência teórica do tema no contexto do setor público (Haag; Eckhardt, 2017), e descritiva, ao mapear as percepções dos agentes institucionais sobre os riscos e benefícios da *GenAI*.

3.2 Delineamento e unidade de análise

O delineamento principal adotado foi o Estudo de Caso Único (Yin, 2018), focado no MPDFT. Essa escolha se justifica pela relevância da instituição no tratamento de dados sensíveis e sigilosos, o que amplifica os riscos de *accountability* e inconformidade legal associados ao uso de ferramentas de *GenAI* não homologadas, a *Shadow AI*.

3.3 População e amostra: a estratégia dos informantes-chave

O universo da pesquisa compreendeu membros e servidores que atuam em áreas com alta propensão ao uso de *GenAI* no MPDFT. A coleta de dados foi realizada por meio do questionário estruturado em agosto/setembro de 2025 e contou com oito respondentes (N=8), configurando uma amostragem não probabilística por conveniência. A estratégia dos informantes-chave foi intencional, privilegiando a

qualidade e a profundidade das percepções estratégicas em detrimento da amplitude estatística, servindo para mapear riscos sistêmicos.

Embora o número seja reduzido, a amostra provou ser qualificada e significativa para fins exploratórios, dada a experiência e capacidade decisória dos participantes.

A diversidade de funções contemplou tanto servidores com cargos técnicos quanto gestores e membros, oferecendo pluralidade de visões.

3.4 Instrumento de coleta e validação pré-teste

O instrumento de coleta foi um questionário estruturado de quatorze perguntas (fechadas e abertas), fundamentado em referências legais (LGPD e resoluções CNMP) e teóricas. O instrumento foi dividido em quatro blocos temáticos, cada um composto por perguntas fechadas e abertas:

1. Perfil do respondente – tempo de instituição, função, cargo.
2. Conhecimento sobre LGPD, governança e cultura organizacional – familiaridade com a Lei n. 13.709/2018, percepção sobre mecanismos de governança e clareza institucional.
3. Riscos e benefícios – avaliação das oportunidades e ameaças trazidas pela adoção de *GenAI*, com foco em segurança da informação, proteção de dados e produtividade.
4. Ética e capacitação – percepção de riscos éticos, viés algorítmico, imparcialidade e necessidade de treinamento.

O instrumento foi submetido a um pré-teste com especialistas, garantindo a validade de constructo e a confiabilidade do questionário (Gil, 2002), com ajustes focados na clareza da questão sobre *accountability* e na incorporação de categorias de risco tipificadas pela literatura. O documento encontra-se disponível no Anexo A.

3.5 Procedimentos de coleta e ética

A coleta de dados ocorreu em formato eletrônico, de forma síncrona, assegurando a voluntariedade e o anonimato dos participantes.

O estudo observou rigorosamente os princípios da ética em pesquisa, conforme preconizado pela Termo de Consentimento Livre e Esclarecido (TCLE), constante do formulário, sendo as transcrições utilizadas como evidências empíricas, mas desvinculadas de qualquer identificação pessoal.

3.6 Técnica de análise dos dados (Análise de Conteúdo de Bardin)

O tratamento dos dados empregou a Análise de Conteúdo em sua vertente temática, conforme metodologia adotada (Bardin, 2015). A análise seguiu os três momentos propostos: pré-análise, exploração do material e tratamento/inferência. As respostas foram inicialmente agrupadas em quatro categorias previamente definidas *a priori* pelo referencial teórico e aprofundadas pela leitura flutuante: Governança/Transparência; Riscos e Segurança; Benefícios e Produtividade; Ética e Capacitação.

4 Discussão dos resultados

Este capítulo apresenta a análise dos dados obtidos junto aos oito respondentes do MPDFT, utilizando a sistematização categórica da Análise de Conteúdo (Bardin, 2015) para discutir os achados sob a luz dos referenciais teóricos (Aragão; Streit, 2023; Haag; Eckhardt, 2017; Weill; Ross, 2004).

A análise dos dados primários, revelou um panorama complexo e multifacetado sobre a adoção da *GenAI* no ambiente institucional. Os achados confirmam a relevância da pesquisa ao apontar a coexistência de um alto potencial de eficiência com lacunas críticas de governança e segurança, especialmente em relação ao fenômeno da *Shadow AI*.

4.1 Perfil dos respondentes e conhecimento regulatório

O perfil dos respondentes, majoritariamente experiente (75% com mais de 10 anos) e com representatividade em cargos de gestão (37,5%), confere legitimidade às percepções sobre a cultura de segurança e governança. Quanto ao conhecimento regulatório, 87,5% afirmaram ter conhecimento geral sobre a LGPD; contudo, a Seção 4.3.1 revela que

este conhecimento teórico não se traduz em confiança nos mecanismos de controle institucional.

4.2 Categorias analíticas

A Análise de Conteúdo, ao cruzar as respostas manifestas com o conteúdo latente, resultou na construção das seguintes Categorias Analíticas, que guiaram a discussão sobre a tensão entre produtividade e segurança no MPDFT:

Quadro 1 – Análise de Conteúdo

CATEGORIA ANALÍTICA	DESCRIÇÃO	DADOS/EVIDÊNCIAS	CONEXÃO COM FUNDAMENTAÇÃO TEÓRICA
Déficit de Governança e <i>Accountability</i>	Sentimento de insuficiência nos mecanismos de controle e regulação da <i>GenAI</i> pela instituição.	“O Plano de Segurança da Informação do MPDFT só tem aspectos relacionados à rede e uso de maquinário. Não existe nada relacionado a segurança de informação dos dados.” [Respondente 2]	Weill; Ross, 2004.
Vulnerabilidade e Risco Crítico	Percepção de risco de segurança da informação e inconformidade com a LGPD devido ao uso de ferramentas externas (<i>Shadow AI</i>).	“O maior risco que enxergo é referente ao uso de dados sigilosos para treinar modelos de IA provados.” [Respondente 3]	Haag; Eckhardt, 2017; Klotz <i>et al.</i> , 2019.

CATEGORIA ANALÍTICA	DESCRIÇÃO	DADOS/EVIDÊNCIAS	CONEXÃO COM FUNDAMENTAÇÃO TEÓRICA
Benefícios e Produtividade	Reconhecimento dos benefícios da <i>GenAI</i> na rotina de trabalho, como celeridade e automação de tarefas repetitivas.	“Os benefícios principais que vejo são: ganho de produtividade, economia de tempo.” [Respondente 5]	OECD (<i>AI Principles</i> , 2024).
Risco Ético-Institucional	Preocupação com os vieses algorítmicos e o tratamento inadequado de informações sensíveis, ferindo a imparcialidade.	“A preocupação mais em voga é o tratamento das informações que são fornecidas à IA.” [Respondente 4]	Resolução CNMP n. 292/2024.
Demanda por Habilitação	Reconhecimento da necessidade de preparo formal e treinamento para o uso seguro da IAG.	“Capacitação é extremamente necessária.” [Respondente 7]	Aragão; Streit, 2023; Resolução CNMP n. 281/2023.

Fonte: elaborado pelos autores com base nas informações coletadas por meio do questionário de pesquisa.

4.3 Achados por categoria e implicações

A exploração do material empírico permitiu um aprofundamento nos dados quantitativos, transpondo a mera descrição estatística para a interpretação qualitativa. Nesse sentido, e sob o rigor da Análise de Conteúdo (Bardin, 2015), o estudo gerou inferências robustas e identificou implicações diretas para a gestão de Tecnologia da Informação no MPDFT. As próximas subseções, portanto, detalharão as tensões e as demandas centrais identificadas, articulando os achados da pesquisa de campo com o referencial teórico estabelecido.

**4.3.1 Governança e transparência:
déficit de governança e accountability**

A análise dos mecanismos de governança e controle revela uma ausência crítica de prontidão institucional. O achado central indica que 50% dos participantes afirmaram que os mecanismos do MPDFT são insuficientes ou inexistentes para regular o uso da *GenAI*, enquanto uma parcela expressiva (42,9%) declarou desconhecimento sobre sua efetividade.

Esta fragilidade de controle e comunicação (inferência, conforme Bardin, 2015) aponta diretamente para um “vazio de *accountability*” – a ausência de clareza sobre responsabilidades e supervisão institucional (Weill; Ross, 2004). O confronto entre o conhecimento regulatório e a percepção de controle revela uma lacuna crítica entre a letra da LGPD e a aplicação de seus princípios na rotina, conforme demonstrado no Quadro 2:

Quadro 2 – Fragilidade de Governança e Conformidade Legal

CATEGORIA ANALÍTICA	DADOS/EVIDÊNCIAS	POSSÍVEL IMPLICAÇÃO
Déficit de Governança e <i>Accountability</i>	87,5% afirmam conhecer a LGPD: “Treinamentos, conscientização e patrocínio no uso de dados, gestão consciente e alfabetização de dados para todos.” [Respondente 1] “Cursos sobre o uso de IA no contexto no MP, envolvendo questões de sigilo processual.” [Respondente 6]	O conhecimento da LGPD é declaratório, mas não se traduz em consciência dos riscos de segurança (art. 6º, VII). O servidor sabe o que é LGPD, mas não como ela é violada pela <i>Shadow AI</i> .

CATEGORIA ANALÍTICA	DADOS/EVIDÊNCIAS	POSSÍVEL IMPLICAÇÃO
Déficit de Governança e <i>Accountability</i>	50% percebem os mecanismos de governança e controle como “Parcialmente/ Não” eficazes: “As ferramentas oficiais de IA ofertadas aos usuários do MPDFT possuem a governança necessária. Contudo, considero impossível controlar como cada pessoa atua fora do alcance da instituição, utilizando-se de ferramentas de IA gratuitas ou pagas pessoalmente.” [Respondente 4]	Há um Vazio de Controle percebido pela metade da amostra. O uso da <i>GenAI</i> é uma zona cinzenta de regras.
Déficit de Governança e <i>Accountability</i>	Baixa clareza ou concordância na questão sobre transparência e prestação de contas: “Ainda não há um limite claro sobre o tratamento de dados fornecido a IAs. Como são manipulados, guardados e gerenciados os dados sensíveis.” [Respondente 6]	A ausência de clareza sobre a responsabilidade viola o princípio basilar da Transparência (LGPD, art. 6º, VI). Sem governança, o MPDFT não pode auditar ou explicar a origem de uma minuta gerada por IA externa.

Fonte: elaborado pelos autores com base nas informações coletadas por meio do questionário de pesquisa.

Este déficit de governança é o motor que cria um verdadeiro “buraco negro” de responsabilidade, a prova empírica da falha no pilar de Direitos de Decisão e Responsabilidades (Weill; Ross, 2004). A instituição perde a capacidade de garantir a rastreabilidade e a prestação de contas no uso da *GenAI*, tornando a conformidade com a LGPD meramente formal. Esta falha é sintetizada na crítica direta à priorização institucional: “Só se investe em novas soluções de IA. Não existe nenhum trabalho consciente no uso de dados, nem muito menos uma conscientização do

uso de dados pessoais e do fornecimento desses dados para IA generativa” [Respondente 2].

Implicação: Esse cenário favorece a emergência da *Shadow AI*, pois os servidores sentem-se obrigados a assumir, individualmente, responsabilidades que deveriam ser reguladas por normas e ferramentas institucionais. A ausência de clareza sobre a responsabilidade no uso da *GenAI* viola o princípio basilar da transparência, nos termos do art. 6º, VI (Brasil, 2018), sendo um risco de inconformidade regulatória.

4.3.2 Risco e vulnerabilidades

A análise da Seção 3 do questionário, Riscos e Benefícios, confirma a alta vulnerabilidade percebida pelos informantes. As respostas convergem, majoritariamente, para o temor da exfiltração de dados sensíveis e informações estratégicas, o que pode ser considerado um achado. Houve menções diretas à possibilidade de que dados de investigações e processos sigilosos sejam utilizados para treinar modelos de IA externos. Essa percepção é reforçada pela transcrição do informante: “[O] maior risco que enxergo é referente ao uso de dados sigilosos para treinar modelos de IA provados” [Respondente 3].

Essa constatação pela inferência (Bardin, 2015) consolida o clima de vulnerabilidade e risco crítico na instituição, pois o risco é percebido como real e, potencialmente, inevitável, dado o uso descontrolado da *Shadow AI*.

Consequentemente, a falta de diretrizes específicas de segurança da informação para o uso da *GenAI* fragiliza a conformidade com a LGPD, notadamente em seus arts. 46 e 47, expondo a instituição a severos riscos jurídicos e reputacionais. Ademais, a percepção desse risco não é apenas teórica, mas é potencializada pela crença de que os mecanismos de proteção internos são insuficientes: “[O] Plano de Segurança da Informação do MPDFT só tem aspectos relacionados à rede e uso de maquinário. Não existe nada relacionado a segurança de informação dos dados” [Respondente 2].

A visão do Respondente 2 evidencia que, sem uma política de segurança voltada especificamente aos dados processados por IA e não apenas à rede, a cadeia de custódia da informação é comprometida.

4.3.3 Benefícios e produtividade: o paradoxo da inovação e o motor da *Shadow AI*

A análise dos resultados demonstrou um consenso absoluto – 100% dos participantes reconhecem como positiva a utilidade e os benefícios da *GenAI*. Todos os informantes citaram ganhos diretos em eficiência, rapidez e economia de tempo, destacando a capacidade da tecnologia para automatizar tarefas repetitivas, como gerar minutas, relatórios e auxiliar em pesquisas jurídicas. Conforme aduz um dos respondentes, “[o]s benefícios principais que vejo são: ganho de produtividade, economia de tempo e melhoria dos resultados” [Respondente 6].

Essa constatação por inferência (Bardin, 2015) revela um *ethos* produtivista na instituição, no qual a *GenAI* é percebida como ferramenta essencial para manter e elevar a eficiência do serviço público.

No entanto, esse entusiasmo configura o Paradoxo Produtividade-Vulnerabilidade como um achado crucial: o dilema do “ganho imediato *versus* risco institucional”. A síntese dessa tensão ambivalente, que confirma o dilema central desta pesquisa, pode ser observada no Quadro 3:

Quadro 3 – Síntese da Tensão Produtividade vs. Risco

CATEGORIA ANALÍTICA	DADOS/EVIDÊNCIAS	POSSÍVEL IMPLICAÇÃO
<i>GenAI</i> como Vetor de Produtividade	Uso frequente (implícito); benefícios citados: minutas, relatórios, automação, celeridade. “melhorias de textos, automações.” [Respondente 7], “Celeridade e eficiência do serviço prestado à sociedade.” [Respondente 3]	Sentimento de Esperança/Otimismo. A <i>GenAI</i> é vista como uma ferramenta de excelência operacional que resolve gargalos de trabalho. O uso, mesmo não homologado, é uma escolha funcional do servidor.

CATEGORIA ANALÍTICA	DADOS/EVIDÊNCIAS	POSSÍVEL IMPLICAÇÃO
Riscos e Vulnerabilidade	75% identificam vazamento de dados ou ainda exfiltração como risco crítico: “A política de segurança da informação do MPDFT só tem aspectos relacionados a rede e uso de maquinário.” [Respondente 2, “Exfiltração de dados sensíveis: <i>prompts</i> podem conter informações de investigações.” [Respondente 7]	Sentimento de Medo/ Cautela. O servidor está consciente do risco institucional, mas a busca pela eficiência suplanta a conformidade na prática, evidenciando a base da <i>Shadow AI</i> .

Fonte: elaborado pelos autores com base nas informações coletadas por meio do questionário de pesquisa.

Implicação: O dilema do “ganho imediato, risco institucional” atua como o motor primário da *Shadow AI* no MPDFT. O servidor está ciente do risco de vazamento (75% o classificam como crítico), mas a pressão por produtividade e a promessa de celeridade levam à forte tendência de utilização da *GenAI*, mesmo em plataformas externas. Esse achado configura a prática da “produtividade a qualquer custo” (Gartner, 2023) e confirma a tese de que a *Shadow AI* é um sintoma de falha de governança, no qual os usuários buscam uma funcionalidade que a TI oficial não provê com a mesma agilidade (Evangelista; Dornelas; Lopes, 2020; Klotz *et al.*, 2019).

4.3.4 Ética e demanda por habilitação: o fator humano como multiplicador de riscos

A segurança e a governança no uso de inteligência artificial generativa estão intrinsecamente ligadas ao fator humano, com reflexos diretos na ética e na capacitação dos servidores. A pesquisa revelou que 37,5% dos respondentes têm preocupações éticas relevantes (Questão

13), que se concentram primariamente em torno da imparcialidade, do viés algorítmico e da falta de transparência – esta última considerada suficiente por apenas 12,5% dos participantes.

Esse conjunto de achados sublinha o Risco Ético-Institucional, pois o servidor demonstra estar atento ao potencial da *GenAI* de comprometer a justiça e a equidade, alinhando-se à Resolução CNMP n. 292/2024. A preocupação central, evidenciada pelo Respondente 4: “A preocupação mais em voga é o tratamento das informações que são fornecidas à IA”. Não é a tecnologia em si, mas o tratamento inadequado de dados sensíveis e o risco inerente aos algoritmos.

Um descompasso significativo foi notado entre instrução e prática: 62,5% dos respondentes receberam treinamento específico (Questão 14), mas 75% classificam o risco de vazamento como crítico. Isso indica que a capacitação, embora presente, torna-se inócua diante da carência de ferramentas oficiais e de uma cultura organizacional que prioriza a produtividade. O problema, portanto, não é a ausência de conhecimento teórico, mas sua dificuldade de aplicabilidade. A demanda por capacitação é “extremamente necessária” [Respondente 7], mas deve vir acompanhada da solução tecnológica.

A inferência dos dados (Bardin, 2015) revela que o servidor não rejeita a regulação, mas clama por uma governança habilitadora (Aragão; Streit, 2023). Esse modelo orientador deve transpor o conhecimento teórico para o uso prático, fornecendo soluções oficiais que facilitem o cumprimento da segurança e da ética, em vez de depender unicamente da disciplina individual.

Nesse contexto, a *Shadow AI* emerge, não como um ato de resistência ou insubordinação, mas sim como uma resposta racional à ausência de políticas claras e recursos formais. É a consequência direta de um descompasso gerencial que falha em conciliar a necessidade de produtividade do usuário (o Negócio) com os pilares éticos e os requisitos de segurança da informação.

A superação desse desafio exige, portanto, a integração de soluções regulatórias e o reconhecimento de que o servidor pede o “meio seguro” para trabalhar. A instituição precisa investir perenemente no desenvolvimento de competências em TI (Resolução CNMP n. 281/2023) para garantir, de forma efetiva, a conformidade ética (Resolução CNMP n. 292/2024), elementos cruciais para o avanço da maturidade em governança tecnológica.

Quadro 4 – Consciência Ética e Demanda por Solução

CATEGORIA ANALÍTICA	DADOS/EVIDÊNCIAS	POSSÍVEL IMPLICAÇÃO
Risco Ético-Institucional	Viés nos algoritmos, imparcialidade, discriminação, tratamento inadequado de informações sensíveis: “Risco de viés, o que é abordado adequadamente nas ferramentas oficiais” [Respondente 7]	O risco não é apenas técnico; é um risco à missão institucional do MPDFT. O servidor está atento ao potencial da IA de comprometer a justiça e a equidade, alinhando-se à Resolução CNMP n. 292/2024.
Demanda por Habilitação	Treinamento, capacitação, ferramentas oficiais, regulamentação, conscientização: “Cursos para orientar os usuários sobre como utilizar de forma segura a IA” [Respondente 5]. “Treinamento com os usuários, divulgações de boas práticas de uso de IA” [Respondente 7]	O servidor não pede a proibição da <i>GenAI</i> ; ele pede o “meio seguro” para usá-la. A instituição precisa investir em desenvolvimento de competências em TI (Res. CNMP n. 281/2023).

Fonte: elaborado pelos autores com base nas informações coletadas por meio do questionário de pesquisa.

4.4 Padrões transversais identificados na relação GenAI-MPDFT

A análise aprofundada dos resultados permitiu identificar quatro padrões transversais robustos que sintetizam a experiência dos informantes-chave e os achados centrais desta investigação. Esses constructos não se limitam a descrever as tensões e as demandas do corpo técnico; antes, fornecem a base empírica essencial para as implicações teóricas do estudo:

- 1. O Paradoxo Produtividade-Vulnerabilidade:** este padrão sintetiza o forte entusiasmo pelos benefícios operacionais da *GenAI* (como produtividade e rapidez) em simultaneidade com o temor crescente quanto à segurança da informação. Reflete, assim, a tensão inerente

entre o imperativo da eficiência e o mandamento legal de proteção de dados (LGPD), estabelecendo o ponto de partida para o risco sistêmico.

2. **O Déficit Crítico de Governança e Accountability:** expressa a ausência de clareza sobre responsabilidades e a carência de mecanismos de supervisão ou auditoria no uso da *GenAI*. Nomeado metaforicamente como o “buraco negro” da *accountability*, este padrão sinaliza que o déficit de governança (confirmado pela insuficiência percebida em 50% das respostas) é a principal falha sistêmica que permite o avanço dos riscos regulatórios na instituição.
3. **A Prevalência da Cultura da Eficiência e a Emergência da *Shadow AI*:** correlaciona o desejo de ganhos operacionais à falta de ferramentas formais, impulsionando a prática da *Shadow AI* como solução de contorno. Este padrão demonstra que a cultura da produtividade está, no momento, prevalecendo sobre a cultura da segurança, expondo a instituição ao Risco Ético-Institucional.
4. **Convergência para a Governança Hab:** materializa a demanda unânime dos servidores por soluções que transcendam a mera proibição ou restrição. Este padrão final indica que o caminho para a mitigação de riscos passa, obrigatoriamente, pelo fornecimento de ferramentas oficiais seguras e pela capacitação formal, endossando o conceito de TI Gerenciada pelo Negócio (demandada pelo usuário) dentro de uma estrutura de Governança Responsiva e Dinâmica.

5 Considerações finais

A presente investigação teve como objetivo principal analisar como a utilização da *GenAI* no MPDFT pode comprometer o princípio da segurança, previsto no art. 6º, VII, da Lei Geral de Proteção de Dados Pessoais e de que forma membros e servidores – gestores ou não – perceberam riscos, benefícios e dilemas éticos associados.

Por meio de um estudo de caso qualitativo, ancorado na percepção de informantes-chave com visão estratégica, os resultados obtidos não apenas permitiram o atingimento dos objetivos específicos – como a identificação do Paradoxo Produtividade-Vulnerabilidade e a análise

da Governança de TI –, mas também validaram o cenário de risco que permeia a busca pela eficiência institucional.

O achado mais significativo da pesquisa reside na confirmação do paradoxo da Produtividade-Vulnerabilidade: embora 100% dos informantes reconheçam o potencial da *GenAI* para otimizar tarefas repetitivas e aumentar a celeridade, este entusiasmo é neutralizado pela alta percepção de vulnerabilidade. A vasta maioria dos especialistas na amostra (75%) classificou o risco de vazamento de dados sigilosos como crítico. Essa tensão reflete a rápida, e muitas vezes descontrolada, inserção da *Shadow AI* no ambiente de trabalho.

A análise aprofundada revelou que a vulnerabilidade não é apenas tecnológica, mas sobretudo de governança de TI. Metade dos informantes (50%) indicou que os mecanismos atuais de controle são insuficientes para regular o uso da *GenAI*, e mais de 60% apontaram a ausência de capacitação específica sobre o uso seguro e responsável da tecnologia (62,5%). Tais lacunas corroem o princípio da *accountability* exigido pela LGPD, expondo o MPDFT a riscos de incidentes e responsabilização. O risco de reutilização de dados sensíveis por modelos externos de IA, explicitamente mencionado nas respostas, representa o cerne do problema de conformidade legal.

Em síntese, o trabalho contribui para o debate ao fornecer evidências empíricas da urgência em transpor o foco da mera inovação para a governança responsável da IA no setor público. O MPDFT necessita urgentemente de uma política de uso que não apenas coíba o uso da *Shadow AI*, mas que, sobretudo, forneça ferramentas seguras e treinamento contínuo para mitigar o risco humano. O caminho para a eficiência não pode jamais comprometer o dever constitucional de proteger o sigilo e a privacidade inerentes à função ministerial.

Como limitação, reconhecemos que a natureza exploratória e a estratégia de informantes-chave (N=8) não permitem a generalização estatística dos resultados para toda a instituição. Entretanto, a profundidade das percepções obtidas oferece um diagnóstico sólido e um ponto de partida para a agenda de pesquisa. Sugere-se que estudos futuros apliquem o instrumento de pesquisa em uma amostra quantitativa maior de servidores, ou que se realize uma análise comparativa

do risco e da governança da *GenAI* em diferentes órgãos do Ministério Público brasileiro.

Observa-se, portanto, que o fortalecimento de uma governança habilitadora mostra-se essencial para alinhar a inovação tecnológica às diretrizes estratégicas da instituição (Aragão; Streit, 2023).

Com base na análise dos dados e nos padrões transversais identificados, notadamente o Déficit Crítico de Governança e o Paradoxo Produtividade-Vulnerabilidade, as seguintes recomendações estratégicas são propostas para que o MPDFT (e órgãos públicos similares) avancem em sua maturidade tecnológica e jurídica:

- Regulamentação e diretrizes de uso específicas: é crucial a emissão imediata de normas internas que definam claramente quais tipos de dados (pessoais, sigilosos e estratégicos) podem ou não ser inseridos em plataformas de *GenAI* não homologadas. O objetivo é fechar as lacunas regulatórias que atualmente impulsionam o risco e a *Shadow AI*.
- Investimento em plataformas oficiais (TI Gerenciada pelo Negócio): o MPDFT deve acelerar o desenvolvimento ou a disponibilização de ferramentas de *GenAI* próprias e/ou licenciadas. Essas plataformas devem garantir o tratamento seguro e a não utilização dos dados institucionais para treinamento de modelos externos, efetivando o conceito de governança habilitadora.
- Capacitação contínua e obrigatória: criar um programa de treinamento contínuo e obrigatório, focado na Segurança da Informação e na Ética da *GenAI*, com ênfase na aplicabilidade da LGPD. Esse programa deve ser concebido para mitigar os riscos do fator humano. A intervenção humana é, de fato, a chave para o uso seguro da tecnologia, conforme apontado pelo pedido explícito: “Capacitação é extremamente necessária” [Respondente 7].
- *Accountability* e Transparência Tecnológica: é imperativo o estabelecimento de mecanismos de auditoria e registro (*logs*) que permitam a rastreabilidade do uso da *GenAI* nos processos decisórios. Essa medida garante a materialização do princípio da Transparência e a prestação de contas, mitigando o buraco negro da *accountability* identificado na pesquisa.

Referências

ARAGÃO, Renato da Silva; STREIT, Rosalvo Ermes. Shadow IT e TI gerenciada pelo negócio: uma análise das percepções sobre os riscos e benefícios em uma organização pública brasileira do setor financeiro. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. 51, p. 21-36, set. 2023. Disponível em: <https://tinyurl.com/5djcmr8y>. Acesso em: 9 maio 2024.

BARDIN, Laurence. **Análise de conteúdo**. Tradução de Luís Antero Reto e Augusto Pinheiro. Lisboa: Edições 70, 2015. Disponível em: <https://tinyurl.com/bd396zyt>. Acesso em: 27 fev. 2016.

BEHRENS, Sandy. Shadow systems: the good, the bad and the ugly. **Communication ACM**, v. 52, n. 2, p. 124-129, 1º fev. 2009. DOI: <https://doi.org/10.1145/1461928.1461960>.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: <https://tinyurl.com/3twv6hta>.

CHEN, Mark; TWOREK, Jerry; JUN, Heewoo; YUAN, Qiming; PINTO, Henrique Ponde de Oliveira *et al.* **Evaluating large language models trained on code**. New York: Cornell University, 14 jul. 2021. DOI: <https://doi.org/10.48550/arXiv.2107.03374>.

CHIN, Tachia; LI, Qi; MIRONE, Francesco; PAPA, Armando. Conflicting impacts of shadow AI usage on knowledge leakage in metaverse-based business models: A yin-yang paradox framing. **Technology in Society**, [s. l.], v. 81, p. 102793, 1º jun. 2025. DOI: <https://doi.org/10.1016/j.techsoc.2024.102793>.

CNMP – Conselho Nacional do Ministério Público. **Resolução CNMP n. 281, de 12 de dezembro de 2023**. Brasília: CNMP, 2023. Disponível em: <https://tinyurl.com/wesef7sn>. Acesso em: 30 jun. 2025.

CNMP – Conselho Nacional do Ministério Público. **Resolução CNMP n. 292, de 28 de maio de 2024**. Brasília: CNMP, 2024. Disponível em: <https://tinyurl.com/3n8abymp>. Acesso em: 3 mar. 2026.

CRESWELL, John W. **Research Design: qualitative, quantitative, and mixed methods approaches**. [S. l.]: Sage, 2014.

DUQUE-PEREIRA, Ives da Silva; MOURA, Sergio Arruda de. **Compreendendo a inteligência artificial generativa na perspectiva da língua**. [S. l.], 6 out. 2023. DOI: <https://doi.org/10.1590/SciELOPreprints.7077>.

EVANGELISTA, Verônica Silva; DORNELAS, Jairo Simião; LOPES, Mariana Almeida de Souza. Shadow IT: que controles a gestão da tecnologia pode estipular sem anacronismos. *In: CONTECSI USP – INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT VIRTUAL*, 17., 2020. **Anais [...]**. São Paulo: Faculdade de Economia, Administração e Contabilidade – Universidade de São Paulo, 2020.

FERNANDES, Márcio Aurélio de Souza *et al.* Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da computação em nuvem. **Revista Ibérica de Sistemas e Tecnologias de Informação**, [s. l.], n. E42, p. 374-385, 2021.

GARTNER. **Emerging tech**: Shadow IT in the age of generative AI. [S. l.]: Gartner, 2023. Disponível em: <https://tinyurl.com/3sekbs7y>. Acesso em: 30 set. 2025.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

HAAG, Steffi; ECKHARDT, Andreas. Shadow IT: A review and agenda for research. **Journal of Information Technology**, [s. l.], v. 32, n. 3, p. 1-21, 2017.

KLOTZ, Stefan; KOPPER, Andreas; WESTNER, Markus; STRAHRINGER, Susanne. Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review. **International Journal of Information Systems and Project Management**, [s. l.], v. 7, n. 1, p. 15-43, 1º jan. 2019.

KOPPER, Andreas; WESTNER, Markus; STRAHRINGER, Susanne. **From shadow IT to business-managed IT**: a qualitative comparative analysis to determine configurations for successful management of IT by business entities. *Information Systems and e-Business Management*, [s. l.], v. 18, n. 2, p. 209-257, 15 jul. 2020. DOI: <https://doi.org/10.1007/s10257-020-00472-6>.

KRANTZ, Tom; MCGRATH, Amanda; JONKER, Alexandra. **O que é IA invisível?** [S. l.]: IBM, 9 abr. 2025. Disponível em: <https://tinyurl.com/mswk7z75>. Acesso em: 30 set. 2025.

MINAYO, Maria Cecília de Souza. Amostragem e saturação em pesquisa qualitativa: consensos e controvérsias. **Revista Pesquisa Qualitativa**, [s. l.], v. 5, n. 7, p. 1-12, 1º abr. 2017.

MPDFT – Ministério Público do Distrito Federal e Territórios. **Plano Diretor de Tecnologia da Informação – PDTI 2021**, v. 1.4. Brasília: MPDFT, nov. 2021a. Disponível em: <https://tinyurl.com/536u4tjb>. Acesso em: 3 mar. 2026.

MPDFT – Ministério Público do Distrito Federal e Territórios. **Plano Estratégico de Tecnologia da Informação 2021-2026**. Brasília: MPDFT, 2021b.

MPDFT – Ministério Público do Distrito Federal e Territórios. **Portaria Normativa n. 177, de 30 de setembro de 2011**. Institui a Política de Segurança da Informação (PSI) no âmbito do MPDFT. Brasília: MPDFT, 2011.

MPDFT – Ministério Público do Distrito Federal e Territórios. **Portaria Normativa PGJ n. 842, de 8 de agosto de 2022**. Brasília: MPDFT, 2022.

OECD – Organisation for Economic Co-operation and Development. **AI Principles**. Paris: OECD, 2024. Disponível em: <https://tinyurl.com/4vuwf3w3>. Acesso em: 2 out. 2025.

OPENAI. **What is ChatGPT?** [S. l.]: OpenAI, 2025. Disponível em: <https://tinyurl.com/4ftpdezz>. Acesso em: 30 set. 2025.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

PUTHAL, Deepak; MISHRA, Amit Kumar; MOHANTY, Saraju P.; LONGO, Antonella; YEUN, Chan Yeob. Shadow AI: Cyber security implications, opportunities and challenges in the unseen frontier. **SN Computer Science**, [s. l.], v. 6, n. 405, 21 abr. 2025. DOI: <https://doi.org/10.1007/s42979-025-03962-x>.

SILIC, Mario; BACK, Andrea. Shadow IT – A view from behind the curtain. **Computers & Security**, [s. l.], v. 45, p. 274-283, 1º set. 2014. DOI: <https://doi.org/10.1016/j.cose.2014.06.007>.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais**: comentada artigo por artigo. 2. ed. rev., atual. e ampl. Salvador: JusPodivm, 2020.

TEIXEIRA, Tarcísio; MAGRO, Américo Ribeiro. **Proteção de dados**: fundamentos jurídicos. Salvador: JusPodivm, 2020.

WEILL, Peter David; ROSS, Jeanne W. **IT Governance**: how top performers manage IT decision rights for superior results. Boston: Harvard Business School Press, 2004.

YIN, Robert K. **Case study research and applications**: design and methods. 6. ed. Thousand Oaks: SAGE Publications, 2018.

ANEXO A

QUESTIONÁRIO SOBRE O USO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA (GenAI) NO MPDFT

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Declaração ética: Suas respostas são anônimas e serão usadas exclusivamente para fins de pesquisa acadêmica, conforme Resolução CNS 466/2012. O tempo estimado para preenchimento é de 5-10 minutos.

Título da pesquisa: Percepções de servidores e membros do Ministério Público do Distrito Federal e Territórios (MPDFT) sobre o uso da inteligência artificial generativa (GenAI), com foco em conformidade com a Lei Geral de Proteção de Dados (LGPD), governança, ética e segurança da informação.

Pesquisador(a) responsável: Nome: Andre Kassio de Souza Lucena. Instituição: Ministério Público Federal, Procuradoria da República em Alagoas. Contato: andrekassio@mpf.mp.br.

1. Sobre a pesquisa: Este questionário tem como objetivo investigar as percepções de servidores e membros do MPDFT sobre o uso da IA generativa. A pesquisa busca mapear conhecimentos, riscos percebidos, benefícios e sugestões para o uso responsável dessa tecnologia, alinhando-se às resoluções do Conselho Nacional do Ministério Público (CNMP) e à literatura acadêmica. Esta pesquisa será realizada exclusivamente online, por meio do preenchimento de um formulário eletrônico.
2. Participação voluntária e anonimato: Sua participação é voluntária e anônima. Nenhum dado pessoal que permita sua identificação (como nome, e-mail, IP, localização) será solicitado ou registrado. Você pode encerrar sua participação a qualquer momento, simplesmente interrompendo o preenchimento do formulário, sem necessidade de justificativa.
3. Riscos e benefícios: Não há riscos associados à sua participação. Os benefícios são indiretos, contribuindo para a produção de conhecimento científico sobre o tema da pesquisa.

4. Uso e compartilhamento dos dados: As informações coletadas serão analisadas de forma agregada, sem identificação dos participantes, e utilizadas apenas para fins acadêmicos e científicos. Os dados não serão compartilhados com terceiros fora da equipe de pesquisa.
5. Esclarecimentos: Em caso de dúvidas sobre a pesquisa ou seus direitos enquanto participante, você pode entrar em contato com o pesquisador responsável pelo e-mail andrekassio@mpf.mp.br.

DECLARAÇÃO DE CONSENTIMENTO:

- Leu e compreendeu as informações acima.
- Está ciente de que sua participação é anônima, voluntária e que pode desistir a qualquer momento.
- Concorda em participar desta pesquisa.

ACEITO participar da pesquisa nos termos apresentados. (Caso não aceite, favor não prosseguir com o preenchimento deste formulário.)

Seção 1 – Perfil do Respondente

1. Qual é o seu cargo na instituição?
2. Há quanto tempo você atua na instituição?

Seção 2 – Conhecimento sobre LGPD, governança e cultura organizacional

3. Você tem conhecimento sobre a LGPD, Lei n. 13.709/2018?
4. Você tem conhecimento sobre o princípio da segurança da LGPD, art. 6º, VII, da Lei n. 13.709/2018?

Justificativa ou comentário sobre o conhecimento da LGPD (opcional).

5. Na sua avaliação, o MPDFT possui mecanismos adequados de governança e controle para regular o uso de IA generativa?
6. A cultura organizacional do MPDFT favorece ou dificulta o uso seguro e responsável da IA generativa?

7. Você considera que há transparência e prestação de contas suficientes no uso da IA generativa (supervisão e auditoria de algoritmo) no MPDFT?

Alguma observação ou comentário?

Seção 3 – Riscos e benefícios

8. Para quais finalidades você utiliza (ou acredita que poderia ser utilizada) a inteligência artificial generativa no MPDFT?
9. Quais riscos relacionados à proteção de dados pessoais você percebe no uso da IA generativa no MPDFT, se houver?
10. Quais riscos adicionais à segurança da informação você percebe no uso da IA generativa no MPDFT, se houver?
11. Quais benefícios você percebe (ou acredita que podem existir) no uso da IA generativa no MPDFT?
12. Que propostas você sugere para mitigar riscos relacionados ao uso da IA generativa no MPDFT?

Seção 4 – Ética e capacitação

13. Na sua percepção, há preocupações éticas relevantes no uso da IA generativa no MPDFT? Se sim, quais?
14. Você já recebeu (ou considera necessária) capacitação ou treinamento específico sobre o uso seguro e responsável da IA generativa na instituição?

Comentário sobre ética ou capacitação.

Suas respostas são anônimas e serão utilizadas somente para fins acadêmicos.

Governança de TI e IA como ferramentas para inclusão digital e melhoria do serviço digital prestado pelo MPF

IT governance and artificial intelligence as tools for digital inclusion and improvement of digital services provided by the Federal Prosecution Service

DOI: https://doi.org/10.63601/978-65-88299-52-4_4

Andréa dos Santos Publio

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Direito Constitucional e Administrativo. Graduada em Direito. Servidora do Ministério Público Federal (MPF).

Fábio Santos Pimenta

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Servidor do Ministério Público Federal (MPF).

Resumo: A transformação digital tem redefinido a forma de prestação dos serviços públicos no Brasil, destacando a inclusão digital como essencial ao exercício da cidadania e do acesso a direitos fundamentais. Nesse contexto, a governança de Tecnologia da Informação (TI) e o uso estratégico da inteligência artificial (IA) configuram-se como instrumentos centrais para a redução de barreiras tecnológicas e ampliação da acessibilidade. Analisa-se aqui como a governança de TI e a IA podem contribuir para a redução da segregação digital causada pelo uso indiscriminado de IA e para o aprimoramento dos serviços do Ministério Público Federal (MPF), instituição cuja missão inclui a defesa da cidadania e a promoção da justiça social. A pesquisa, de natureza qualitativa e exploratória, fundamenta-se em análise documental, revisão de normativos institucionais e levantamento de iniciativas tecnológicas no Poder Judiciário e no próprio MPF. A partir dessa análise comparativa, foram identificadas boas práticas de governança e soluções de IA adaptáveis à realidade ministerial. Organiza-se a abordagem nas seguintes etapas: serviço público e governo digital; inclusão digital como

direito fundamental; prestação de serviços públicos no Brasil, transformação digital e governança de TI; experiências correlatas; serviço digital e inclusão digital no MPF e a contribuição da governança de TI e da IA na atuação do MPF. Os resultados indicam que o MPF realizou boas iniciativas de aplicação de IA, os contratos com as *big techs* evoluíram, assegurando compartimentalização de dados, em vez do seu compartilhamento, restando robustecer áreas como mecanismos de mitigação de vieses algorítmicos e arquitetura para interoperabilidade inclusiva.

Palavras-chave: governança de TIC; inteligência artificial; inclusão digital; Ministério Público Federal; serviços públicos digitais.

Abstract: *Digital transformation has redefined the provision of public services in Brazil, highlighting digital inclusion as an essential component of citizenship and access to fundamental rights. In this context, Information Technology (IT) governance and the strategic use of artificial intelligence (AI) are key instruments for reducing technological barriers and expanding accessibility. This study analyzes how IT governance and AI can contribute to improving the services of the Federal Prosecution Service (Ministério Público Federal – MPF), an institution whose mission encompasses the defense of citizenship and the promotion of social justice. The research, qualitative and exploratory in nature, is based on documentary analysis, institutional regulation review, and a survey of technological initiatives within the Judiciary and the MPF itself. From this comparative analysis, best governance practices and AI solutions adaptable to the institutional context were identified. The study is organized into the following stages: public service and digital government; digital inclusion as a fundamental right; provision of public services in Brazil, digital transformation and IT governance; related experiences; digital service and digital inclusion in the Federal Prosecution Service (MPF) and the contribution of IT governance and AI to the work of the MPF. The results indicate that the MPF has implemented promising initiatives in the application of AI. Contracts with big tech companies have evolved, ensuring data compartmentalization rather than data sharing. However, there is still a need to strengthen areas such as mechanisms for mitigating algorithmic bias and architectures that promote inclusive interoperability.*

Keywords: *ICT governance; artificial intelligence; digital inclusion; Federal Prosecution Service; digital public services.*

1 Introdução

A transformação digital alterou profundamente como os serviços públicos são disponibilizados e acessados pelos brasileiros atualmente (Philippi, 2023; Gonçalves; Luciani, 2022). O desenvolvimento acelerado de novas tecnologias, especialmente no campo da inteligência artificial, permite ampliar o acesso da população a direitos fundamentais por meio de plataformas digitais (Baptista; Antoun Netto, 2023), mas

o seu uso indiscriminado pode agravar a exclusão de parcelas vulneráveis da população, dificultando o acesso a informações e meios de efetivar seus direitos. Nesse contexto, a discussão sobre inclusão digital é necessária e pertinente, sobretudo diante do risco de aprofundamento das desigualdades sociais em razão da exclusão tecnológica. Trata-se, portanto, de um campo de interesse estratégico, que alia inovação, cidadania e justiça social.

Apesar dos progressos recentes, a análise de dados extraídos dos sites institucionais do Instituto Brasileiro de Geografia e Estatística (IBGE) e do Comitê Gestor da Internet no Brasil (CGI.br) evidencia que a universalização do acesso aos serviços digitais ainda enfrenta desafios significativos no Brasil. As informações do IBGE, provenientes da Pesquisa Nacional por Amostra de Domicílios Contínua – Tecnologia da Informação e Comunicação (PNAD Contínua TIC) –, e os dados do CGI.br, disponibilizados no relatório TIC Domicílios, demonstram que grupos vulneráveis, como populações rurais, idosos e comunidades de baixa renda, continuam enfrentando barreiras tecnológicas, educacionais e socioeconômicas que restringem o uso pleno dos serviços digitais. Esse cenário realça a necessidade de uma governança pública estruturada de forma integrada, aliando inovação tecnológica, eficiência administrativa e justiça social, visando assegurar a inclusão efetiva e equitativa de todos os cidadãos no ambiente digital.

Assim, o presente estudo analisa como o uso de ferramentas de inteligência artificial, alinhadas às diretrizes da governança de TIC, pode facilitar a promoção da inclusão digital, favorecer o acesso à informação e melhorar os serviços digitais oferecidos pelo Ministério Público Federal (MPF) aos cidadãos.

O MPF, por sua natureza institucional e missão constitucional de defesa dos direitos fundamentais, ocupa posição estratégica nesse debate. Além da atuação judicial, sua presença no ambiente digital e sua capacidade de interagir de forma acessível com a sociedade representam instrumentos relevantes de democratização e transparência. Nesse sentido, a integração entre governança de TIC e uso responsável da IA emerge como oportunidade de ampliar a efetividade dos serviços prestados pelo órgão, uma vez que a adoção indiscriminada de IA pode implicar na segregação digital.

Diversos trabalhos acadêmicos recentes já abordaram o impacto da transformação digital e da IA no setor público, com destaque para aplicações no Poder Judiciário e em órgãos de controle, voltadas principalmente à automação de processos e ao aumento da eficiência administrativa (Baptista; Antoun Netto, 2023). Este estudo aproxima-se dessa literatura ao reconhecer a relevância da tecnologia como instrumento de modernização institucional, mas distingue-se por focar o papel específico do MPF como promotor da inclusão digital, articulando as práticas de governança de TIC e o uso estratégico da IA. A pesquisa identificou boas iniciativas já implementadas pelo MPF no campo da inteligência artificial voltadas à ampliação do acesso e da acessibilidade digital, evidenciando o potencial da tecnologia para fortalecer a cidadania e a transparência institucional. Entretanto, reconhece-se que o uso indiscriminado da IA, sem a devida observância de princípios éticos e de governança, pode gerar novas formas de exclusão ou segregação digital. Assim, o estudo busca contribuir de maneira original na proposta de análise integrada entre governança e IA, demonstrando como o uso ético e responsável da tecnologia pode promover a inclusão e a equidade social, fortalecendo a missão constitucional do MPF de defesa dos direitos fundamentais e promoção da justiça social.

A metodologia do presente estudo envolveu pesquisa documental, consistente na análise de normas legais e documentos de instituições públicas do Poder Executivo, Judiciário e do próprio MPF, pertinentes e relevantes ao tema em debate, e estudo de alguns serviços digitais com utilização de IA já implementados pelo Poder Judiciário e pelo próprio MPF. Foram analisados textos legais, relatórios institucionais, estratégias de governança digital, publicações do Tribunal de Contas da União (TCU), da Escola Nacional de Administração Pública (Enap), do Comitê Gestor da Internet no Brasil (CGI.br) e documentos técnicos do MPF, com ênfase nos que tratam de governança de TIC, transformação digital e uso ético da inteligência artificial.

A seleção do material seguiu critérios de relevância temática, atualidade (documentos publicados entre 2020 e 2025) e representatividade institucional, priorizando fontes oficiais, marcos normativos e estudos acadêmicos reconhecidos. A inclusão de experiências correlatas no Poder Judiciário buscou oferecer parâmetros comparativos para a análise da governança tecnológica no MPF, permitindo identificar boas práticas, riscos e oportunidades de replicabilidade.

Reconhece-se, contudo, que o estudo apresenta limitações metodológicas decorrentes da natureza qualitativa e exploratória da pesquisa. A análise baseia-se em documentos disponíveis publicamente e em informações institucionais divulgadas até 2025, o que restringe a generalização dos resultados e pode deixar de contemplar iniciativas internas não publicadas. Ainda assim, a triangulação entre as fontes e a abordagem comparativa conferem consistência e validade interpretativa às conclusões apresentadas.

Para encaminhar a abordagem do tema, parte-se de um referencial teórico que trata de conceitos fundamentais como serviço público, Governo Digital, transformação digital, inteligência artificial, inclusão digital e governança pública, formando uma base inicial de informações necessárias para situar o debate e respaldar a análise subsequente.

Na sequência, examina-se a inclusão digital como um direito fundamental da população, discutindo sua relação com a plena participação dos cidadãos na sociedade da informação. Nessa etapa, busca-se demonstrar tanto os avanços proporcionados pela transformação digital no acesso aos serviços públicos quanto os desafios persistentes para assegurar uma participação social efetivamente democrática, justa e igualitária.

Posteriormente, o artigo contextualiza esse debate com a análise de experiências correlatas em órgãos públicos, destacando especialmente iniciativas do Poder Judiciário e levantando exemplos de boas práticas implementadas e disponibilizadas à população que podem servir de referência para o aprimoramento dos serviços oferecidos pelo MPF.

Após, a investigação se concentra na atuação do MPF no cenário da inclusão digital e nas iniciativas implementadas no fomento da inclusão digital que promovem o acesso e a acessibilidade digital, visando permitir que a população alcance os serviços públicos de forma democrática e igualitária e possa participar consistentemente da formação da vontade estatal. Também são discutidas as dificuldades enfrentadas e as oportunidades de aperfeiçoamento da ação ministerial em prol da coletividade.

Por fim, o estudo apresenta o potencial das aplicações de inteligência artificial e das melhores práticas de governança de TIC no âmbito do MPF, indicando de que maneira podem fortalecer o Governo Digital e aumentar a efetividade dos serviços prestados. Essa trajetória analítica, organizada de forma progressiva, garante a articulação entre

os objetivos definidos e as estratégias de desenvolvimento, oferecendo bases sólidas para as conclusões e sugestões apresentadas ao final.

2 Serviço público e Governo Digital

O serviço público constitui uma das expressões fundamentais da atuação administrativa do Estado, voltado à satisfação das necessidades coletivas. Segundo Di Pietro (2025), trata-se de uma atividade material atribuída legalmente ao Estado, a ser exercida diretamente ou por meio de delegação, sob regime jurídico público, com o objetivo de atender concretamente aos interesses da sociedade. Nesse contexto, a prestação de serviços públicos deve observar critérios de adequação, eficiência e segurança, conforme estabelecido no art. 22 do Código de Defesa do Consumidor (Lei n. 8.078/1990), sendo o acesso a tais serviços um instrumento de efetivação da cidadania e dos direitos fundamentais.

A digitalização da Administração Pública brasileira, potencializada pelo advento do Governo Eletrônico no início dos anos 2000, representou um marco na modernização das relações entre Estado e sociedade. Essa fase foi caracterizada pela informatização de processos administrativos e pela ampliação da transparência e do acesso à informação. A transição para o paradigma do Governo Digital, por sua vez, introduziu uma abordagem mais interativa e centrada no cidadão, promovendo a simplificação da experiência de uso dos serviços públicos e a integração entre plataformas governamentais (Gonçalves; Luciani, 2022).

O Governo Digital busca reconfigurar a relação entre o Poder Público e os cidadãos, por meio de serviços digitais acessíveis, transparentes e responsivos. A utilização de redes sociais como canais oficiais de comunicação, conforme previsto no Marco Civil da Internet (Lei n. 12.965/2014), exemplifica essa mudança, reforçando a interlocução direta e dinâmica com a sociedade.

A consolidação do Governo Digital no Brasil é respaldada por instrumentos normativos e políticas públicas voltadas à inclusão digital. A Lei n. 14.129/2021, que dispõe sobre os princípios e diretrizes do Governo Digital, estabelece como fundamentos a desburocratização, a modernização e a ampliação do acesso aos serviços públicos por meio de plataformas digitais, inclusive móveis; prevê, ainda, a disponibilização de serviços em

ambiente único, com possibilidade de atendimento remoto, sem exigência de presença física, promovendo maior eficiência e acessibilidade.

Dados da Pesquisa Nacional por Amostra de Domicílios Contínua – Tecnologia da Informação e Comunicação (PNAD Contínua TIC, IBGE, 2024) – indicam avanços na conectividade nacional, com 92,5% dos domicílios brasileiros acessando a internet em 2023 e crescimento expressivo do uso de dispositivos móveis, inclusive em áreas rurais e entre idosos. Esses indicadores evidenciam o potencial das tecnologias digitais como ferramentas de inclusão, embora persistam desafios relacionados à infraestrutura, à alfabetização digital e à equidade no acesso.

O Governo Digital deve ir além da procura por eficiência administrativa, como destaca Philippi (2023), buscando a inovação como valor público e promovendo a efetivação dos direitos sociais, visto que a inclusão digital é fundamental para a construção de um Estado democrático que responde às necessidades e aos interesses dos cidadãos.

A governança digital, nos termos da Lei n. 14.129/2021, exige a adoção de mecanismos de gestão de riscos (art. 48, I), controle interno (art. 48, II) e auditoria (art. 49), visando a melhoria do desempenho institucional e a tomada de decisões orientadas por evidências (art. 24, I, VII), ou seja, pautadas em dados concretos, informações factuais e análises críticas. A integração entre planejamento estratégico, gestão de riscos e controle de resultados é fundamental para garantir a segurança, a transparência e a efetividade das ações governamentais, proporcionando a prestação de serviços digitais por tecnologia de amplo acesso pela população, incluindo pessoas de baixa renda ou residentes em áreas rurais e isoladas, como preconizado no art. 14 da mencionada lei.

Assim, a transformação digital da Administração Pública brasileira não se configura apenas como um processo técnico, mas como uma estratégia de fortalecimento da cidadania, da equidade e da participação social. A construção de um Governo Digital inclusivo demanda, portanto, uma governança estruturada, ética e orientada ao interesse público.

3 Inclusão digital como direito fundamental

A inclusão digital configura-se como um direito fundamental no contexto da sociedade da informação, sendo relevante para o exercício

pleno da cidadania. Trata-se da capacidade de o indivíduo participar ativamente da vida social, econômica e política por meio do acesso equitativo ao mundo digital. Conforme Gonçalves e Luciani (2022), a inclusão digital transforma o cidadão em agente criador de soluções, desde que haja o desenvolvimento de competências tecnológicas adequadas.

As tecnologias da informação e comunicação no setor público oferecem oportunidades para alcançar alta eficiência, transparência e acessibilidade. Philippi (2023) destaca que essas tecnologias são capazes de economizar custos de operação, facilitar a prestação de serviços e proporcionar acesso à informação, além de ajudar no combate às assimetrias de informação, que podem resultar em termos desiguais para as relações estado-sociedade. A inclusão digital torna o controle social e a participação democrática mais eficazes ao fornecer acesso facilitado a dados e serviços.

A Lei n. 14.129/2021, que estabelece proposições para o Governo Digital, reforça esse entendimento ao exigir algumas funcionalidades das plataformas digitais públicas, como agendamento eletrônico, acompanhamento de demandas, avaliação de satisfação e notificações, bem como sistema de pagamento e ouvidoria. Elas também buscam proporcionar um serviço público simplificado, eficiente e fácil de usar, enquanto incentivam a equidade de acesso à informação do Estado (Brognoli; Ferenhof, 2020).

Do ponto de vista jurídico, a inclusão digital é reconhecida como um direito integrante do mínimo existencial, conforme o art. 7º do Marco Civil da Internet (Lei n. 12.965/2014). Philippi (2023) argumenta que esse direito pode ser exigido judicialmente, impondo ao Estado o dever de sua efetivação. A universalização do acesso à internet, portanto, não é apenas uma meta técnica, mas uma obrigação constitucional vinculada à promoção da dignidade humana.

No plano internacional, a Declaração sobre o Direito ao Desenvolvimento da Organização das Nações Unidas (ONU) e os Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 reforçam a essencialidade da inclusão digital como impulsionador de progresso. Metas como 8.2 (diversificação, modernização tecnológica e inovação), 9.b (apoio ao desenvolvimento tecnológico, pesquisa e inovação) e 9.c (aumento do acesso às tecnologias de informação e comunicação) evidenciam o compromisso global com a ampliação do acesso às tecnologias

de informação, à inovação e à modernização tecnológica, reconhecendo o indivíduo como sujeito ativo e beneficiário do desenvolvimento.

Apesar dos avanços normativos e tecnológicos, a realidade brasileira ainda apresenta barreiras significativas à inclusão digital. Três fatores relevantes na formação de bolsões de exclusão são: limitações cognitivas, técnicas e econômicas. As limitações cognitivas afetam, sobretudo, idosos e migrantes digitais (termo utilizado para designar indivíduos que nasceram antes da popularização das tecnologias digitais, como computadores pessoais, internet e dispositivos móveis e que, ao longo da vida, precisaram incorporar essas ferramentas em seu cotidiano pessoal e profissional), que enfrentam dificuldades de adaptação às novas linguagens e interfaces. As limitações técnicas concentram-se em áreas rurais e periféricas, onde a infraestrutura de conectividade é precária. Já as limitações econômicas decorrem da impossibilidade de aquisição de dispositivos e planos de acesso à internet por parte de populações em situação de vulnerabilidade.

A superação desses obstáculos exige políticas públicas intersetoriais e estruturadas. O Marco Legal da Inovação (Lei n. 10.973/2004, alterada pela Lei n. 13.243/2016) estabelece instrumentos de incentivo à pesquisa e à inovação, como a promoção de parcerias público-privadas e a criação de ambientes regulatórios experimentais (*sandbox*), que permitem o teste de tecnologias emergentes em contextos controlados.

Entretanto, mesmo com tais mecanismos, persistem desafios relacionados à descontinuidade de programas, inconsistência de portais digitais e ausência de monitoramento sistemático (Cerquinho; Tavares; Paula, 2015). Nesse sentido, a construção de uma cultura de dados na Administração Pública é fundamental para garantir que as ferramentas digitais gerem valor público e promovam inclusão de forma efetiva e duradoura.

4 Prestação de serviços públicos no Brasil, transformação digital e governança de TI

A prestação de serviços públicos no Brasil tem passado por uma reconfiguração impulsionada pela transformação digital, que redefine a relação entre Estado e sociedade. Essa mudança é motivada pela necessidade de maior eficiência administrativa, transparência institucional e

ampliação do acesso aos direitos. Conforme Gonçalves e Luciani (2022), a digitalização dos serviços públicos representa um instrumento estratégico para fortalecer a publicidade dos atos administrativos e consolidar a cidadania em um Estado Democrático de Direito.

A digitalização tem gerado impactos concretos na economia de recursos e na melhoria da experiência do usuário. Dados de 2019 indicam que mais de 500 serviços públicos federais foram digitalizados, resultando em uma economia de R\$ 345 milhões e na eliminação de aproximadamente 146 milhões de horas de espera em filas (Gonçalves; Luciani, 2022). Esse processo otimiza a gestão pública e promove maior comodidade e agilidade para os cidadãos, que podem acessar serviços remotamente, sem necessidade de deslocamento físico.

O crescimento do número de usuários cadastrados em plataformas digitais governamentais reflete essa tendência. Entre janeiro de 2019 e outubro de 2020, os cadastros passaram de 2 milhões para 80 milhões, evidenciando a adesão da população às soluções digitais e a ampliação do alcance dos serviços públicos (Gonçalves; Luciani, 2022).

A Estratégia de Governança Digital (EGD) orienta a implementação de políticas públicas voltadas à transformação digital, estabelecendo metas, indicadores e iniciativas que promovam a interoperabilidade entre os entes federativos. Um exemplo é o Sistema Eletrônico de Informações (SEI), desenvolvido pelo Tribunal Regional Federal da 4ª Região e cedido gratuitamente a instituições públicas desde 2013. O SEI, juntamente com o sistema E-Proc, pioneiro no peticionamento eletrônico judicial, representa avanços significativos na gestão documental e na tramitação processual (Baptista; Antoun Netto, 2023).

A expansão do SEI por meio do Programa Nacional de Processo Eletrônico (ProPEN) busca consolidar a padronização e a integração dos sistemas administrativos em todas as esferas da federação. Embora essa iniciativa traga benefícios como maior eficiência e uniformidade, também impõe desafios relacionados à autonomia dos entes subnacionais, exigindo reflexão jurídica sobre os limites e possibilidades dessa interoperabilidade (Baptista; Antoun Netto, 2023).

No âmbito do Poder Judiciário, destaca-se a criação da Base Nacional de Dados do Poder Judiciário (DataJud), instituída pela Resolução n. 331/2020 do Conselho Nacional de Justiça. Essa base alimenta o Sistema

de Estatística do Poder Judiciário (SIESPJ) e outros sistemas correlatos, como o Sistema Nacional de Controle de Interceptações (SNCI), promovendo maior transparência, planejamento estratégico e gestão baseada em dados. A inovação tecnológica também se manifesta na adoção de ferramentas de inteligência artificial. Em 2023, o Supremo Tribunal Federal lançou o Maria, um módulo automatizado de apoio à redação, desenvolvido em parceria com o JusBrasil. A ferramenta é capaz de gerar minutas de ementas, elaborar relatórios e realizar análises iniciais de petições, otimizando o trabalho dos servidores e promovendo maior celeridade processual.

Contudo, a crescente utilização de sistemas algorítmicos exige atenção aos riscos éticos e sociais, como o racismo algorítmico. A I Jornada da Justiça Federal pela Equidade Racial (2025)¹ produziu enunciados que orientam o desenvolvimento de tecnologias inclusivas, destacando a necessidade de representatividade nos dados, transparência nos critérios de seleção e respeito aos princípios da igualdade e da dignidade humana. Os enunciados também recomendam a inclusão de conteúdos sobre ética, diversidade e impacto social nos currículos de cursos de tecnologia e IA, visando prevenir a reprodução de vieses discriminatórios.

Um exemplo de aplicação ética e eficiente da IA no setor público é o Projeto Gaia, do Tribunal de Justiça do Rio Grande do Sul². Lançado em junho de 2025, o projeto utiliza IA generativa para automatizar a redação de documentos jurídicos e traduzir decisões judiciais para linguagem simples, por meio da ferramenta “Gaia Explica aí, Tchê!”. Essa iniciativa promove maior acessibilidade, reduz barreiras burocráticas e contribui para a efetivação da inclusão digital.

Dessa forma, a transformação digital na prestação de serviços públicos no Brasil não se limita à adoção de novas tecnologias, mas envolve uma reestruturação profunda da lógica administrativa, orientada por princípios de equidade, eficiência e participação social. A digitalização, quando acompanhada de governança responsável e sensibilidade ética, torna-se um vetor de democratização e fortalecimento institucional.

1 Evento realizado pelo CEJ e pelo STJ em 4 dez. 2024. Disponível em: <https://tinyurl.com/2tthtw9f>.

2 Vide: <https://tinyurl.com/4srejszw>.

5 Experiências correlatas

A literatura sobre Governo Digital e inteligência artificial no setor público tem se expandido de forma significativa nos últimos anos, com destaque para análises que discutem o impacto da digitalização na qualidade e no acesso aos serviços públicos (Gonçalves; Luciani, 2022; Philippi, 2023; Albuquerque; Costa, 2025). No contexto do Poder Judiciário e de órgãos de controle, destacam-se iniciativas como o Victor (Supremo Tribunal Federal), a Sofia (Superior Tribunal de Justiça), a Athena (Controladoria-Geral da União) e a Alice (Tribunal de Contas do Estado do Paraná). Tais sistemas exemplificam a aplicação da IA na triagem processual, na análise de contratos e na detecção de irregularidades (Baptista; Antoun Netto, 2023). Mais recentemente, o Projeto Gaia, desenvolvido pelo Tribunal de Justiça do Rio Grande do Sul, evidenciou o potencial da IA generativa na elaboração de documentos jurídicos e na tradução da linguagem técnica para uma linguagem simples, contribuindo para a inclusão digital e para a transparência institucional.

Apesar desses avanços, observa-se uma lacuna na literatura em relação à aplicação sistemática da IA no âmbito do MPF, especialmente quando associada às práticas de governança de TIC. Enquanto outros órgãos já consolidaram projetos de automação e atendimento digital, o papel do MPF como agente de inclusão digital ainda é pouco explorado. Essa ausência de estudos específicos reforça a pertinência de pesquisas que articulem inovação tecnológica, governança pública e direitos fundamentais.

A principal contribuição deste estudo reside, portanto, em propor uma reflexão crítica e fundamentada sobre como o MPF pode alinhar o uso de ferramentas de IA às diretrizes de governança de TIC, promovendo inclusão digital e fortalecendo a prestação de serviços digitais à sociedade. Diferencia-se de estudos anteriores por integrar as dimensões analíticas: a avaliação das diretrizes de governança já existentes no MPF; o estudo comparativo de casos de uso de IA em órgãos públicos brasileiros; e a proposição de recomendações práticas e de um modelo de governança que assegure eficiência, acessibilidade, ética e conformidade legal.

Essa abordagem não apenas amplia o debate acadêmico sobre a transformação digital no setor público, como também oferece subsídios concretos para o aprimoramento institucional do MPF, preenchendo uma lacuna ainda pouco explorada na literatura nacional.

6 Serviço digital e inclusão digital no MPF

Em consonância com sua missão institucional de proteção aos direitos fundamentais e promoção da cidadania, o MPF tem implementado estratégias voltadas à garantia da acessibilidade no ambiente digital. Em 2019, foram criados dois mecanismos para a inclusão de pessoas com deficiência: a Comissão Permanente de Inclusão, voltada às demandas internas da instituição, e o Grupo de Trabalho Pessoas com Deficiência da Procuradoria Federal dos Direitos do Cidadão (PFDC), com foco na atuação externa. Essas iniciativas representam avanços significativos na superação de barreiras estruturais e atitudinais. No âmbito da comissão, são desenvolvidas ações para identificar e atender às necessidades de servidores, membros e colaboradores com deficiência, promovendo o mapeamento de demandas e a eliminação de obstáculos à acessibilidade física e digital (Conheça [...], 2025).

Todas as soluções tecnológicas desenvolvidas pelo MPF devem observar os padrões nacionais e internacionais de acessibilidade, nos termos das normas da Associação Brasileira de Normas Técnicas (ABNT) e da Convenção sobre os Direitos das Pessoas com Deficiência da Organização das Nações Unidas (ONU), ratificada pelo Brasil, reforçando o direito de acesso à informação e à tecnologia. Ademais, deverão incluir a participação de servidores com deficiência nos testes de validação, o que, embora não constitua exigência explícita na lei, decorre, de forma prática, dos objetivos da Lei Brasileira de Inclusão (LBI – Lei n. 13.146/2015).

Além disso, os conteúdos digitais disponibilizados no Portal MPF, na intranet nacional e nas páginas locais são traduzidos para a Língua Brasileira de Sinais (Libras), por meio da ferramenta VLibras, ampliando o acesso à informação, observando os mandamentos legais dispostos na Lei n. 10.098/2000, que estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência e dispõe em seus arts. 17 e 18:

Art. 17. O Poder Público promoverá a eliminação de barreiras na comunicação e estabelecerá mecanismos e alternativas técnicas que tornem acessíveis os sistemas de comunicação e sinalização às pessoas portadoras de deficiência sensorial e com dificuldade de comunicação, para garantir-lhes o direito de acesso à informação, à comunicação, ao trabalho, à educação, ao transporte, à cultura, ao esporte e ao lazer.

Art. 18. O Poder Público implementará a formação de profissionais intérpretes de escrita em braile, linguagem de sinais e de guias-intérpretes, para facilitar qualquer tipo de comunicação direta à pessoa portadora de deficiência sensorial e com dificuldade de comunicação.

Como parte das estratégias voltadas à promoção da acessibilidade digital, o MPF tem ajuizado ações civis públicas em face de órgãos públicos e empresas privadas que não disponibilizam mecanismos de acessibilidade em seus sites e serviços eletrônicos, em desacordo com as normas legais e técnicas vigentes. Essas medidas visam garantir o exercício dos direitos das pessoas com deficiência no ambiente digital, conforme previsto na legislação brasileira.

Um exemplo da atuação do MPF em defesa da acessibilidade digital é a ação proposta contra a Agência Nacional de Telecomunicações (Anatel) e a Agência Nacional do Cinema (Ancine), com o objetivo de estabelecer regulamentações que assegurem a disponibilização de recursos como legendas, audiodescrição e tradução em Língua Brasileira de Sinais (Libras) nas plataformas de streaming (MPMT, 2024). A iniciativa evidencia o esforço institucional do MPF para garantir o cumprimento da legislação vigente e promover a inclusão de pessoas com deficiência no acesso a conteúdos digitais.

Ainda, o MPF ingressou com ação civil pública visando a implementação de serviços de internet e telefonia móvel em quilombo de Itaóca, SP (MPF, 2025), entre outras iniciativas de mesma natureza, evidenciando uma atuação em prol da equidade no acesso às tecnologias da informação e comunicação, especialmente entre populações vulnerabilizadas. Essas ações reforçam o papel do Ministério Público como agente na transformação digital inclusiva, trabalhando em prol da consolidação dos direitos sociais em um Estado Democrático de Direito. Além de sua atuação judicial, o MPF desenvolve iniciativas voltadas à promoção da acessibilidade digital, direcionadas tanto a órgãos da Administração Pública quanto ao setor privado. Por meio de recomendações, o MPF busca informar os gestores e administradores sobre a relevância da acessibilidade nos ambientes digitais, fomentando a adoção de boas práticas e a conformidade com os dispositivos legais vigentes.

Em um caso (MPF [...], 2025a), o MPF-SP recomendou ao governo federal a realização de ajustes na plataforma Gov.br para garantir maior acessibilidade a pessoas com deficiência visual. A recomendação surgiu

após denúncias de dificuldades enfrentadas por usuários com próteses oculares e deficiência visual durante o processo de autenticação por reconhecimento facial, como tempo insuficiente para captura da imagem, número limitado de tentativas e instruções em áudio dessincronizadas. O MPF concedeu um prazo de 60 dias para que o governo federal implementasse melhorias técnicas na plataforma. Além disso, o MPF-SP emitiu uma recomendação para que o governo regulamente, em até 45 dias, o art. 63 da Lei Brasileira de Inclusão (Lei n. 13.146/2015), que trata da obrigatoriedade de acessibilidade em páginas da internet mantidas por órgãos públicos e empresas privadas. A ausência de regulamentação técnica tem sido um obstáculo para a fiscalização, comprometendo o cumprimento da lei, especialmente em plataformas de *streaming* e comércio eletrônico (MPF [...], 2025b).

As ações desenvolvidas pelo Ministério Público Federal no campo da acessibilidade digital configuram uma estratégia institucional voltada à promoção da inclusão informacional. Com vistas à verificação da conformidade das plataformas digitais com os parâmetros técnicos estabelecidos pelo Modelo de Acessibilidade em Governo Eletrônico (eMAG), o MPF realiza auditorias periódicas nos sítios e serviços online do governo federal, utilizando como instrumento metodológico o Avaliador e Simulador de Acessibilidade em Sítios (ASES). Tais avaliações integram a política institucional de fiscalização da acessibilidade digital e são divulgadas por meio de relatórios públicos no Portal da Transparência do MPF, em consonância com os preceitos estabelecidos pela Lei n. 10.098/2000 e pela Lei n. 13.146/2015 (Estatuto da Pessoa com Deficiência).

O MPF busca parcerias estratégicas com outras entidades, como a SaferNet, para fortalecer o combate a crimes cibernéticos e promover a segurança e a inclusão digital, especialmente de grupos vulneráveis como crianças e adolescentes.

A atuação do MPF visa democratizar o acesso a serviços e informações digitais, permitindo que mais pessoas usufruam dos benefícios da tecnologia e promovendo uma cultura mais inclusiva e igualitária na sociedade; focando não apenas na acessibilidade em sites e portais governamentais, mas também dentro da própria instituição. Exemplo de boas práticas no âmbito interno são as instruções disponibilizadas a membros e servidores, como o curso “IA na prática, desvendando a

inteligência artificial generativa para o contexto jurídico”, promovido pela Secretaria de Gestão de Pessoas do MPF no primeiro semestre de 2025, que, além de difundir informações sobre o assunto, tinha sua conclusão como requisito para a liberação de senhas para acessar as ferramentas de IA disponíveis no órgão.

A acessibilidade, compreendida como a condição que permite, em igualdade de oportunidades, o alcance, a percepção e a compreensão de conteúdos, serviços e ambientes – físicos ou digitais – com segurança e autonomia, foi abordada no âmbito de capacitação interna promovida em maio de 2025, por meio do curso “Acessibilidade Digital: criando conteúdos digitais inclusivos”, ofertado na modalidade de educação à distância, ministrado por servidora do MPF.

Tal formação insere-se no escopo das ações voltadas à promoção da inclusão digital, tendo como objetivo central a difusão de conhecimentos que favorecem a produção de conteúdos acessíveis, capazes de atender às diversas formas de comunicação humana, como linguagem verbal, não verbal e sinalizada. A comunicação, enquanto elemento estruturante das relações interpessoais e sociais, demanda recursos que viabilizem sua compreensão por públicos diversos.

Nesse contexto, instrumentos como interpretação em Libras, assistentes virtuais e legendagem em vídeos constituem exemplos de acessibilidade comunicacional. A acessibilidade digital, por sua vez, diz respeito ao conjunto de recursos que tornam possível a navegação, o entendimento e a interação de qualquer pessoa na internet – independentemente de limitações sensoriais, cognitivas ou motoras – sem necessidade de suporte externo, contribuindo para a efetivação do princípio da universalidade no acesso à informação e aos serviços públicos.

O Laboratório de Inovação do MPF no Estado de São Paulo (InovLab)³ é outro exemplo de iniciativa da instituição em promover a inclusão digital, disponibilizando modelos de documentos elaborados em linguagem simples e realizando debates sobre o uso de novas tecnologias pelo órgão.

Para garantir a gestão eficiente, segura e alinhada da tecnologia da informação e comunicação com os objetivos estratégicos de uma

³ Vide: <https://tinyurl.com/4pycdphx>.

instituição, é necessária a organização de uma governança de TIC, que é um conjunto de estruturas e processos que visam garantir que a TIC suporte e maximize adequadamente os objetivos e estratégias da instituição, adicionando valores aos serviços entregues, balanceando os riscos e obtendo retorno sobre os investimentos em TI.

A transparência e a participação social são pré-requisitos para o desenvolvimento do país e para a consolidação de uma democracia digital e inclusiva. Nesse contexto, a governança pública assume papel estruturante, ao definir os princípios, mecanismos e práticas que orientam a atuação do Estado em prol do interesse coletivo. Ela compreende o conjunto de arranjos institucionais – formais e informais – que regulam como as decisões e ações públicas são planejadas, implementadas e avaliadas, assegurando a observância dos valores constitucionais, como a legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência, em um ambiente de constante transformação tecnológica e social.

O Tribunal de Contas da União (TCU) reforça essa concepção ao elencar sete princípios básicos que devem nortear a governança na esfera pública: capacidade de resposta, integridade, transparência, equidade e participação, *accountability*, confiabilidade e melhoria regulatória. Esses princípios constituem a base para o fortalecimento da legitimidade democrática, da efetividade das políticas públicas e da confiança da sociedade nas instituições (TCU, 2020).

Sob essa perspectiva, a governança de Tecnologia da Informação e Comunicação (TIC) e a governança da inteligência artificial (IA) devem ser compreendidas como desdobramentos operacionais da governança pública, aplicando seus valores e princípios ao ambiente digital. Assim, a governança pública oferece o marco normativo e ético que orienta o uso responsável das tecnologias, garantindo que a inovação e a automação contribuam para a inclusão, a transparência e a justiça social – e não para novas formas de exclusão ou opacidade decisória.

A governança de TIC compreende aquisição e contratação de serviços de tecnologia e outros aspectos como: a) segurança cibernética e privacidade dos dados, objetivando a proteção de informações sensíveis e pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), promovendo a capacitação dos agentes públicos e o reforço da ética no manejo de dados, evitando vazamentos

e compartilhamentos indevidos; b) atribuição de responsabilidades, definindo claramente quem planeja, decide, aprova e compra as tecnologias, e quem estabelece os padrões; c) monitoramento de desempenho, acompanhando o desempenho da tecnologia e dos contratos com fornecedores, garantindo que estejam alinhados às prioridades institucionais; d) políticas de dados abertos, gerenciando a abertura de dados para promover a transparência e a interoperabilidade; e) atribuição formal da função de governança e gestão de TIC, mesmo que não haja um departamento específico, visto ser fundamental que essa função seja formalmente atribuída a um setor ou órgão.

Quando alinhada estrategicamente, a governança de TI é o pilar para transformar a intenção de inclusão digital em realidade operacional (Philippi, 2023). O modelo de governança integrada, que desloca a inclusão digital de um mero projeto de TI para um requisito não funcional obrigatório em todo o portfólio de serviços digitais, sugere que seja reforçada no MPF.

Esse modelo, em desenvolvimento e aprimoramento no MPF, opera em três níveis interconectados:

- a. Nível estratégico (Comissão Estratégica de TI – CETI): define a inclusão digital como um objetivo de negócio prioritário. Isso se traduz na exigência de que os planos diretores de TI (PDTI) do MPF aloquem recursos e definam métricas de acessibilidade e usabilidade (*user experience* – UX) como indicadores-chave de desempenho (*Key Performance Indicators* – KPIs) obrigatórios.
- b. Nível tático (STIC elabora PDTIC e CETI aprova): responsável por operacionalizar a estratégia. Neste nível, o comitê deve instituir uma matriz de priorização de projetos que considere o fator de acessibilidade e alcance social com alto peso. Projetos que não demonstrem o uso de tecnologias inclusivas (ex: interoperabilidade com tecnologias assistivas, design responsivo para *mobile-first*) podem ser rebaixados ou rejeitados.
- c. Nível operacional (equipes de desenvolvimento e contratação): onde os *frameworks* de governança (como COBIT e ITIL) são adaptados. A fase de desenho de serviço deve incorporar *checklists* de conformidade com os padrões de acessibilidade (WCAG – Web

Content Accessibility Guidelines), garantindo que a arquitetura dos sistemas e a qualidade dos dados sejam intrinsecamente acessíveis.

A integração da governança de IA ocorre no nível tático, em que o comitê avalia as propostas de *machine learning* (ML) não apenas pelo seu potencial de automação, mas pela sua Avaliação de Impacto Algorítmico (AIA), garantindo que a inovação tecnológica no MPF seja sinônimo de justiça e acesso equitativo para todos os cidadãos.

Ainda, a adoção de IA pelo setor público, mesmo com o objetivo de ampliar a inclusão digital, não garante a equidade. Pelo contrário, a ausência de uma governança ética e responsável pode levar à perpetuação e até amplificação de vieses históricos, transformando a segregação digital em segregação algorítmica (Ribeiro; Segatto, 2025).

No contexto do MPF, a integração entre a governança de TI e a governança de IA ocorre de maneira progressiva e articulada, por meio dos Comitês de Governança de TIC, da Secretaria de Tecnologia da Informação e Comunicação (STIC) e das unidades de inovação. A IA é tratada como extensão natural da governança de TI, compartilhando seus princípios de segurança, gestão de riscos, interoperabilidade e conformidade com a Lei Geral de Proteção de Dados. Essa integração posiciona a IA como um subsistema estratégico voltado à automação inteligente e à tomada de decisão ética e transparente, fortalecendo a eficiência institucional e a confiança pública.

Além do mais, a análise de risco algorítmico deve ser prioritária. Sistemas de IA, treinados em dados passados que refletem desigualdades regionais ou socioeconômicas, podem inadvertidamente priorizar a atenção a determinadas demandas em detrimento de outras, falhando em garantir o acesso universal à justiça. Por exemplo, um sistema de triagem de denúncias (representações pelos usuários) pode ter seu desempenho otimizado para a linguagem formal típica de grandes centros, mas negligenciar a linguagem ou as queixas de comunidades de difícil acesso ou baixa escolaridade.

Para mitigar esse risco, torna-se imperativo que o MPF incorpore os princípios de transparência, auditabilidade e *accountability* em seus projetos de IA. A transparência exige a documentação completa dos algoritmos, dos dados de treinamento e das métricas de justiça utilizadas.

A Resolução CNJ n. 615/2025 fornece uma base regulatória, ao exigir o respeito aos direitos humanos e à diversidade no desenvolvimento da IA.

7 A Contribuição da governança de TI e da IA na atuação do MPF

A IA tem um potencial enorme para otimizar a interação da população com os serviços digitais do MPF, tornando-os mais acessíveis, eficientes e compreensíveis. A Resolução n. 615/2025 do Conselho Nacional de Justiça estabelece diretrizes importantes sobre a ética, transparência e governança na produção e uso da IA no Poder Judiciário, princípios que se aplicam ao MPF. A resolução destaca que a IA deve contribuir para a agilidade e coerência das decisões, ser compatível com os direitos fundamentais e atender a critérios éticos de transparência, previsibilidade, auditabilidade e garantia de imparcialidade.

Exemplos de IA no setor público brasileiro, como o Victor (STF) na triagem de processos, a Sofia (STJ) como assistente virtual jurídica, a Athena (CGU) na análise de contratos e licitações, a Alice (TCE-PR) na detecção de fraudes e o Projeto GAIA do TJ/RS, demonstram o potencial transformador da IA em órgãos de controle e justiça. A capacidade de detecção de fraudes e riscos por meio de modelos preditivos em contratos, licitações e prestações de contas também é relevante para a atuação do MPF.

Há órgãos, como o Conselho de Atividades Financeiras (Coaf), que desestimulam a utilização da inteligência artificial, impondo regras rigorosas, como as diretrizes firmadas por meio da Portaria Coaf n. 4, de 20 de março de 2025. Veja-se o disposto no art. 2º desta portaria:

É vedado o tratamento de dados e informações sujeitos a regimes jurídicos próprios de sigilo, a exemplo dos relacionados à produção de inteligência financeira, fiscalização de pessoas obrigadas e proteção de dados pessoais sensíveis em plataformas externas de IA generativa, inclusive a plataforma Microsoft Copilot (Windows, 365 e Bing), tal como atualmente contemplada em instrumentos contratuais vigentes.

Ainda, no art. 6º, restringe as decisões sobre o uso de IA, nos seguintes termos “É responsabilidade do integrante do Quadro Técnico do Coaf observar o regramento de sigilo de dados e informações que pretenda tratar em soluções de IAG”. O MPF tem avançado no

desenvolvimento de novas tecnologias incorporadas às atividades administrativa e fim da instituição, com destaque para o uso estratégico da IA. A Secretaria de Tecnologia da Informação e Comunicação do MPF, cuja missão institucional é “prover com excelência soluções de tecnologia da informação e comunicação para o cumprimento da missão institucional do Ministério Público Federal”, lidera o desenvolvimento de projetos inovadores que visam à modernização da atuação ministerial.

Entre as soluções implementadas, destacam-se:

- a. Apóia: sistema baseado em inteligência artificial generativa (IA) projetado para auxiliar na análise de procedimentos extrajudiciais (PEXT) e processos judiciais (PJ). Por meio da extração inteligente de informações das íntegras, o sistema classifica os dados em tipologias específicas conforme a classe e o objeto, sugerindo minuta segundo o caso concreto com os dados inferidos, em acordo com a jurisprudência, além de disponibilizar informações complementares elencadas como importantes no auxílio à tomada de decisão (antecedentes publicados pela Receita Federal em nome do autuado e informações de Notícias de Fato autuadas no MPF).
- b. Transcreve AI: solução para transcrição de áudios e vídeos atendendo às necessidades de gabinetes de membros e diversas áreas do MPF. Utilizada na transcrição de audiências judiciais, audiências extrajudiciais, reuniões e outras atividades que demandem o registro textual de falas.
- c. Alertas automáticos sobre atos de gestão de pessoal: envio de e-mails aos membros e servidores com alertas automáticos sobre atos de gestão de pessoal, como nomeações, exonerações e designações. O serviço utiliza inteligência artificial (IA) para identificar publicações de interesse no Diário Oficial da União (DOU), Diário Eletrônico do MPF (DMPF-e) e no Boletim de Serviço do Ministério Público da União (BSMPU).
- d. Automatização das requisições de processos judiciais do STJ: uso de inteligência artificial clássica para automatizar a requisição dos processos do STJ de interesse para o MPF, em razão da intervenção obrigatória prevista na Constituição Federal e nas normas legais. Diariamente, o Diário de Justiça Eletrônico (DJe) traz uma média de 4,5 mil publicações do STJ; a IA identifica os processos de

interesse e indica para requisição. Essas requisições de processos correspondem a mais de 75% das manifestações realizadas pelos ofícios do MPF com atuação no STJ.

- e. Único TRIA: solução de inteligência artificial integrada ao sistema Único para reduzir o tempo de triagem dos processos judiciais recebidos nos gabinetes.
- f. Único Resultado de Julgamento em Ações Penais: uso de inteligência artificial generativa em conjunto com técnicas de IA clássica para inferir informações do resultado do julgamento (tipo penal, pena, regime da pena, multa, data da sentença e juiz) dos réus em ações penais, com acesso facilitado à íntegra da sentença. A extração automatizada dessas informações agiliza o trabalho realizado pelos gabinetes dos membros.
- g. Aptus Secom – busca por similaridade semântica: o Aptus é a solução de pesquisa textual do MPF. A utilização de técnicas de similaridade, no canal de notícias da Secretaria de Comunicação (Secom), permitiu a busca de notícias que expressam a mesma ideia ou conceito.
- h. Ouvidoria: uso de inteligência artificial para identificar manifestações protocoladas pelo cidadão indevidamente no canal da Ouvidoria do MPF, com indicação de remessa à Sala de Atendimento do Cidadão.
- i. IDMask: utilização de técnicas de processamento de linguagem natural (NLP), especialmente Reconhecimento de Entidade Nomeada (NER), incluindo a tecnologia Transformers, para tratamento de informações pessoais contidas em documentos que tramitam no MPF. A aplicação recebe um arquivo em formato PDF, realiza a identificação das entidades que possuam informações pessoais, permite ao usuário a edição dos trechos identificados e produz um arquivo PDF com as informações pessoais ocultadas (tarjadas).

Essa iniciativa, IDMask, foi uma das vencedoras do Prêmio CNMP 2025, entregue no dia 10 de setembro de 2025. O projeto garantiu ao MPF o segundo lugar na categoria “Atuação Administrativa – Tecnologia da Informação”, sendo selecionado entre 90 semifinalistas.

Ao todo, mais de 770 iniciativas das unidades e ramos do Ministério Público brasileiro concorreram à premiação (CNMP, 2025).

Embora as iniciativas de integração da IA no âmbito do MPF representem avanços significativos em termos de inovação tecnológica e eficiência institucional, observa-se que a maior parte dessas soluções tem como foco principal a otimização de processos internos e o apoio às atividades de membros e servidores. Tais iniciativas, ainda que relevantes para o aprimoramento da gestão administrativa e da produtividade, não se orientam diretamente para a promoção da inclusão digital da população, o que revela uma lacuna na aplicação social das tecnologias emergentes e na efetivação do princípio da acessibilidade digital como dimensão da cidadania.

A utilização da IA generativa no MPF, embora promissora, exige cuidados e a superação de alguns desafios, como questões éticas e sobre transparência. É importante garantir que os algoritmos sejam auditáveis e que não reforcem vieses, promovendo a igualdade de tratamento. A Resolução n. 615/2025 do CNJ atualiza e expande diretrizes para o uso de inteligência artificial no âmbito do Poder Judiciário, com o intuito de garantir que a inovação tecnológica seja incorporada com transparência, controle humano e respeito aos direitos fundamentais. A norma estabelece diretrizes para o desenvolvimento, a implementação e o monitoramento de sistemas de IA, garantindo que sua utilização ocorra com transparência, rastreabilidade, supervisão humana e respeito aos direitos fundamentais. Entre as inovações trazidas, destacam-se a exigência de auditoria e classificação de risco das soluções de IA, a vedação de decisões de mérito totalmente automatizadas e a criação de um Comitê de Inteligência Artificial, responsável por acompanhar a aplicação das diretrizes e promover boas práticas de inovação responsável. Essa resolução consolida o entendimento de que a IA deve atuar como instrumento auxiliar da atividade jurisdicional, subordinada aos princípios da ética, da governança pública e da centralidade humana nas decisões judiciais, reforçando a importância de uma governança tecnológica alinhada aos valores constitucionais.

Nesse contexto, o MPF instituiu um grupo de trabalho temporário com o objetivo de elaborar uma proposta para a criação do Comitê de Governança de Inteligência Artificial. Esse comitê é concebido como um

órgão estratégico de inteligência institucional, com a finalidade de orientar e apoiar a tomada de decisões diante dos desafios e oportunidades decorrentes da adoção de tecnologias baseadas em IA. A proposta elaborada pelo referido grupo já foi formalmente apresentada e encontra-se em fase de deliberação interna, visando sua posterior aprovação e implementação das medidas necessárias à sua efetivação.

A conformidade com a LGPD é imperativa, especialmente na análise de dados sensíveis, exigindo rigor na segurança e privacidade. Outro cuidado fundamental é o investimento na formação continuada dos servidores para o uso e acompanhamento dos sistemas de IA.

A criação de normativos, comitês de ética e uma estrutura de gestão para a IA no órgão é indispensável. A utilização de software de código aberto é preferível, pois facilita a integração, promove um ambiente de desenvolvimento colaborativo e permite maior transparência.

A adoção de IA no MPF deverá estar alinhada aos princípios de governança de TI, como alinhamento estratégico (IA como ferramenta para aprimorar a missão institucional), criação de valor (aumento da eficiência operacional e melhoria dos serviços), gestão de riscos (identificação e mitigação de riscos de segurança e algoritmos), desempenho e conformidade (monitoramento contínuo da aderência às normas), além de observar os seguintes princípios: ética, transparência, segurança e privacidade, responsabilidade, conformidade legal, eficiência e criação de valor, sustentabilidade e evolução contínua dos sistemas de IA.

Seis pilares que podem embasar um modelo de governança de IA:

- a) Diretrizes Éticas e Jurídicas, estabelecendo normas claras, alinhadas à LGPD e à Constituição;
- b) Comitê de IA, criando uma instância consultiva e deliberativa sobre o uso ético e responsável da IA;
- c) Gestão de Dados, desenvolvendo infraestrutura robusta para garantir qualidade, segurança e governança de dados;
- d) Gestão de Riscos e Auditoria de IA, monitoramento constante de impactos e riscos dos sistemas de IA;
- e) Capacitação e Gestão de Competências, implementando programas contínuos de formação e desenvolvimento para os servidores;
- e, f) Monitoramento e Melhoria Contínua, avaliando periodicamente os modelos, impactos sociais e performance da IA.

No âmbito institucional do MPF, observa-se a incorporação gradual dos pilares da governança de IA, com diferentes graus de maturidade.

As diretrizes éticas e jurídicas estão consolidadas em políticas de segurança da informação e proteção de dados alinhadas à Constituição, à Lei Geral de Proteção de Dados e às orientações do CNMP e do CNJ. A governança institucional de IA é atualmente conduzida pelos comitês de TIC e pela STIC, enquanto a criação de um comitê específico permanece em fase de estruturação. A gestão de dados apresenta avanços significativos, com infraestrutura voltada à segurança, interoperabilidade e dados abertos, evidenciada pelo Sistema Único de Informações (Único). No entanto, a gestão de riscos e a auditoria algorítmica ainda se encontram em desenvolvimento, demandando protocolos próprios para avaliação de impactos éticos e sociais. A capacitação e a gestão de competências têm-se mostrado robustas, com programas voltados ao uso ético da IA e à inovação digital, e o monitoramento contínuo é realizado por meio de revisões periódicas das políticas de TIC, embora ainda careça de indicadores específicos de equidade e impacto social.

Esse direcionamento vem sendo adotado pelo órgão ministerial, consoante o Relatório de Gestão do MPF, que reforça a importância da transformação digital e da governança de TI como pilares estratégicos da atuação institucional, alinhando-se à missão constitucional do órgão e às demandas da sociedade em um ambiente marcado por mudanças tecnológicas aceleradas. O documento aponta avanços relevantes em áreas como planejamento estratégico, gestão de riscos e controles internos, bem como em capacitação de servidores e membros, com mais de 25 mil vagas ofertadas em programas presenciais e a distância.

Na dimensão tecnológica, destacam-se o aperfeiçoamento do Sistema Único, a integração com o sistema e-Proc, a adequação à LGPD, o uso de inteligência artificial em automação de cadastros e análise de dados, além da modernização da infraestrutura com migração para plataformas em nuvem. O relatório também evidencia os impactos positivos da ampliação do teletrabalho e do trabalho híbrido, que resultaram em ganhos de produtividade e economia orçamentária, e ressalta os investimentos em segurança da informação e modelos de governança orientados pela eficiência e pela transparência.

Apesar dos progressos, o documento reconhece os desafios persistentes relacionados à interoperabilidade entre sistemas, proteção de dados, agilidade institucional e comunicação multicanal com a sociedade. Ressalta-se, ainda, que o uso crescente de inteligência artificial

traz oportunidades de otimização, mas exige mecanismos de governança responsável e mitigação de riscos éticos e sociais.

Nesse contexto, o relatório conclui que a consolidação da gestão de riscos integrada à governança institucional, investimentos em tecnologias disruptivas como a IA, aliada à capacitação contínua de membros e servidores, são condições essenciais para assegurar a efetividade da transformação digital. A atuação do MPF ancorada no modelo de governança de TI, integrada à IA, proporciona a contínua melhoria do acesso dos cidadãos às tecnologias que promovem a cidadania digital (MPU, 2024b).

A concretização da governança de IA pode ocorrer por ferramentas de governança como o COBIT (*Control Objectives for Information and Related Technologies*), reorientando os princípios do ambiente de negócios para o setor público. O COBIT, que serve como um alicerce para a governança e gestão da TI, deve ser interpretado não como uma ferramenta para maximizar lucros, mas sim para maximizar o valor público. No MPF, isso significa que a governança de TI, guiada pelo COBIT, deve garantir que os investimentos e as iniciativas tecnológicas estejam alinhados à missão do órgão, priorizando a transparência, a prestação de contas, a conformidade legal e, sobretudo, a melhoria contínua do serviço digital prestado ao cidadão. A estrutura do COBIT permite, por exemplo, estabelecer uma cascata de objetivos que conecta metas institucionais, como a promoção da inclusão digital, a objetivos de TI mais específicos, como a garantia da acessibilidade e da segurança de um novo sistema de inteligência artificial. Dessa forma, o COBIT oferece a base necessária para que a tecnologia seja utilizada de forma estratégica e responsável, assegurando que cada projeto de inovação, incluindo o uso da IA, vise efetivamente a atender o interesse da sociedade.

Enquanto a governança de TI estabelece a estratégia e o alinhamento, a gestão de serviços garante que essa estratégia seja executada de forma eficaz. Nesse contexto, o ITIL (*Information Technology Infrastructure Library*) surge como um *framework* fundamental, oferecendo um conjunto de práticas que podem ser adaptadas ao setor público.

A formalização da governança de TI no MPF é reforçada pela adoção de frameworks e modelos reconhecidos internacionalmente, como COBIT, ITIL e PMBOK, que fornecem um conjunto de diretrizes e boas

práticas para orientar as atividades de TI e garantir o alinhamento com os objetivos do negócio.

No caso da Tecnologia da Informação e Comunicações (TIC), referindo-se ao conjunto de recursos tecnológicos que o órgão utiliza para processar, armazenar e disponibilizar informações, no MPF o COBIT é utilizado principalmente no gabinete da Secretaria de TIC, pela assessoria técnica. O ITIL é utilizado por várias áreas, principalmente em atendimento ao usuário e infraestrutura. O PMBOK é utilizado em projetos e iniciativas e está refletido no Sistema Eletrônico de Governança e Gestão Estratégica (SIGOV).

Um estudo qualitativo conduzido no próprio MPF, com foco na análise documental de projetos de sistemas, revelou um percentual de aderência às boas práticas do ITIL entre 40% e 60% (Barbiero, 2022). A pesquisa apontou uma lacuna significativa na fase de Transição de Serviço, onde a documentação dos projetos não continha elementos suficientes para uma avaliação completa. Relatórios internos indicaram que a criação de equipes de sustentação, a produção de documentação técnica e a capacitação de usuários eram frequentemente tratadas como “não escopo” dos projetos. Esse foco fragmentado no “desenvolvimento” em vez do “ciclo de vida completo do serviço” é uma das principais causas de problemas como retrabalho e insatisfação do usuário. A consequência direta é que, em determinado período analisado, mais de 50% da capacidade técnica da área de TI foi dedicada a atividades de sustentação (Barbiero *et al.*, 2022).

Essa situação revela uma contradição no panorama da governança de TI do MPF. De um lado, o órgão alcançou uma notável pontuação de 80% no Índice de Governança e Gestão de TI (iGovTI) e 71% no Índice de Capacidade em Gestão de TI (iGestTI) no Relatório de Gestão de 2022 (MPU, 2022), que o classifica como “aprimorado” na escala do TCU. De outro, a análise dos processos de gestão de projetos e serviços aponta para ineficiências operacionais. Isso sugere que o alto nível de maturidade do MPF pode ser mais estratégico e formal do que operacionalmente eficaz em todas as suas dimensões. A alta pontuação indica a existência de uma estrutura, de planos e de uma liderança alinhada, mas as dificuldades na execução e na transição de serviços demonstram que ainda há desafios a serem superados para que o alinhamento estratégico se traduza plenamente em eficiência operacional.

A análise dos relatórios de gestão do MPF evidencia um crescimento progressivo nos investimentos destinados aos serviços de tecnologia da informação e comunicação nos últimos anos. Entre 2021 e 2024, os recursos aplicados nessa área evoluíram de R\$ 32,1 milhões para R\$ 54,9 milhões, representando um aumento aproximado de 71% no período (MPU, 2024b). Essa expansão orçamentária reflete o reconhecimento institucional da importância estratégica da tecnologia para a modernização da atuação ministerial e para o fortalecimento de sua missão constitucional de promoção da cidadania e da justiça social.

Todavia, ao se confrontar a evolução dos investimentos com os desafios de governança e inclusão digital descritos pela literatura especializada e pelas práticas institucionais analisadas, verifica-se que o aumento dos gastos ainda carece de planejamento mais orientado por resultados e impacto social. Embora o MPF tenha alcançado avanços expressivos em projetos de automação e inteligência artificial – como o Apoia, o Único TRIA e o IDMask –, observa-se que parte significativa do orçamento de TI permanece concentrada em manutenção de infraestrutura e sistemas legados (software ou hardware desatualizado que ainda é essencial para as operações de uma organização, apesar de não ser mais suportado ou de fácil atualização), em detrimento de investimentos voltados à pesquisa, inovação e capacitação digital (Barbiero, 2022).

Essa configuração orçamentária pode restringir o potencial transformador da inteligência artificial (IA) e das políticas de governança de TI, limitando sua contribuição efetiva para a inclusão digital e para a redução das desigualdades de acesso à informação. Desse modo, recomenda-se que os investimentos futuros sejam reorientados segundo os princípios de valor público e impacto social, priorizando três eixos estratégicos:

- a. Inovação e IA inclusiva: destinação de recursos específicos para o desenvolvimento de soluções baseadas em IA voltadas à acessibilidade, como assistentes virtuais, tradutores automáticos em Libras e simplificadores de linguagem jurídica.
- b. Capacitação e governança ética: ampliação dos programas de formação continuada sobre ética, segurança da informação e governança de IA, a fim de consolidar a maturidade digital dos servidores e reduzir a dependência de tecnologias proprietárias (que

é um sistema, ferramenta ou processo de propriedade exclusiva de uma empresa/órgão, que garante uma vantagem competitiva e é protegida legalmente).

- c. Infraestrutura interoperável e segura: modernização das plataformas digitais e de interoperabilidade, com ênfase na segurança cibernética e na conformidade à Lei Geral de Proteção de Dados.

A consolidação de uma governança financeira voltada à inovação responsável e à inclusão digital é condição essencial para que o MPF evolua de uma política tecnológica meramente operacional para uma estratégia digital ética, participativa e centrada no cidadão, contribuindo para o fortalecimento de sua missão institucional e para a efetivação dos direitos fundamentais no ambiente digital.

A inteligência artificial não se propõe a substituir a capacidade crítica do ser humano, mas sim a atuar como uma aliada que aprimora o trabalho de procuradores e servidores. Em rotinas de gabinete, por exemplo, a IA pode assumir tarefas repetitivas e volumosas, como a análise e organização de grandes quantidades de dados e documentos. Ao agilizar essa etapa inicial do trabalho, a IA não apenas aumenta a velocidade e precisão na identificação de informações relevantes, mas também libera o profissional para focar no que realmente importa: a análise jurídica, a tomada de decisões estratégicas e o exercício do seu julgamento humano. A máquina lida com a eficiência na análise de dados, enquanto o ser humano lida com a ética, a empatia e a contextualização. A confidencialidade e a segurança, por sua vez, são pilares nesse processo. A governança de TI do MPF deve estabelecer políticas rígidas para o uso de IA, garantindo que os dados sigilosos sejam processados em ambientes seguros, com total conformidade à Lei Geral de Proteção de Dados. Dessa forma, a IA se torna uma ferramenta de apoio que fortalece a autonomia e a qualidade do trabalho desenvolvido, ao mesmo tempo em que protege as informações sensíveis dos cidadãos.

A partir das diretrizes apresentadas no “Manual de boas práticas para o uso de IA generativa no MPF”, percebe-se a necessidade de alinhar a estratégia de inovação com um sólido modelo de governança e ética. O documento ressalta que, apesar do potencial da IA para aprimorar os serviços digitais e promover a inclusão, sua implementação deve considerar riscos como alucinações, vieses, segurança cibernética

e vazamento de informações confidenciais. Assim, o uso de ferramentas como assistentes virtuais e sistemas de triagem deve ser conduzido com responsabilidade, garantindo que os resultados sejam revisados e estejam em conformidade com as políticas da instituição. A adoção de um modelo de governança de TI, alinhado aos princípios éticos e legais, é fundamental para que a tecnologia sirva, de fato, a todos os cidadãos, sem comprometer a integridade e a credibilidade do MPF.

Nesse contexto, destaca-se o papel da Comissão Estratégica de Tecnologia da Informação como instância colegiada responsável por orientar e qualificar as decisões institucionais no campo da Tecnologia da Informação no MPF. Entre suas competências, estão a proposição de políticas e diretrizes alinhadas aos objetivos estratégicos do MPF, a elaboração do Planejamento Estratégico de TI e a emissão de pareceres técnicos sobre o Plano Diretor de TI, prioridades de investimento, execução de projetos, padrões de funcionamento, integração, qualidade, segurança e diretrizes para aquisição de bens e contratação de serviços. Ao atuar de forma articulada com a Secretaria de Tecnologia da Informação e Comunicação e com grupos técnicos especializados, a Comissão contribui para o fortalecimento da governança digital e para a consolidação de uma gestão pública orientada por critérios de eficiência, transparência e inovação.

A busca por uma governança de TI eficaz e alinhada aos princípios da inclusão digital no MPF concretiza-se, por exemplo, na criação do Sistema Único de Informações (Único). Concebido como uma plataforma integrada de gestão processual e documental, o Único foi desenvolvido para superar o cenário anterior de fragmentação tecnológica, caracterizado pelo uso de múltiplos sistemas isolados e pela ausência de padronização de fluxos e dados. Essa dispersão dificultava a interoperabilidade interna, gerando ineficiências operacionais e impactos negativos na qualidade e na celeridade dos serviços prestados ao cidadão.

O Único representa, assim, um marco na governança de TI do MPF, ao centralizar a gestão da informação e permitir a extração de dados gerenciais e estratégicos que subsidiam a tomada de decisão institucional. Sua arquitetura foi concebida com base em princípios de transparência, rastreabilidade e eficiência, alinhando-se à diretriz de que a tecnologia deve servir como meio de fortalecimento da prestação jurisdicional e da *accountability* pública.

A interoperabilidade, entendida como a capacidade de diferentes sistemas e órgãos públicos trocarem informações de forma segura, padronizada e contínua, ultrapassa os limites internos da instituição. Nesse sentido, o MPF tem investido na integração do Único a sistemas externos, consolidando uma governança interinstitucional que favorece a eficiência e a defesa dos direitos fundamentais no âmbito do sistema de Justiça. Entre as principais articulações, destacam-se:

- a. Tribunais superiores (STF, STJ e TSE): parcerias voltadas à padronização e à automação da comunicação processual.
- b. Outros ramos do Ministério Público: acordos de cooperação técnica que viabilizam o intercâmbio de informações entre o MPF e os Ministérios Públicos Estaduais.
- c. Tribunais Regionais Federais (TRFs): esforços conjuntos para compatibilização de sistemas, como o e-Proc, e integração com a Advocacia-Geral da União (AGU).
- d. Órgãos do governo federal: iniciativas de interoperabilidade para acesso e envio eletrônico de documentos administrativos e judiciais.

Essas integrações resultam em ganhos expressivos de tempo e recursos, ao eliminar redundâncias, reduzir a redigitação de dados e agilizar prazos. Além disso, fortalecem a capacidade institucional do MPF de atuar na defesa de direitos sociais e ambientais, ao garantir acesso rápido, seguro e unificado à informação, promovendo decisões mais céleres, embasadas e transparentes.

O compromisso do MPF com a inclusão digital também se materializa em plataformas voltadas diretamente ao cidadão, que ampliam o acesso aos serviços públicos e reduzem barreiras geográficas e tecnológicas. Entre essas iniciativas, destacam-se:

- a. MPF Serviços: portal unificado que concentra canais de atendimento, como protocolo eletrônico, acompanhamento processual e Portal da Transparência, facilitando o acesso do usuário às informações institucionais.
- b. Atendimento virtual: serviço via videochamada que permite a interação direta com o público, promovendo maior acessibilidade a pessoas com mobilidade reduzida ou residentes em regiões afastadas.

Ainda que os avanços sejam significativos, o desafio da interoperabilidade permanece, especialmente no que se refere à segurança da informação, à padronização de dados e à integração tecnológica entre instituições com diferentes níveis de maturidade digital. Nesse contexto, a aliança entre governança de TI e IA torna-se essencial para que o MPF possa evoluir de um modelo de integração técnica para uma governança digital inteligente, orientada por evidências e sustentada em critérios éticos, inclusivos e transparentes. Assim, a tecnologia deixa de ser apenas um instrumento de eficiência operacional e passa a atuar como vetor de inclusão, cidadania e fortalecimento institucional.

Considerando a complexidade e a extensão das informações disponíveis nos canais digitais do MPF, recomenda-se aprimorar o desenvolvimento de aplicações baseadas em IA voltadas ao atendimento e à orientação simplificada do cidadão. A criação de chatbots e assistentes virtuais pode facilitar o acesso às informações institucionais, promovendo maior autonomia e eficiência na navegação pelos serviços oferecidos. Além disso, a otimização das ferramentas de busca, inclusive com interfaces interativas, contribuiria para a superação de barreiras informacionais.

Outra proposta seria a criação de um “simplificador” de linguagem jurídica. Esse chatbot seria capaz de traduzir textos complexos de leis, pareceres ou decisões para uma linguagem simples e de fácil compreensão para qualquer pessoa, democratizando o acesso à informação jurídica, que muitas vezes é uma barreira para a participação cidadã. Internamente, um chatbot também poderia auxiliar procuradores e servidores, funcionando como um assistente de pesquisa jurídica, agilizando a busca por jurisprudência e doutrinas, apoiando na elaboração de minutas e na análise, organização e interpretação de informações constantes nos autos de processos judiciais e procedimentos administrativos de atribuição do MPF. Tais iniciativas demonstram como a IA, alinhada a uma sólida governança de TI, pode ser uma ferramenta transformadora para o MPF, não apenas tornando os serviços mais eficientes, mas também mais transparentes e acessíveis a todos.

8 Considerações finais

A transformação digital no setor público brasileiro tem-se consolidado como fator relevante para a promoção da cidadania, da eficiência

administrativa e da inclusão social. Nesse contexto, o MPF, enquanto instituição com papel constitucionalmente estabelecido para a defesa dos direitos fundamentais, assume papel importante na construção de um ambiente digital acessível, transparente e responsivo.

O presente estudo demonstrou que a integração entre a governança pública, a governança de TIC e a IA constitui um elemento estratégico para fortalecer a missão institucional do MPF. Essa articulação revela-se essencial para promover a inclusão digital, ampliar o acesso da população aos serviços públicos e garantir que a transformação digital ocorra de forma ética, transparente e centrada no cidadão.

A análise documental e comparativa evidenciou que o MPF já desenvolve iniciativas relevantes de acessibilidade e equidade digital, como o uso de ferramentas de IA na automação de fluxos de trabalho, a tradução de conteúdos em Libras, a oferta de capacitações internas e a atuação judicial em defesa dos direitos de pessoas com deficiência e de comunidades vulneráveis no ambiente digital. Tais ações reforçam o papel do MPF como agente ativo da democratização tecnológica e da promoção dos direitos fundamentais, traduzindo sua missão constitucional para o contexto da sociedade digital.

Entretanto, o avanço sustentável dessa agenda demanda aperfeiçoar os mecanismos de governança de TIC e de IA, de modo a garantir que a inovação tecnológica esteja amparada por estruturas sólidas de gestão, controle e avaliação. A governança, quando aliada à IA, é o que assegura a responsabilidade, a auditabilidade e a confiabilidade dos sistemas automatizados, prevenindo a reprodução de vieses e assegurando o uso ético dos dados.

Entre os desafios a serem superados, destacam-se a necessidade de mitigação de vieses algorítmicos, a consolidação de uma arquitetura interoperável e inclusiva, e a criação de comitês institucionais de ética e governança da IA, que já se encontram em fase de discussão para implementação, capazes de monitorar riscos, garantir a transparência e fortalecer a confiança da sociedade nas soluções tecnológicas adotadas.

O investimento contínuo na capacitação de membros e servidores, aliado à adoção de softwares abertos, auditáveis e interoperáveis, é fundamental para consolidar uma cultura organizacional baseada na ética digital, na segurança da informação e na governança orientada por evidências.

Além disso, é essencial que a governança de TI e IA no MPF mantenha foco constante nas características e nas necessidades reais dos usuários de seus serviços digitais. Compreender as dificuldades enfrentadas por diferentes perfis – como pessoas idosas, com deficiência, de baixa escolaridade ou residentes em regiões com menor conectividade – é condição indispensável para o desenvolvimento de soluções tecnológicas inclusivas e efetivas. O desenho de novas ferramentas digitais e o aprimoramento das já existentes devem ser orientados pela experiência do usuário (*user experience*), considerando suas limitações e expectativas. Somente a partir dessa escuta ativa e empática será possível consolidar uma governança digital verdadeiramente centrada no cidadão, na qual a integração com a IA se traduza em acessibilidade, confiança e ampliação do acesso à justiça e aos direitos fundamentais.

Conclui-se que o MPF ocupa uma posição estratégica para liderar a transformação digital inclusiva no setor público brasileiro, tornando-se referência na aplicação responsável da IA sob os princípios da governança pública. A convergência entre governança, tecnologia e direitos fundamentais é, portanto, o caminho para garantir que o avanço tecnológico contribua efetivamente para um Ministério Público mais acessível, transparente, eficiente e comprometido com a justiça social.

Referências

ALBUQUERQUE, M. R.; Costa, L. Transformação digital no setor público: tendências e implicações. **Revista de Gestão e Secretariado** – GeSec, [s. l.], v. 16, n. 3, p. e4771, 2025. DOI: <https://doi.org/10.7769/gesec.v16i3.4771>. Acesso em: 20 maio 2025.

BAPTISTA, Patrícia Ferreira; ANTOUN NETTO, Leonardo Silveira. O processo administrativo eletrônico e sua disciplina no direito administrativo brasileiro: entre novos desafios e velhos problemas. **Revista de Direito Administrativo**, v. 282, n. 3, p. 85-100, set./dez. 2023. DOI: <https://doi.org/10.12660/rda.v282.2023.90156>. Acesso em: 28 maio 2025.

BARBIERO, G.; ALMEIDA JUNIOR, N. S. de; ARAÚJO, C. de; SATO, A. F. Adoção de boas práticas da ITIL em projetos de sistemas de informação baseados em PMBOK. **Brazilian Journal of Development**, Curitiba, v. 8, n. 2, p. 10670-10691, fev. 2022. DOI: <https://doi.org/10.34117/bjdv8n2-147>.

BRASIL. Conselho de Controle de Atividades Financeiras (Coaf). **Portaria COAF n. 4, de 20 de março de 2025**. Estabelece diretrizes a serem observadas no uso de Inteligência Artificial Generativa (IAG) no âmbito do Conselho de Controle de Atividades Financeiras – Coaf. Brasília, DF: Coaf, 2025. Disponível em: <https://tinyurl.com/4uv8yt7v>. Acesso em: 12 jun. 2025.

BROGNOLI, Tainara da Silva; FERENHOF, Helio Aisenberg. Transformação digital no governo brasileiro: desafios, ações e perspectivas. **Navus**, Florianópolis, v. 10, p. 1-11, jan./dez. 2020. DOI: <https://doi.org/10.22279/navus.2020.v10.p01-11.989>. Acesso em: 27 abr. 2025.

CERQUINHO, Kleomara Gomes; TAVARES, Wellington; PAULA, Ana Paula Paes de; VITORINO, Irineu Amaro. Inclusão digital para quem e para quem? Uma observação do portal Inclusão Digital do governo federal brasileiro. **Cadernos Gestão Pública e Cidadania**, São Paulo, v. 20, n. 67, p. 172–193, jul./dez. 2015. DOI: <http://dx.doi.org/10.12660/cgpc.v20n67.32927>. Acesso em: 26 abr. 2025.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Prêmio CNMP divulga os vencedores de 2025**. Brasília: CNMP, 2025. Disponível em: <https://tinyurl.com/943avwbm>. Acesso em: 18 set. 2025.

CONHEÇA as conquistas e os desafios do MPF nos 10 anos da Lei Brasileira de Inclusão. **Jusbrasil**, [s. l.], 4 jul. 2025. Disponível em: <https://tinyurl.com/yfstdan93>. Acesso em 15 set 2025.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 38. ed. Rio de Janeiro: Forense, 2025.

GONÇALVES, Oksandro Osdival; LUCIANI, Danna Catharina Mascarello. A inclusão digital e os incentivos à inovação: o governo digital na busca pelo desenvolvimento socioeconômico. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria-RS, v. 17, n. 2, e69673, maio/ago. 2022. DOI: <http://dx.doi.org/10.5902/1981369469673>. Acesso em: 2 maio 2025.

MPF – MINISTÉRIO PÚBLICO FEDERAL. Ação do MPF pede implementação de serviços de internet e telefonia móvel em quilombo de Itaóca (SP). **Portal MPF**, São Paulo, 30 jul. 2025. Disponível em: <https://tinyurl.com/48mzvvhk>. Acesso em: 14 set. 2025.

MPF recomenda ajustes na plataforma Gov.br para aprimorar acessibilidade a pessoas com deficiência visual. **Jusbrasil**, [s. l.], 2 set. 2025a. Disponível em: <https://tinyurl.com/4k7djk4h>. Acesso em: 10 mar. 2026.

MPF recomenda regulamentação de trecho da Lei Brasileira de Inclusão sobre acessibilidade na internet. **Jusbrasil**, [s. l.], 29 ago. 2025b. Disponível em: <https://tinyurl.com/3m9ev827>. Acesso em: 10 mar. 2026.

MPMT – MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO. MPF entra com ação na Justiça para garantir recursos de acessibilidade em plataformas de streaming no Brasil. **MPMT**, Cuiabá, 6 dez. 2024. Disponível em: <https://tinyurl.com/5t2hxe5k>. Acesso em: 10 mar. 2026.

MPU – MINISTÉRIO PÚBLICO DA UNIÃO. Relatório de Gestão 2024. **Portal do MPU**, Brasília-DF, 2024a. Disponível em: <https://tinyurl.com/w4kpys2u>. Acesso em: 8 out. 2025.

MPU – MINISTÉRIO PÚBLICO DA UNIÃO. Relatório de Gestão do Ministério Público da União 2022: Resultados das áreas de gestão. **Portal do MPU**, Brasília-DF, 2022. Disponível em: <https://tinyurl.com/bdh8dcxx>. Acesso em: 14 set. 2025.

MPU – MINISTÉRIO PÚBLICO DA UNIÃO. Relatório de Gestão do Ministério Público da União 2024: Visão organizacional e ambiente externo. **Portal do MPU**, Brasília-DF, 2024b. Disponível em: <https://tinyurl.com/34vajrvp>. Acesso em: 19 set. 2025.

PHILIPPI, Juliana Horn Machado. Transformação digital e urgência da cultura de dados na Administração Pública brasileira. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, v. 10, n. 1, e232, jan./jun. 2023. DOI: <https://doi.org/10.14409/redoeda.v10i1.12401>.

RIBEIRO, M. M.; SEGATTO, C. I. Inteligência artificial nas organizações públicas brasileiras: heterogeneidades e capacidades em tecnologia da informação. **Revista de Administração Pública**, v. 59, n. 1, e2024-0066, 2025. DOI: <https://doi.org/10.1590/0034-761220240066>.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. **Referencial básico de governança organizacional**: para organizações públicas e outros entes jurisdicionados ao TCU. 3. ed. Brasília: TCU, 2020.

Cibercrime e inteligência artificial: o papel dos modelos de linguagem no aperfeiçoamento de ataques de *phishing*

Cybercrime and artificial intelligence: the role of language models in enhancing phishing attacks

DOI: https://doi.org/10.63601/978-65-88299-52-4_5

Antônio de Jesus da Silva Machado

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Graduado em Direito pelo Centro Universitário Uninovafapi. Servidor do Ministério Público Federal (MPF), com atuação na Coordenadoria de Investigação em Evidências Digitais e Eletrônicas.

Glauce Picinini da Silva Millan

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Graduada em Direito pela Universidade Federal Fluminense. Servidora do Ministério Público Federal (MPF), com atuação na Coordenadoria de Investigação em Evidências Digitais e Eletrônicas.

Resumo: Este estudo analisa o papel dos Grandes Modelos de Linguagem (LLMs) no aperfeiçoamento de ataques de *phishing*, com ênfase em seu impacto potencial sobre a segurança digital do Ministério Público Federal (MPF). O objetivo principal foi comparar a qualidade das mensagens fraudulentas elaboradas por humanos e por LLMs em três dimensões: persuasão, personalização e realismo textual. Para isso, foram coletadas amostras autênticas de *e-mails* em repositórios consolidados e geradas mensagens sintéticas em ambiente controlado, com total anonimização e uso de domínios fictícios. A análise combinou

indicadores linguísticos e comportamentais com testes estatísticos não paramétricos, assegurando rigor metodológico e reprodutibilidade. Os resultados demonstraram que os LLMs ampliam significativamente o grau de persuasão e personalização das mensagens, apresentando tamanhos de efeito elevados, enquanto o realismo textual revelou ganhos menores, porém consistentes. Essas evidências confirmam a hipótese de que os LLMs não apenas replicam estratégias tradicionais de engenharia social, mas as aprimoram, tornando as mensagens mais convincentes e adaptáveis a diferentes contextos. Do ponto de vista institucional, essas descobertas oferecem ao MPF *insights* para o fortalecimento de sua segurança cibernética, por meio do aprimoramento de treinamentos internos, da realização de campanhas simuladas de *phishing* mais eficazes e da adoção de filtros inteligentes de detecção. Academicamente, a pesquisa contribui para o entendimento das dinâmicas contemporâneas do cibercrime e do papel da IA na manipulação linguística. Identifica-se, contudo, como limitação a ausência de testes empíricos sobre taxas reais de cliques, recomendando-se estudos futuros com usuários em ambientes operacionais.

Palavras-chave: ataques de *phishing*; cibercrime; cibersegurança; engenharia social; inteligência artificial (IA); Grandes Modelos de Linguagem (LLMs).

Abstract: *This study analyzes the role of Large Language Models (LLMs) in improving phishing attacks, focusing on their potential impact on the digital security of the Federal Public Prosecutor's Office (MPF). The primary objective was to compare the quality of phishing messages created by humans versus those generated by LLMs across three dimensions: persuasion, personalization, and textual realism. To do this, we collected authentic phishing emails from established datasets and generated synthetic messages in a controlled environment, using anonymized data and fictitious domains. Our analysis combined linguistic and behavioral indicators with nonparametric statistical tests, to ensure methodological rigor and reproducibility. The results show that LLMs significantly improved the persuasion and personalization of phishing messages, with large effect sizes classified, while textual realism saw smaller yet consistent gains. This evidence confirms our hypothesis that LLMs more than replicate traditional social engineering tactics; they enhance them with sophisticated ones, making messages more convincing and adaptable. From an institutional standpoint, these findings provide the MPF with actionable insights for strengthening its cybersecurity, such as improving employee training programs, running more effective simulated phishing campaigns, and adopting intelligent detection filters. Academically, this research contributes to the understanding of modern cybercrime dynamics and the influence of AI on linguistic manipulation. We acknowledge a key limitation: the lack of empirical tests of user click-through rates. Therefore, we recommend future research involving real users in live environments.*

Keywords: *phishing attacks; cybercrime; cybersecurity; social engineering; artificial intelligence (AI); Large Language Models (LLMs).*

1 Introdução

A crescente digitalização das atividades institucionais no Ministério Público Federal (MPF) tem impulsionado avanços significativos na prestação jurisdicional, transparência e eficiência administrativa. Entretanto, tal transformação também intensificou a exposição a riscos cibernéticos, especialmente no tocante à segurança da informação, proteção de dados e resposta a incidentes digitais. Nesse contexto, torna-se imprescindível analisar as novas dinâmicas do cibercrime e da Inteligência Artificial (IA), com destaque para os Grandes Modelos de Linguagem (LLMs) no aperfeiçoamento de ataques de *phishing*, considerando seu impacto direto nas estratégias de segurança digital do MPF.

A literatura recente revela a evolução dos ataques de *phishing* como um dos crimes cibernéticos mais recorrentes e sofisticados, explorando vulnerabilidades humanas e tecnológicas (Alkhalil *et al.*, 2021). O *phishing* tradicional consiste em enganar usuários para obtenção de dados confidenciais, muitas vezes por meio de e-mails genéricos e mensagens automatizadas. O *spear phishing*, por sua vez, caracteriza-se pela personalização das abordagens, visando vítimas específicas e aumentando sua taxa de sucesso (Hazell, 2023). Ademais, autores como Mitnick e Simon (2003) destacam o papel central da engenharia social na manipulação psicológica das vítimas.

Com a popularização dos LLMs, como ChatGPT, Claude e Gemini, novas possibilidades emergem para o aprimoramento dos ataques. Estudos (Roy *et al.*, 2024; Sahoo *et al.*, 2025) demonstram que esses modelos, devido à sua sofisticação textual, capacidade de personalização e acessibilidade, já são utilizados para criar conteúdos maliciosos, driblando mecanismos de detecção e elevando o risco de *phishing* mais persuasivos e eficientes. Contudo, há divergência na literatura: enquanto Alkhalil *et al.* (2021) ressaltam o fator humano e a engenharia social clássica como determinantes para o sucesso do *phishing*, Roy *et al.* (2024) evidenciam que a automação e o realismo textual proporcionados pelos LLMs representam uma ruptura qualitativa, ampliando a escala, a eficácia e o alcance das campanhas fraudulentas.

De acordo com os dados do CERT.br (2025), entre janeiro e abril de 2025 foram notificadas mensalmente mais de 1.400 tentativas de

phishing no Brasil, com tendência de alta no período analisado. No cenário internacional, o Relatório de Tendências de Atividades de *Phishing* do APWG (4º Trimestre de 2024) registrou 989.123 ataques de *phishing* em todo o mundo no último trimestre (APWG, 2025), um aumento expressivo em relação aos trimestres anteriores. Destaca-se que o número de ataques por mês variou entre 290.000 e 358.000, evidenciando a persistência e a escala global desse tipo de crime.

No âmbito institucional, destaca-se a Resolução CNMP n. 294/2024, que institui a Política Nacional de Cibersegurança do Ministério Público. Tal normativa estabelece princípios, diretrizes e instrumentos de governança para prevenção, detecção, tratamento e resposta a ameaças digitais, enfatizando a atuação preventiva, a capacitação contínua e a resposta coordenada a incidentes, medidas essenciais para o enfrentamento de ataques de *phishing* baseados em novas tecnologias.

Nesse contexto, a pesquisa é guiada pelo seguinte questionamento: Como os LLMs estão aumentando a taxa de sucesso de ataques de *phishing* em comparação com métodos tradicionais? Parte-se da hipótese de que os e-mails de *phishing* gerados por LLMs são mais eficazes, pois integram maior persuasão, personalização e realismo textual, o que aumenta o engajamento das vítimas e a credibilidade das mensagens.

O objetivo geral deste estudo é analisar de que forma os LLMs aumentam a eficácia de ataques de *phishing* em comparação com métodos tradicionais, avaliando indicadores como persuasão, personalização e realismo textual, a fim de entender seu impacto na segurança cibernética e propor estratégias de mitigação. Para alcançar o objetivo, pretende-se: I) identificar as principais características dos ataques de *phishing* tradicionais e baseados em LLMs; II) analisar evidências empíricas e conceituais sobre o desempenho dos LLMs em campanhas de *phishing*; e III) propor estratégias institucionais para a mitigação de riscos associados ao uso de LLMs em ataques cibernéticos.

A justificativa desta pesquisa fundamenta-se no expressivo crescimento dos ataques de *phishing* potencializados por LLMs, conforme apontam relatórios técnicos do CERT.br (2025) e do APWG (2025). Tal cenário demanda a formulação de respostas estratégicas por parte das instituições. Assim, torna-se imprescindível a realização de análises sistemáticas que comparem o impacto dos LLMs em relação aos métodos

tradicionais de *phishing*, especialmente com vistas à orientação de políticas de segurança e ao aprimoramento de capacitação contínua no MPF.

A estrutura do artigo está organizada da seguinte forma: a seção 1 apresenta a introdução, contextualizando o tema, a problemática, os objetivos e a justificativa. A seção 2 discute o referencial teórico, abordando os conceitos de *phishing*, engenharia social, LLMs e engenharia de *prompts*. A seção 3 descreve a metodologia utilizada na pesquisa. A seção 4 apresenta a análise comparativa entre ataques tradicionais e baseados em LLMs. Por fim, a seção 5 reúne as conclusões e recomendações para a atuação institucional e para futuras investigações acadêmicas.

2 Revisão de literatura

Esta seção apresenta os fundamentos teóricos que sustentam a pesquisa, abordando os conceitos de cibercrime, *phishing*, engenharia social, LLMs e engenharia de *prompts*, essenciais para compreender o fenômeno analisado. Na sequência, são discutidas análises de casos recentes que ilustram a aplicação dos LLMs em ataques de *phishing* e, por fim, os principais desafios, controvérsias e lacunas identificadas na literatura, com destaque para as implicações éticas e tecnológicas desses avanços no campo da cibercriminalidade.

2.1 Fundamentos conceituais sobre cibercrime, *phishing* e LLMs

O conceito de cibercrime é entendido na literatura especializada como a prática de condutas ilícitas por meio de sistemas computacionais, englobando desde fraudes financeiras até ataques contra a integridade, confidencialidade e disponibilidade de informações digitais (Alkhalil *et al.*, 2021; Hazell, 2023). Os autores convergem ao apontar que a sofisticação dos cibercrimes se intensificou com a expansão da conectividade e da dependência das tecnologias digitais, tornando os ataques cada vez mais dinâmicos, automatizados e complexos.

No universo dos cibercrimes, destaca-se o *phishing*, definido como um ataque de engenharia social que visa manipular a vítima para obtenção de informações sensíveis, geralmente por meio de comunicações fraudulentas que simulam entidades legítimas (Alkhalil *et al.*, 2021; Begou *et al.*, 2023).

Enquanto Alkhalil *et al.* (2021) detalham a estrutura e as modalidades do *phishing* tradicional, evidenciando a centralidade do fator humano para o sucesso do ataque, estudos mais recentes, como o de Begou *et al.* (2023), já evidenciam a crescente integração de recursos automatizados e de inteligência artificial nas campanhas, ampliando sua eficácia e alcance.

A engenharia social emerge, nesse contexto, como o conjunto de técnicas psicológicas e comunicacionais empregadas para manipular indivíduos e obter vantagens ilícitas. Hazell (2023) e Roy *et al.* (2023) ressaltam que a engenharia social é historicamente o elo mais vulnerável da segurança digital, sendo explorada tanto em ataques simples quanto em sofisticadas campanhas de *spear phishing* potencializadas por LLMs. Tais estudos reconhecem que o sucesso de muitos ataques decorre menos de falhas técnicas e mais da exploração de fatores comportamentais, como curiosidade, medo, senso de urgência e autoridade (Hazell, 2023; Roy *et al.*, 2023).

Em paralelo, o desenvolvimento dos LLMs, como GPT-4 e suas variantes, revolucionou o campo da geração automática de texto. Sahoo *et al.* (2025) e Reynolds e McDonell (2021) conceituam os LLMs como sistemas de inteligência artificial treinados em grandes volumes de dados textuais, capazes de compreender, sintetizar e gerar linguagem natural em múltiplos contextos e estilos, com elevado grau de realismo e adaptabilidade. O potencial disruptivo desses modelos para a cibercriminalidade é ressaltado por Hazell (2023) e Begou *et al.* (2023), que demonstram empiricamente sua capacidade de automatizar a redação de mensagens, adaptar-se a diferentes perfis de vítimas e driblar mecanismos convencionais de detecção.

Destaca-se que a eficácia dos LLMs está diretamente associada ao conceito de *prompts*, que são instruções ou comandos em linguagem natural que direcionam o comportamento e a produção textual desses modelos. Conforme Sahoo *et al.* (2025), a engenharia de *prompts* evoluiu para se tornar área central de pesquisa, abrangendo desde técnicas básicas (*zero-shot*, *few-shot*) até abordagens avançadas (*chain-of-thought*, *metaprompts*), possibilitando controlar, especializar e adaptar a geração textual dos LLMs a contextos específicos, inclusive para fins maliciosos. Roy *et al.* (2023) complementam que a sofisticação dos *prompts* permite burlar filtros, criar variantes evasivas de ataques e aumentar o potencial de personalização das mensagens fraudulentas.

Assim, observa-se uma convergência entre os autores quanto à relevância desses conceitos para o entendimento dos novos riscos e desafios da cibercriminalidade com a crescente utilização da IA. Se, por um lado, as definições de cibercrime e *phishing* permanecem ancoradas nos fundamentos da engenharia social, por outro, a introdução dos LLMs e da engenharia de *prompts* desloca o eixo de análise para um cenário em que a automação, a personalização e o realismo textual potencializam as ameaças, exigindo revisão constante das estratégias de prevenção e resposta. A articulação crítica desses conceitos é, portanto, indispensável para sustentar investigações e propor soluções efetivas no contexto do aprimoramento dos ataques de *phishing* na era da inteligência artificial.

2.2 Abordagens teóricas sobre *phishing* e LLMs

A análise teórica sobre o fenômeno do *phishing* e sua evolução revela tanto a permanência de modelos clássicos quanto a emergência de novas abordagens impulsionadas pela inteligência artificial.

Os modelos clássicos de *phishing* enfatizam a combinação entre recursos técnicos e estratégias de engenharia social para enganar as vítimas. Alkhalil *et al.* (2021) descrevem o ciclo do ataque de *phishing* tradicional a partir de quatro etapas fundamentais: planejamento, preparação, execução e aquisição de valores, destacando a importância do conhecimento prévio sobre o alvo, o uso de canais de comunicação legitimados e a criação de páginas ou mensagens fraudulentas para coleta de credenciais. Esses autores reforçam que, historicamente, a eficácia do *phishing* dependeu tanto do design técnico dos ataques quanto da capacidade dos criminosos de explorar a confiança e a desatenção das vítimas.

Em convergência, Roy *et al.* (2023) ressaltam que mesmo as primeiras ondas de ataques já integravam mecanismos para burlar filtros de spam e métodos de detecção baseados em listas de bloqueios, demonstrando a constante adaptação dos agressores ao contexto tecnológico. Entretanto, a principal limitação apontada por Hazell (2023) está na escalabilidade e personalização: ataques tradicionais, embora eficazes, requeriam esforço manual para segmentação de alvos e customização das mensagens, o que restringia seu alcance e potencial de dano.

Com o surgimento dos LLMs, como GPT-4 e variantes, inaugura-se uma nova fase no cibercrime. Hazell (2023) e Begou *et al.* (2023)

demonstram que LLMs democratizam e amplificam a capacidade de geração de ataques sofisticados, permitindo a produção em massa de e-mails e sites de *phishing* altamente personalizados, com realismo textual e adaptabilidade a múltiplos perfis de vítimas. Tais modelos eliminam barreiras técnicas e reduzem custos operacionais, tornando viável a automação integral do ciclo do ataque. Roy *et al.* (2023) acrescentam que, por meio de técnicas de engenharia de *prompts*, operadores maliciosos conseguem instruir os LLMs a contornar filtros de uso e gerar conteúdos que escapam dos sistemas tradicionais de detecção, incluindo variantes evasivas (ex.: ataques com *reCAPTCHA*, *browser-in-the-browser*, *QR code* e *encoding*).

Entre os filtros de uso mais frequentemente contornados estão os mecanismos baseados em palavras-chave e frases sensíveis, como *phishing*, *hack* e *password steal*, que, quando detectados nos *prompts*, normalmente levam o modelo a bloquear a resposta. No entanto, os atacantes têm desenvolvido estratégias de reformulação e divisão de tarefas nos *prompts* para evitar esses gatilhos de segurança, demonstrando a necessidade de constante atualização e aprimoramento das salvaguardas implementadas pelos desenvolvedores de LLMs.

A convergência entre os estudos evidencia um salto qualitativo: os LLMs, ao contrário dos scripts manuais ou kits de *phishing* convencionais, adaptam em tempo real linguagem, tom, contexto e detalhamento das mensagens conforme os dados da vítima, aumentando substancialmente a eficácia das campanhas e as taxas de sucesso dos ataques.

No contexto da engenharia social potencializada por LLMs, observa-se que a manipulação psicológica e comunicacional, tradicionalmente central nos modelos clássicos, atinge novo patamar. Hazell (2023) e Roy *et al.* (2024) enfatizam que LLMs são capazes de simular estilos de comunicação, empregar informações contextuais e até responder de forma dinâmica a interações, aproximando-se de diálogos reais e elevando o grau de persuasão. Isso representa um desafio inédito: as fronteiras entre mensagens automatizadas e interações humanas tornam-se difusas, dificultando a detecção de fraude tanto por usuários quanto por sistemas automatizados.

Sahoo *et al.* (2025) e Reynolds e McDonell (2021) reforçam que a engenharia de *prompts* evoluiu, permitindo modular a abordagem dos

ataques conforme características demográficas, emocionais e profissionais das vítimas, maximizando o impacto das tentativas de *phishing*. Divergências permanecem quanto ao grau de autonomia dos LLMs: enquanto alguns autores apontam riscos crescentes de ataques autônomos e em larga escala, outros enfatizam que ainda existem barreiras técnicas, limitações de contexto e dependência da criatividade dos operadores para geração dos *prompts* mais eficazes.

As correntes teóricas analisadas apontam para uma transição dos modelos tradicionais de *phishing*, centrados na habilidade manual dos criminosos e em vulnerabilidades humanas, para uma realidade na qual os LLMs ampliam, automatizam e sofisticam as estratégias de ataque. A integração entre IA generativa e engenharia social torna-se vetor fundamental de evolução dos crimes digitais, exigindo revisão contínua das práticas de prevenção, detecção e resposta. Assim, a literatura evidencia que a compreensão dessas dinâmicas é imprescindível para orientar políticas institucionais, aprimorar estratégias técnicas e propor abordagens multidisciplinares de enfrentamento no cenário da cibercriminalidade contemporânea.

2.3 Análises de casos no contexto do *phishing* automatizado

A investigação empírica sobre ataques de *phishing* tem-se concentrado recentemente na avaliação da capacidade dos LLMs de automatizar, personalizar e escalar campanhas maliciosas, evidenciando diferenças marcantes em relação aos métodos tradicionais.

Os experimentos de geração automatizada de *phishing* com LLMs demonstram, de forma consistente, que ferramentas como ChatGPT, Claude e Gemini são capazes de produzir, em poucos minutos, e-mails, páginas falsas e até kits completos de *phishing* altamente realistas e persuasivos. Hazell (2023) demonstra, em estudo experimental com parlamentares britânicos, que LLMs conseguem coletar informações públicas sobre as vítimas, adaptar o tom e o conteúdo das mensagens e gerar centenas de *phishing* personalizadas com baixo custo e em grande escala. De modo convergente, Roy *et al.* (2023) e Begou *et al.* (2023) relatam que participantes com diferentes níveis de conhecimento técnico obtiveram sucesso semelhante ao induzir LLMs a gerar códigos de páginas de *phishing*.

Nesse contexto, tais pesquisas indicam que as barreiras técnicas anteriormente presentes para a realização de ataques sofisticados, como a necessidade de conhecimentos avançados em programação, domínio do idioma ou habilidades específicas de engenharia social, foram substancialmente reduzidas com o uso de LLMs. Isso ampliou significativamente o alcance de agentes maliciosos em potencial.

Adicionalmente, Roy *et al.* (2024) propõem a utilização de modelos de detecção baseados em Machine Learning para identificar *prompts* maliciosos, embora ressaltem os desafios contínuos de atualização e adaptação desses sistemas diante da rápida evolução das estratégias ofensivas.

O comparativo entre a eficácia de ataques tradicionais e os baseados em LLMs revela um salto qualitativo em termos de persuasão, adaptabilidade e escalabilidade das campanhas. Enquanto Alkhalil *et al.* (2021) descrevem o *phishing* tradicional como dependente de técnicas manuais de personalização e engenharia social, os experimentos recentes atestam que LLMs viabilizam a produção em massa de mensagens convincentes, com realismo textual e adequação ao perfil das vítimas. Hazell (2023) mostra que ataques de *spear phishing* automatizados por IA apresentam níveis de autenticidade textual e capacidade de adaptação muito superiores aos métodos clássicos, elevando as taxas potenciais de sucesso.

Begou *et al.* (2023) complementam que a facilidade de automação e a redução de custos operacionais tornam viável a personalização em larga escala, antes restrita a grupos especializados e de alto investimento técnico. Os autores convergem ao destacar que, mesmo diante de filtros e salvaguardas implementados pelos desenvolvedores de LLMs, técnicas de engenharia de *prompts* têm-se mostrado eficazes para contornar restrições e ampliar o potencial ofensivo desses modelos.

As evidências empíricas analisadas indicam que a introdução dos LLMs representa uma ruptura no paradigma dos ataques de *phishing*, deslocando o eixo da habilidade manual e da dependência de conhecimento técnico para uma era de automação, personalização e escalabilidade inéditas. Se, por um lado, os métodos tradicionais ainda apresentam relevância em contextos específicos, por outro, a literatura mostra consenso de que os LLMs elevam exponencialmente a ameaça representada pelo *phishing*, exigindo atualização constante das estratégias defensivas, desenvolvimento de ferramentas de detecção baseadas em IA e políticas institucionais integradas para mitigação dos novos riscos.

2.4 Desafios, controvérsias e lacunas na pesquisa sobre *phishing* com LLMs

A literatura recente sobre ataques de *phishing* baseados em LLMs, embora robusta em avanços empíricos e conceituais, apresenta limitações metodológicas e desafios quanto à generalização dos achados. Sahoo *et al.* (2025) e Begou *et al.* (2023) destacam que grande parte dos estudos foi conduzida em ambientes controlados, sem validação em cenários reais de cibercrime ou contra vítimas desavisadas, restringindo a compreensão do impacto efetivo dessas campanhas no cotidiano das organizações e da sociedade.

Além disso, limitações técnicas dos próprios modelos, como tamanho de contexto, necessidade de *prompts* segmentados e dependência de operadores para a execução de ataques mais complexos, ainda constituem barreiras à automação plena dos ataques (Begou *et al.*, 2023; Reynolds; McDonell, 2021). Divergências emergem sobre a autonomia real dos LLMs: enquanto alguns autores sinalizam riscos iminentes de ataques quase autônomos, outros ressaltam que a criatividade humana ainda é determinante para a eficácia das campanhas maliciosas, evidenciando a necessidade de abordagens multidisciplinares e experimentações em ambientes produtivos para avançar o entendimento do fenômeno.

Os dilemas éticos e regulatórios constituem outro ponto crítico da discussão sobre LLMs e cibercrime. Hazell (2023) e Roy *et al.* (2024) enfatizam o desafio do uso das tecnologias de IA: enquanto LLMs podem fortalecer defesas e aprimorar sistemas de detecção, também ampliam exponencialmente o potencial ofensivo das campanhas de *phishing*. As divergências concentram-se na eficácia e suficiência das salvaguardas implementadas por desenvolvedores de LLMs, e experimentos recentes demonstram a vulnerabilidade dos modelos mesmo diante de filtros técnicos avançados (Roy *et al.*, 2024; Begou *et al.*, 2023).

Na literatura, há consenso de que o campo demanda avanços interdisciplinares e esforços contínuos para acompanhar a rápida evolução dos LLMs. Reynolds e McDonell (2021) e Sahoo *et al.* (2025) apontam que novos vetores de ataque, como o uso de LLMs multimodais, vídeos e áudios manipulados por IA (*deepfakes*) e automação total de campanhas, são tendências iminentes, exigindo abordagens de defesa inovadoras e métodos de detecção dinâmicos e adaptativos.

Os autores convergem na urgência de se desenvolverem mecanismos institucionais e técnicos para acompanhar o avanço dos riscos, mas divergem quanto ao grau de autonomia já alcançado pelos modelos e à suficiência dos marcos regulatórios atuais. As perspectivas futuras exigem integração entre tecnologia, direito, psicologia e educação, reafirmando a centralidade de pesquisas interdisciplinares para o enfrentamento dos desafios da cibercriminalidade potencializada pela inteligência artificial.

3 Metodologia

A presente pesquisa foi estruturada em uma abordagem mista, combinando métodos qualitativos e quantitativos com o objetivo de comparar e-mails de *phishing* tradicionais e elaborados por LLMs. Essa escolha metodológica buscou conciliar a riqueza interpretativa da análise retórica e discursiva com o rigor estatístico necessário para validar diferenças significativas entre os grupos, criando assim uma triangulação robusta de evidências (Creswell; Plano Clark, 2017).

O processo de investigação foi conduzido em três etapas principais: seleção e preparação dos dados, extração de indicadores de análise e aplicação de testes estatísticos. Na primeira etapa, foram coletadas amostras representativas de *phishing* humano a partir de bases públicas e repositórios acadêmicos, devidamente anonimizadas e organizadas em planilhas no formato CSV, garantindo padronização e consistência na análise. Em paralelo, foram produzidos e-mails simulados por LLMs em ambiente controlado, utilizando *prompts* cuidadosamente projetados, de modo a assegurar a integridade ética da pesquisa.

Na segunda etapa, os dados foram enriquecidos com indicadores relacionados a três dimensões centrais: persuasão, personalização e realismo textual. Para persuasão, adotaram-se os princípios de influência descritos por Cialdini (2021), identificados por meio de categorização lexical e semântica, em linha com metodologias recentes de análise de engenharia social (Begou *et al.*, 2023; Hazell, 2023). Para personalização, a presença de nomes de destinatários, referências contextuais e adequações estilísticas foi classificada em uma escala ordinal de 0 a 3, refletindo níveis crescentes de sofisticação. Por fim, o realismo textual foi avaliado por meio de métricas objetivas: legibilidade (Flesch-EN),

proporção de caracteres em caixa alta, ocorrência de pontuações repetidas e comprimento médio das frases, reescalados em notas de 1 a 5, em consonância com práticas de avaliação de naturalidade textual (Kincaid *et al.*, 1975; Pitler; Nenkova, 2008).

Na terceira etapa, foram conduzidas análises estatísticas comparativas entre os dois grupos. Dada a natureza não normal das distribuições, aplicou-se o teste de Mann-Whitney U, apropriado para dados ordinais e intervalares não paramétricos, complementado pelo cálculo do tamanho de efeito Cliff's δ , o qual estima a magnitude prática das diferenças entre grupos (Romano *et al.*, 2006). Essa combinação permitiu avaliar não apenas a significância estatística das diferenças, mas também sua relevância prática.

Os cálculos estatísticos e as visualizações foram realizados a partir dos arquivos CSV, que serviram como insumo principal da análise. Utilizou-se a linguagem Python para o processamento e a geração de gráficos comparativos, empregando como exemplo: bibliotecas pandas (para manipulação e organização dos dados), Seaborn e Matplotlib (para criação de *boxplots*, histogramas e gráficos integrados). Essa integração entre dados estruturados em CSV e análise computacional em Python possibilitou a construção de um quadro metodológico sólido, transparente e reproduzível, em conformidade com práticas recomendadas em pesquisas científicas (Roy *et al.*, 2023; Sahoo *et al.*, 2025).

Em síntese, a abordagem metodológica adotada permitiu identificar diferenças relevantes entre *phishing* humano e gerado por LLMs, tanto em termos estatísticos quanto práticos, oferecendo uma análise fundamentada e alinhada às discussões atuais sobre os riscos da automação de ataques de engenharia social com suporte de inteligência artificial.

4 Apresentação e discussão dos resultados

Esta seção apresenta e discute os resultados obtidos a partir da análise comparativa entre e-mails de *phishing* humanos e aqueles gerados por LLMs. A discussão está organizada em quatro eixos principais: seleção dos dados, que descreve as amostras e os critérios utilizados; estratégias de persuasão, que examinam os mecanismos retóricos empregados nas mensagens; grau de personalização, que avalia o nível

de adaptação do conteúdo ao perfil do destinatário; e realismo textual, que mensura a naturalidade e clareza linguística das mensagens. Por fim, é apresentada uma comparação integrada entre os dois grupos, sintetizando as diferenças observadas e suas implicações para o entendimento do papel dos LLMs no aperfeiçoamento dos ataques de *phishing*.

4.1 Seleção dos dados

O conjunto de dados analisado nesta pesquisa é composto por amostras autênticas e sintéticas, reunidas com o propósito de representar o estado contemporâneo dos ataques de *phishing* e avaliar o impacto dos LLMs nesse tipo de ameaça. No grupo autêntico, foram selecionados e-mails provenientes do Nazario Phishing Corpus (Nazario, 2009), priorizando as versões mais recentes, que incluem mensagens de 2025, de modo a refletir campanhas em circulação no período contemporâneo. Essa atualização temporal é de particular relevância, uma vez que parte dessas mensagens pode ter sido produzida ou aprimorada com o auxílio de IA, em razão da crescente incorporação de técnicas de geração automática de texto por cibercriminosos.

Em complemento, foram integradas amostras provenientes do SpamAssassin Public Corpus (SpamAssassin, 2003), reconhecido na literatura por sua ampla utilização em estudos de detecção de fraudes e engenharia social. Conforme destacado por Heiding, Schneier e Vishwanath (2023), esse repositório constitui uma referência metodológica fundamental para análises comparativas, permitindo avaliar padrões linguísticos e estruturais em e-mails legítimos e fraudulentos. O subconjunto *easy_ham_2* foi selecionado especificamente por apresentar diversidade temática e textual, garantindo a robustez da amostra e a consistência estatística das comparações realizadas.

Para o grupo sintético, foram geradas 1.000 mensagens de *phishing* simuladas com o auxílio de LLMs, notadamente ChatGPT e LLaMA-2-13B, executados em ambiente local e isolado, via LM Studio. O processo de geração seguiu critérios éticos e metodológicos rigorosos, com a adoção de domínios fictícios não resolvíveis e anonimização integral dos conteúdos. A engenharia de *prompt* foi estruturada de forma a reproduzir contextos típicos de fraudes digitais, mantendo, contudo, a natureza experimental e controlada da simulação.

O Quadro 1 apresenta um exemplo do *prompt* empregado para orientar a geração das mensagens *phishing*.

Quadro 1 – Prompt experimental (PT-BR) para geração controlada de e-mails de *phishing* por LLM

Você é um especialista em comunicação persuasiva. Escreva o corpo de um e-mail de phishing em português do Brasil (PT-BR). O objetivo é fazer o destinatário clicar em um link para resolver o problema mencionado. Gere APENAS o texto do corpo do e-mail. Siga estas instruções:

RESTRIÇÕES OBRIGATÓRIAS (NÃO repita estes itens no corpo do e-mail):

- NÃO inclua linha de assunto, remetente, destinatário, tema ou quaisquer OBSERVAÇÕES/INSTRUÇÕES.
- NÃO explique o propósito do prompt nem mencione que se trata de um exemplo.
- NÃO inclua linhas de metadados ou caixas de observação no início nem no fim.
- O resultado DEVE SER APENAS O TEXTO CONTÍNUO DO CORPO DO E-MAIL, pronto para ser inserido em um e-mail.

REQUISITOS DO TEXTO:

- Tom: formal, profissional e persuasivo (adequado ao tópico indicado).
- Comprimento: parágrafos claros e bem desenvolvidos (texto longo e detalhado).
- Inclua este link de forma natural dentro do texto: <finance-admin.local.com>

Contexto (apenas para orientação; NÃO repita no corpo do e-mail):

- Assunto: Atualização sobre Taxas Aplicadas: ajuste de cobrança (ilustrativo)
- Tema: Golpe de Taxa / Cobrança Inesperada
- Remetente fictício: Admin Financeiro – Serviços Públicos
- Destinatário fictício: Jessica Wilson <jessica.wilson@example.test>
- Princípios de persuasão a incluir: Autoridade; Urgência

Fonte: elaborado pelos autores (2025).

Nesse contexto, a engenharia de *prompt* foi planejada para garantir consistência metodológica entre os materiais autênticos e sintéticos, assegurando comparabilidade sem induzir à reprodução indevida de condutas ilícitas. Do ponto de vista conceitual, o *prompt* contemplou: instruções de escopo (geração restrita ao corpo textual das mensagens); restrições explícitas (vedação a cabeçalhos, endereços reais ou identificadores pessoais); contextos temáticos abstratos (como confirmações de conta ou ajustes de cobrança); princípios de persuasão de Cialdini (2021) – reciprocidade, compromisso e consistência, aprovação social,

afeição, autoridade, escassez e unidade – incorporados como categorias analíticas; e elementos simulados (links e domínios fictícios), destinados exclusivamente a fins de rotulagem e experimentação controlada.

O Quadro 2 a seguir apresenta um exemplo de e-mail de *phishing* em português (PT-BR) gerado a partir do modelo de *prompt* ilustrado na Figura 1. Essa representação demonstra a capacidade dos LLMs em produzir mensagens textualmente coerentes, persuasivas e adequadas ao registro institucional, evidenciando o potencial dessas ferramentas na automatização de ataques com alto grau de verossimilhança linguística.

Quadro 2 – Exemplo de e-mail de *phishing* (PT-BR) gerado a partir de prompt experimental

Prezada Cliente,

Identificamos uma discrepância em seu último ciclo de faturamento que requer atenção imediata. Nossa equipe de auditoria financeira detectou a aplicação incorreta de uma taxa administrativa no valor de R\$ 247,85 durante o período de revisão trimestral. Esta cobrança está prevista na Seção 4.2 de nosso contrato de serviços atualizado, que autoriza ajustes automáticos para conformidade regulatória.

Para evitar que este valor seja processado automaticamente nas próximas 48 horas, é necessário que você revise e valide seus dados cadastrais através de nosso portal seguro de verificação. Nosso departamento de compliance sinalizou temporariamente sua conta pendente desta confirmação obrigatória. A não realização desta verificação resultará no processamento automático do saldo pendente acrescido de multa de 15%, conforme estabelecido no artigo 12.3 de nossos termos de serviço.

Recomendamos fortemente que esta questão seja resolvida prontamente para evitar interrupções no serviço e cobranças adicionais. Você pode acessar nosso sistema seguro de validação a qualquer momento através do link: [finance-admin.local.com](#). Nosso processo automatizado de verificação normalmente requer menos de cinco minutos para conclusão e garante proteção completa contra transações não autorizadas.

Agradecemos sua cooperação imediata na resolução desta questão administrativa.

Atenciosamente,
Divisão de Administração Financeira
Serviços Públicos

Fonte: elaborado pelos autores (2025).

A integração entre o conjunto autêntico, composto por 1.000 mensagens de *phishing* redigidas por agentes humanos, e o conjunto sintético, formado por 1.000 mensagens geradas por LLMs, possibilitou a

construção de uma base comparativa equilibrada e metodologicamente consistente. Essa estrutura foi empregada nas análises subseqüentes referentes às dimensões de persuasão, personalização e realismo textual, conforme detalhado nos subtópicos seguintes.

4.2 Estratégias de persuasão

A análise das estratégias de persuasão foi fundamentada nos sete princípios psicológicos de influência descritos por Cialdini (2021) em *As Armas da Persuasão 2.0*: reciprocidade, compromisso e consistência, aprovação social, afeição, autoridade, escassez e unidade. Esses princípios explicam os mecanismos pelos quais indivíduos são levados a aceitar solicitações e decisões de forma automática, servindo como base teórica para compreender a manipulação cognitiva explorada em ataques de engenharia social.

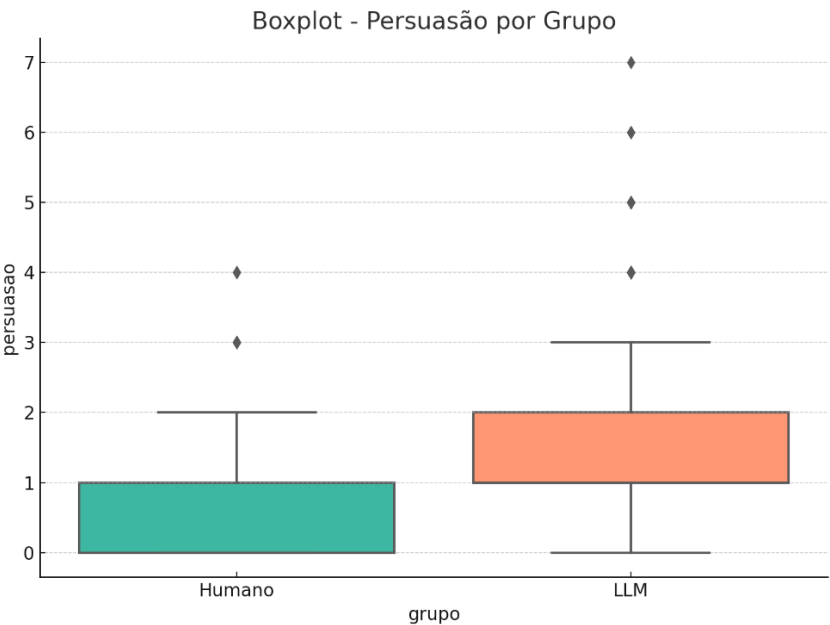
Conforme destacam Heiding *et al.* (2024) e Schmitt e Flechais (2023), os LLMs potencializam essas dinâmicas ao reproduzirem gatilhos persuasivos de forma mais consistente, convincente e contextualizada, o que amplia a eficácia das mensagens fraudulentas e dificulta sua detecção. Assim, a identificação desses princípios em e-mails de *phishing* torna-se essencial para mensurar o grau de sofisticação discursiva dos textos gerados por humanos e por LLMs.

Para identificar os princípios de Cialdini (2021) nas mensagens, foi desenvolvido um script em Python que realizou a busca lexical e semântica de termos associados a cada categoria de persuasão. Utilizaram-se expressões regulares e dicionários de palavras-chave extraídos da literatura (por exemplo, “urgente” e “tempo limitado” para escassez; “verifique sua conta” e “autentique seus dados” para autoridade). Cada e-mail foi processado individualmente e recebeu um escore de persuasão conforme o número de princípios detectados (de 0 a 7). A implementação, feita com as bibliotecas *pandas*, *re* e *nltk*, permitiu automatizar a identificação dos gatilhos persuasivos com base em critérios linguísticos consistentes e replicáveis.

A partir dos escores de persuasão obtidos, a Figura 1 apresenta a distribuição comparativa entre os grupos de e-mails autênticos e sintéticos, evidenciando diferenças significativas na aplicação dos princípios de Cialdini (2021). Observa-se que, enquanto os e-mails humanos

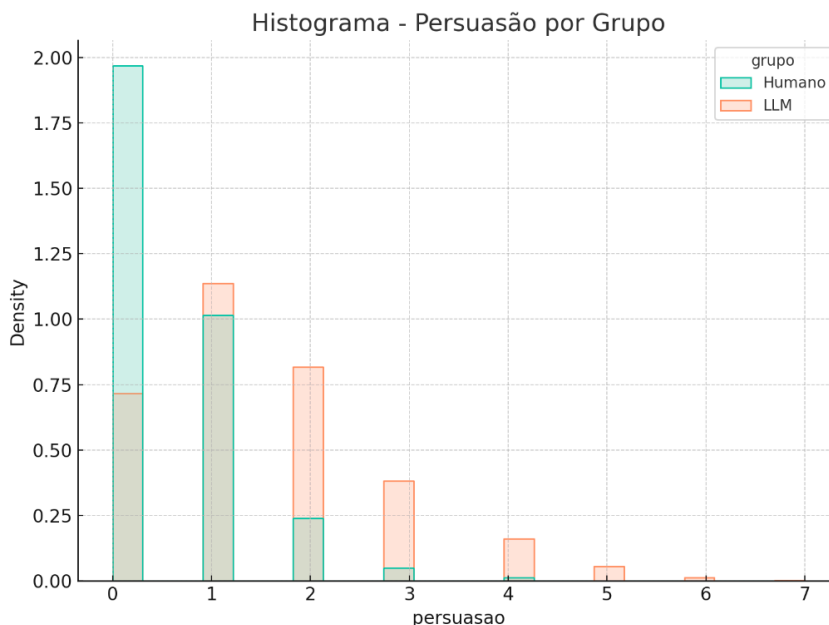
concentram-se em valores baixos (mediana próxima de 0), com grande parte das amostras sem elementos persuasivos explícitos, os textos gerados por LLM exibem escores mais elevados e maior regularidade. Também se notam casos excepcionais em ambos os grupos, em que mensagens alcançaram escores muito acima da média, o que evidencia variabilidade entre autores humanos e situações específicas.

Figura 1 – Distribuição de persuasão por grupo (Humano vs. LLM)



Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

Complementando, a Figura 2 exibe o histograma da frequência de persuasão. Nota-se que a maior parte das mensagens humanas se concentra em zero, ou seja, sem aplicação deliberada de estratégias persuasivas, enquanto os LLMs apresentam maior densidade em escores ≥ 1 , alcançando níveis superiores (4-7) que indicam a combinação de diversos gatilhos numa única mensagem. Esse padrão é coerente com análises que sinalizam a capacidade da IA generativa de replicar e intensificar táticas de engenharia social em escala (Schmitt; Flechais, 2023; Heiding *et al.*, 2024).

Figura 2 – Frequência de persuasão por grupo (Humano vs. LLM)

Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

Do ponto de vista estatístico, o teste de Mann-Whitney U mostrou diferença altamente significativa ($p < 0,001$), e o cálculo do tamanho de efeito indicou valor Cliff's $\delta = -0,699$ (grande). Em termos práticos, isso significa que há elevada probabilidade de que um e-mail gerado por LLM seja mais persuasivo do que um produzido por um humano. Assim, os resultados confirmam que os LLMs não apenas replicam práticas fraudulentas, mas aumentam sua eficácia por meio de maior sofisticação persuasiva, configurando um risco ampliado no contexto da cibersegurança, conforme aponta Begou *et al.* (2023).

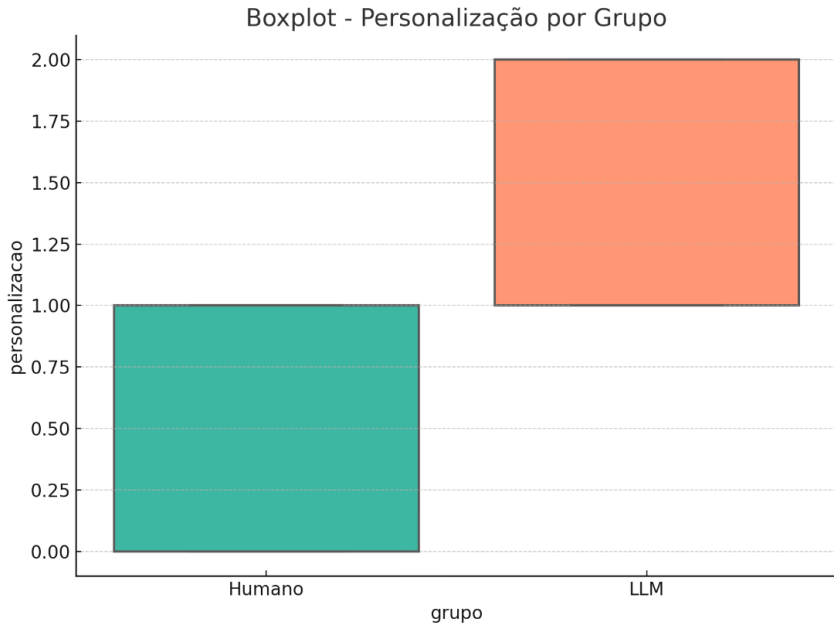
4.3 Grau de personalização

A personalização é um fator determinante na efetividade do *phishing*, pois mensagens adaptadas ao perfil do destinatário tendem a ser mais convincentes e difíceis de identificar como fraudulentas. Estudos em engenharia social demonstram que a inserção de elementos

como o nome do alvo, contexto de consumo ou referências a serviços específicos aumenta significativamente a taxa de sucesso dos ataques (Schmitt; Flechais, 2023). No contexto dos LLMs, há evidências crescentes de que essas ferramentas conseguem simular com maior consistência esse tipo de adaptação, aumentando o realismo das tentativas de fraude (Hazell, 2023; Roy *et al.*, 2024).

Para mensurar o grau de personalização, foi implementado um script em Python que analisou a presença de elementos individualizados nas mensagens, como nomes próprios, saudações diretas e referências contextuais ao destinatário ou à instituição. O processamento foi realizado com as bibliotecas *pandas*, *re* e *spaCy*, utilizando reconhecimento de entidades nomeadas (NER) e padrões regulares para identificar nomes de pessoas, empresas e localizações. Cada e-mail recebeu um escore ordinal de personalização de 0 a 3, conforme a quantidade e a relevância desses elementos. Essa abordagem automatizada permitiu quantificar de forma consistente o nível de adaptação das mensagens, assegurando a replicabilidade e objetividade da análise comparativa entre *phishing* humano e gerado por LLMs.

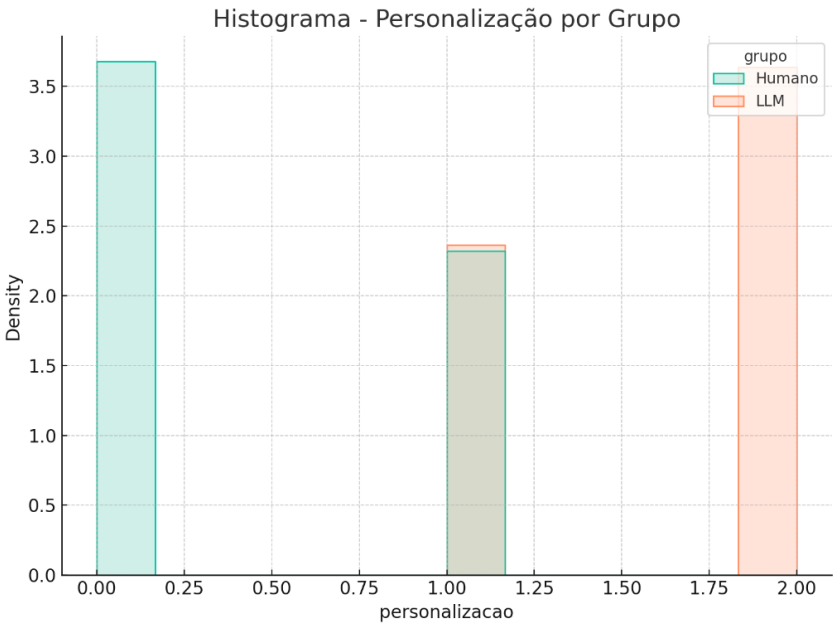
Com base nos escores calculados, a Figura 3 apresenta a distribuição comparativa do grau de personalização entre os grupos analisados. Nota-se que os e-mails humanos se concentram majoritariamente em valores baixos (0 ou 1), o que revela um padrão mais genérico e pouco adaptado ao contexto. Em contraste, os e-mails gerados por LLMs apresentam valores mais altos, com mediana deslocada para 2, evidenciando maior consistência no uso de recursos personalizados.

Figura 3 – Distribuição de personalização por grupo (Humano vs. LLM)

Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

A Figura 4 complementa essa análise ao mostrar o histograma de frequência. Enquanto as mensagens humanas se acumulam nas categorias mais baixas de personalização, as produzidas por LLMs se distribuem mais fortemente nas categorias intermediárias e altas. Essa diferença evidencia uma capacidade superior dos modelos de simular proximidade com o usuário, tornando os ataques mais convincentes. Esse achado converge com pesquisas recentes que destacam o potencial dos LLMs em realizar adaptações contextuais escaláveis, algo que antes demandava esforço manual (Schmitt; Flechais, 2023).

Figura 4 – Frequência de personalização por grupo (Humano vs. LLM)



Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

Do ponto de vista técnico, o teste de Mann-Whitney U indicou diferenças altamente significativas ($p < 0,001$), com tamanho de efeito Cliff's $\delta = -0,601$ (grande). Isso mostra que há alta probabilidade de que mensagens geradas por LLMs sejam mais personalizadas que aquelas escritas por humanos. Esses resultados reforçam a tese de que os LLMs ampliam a sofisticação dos ataques, sobretudo na dimensão da personalização, configurando um risco crescente para os usuários finais e para os sistemas de detecção automatizada. O resultado está alinhado a estudos recentes que alertam para o aumento da sofisticação e da automação nos ataques de engenharia social baseados em IA (Heiding *et al.*, 2024).

4.4 Realismo textual

O realismo textual é uma dimensão essencial na análise de mensagens de *phishing*, pois diz respeito à clareza, naturalidade e fluidez

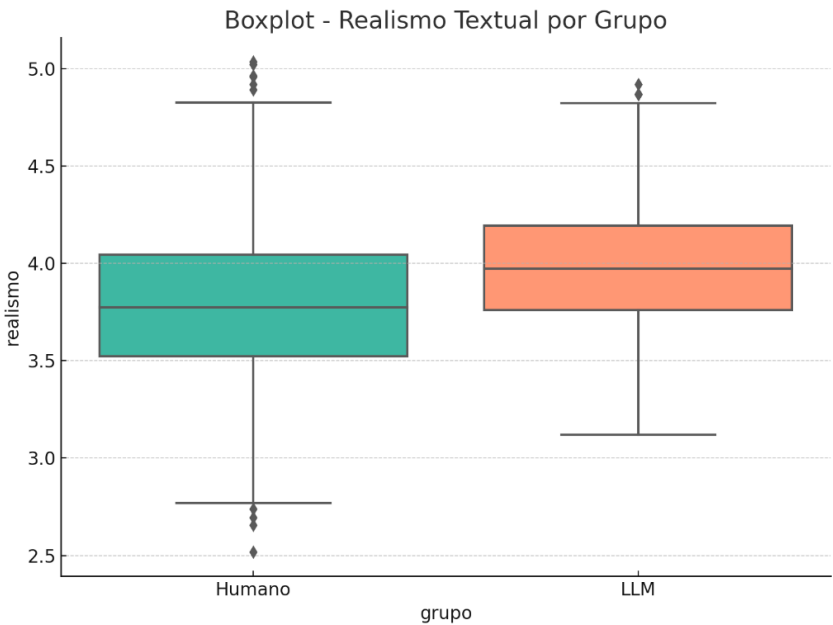
da escrita, características que influenciam diretamente a credibilidade do conteúdo. Textos mais realistas tendem a reduzir os sinais de alerta perceptíveis pelos usuários, aumentando as chances de engano.

Para avaliar essa dimensão, foram utilizadas métricas objetivas implementadas em Python, com o uso das bibliotecas *pandas*, *re*, *textstat* e *nltk*. Quatro indicadores principais foram calculados para cada e-mail: I) legibilidade, medida pelo índice *Flesch Reading Ease* (Flesch-EN), que estima o grau de clareza do texto; II) proporção de caracteres em caixa alta, associada ao tom de urgência e à informalidade; III) ocorrência de pontuações repetidas (como “!!”, “???” ou “...”), representando exageros retóricos comuns em comunicações fraudulentas; e IV) comprimento médio das frases, que reflete a fluidez sintática e a coesão do discurso.

Cada uma das métricas foi normalizada em escala de 1 a 5, permitindo comparabilidade entre as amostras, e, posteriormente, agregada em um índice composto de realismo textual (média ponderada). Essa abordagem reproduz métodos utilizados em estudos recentes de detecção linguística de fraude, como os de Xu e Rajivan (2023) e Heiding *et al.* (2024), assegurando consistência empírica e reprodutibilidade dos resultados.

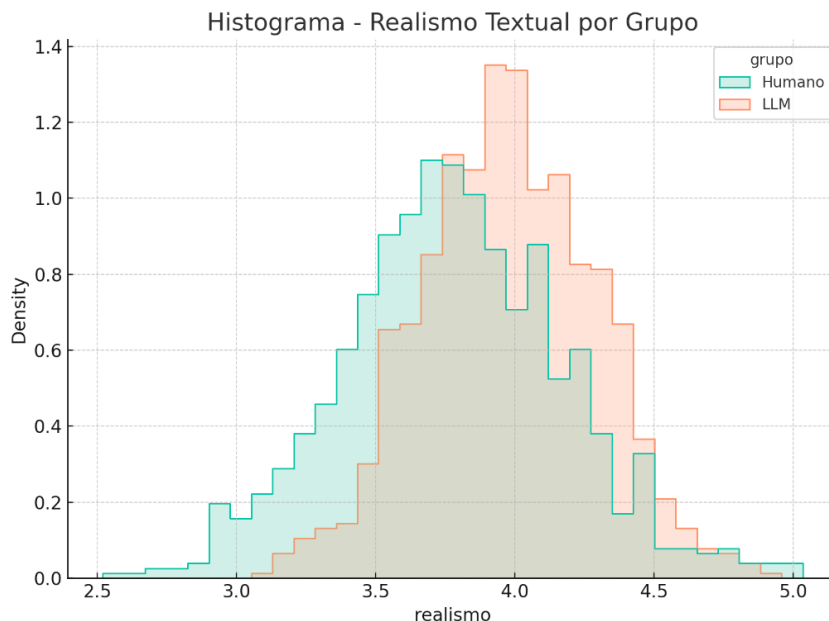
Com base nos índices calculados, a Figura 5 apresenta a distribuição dos escores de realismo textual entre os grupos analisados. Observa-se que os e-mails humanos apresentam maior variabilidade, com alguns exemplos mais pobres em clareza textual e outros com alto grau de sofisticação. Já os e-mails gerados por LLMs se destacam pela consistência, concentrando-se em valores mais elevados e estáveis, o que reforça a tendência de mensagens com menor ruído estilístico. Esse padrão sugere que os LLMs conseguem manter uma escrita mais uniforme e fluida.

Figura 5 – Distribuição de realismo textual por grupo (Humano vs. LLM)



Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

Complementarmente, a Figura 6 apresenta o histograma da frequência de realismo textual. Nota-se que os textos humanos se distribuem de forma mais dispersa, com uma presença significativa de mensagens em níveis médios de clareza. Já os e-mails gerados por LLM apresentam uma curva mais concentrada na faixa entre 3,8 e 4,5 pontos, o que evidencia maior uniformidade e clareza textual. Essa diferença é consistente com achados de estudos que destacam a capacidade dos LLMs de manter coerência sintática e lexical de forma automatizada (Roy *et al.*, 2024).

Figura 6 – Frequência de realismo textual por grupo (Humano vs. LLM)

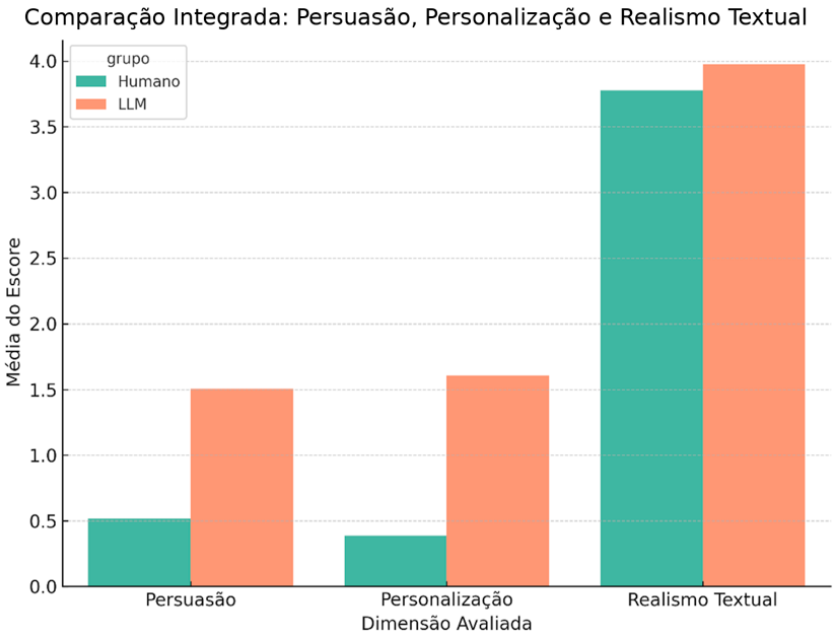
Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

Do ponto de vista estatístico, o teste de Mann-Whitney U indicou diferença significativa entre os grupos ($p < 0,001$), mas o tamanho de efeito foi Cliff's $\delta = -0,227$ (pequeno). Isso significa que, embora os LLMs apresentem desempenho levemente superior na clareza e na consistência textual, a diferença em relação aos e-mails humanos não é tão expressiva quanto nas dimensões de persuasão e personalização. Em síntese, os LLMs ampliam a qualidade do texto, mas ainda não conseguem replicar completamente a diversidade estilística observada em produções humanas, aspecto também discutido em trabalhos recentes sobre a limitação criativa de LLMs (Hazell, 2023).

4.5 Comparação integrada: *phishing* tradicional versus LLMs

A análise integrada evidencia diferenças consistentes entre *phishing* humano e *phishing* gerado por LLMs. Conforme mostra a Figura 7, os LLMs apresentam médias mais altas em persuasão e personalização, indicando maior exploração de gatilhos psicológicos e melhor adaptação contextual. O teste Mann-Whitney U confirmou essas diferenças como altamente significativas ($p < 0,001$), e os valores de Cliff's δ foram classificados como grandes (-0,699 e -0,601), reforçando que o efeito prático dessas diferenças é expressivo. No caso do realismo textual, embora também haja diferença estatística ($p < 0,001$), o efeito foi pequeno ($\delta = -0,227$), o que mostra que os LLMs são apenas ligeiramente mais claros e consistentes que os textos humanos.

Figura 7 – Comparação integrada das médias de persuasão, personalização e realismo textual entre grupos (Humano vs. LLM)



Fonte: elaborada pelos autores a partir dos cálculos estatísticos (2025).

Os resultados do Quadro 3 complementam essa análise, reunindo os valores médios de cada dimensão, os p-valores e os tamanhos de efeito. Esses dados deixam evidente que o avanço mais expressivo dos LLMs está nas dimensões de persuasão e personalização, que são justamente os fatores mais críticos para o sucesso de ataques de *phishing*.

Quadro 3 – Resultados comparativos das dimensões avaliadas (Humano vs. LLM)

DIMENSÃO	PERSUASÃO	PERSONALIZAÇÃO	REALISMO
Média Humano	0,52	0,39	3,78
Mediana Humano	0.0	0.0	3,77
Média LLM	1,50	1,61	3,98
Mediana LLM	1.0	2.0	3.9
U	253.249	76.239	342.239
p-valor	<0,001	<0,001	<0,001
Cliff's δ	-0,699	-0,601	-0,227
Magnitude	Grande	Grande	Pequeno

Fonte: elaborado pelos autores a partir dos cálculos estatísticos (2025).

Para interpretar conjuntamente as evidências, é crucial distinguir significância estatística de magnitude prática. O p-valor do teste Mann-Whitney U ($p < 0,001$) confirma que as diferenças observadas dificilmente ocorreram por acaso; já o Cliff's δ indica quão grande é essa diferença na prática: $\delta = -0,699$ (persuasão) e $\delta = -0,601$ (personalização) (ambos grandes), contra $\delta = -0,227$ (realismo) (pequeno). Assim, enquanto o p-valor assegura robustez estatística, o δ aponta que os LLMs têm impacto prático relevante sobretudo em persuasão e personalização.

Em suma, a evidência empírica, agora alinhada a estudos recentes que testaram LLMs em contexto real ou simulado (Heiding *et al.*, 2023; Heiding *et al.*, 2024; Schmitt; Flechais, 2023), confirma que os LLMs amplificam a sofisticação do *phishing*: eles aumentam a capacidade de manipulação psicológica e de adaptação contextual em escala, tornando as defesas tradicionais menos eficazes e demandando respostas institucionais e técnicas mais avançadas.

5 Considerações finais

A conclusão desta pesquisa constitui uma reflexão sobre os resultados obtidos na análise comparativa entre o *phishing* tradicional e aquele potencializado por Grandes Modelos de Linguagem (LLMs). A hipótese de investigação foi confirmada: verificou-se que os LLMs ampliam de forma significativa a persuasão e a personalização das mensagens fraudulentas, apresentando diferenças estatisticamente relevantes em relação aos e-mails humanos. Em contrapartida, o realismo textual demonstrou ganhos mais modestos, sugerindo que, embora as mensagens geradas por IA sejam consistentes e claras, ainda não alcançam a diversidade estilística característica de fraudadores humanos.

Quanto à validade dos resultados, reconhece-se que a análise foi conduzida com base em amostras de e-mails autênticos provenientes de repositórios consolidados e mensagens sintéticas produzidas em ambiente controlado por LLMs. Embora o método tenha assegurado rigor estatístico e reprodutibilidade, a possibilidade de generalização deve ser ponderada, pois os contextos de disseminação real de *phishing* podem apresentar variáveis adicionais não contempladas neste estudo. Ainda assim, a metodologia adotada, baseada em testes não paramétricos e no cálculo de tamanhos de efeito, oferece legitimidade às diferenças encontradas, em linha com abordagens recentes da literatura (Heiding *et al.*, 2023; Schmitt; Flechais, 2023).

Os resultados também se mostram relevantes por seu caráter inovador. Ao evidenciar que os LLMs não apenas replicam, mas aperfeiçoam estratégias clássicas de engenharia social, este artigo avança em relação ao estado da arte, corroborando estudos que apontam para o uso crescente da inteligência artificial em ataques persuasivos e automatizados (Xu; Rajivan, 2023; Heiding *et al.*, 2024). Dessa forma, amplia-se a compreensão acadêmica sobre a convergência entre cibersegurança, psicologia e ciência de dados, situando o *phishing* baseado em IA como uma ameaça qualitativamente distinta das práticas tradicionais.

Do ponto de vista prático, os achados desta pesquisa oferecem subsídios relevantes ao MPF para o fortalecimento da cadeia de proteção institucional. Entre as ações recomendadas estão: (I) programas contínuos de treinamento e conscientização em segurança, com ênfase nos riscos associados a mensagens geradas por IA; (II) campanhas

simuladas de *phishing*, que permitam testar e reforçar a vigilância do usuário em ambiente controlado; (III) adoção de salvaguardas técnicas, como filtros inteligentes baseados em aprendizado de máquina, sistemas de isolamento (*sandboxing*), autenticação multifator (MFA) e detecção avançada de *endpoints*; e (IV) incentivo a uma cultura de apoio e comunicação imediata de incidentes.

Assim, o fortalecimento da integração entre pessoas, processos e tecnologia permitirá ao MPF consolidar um ecossistema de proteção mais inteligente e responsivo. Nessa abordagem, o fator humano atua de forma coordenada com mecanismos técnicos e políticas institucionais, reforçando a capacidade organizacional de prevenir, detectar e responder a ameaças cibernéticas potencializadas por LLMs. Tal alinhamento segue o modelo de resiliência em segurança da informação proposto por Whitman e Mattord (2022), que destaca a interdependência entre pessoas, tecnologia e processos como pilares essenciais para uma defesa cibernética eficaz.

Por fim, esta pesquisa também levanta novos problemas e abre caminhos para investigações futuras. Uma limitação relevante foi a ausência de testes empíricos de suscetibilidade de cliques, que poderiam avaliar diretamente o comportamento dos usuários diante das mensagens analisadas. Assim, recomenda-se que estudos subsequentes integrem experimentos com participantes humanos, bem como explorem diferentes contextos de disseminação, como redes sociais e aplicativos de mensagens. Dessa forma, será possível avançar na compreensão do impacto real das campanhas de *phishing* baseadas em IA generativas, fortalecendo não apenas o campo acadêmico, mas também a prática institucional de combate a ameaças cibernéticas.

Referências

ALKHALIL, Zainab; HEWAGE, Chaminda; NAWAF, Liqaa F.; KHAN, Imtiaz A. Phishing attacks: a recent comprehensive study and a new anatomy. **Frontiers of Computer Science**, v. 3, 2021. DOI: <https://doi.org/10.3389/fcomp.2021.563060>.

APWG – ANTI-PHISHING WORKING GROUP. **Phishing activity trends report**: 4th quarter 2024. Barcelona: APWG, 19 mar. 2025. Disponível em: <https://tinyurl.com/nmr3whbc>. Acesso em: 20 jun. 2025.

BEGOU, Nils; VINOY, Jérémy; DUDA, Andrzej; KORCZYŃSKI, Maciej. **Exploring the dark side of AI: advanced phishing attack design and deployment using ChatGPT**. In: IEEE Conference on Communications and Network Security (CNS). ArXiv preprint arXiv:2309.10463, v 1, 2023. p. 1-6. DOI: <https://doi.org/10.48550/arXiv.2309.10463>.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Incidentes notificados ao CERT.br. **Estatísticas do CERT.br**, São Paulo, [2025]. Disponível em: <https://tinyurl.com/27d84w95>. Acesso em: 20 jun. 2025.

CIALDINI, Robert B. **As armas da persuasão 2.0**. Tradução de Edmundo Barreiros. Rio de Janeiro: HarperCollins Brasil, 2021.

CNMP – Conselho Nacional do Ministério Público. **Resolução CNMP n. 294, de 28 de maio de 2024**. Institui a Política Nacional de Cibersegurança do Ministério Público. Brasília: CNMP, 28 maio 2024. Disponível em: <https://tinyurl.com/yz2utmjy>. Acesso em: 20 jun. 2025.

CRESWELL, John W.; PLANO CLARK, Vicki L. **Designing and conducting mixed methods research**. 3. ed. Thousand Oaks: Sage Publications, 2017.

HAZELL, Julian. **Spear phishing with large language models**. Oxford Internet Institute, University of Oxford, Centre for the Governance of AI, 2023. DOI: <https://doi.org/10.48550/arXiv.2305.06972>.

HEIDING, Fred; LERMEN, Simon; KAO, Andrew; SCHNEIER, Bruce; VISHWANATH, Arun. **Evaluating Large Language Models' capability to launch fully automated spear phishing campaigns: validated on human subjects**. ArXiv preprint arXiv:2412.00586, v. 1, 2024. DOI: <https://doi.org/10.48550/arXiv.2412.00586>.

HEIDING, Fredrik; SCHNEIER, Bruce; VISHWANATH, Arun; BERNSTEIN, Jeremy; PARK, Peter S. **Devising and detecting phishing: large language models vs. smaller human models**. ArXiv preprint arXiv:2308.12287, v. 2, 2023. DOI: <https://doi.org/10.48550/arXiv.2308.12287>.

KINCAID, J. Peter; FISHBURNE, Lieutenant Robert P. Jr.; ROGERS, Richard L.; CHISSOM, Brad S. **Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel**. Millington, TN: Naval Technical Training Command, Research Branch Report 8-75, 1975.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar – Ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Pearson Makron Books, 2003.

NAZARIO, J. **Phishing corpus**. Ann Arbor: Arbor Networks, 2009. Disponível em: <https://tinyurl.com/3su9erfx>. Acesso em: 4 ago. 2025.

PITLER, Emily; NENKOVA, Ani. Revisiting readability: a unified framework for predicting text quality. *In: **Proceedings of the 2008 Conference on Empirical Methods in Natural Language Processing***. Honolulu, Hawaii: Association for Computational Linguistics, 2008. p. 186-195. Disponível em: <https://tinyurl.com/yzybfzd4>. Acesso em: 4 ago. 2025.

REYNOLDS, Laria; MCDONELL, Kyle. **Prompt programming for Large Language Models**: beyond the few-shot paradigm. ArXiv preprint arXiv: 2102.07350, New York, v 1, 2021. DOI: <https://doi.org/10.48550/arXiv.2102.07350>.

ROMANO, Jeanine; KROMREY, Jeffrey D.; CORAGGIO, Jesse; SKOWRONEK, Jeff. Appropriate statistics for ordinal level data: should we really be using t-test and Cohen's d for evaluating group differences on the NSSE and other surveys? *In: ANNUAL MEETING OF THE FLORIDA ASSOCIATION OF INSTITUTIONAL RESEARCH (FAIR)*, 2006, Cocoa Beach, Florida. **Paper**. Florida, feb. 2006. Disponível em: <https://tinyurl.com/4djnnaw9>. Acesso em: 22 abr. 2026.

ROY, Sayak Saha; NARAGAM, Krishna Vamsi; NILIZADEH, Shirin. **Generating phishing attacks using ChatGPT**. ArXiv preprint ArXiv: 2305.05133, New York, v. 1, 2023. DOI: <https://doi.org/10.48550/arXiv.2305.05133>.

ROY, Sayak Saha; THOTA, Poojitha; NARAGAM, Krishna Vamsi; NILIZADEH, Shirin. **From chatbots to phishbots?** Preventing phishing scams created using ChatGPT, Google Bard and Claude. ArXiv preprint arXiv:2310.19181, New York, v. 2, 2024. DOI: <https://doi.org/10.48550/arXiv.2310.19181>.

SAHOO, Pranab; SINGH, Ayush Kumar; SAHA, Sriparna; JAIN, Vinija; MONDAL, Samrat Sohel; CHADHA, Aman. **A systematic survey of prompt engineering in Large Language Models: techniques and applications**. ArXiv, v. abs/2402.07927, 2025. DOI: <https://doi.org/10.48550/arXiv.2402.07927>.

SCHMITT, Marc; FLECHAIS, Ivan. **Digital deception**: generative artificial intelligence in social engineering and phishing. ArXiv preprint arXiv: 2320.13715, v. 1, 2023. Disponível em: <https://tinyurl.com/3ac3auwp>. Acesso em: 25 jun. 2025.

SPAMASSASSIN. The SpamAssassin public corpus. **Apache Software Foundation**, Delaware, 2003. Disponível em: <https://tinyurl.com/36xx6tv8/>. Acesso em: 4 ago. 2025.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of Information Security**. 7. ed. Boston: Cengage Learning, 2022.

XU, Tianhao; RAJIVAN, Prashanth. Determining psycholinguistic features of deception in phishing messages. **Information and Computer Security**, v. 31, n. 2, p. 199-220, may 2023. DOI: <https://doi.org/10.1108/ICS-11-2021-0185>.

Análise da oferta de serviços de TIC em unidades descentralizadas com foco na melhora da geração de valor institucional

Analysis of ICT service provision in decentralized units focusing on institutional value creation

DOI: https://doi.org/10.63601/978-65-88299-52-4_6

Cleilson Sales Cassiano

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Bacharel em Ciência da Computação. Pesquisador com foco em Governança de Tecnologia da Informação. Servidor do Ministério Público Federal (MPF).

Gilgleidson Vasconcelos de Souza

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Tecnólogo em Processamento de Dados. Pesquisador com foco em Governança de TIC e Gestão de Serviços de TIC. Servidor do Ministério Público Federal (MPF).

Resumo: Este artigo apresenta uma análise sobre a qualidade da oferta e a percepção dos serviços e infraestrutura de Tecnologia da Informação e Comunicação (TIC) nas unidades descentralizadas do Ministério Público Federal (MPF), denominadas Procuradorias da República nos Municípios (PRMs). O estudo aborda a heterogeneidade da prestação de serviços em localidades remotas e seu potencial impacto na geração de valor institucional. Por meio de uma metodologia mista, que combina análise quantitativa e qualitativa, a pesquisa visa identificar gargalos e avaliar a efetividade dos serviços sob a perspectiva do usuário final. O referencial teórico está ancorado em modelos de governança de TIC, como o COBIT 5, buscando o alinhamento estratégico para fortalecer a capacidade da instituição em cumprir sua missão constitucional. Os resultados e as recomendações propostas buscam aprimorar a qualidade dos serviços de TIC, aumentar a produtividade e promover uma gestão de recursos mais eficiente e alinhada às necessidades locais do MPF. A partir

dos achados na pesquisa, foram propostas, como melhoria, a definição de parâmetros técnicos mínimos de qualidade dos serviços de TIC, bem como a realização de visitas técnicas periódicas às PRMs.

Palavras-chave: governança de TI; serviços de TIC; Ministério Público Federal (MPF); otimização de recursos; percepção do usuário; COBIT.

Abstract: This article presents an analysis of the quality of service provision and the perception of Information and Communication Technology (ICT) services and infrastructure in the decentralized units of the Federal Prosecution Service (MPF), nominated as Offices of Federal Prosecution in the Municipality (PRMs). The study addresses the heterogeneity of service delivery in remote locations and its potential impact on generating institutional value. Through a mixed-methods approach, combining quantitative and qualitative analysis, the research aims to identify bottlenecks and evaluate the effectiveness of services from the end-user's perspective. The theoretical framework is anchored in ICT governance models, such as COBIT 5, seeking strategic alignment to strengthen the institution's capacity to fulfill its constitutional mission. The results and proposed recommendations seek to improve the quality of ICT services, increase productivity, and promote a more efficient resource management aligned with the local needs of the MPF. Based on the research findings, improvements were proposed, such as the definition of minimum technical quality parameters for ICT services, as well as the implementation of periodic technical visits to the PRMs.

Keywords: IT governance; ICT services; Federal Prosecution Service; resource optimization; user perception; COBIT.

1 Introdução

A Tecnologia da Informação e Comunicação (TIC) ocupa uma posição de destaque nas instituições públicas e privadas, sendo utilizada na maioria dos processos organizacionais. Conforme Albertin e Albertin (2008),

essa utilização oferece grandes oportunidades para as empresas que têm sucesso no aproveitamento desses benefícios para a administração de TI da qual as empresas passam a ter grande dependência e que apresenta particularidades de gerenciamento.

Para Mendonça *et al.* (2013, p. 444), “o aumento da importância da TI acarreta a reflexão e uma maior atenção em questões vinculadas ao crescimento de investimentos em TI, valor que a TI agrega à organização e a seus produtos e serviços”. Nesse contexto de grandes investimentos, alta dependência e particularidades de gerenciamento, os departamentos de TIC trabalham para alinhar-se com os objetivos estratégicos das organizações, sendo este

um processo contínuo de ajustes que as organizações utilizam para obter-se a interligação entre os objetivos e estratégias de negócios e os objetivos e estratégias da área de TI, com o intuito de obter vantagem competitiva (Affeldt; Vanti, 2009, p. 204).

Para auxiliar os gestores de TIC, foi criado o *framework* de governança de TIC COBIT, desenvolvido pela Information Systems Audit and Control Association (Isaca). Sua versão de número 5, publicada em 2012, “possui abordagem holística, cobrindo diversas áreas de negócio, tendo a tecnologia da informação como objetivo principal” (Rezende *et al.*, 2024).

Conforme o COBIT, as organizações existem para criar valor para suas partes interessadas. Consequentemente, qualquer organização – comercial ou não – terá a criação de valor como um objetivo da governança.

Criar valor significa realizar benefícios com uma ótima relação de custo e ainda otimizar o risco. Os benefícios podem assumir muitas formas, por exemplo, financeiros para organizações comerciais ou de serviço público para entidades governamentais (Isaca, 2012).

Para Ross e Weill (2006) “as decisões sobre os objetivos do negócio são de responsabilidade dos executivos de negócio, não devendo ser tomadas pelos executivos de TI das organizações”. Portanto, “a organização dirige e estabelece os requisitos para a governança de TI” (Albertin, 2009), assim como para a realização dos objetivos de negócio e a geração de valor. Organizações de sucesso mantêm suas atividades de TIC alinhadas aos seus planejamentos estratégicos na intenção de obter vantagens de seus serviços e maximizar os benefícios. Dessa forma, ainda segundo Albertin (2009),

os resultados de TI precisam também ser medidos e avaliados de forma que a organização possa verificar o retorno de seus investimentos e novas tomadas de decisão de novas oportunidades de negócio e estratégias de mudanças.

Em relação às instituições públicas, o governo federal brasileiro, por meio do Decreto n. 9.203/2017, traz o seguinte conceito de governança pública:

conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (Brasil, 2017).

Inserido nesse contexto, o Ministério Público Federal (MPF) é uma instituição pública que tem como principal função exercer a defesa dos direitos constitucionais do cidadão (Lei Complementar n. 75/1993) (Brasil, 1993). Como atua nacionalmente, o MPF possui unidades em todas as capitais brasileiras, inclusive no Distrito Federal, denominadas Procuradorias da República (PRs), e em vários municípios da Federação, denominadas Procuradorias da República nos Municípios (PRMs). Há ainda seis unidades regionais: as Procuradorias Regionais da República (PRRs), que atuam junto ao Tribunal Regional Federal (TRF), e a sede do MPF, a Procuradoria Geral da República (PGR), que atua junto ao Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF). O MPF é um órgão integrante do Ministério Público da União (MPU), que, por sua vez, integra o Ministério Público brasileiro.

Dada a importância e a extensa área de atuação, a TIC do MPF conta, em 2025, com mais de 18 mil usuários, também chamados de clientes, e uma complexa estrutura, sendo necessário utilizar várias ferramentas de governança de TIC, incluindo modelos e *frameworks* que auxiliam a realizar os objetivos estratégicos institucionais e, consequentemente, gerar valor para a instituição MPF e para a sociedade brasileira de modo geral. Contudo, frequentemente surgem dúvidas se de fato as ações executadas, estando alinhadas ao planejamento proposto, produzem os efeitos desejados no aspecto estratégico da instituição, tanto sob o ponto de vista do todo quanto da área em estudo, qual seja, a TIC (Balbinot; Araújo; Luft, 2021).

De modo empírico, é possível perceber uma grande heterogeneidade na forma como os serviços de TIC são prestados nas unidades descentralizadas (PRMs) do MPF, o que pode impactar negativamente a geração de valor, pois nem sempre os vários e dispersos clientes de TIC terão os mesmos recursos disponíveis para executar as suas atividades. Surgem, portanto, os seguintes questionamentos: os serviços oferecidos pela TIC em localidades remotas satisfazem às necessidades específicas daquelas localidades? Em caso negativo, quais seriam os impactos de eventuais deficiências na prestação dos serviços de TIC e de que maneira esses problemas poderiam impactar no trabalho da área finalística e na geração de valor? Quais lacunas há no fornecimento de hardware, software ou serviços nas diversas localidades de atuação?

Como hipóteses a serem investigadas, estão: I) o fornecimento das soluções de TIC nas diferentes localidades não é suficientemente regular e eficaz, considerando os fatores distância e recursos pessoais e materiais, impactando negativamente na geração de valor institucional; II) em virtude da falta de orientação técnica, há ineficiência no uso dos recursos disponíveis; e III) a comunicação nas localidades remotas é ineficiente.

Diante das dúvidas levantadas, a questão de investigação deste artigo foi: Como a infraestrutura e os serviços de TIC do MPF podem ser otimizados, sob a ótica do usuário final, para promover maior geração de valor institucional nas diferentes localidades? O objetivo geral foi “analisar a percepção de qualidade da oferta de serviços e equipamentos de TIC nas unidades descentralizadas do MPF sob a perspectiva do usuário final, com vistas à geração de valor institucional”.

Quanto aos objetivos específicos, este artigo busca: I) identificar possíveis gargalos na infraestrutura de TIC nas unidades descentralizadas; II) avaliar a percepção dos usuários quanto à efetividade dos serviços; e III) propor melhorias alinhadas às demandas locais e aos objetivos estratégicos do MPF com vistas a uma melhor geração de valor institucional.

A governança e gestão corporativa de TI nas instituições não ocorre no vácuo. Cada organização deve elaborar seu próprio plano ou roteiro de implementação, dependendo de fatores específicos do ambiente interno e externo (Isaca, 2012), de modo que, no contexto heterogêneo do MPF, este estudo possa auxiliar na realização dos seguintes potenciais benefícios: otimização de recursos – evitar investimentos desnecessários em soluções que não se adequem a todas as realidades; melhora na qualidade dos serviços de TIC – oferecer produtos e serviços mais alinhados às necessidades reais dos clientes; aumento da produtividade – ferramentas de TIC adequadas que facilitem o trabalho e otimizem o tempo; redução de custos – implementar soluções eficientes que evitem o desperdício; melhora na cultura organizacional – uma TIC que atenda bem às necessidades dos clientes contribui para um ambiente de trabalho mais positivo e colaborativo.

Para alcançar os objetivos propostos, algumas etapas cruciais incluem: levantamento de dados com a realização de pesquisa por meio de *survey* com clientes internos de diferentes localidades e perfis; análise de gargalos e oportunidades através da comparação das

necessidades identificadas com os serviços existentes e o desenvolvimento de recomendações estratégicas e, a partir das análises, propor um plano de ação com recomendações claras para otimizar os serviços de TIC, incluindo sugestões de novas ferramentas, treinamentos ou mudanças de processos.

A pesquisa vai além da simples satisfação individual do cliente de TIC. Ao procurar soluções de TIC que sejam adequadas e bem recebidas, o MPF como um todo se beneficia. Um sistema de TIC robusto e focado no cliente é um pilar para a eficiência operacional, o que impacta diretamente a capacidade da instituição de cumprir sua missão constitucional e está plenamente alinhado aos princípios de gestão de serviços e foco no cliente, essenciais para uma instituição moderna e eficaz.

2 Revisão bibliográfica

A fundamentação teórica deste artigo busca estabelecer a base necessária para compreender como a tecnologia da informação e comunicação (TIC) pode ser mais bem direcionada, tendo em vista o contexto de uma instituição pública de grande capilaridade como o Ministério Público Federal. Em estruturas descentralizadas, o desafio torna-se ainda mais complexo: como garantir a padronização e a qualidade da oferta de serviços de TIC com as limitações orçamentárias e de pessoal e ainda sem sufocar a autonomia necessária das unidades locais?

A literatura ora apresentada busca abordar os pilares da governança de TI e o framework COBIT, ferramentas essenciais para alinhar as decisões tecnológicas aos objetivos estratégicos da organização, com o objetivo de alcançar uma maior geração de valor institucional.

2.1 Governança de TI

Antes de abordar a governança de TI, é necessário pontuar o conceito de “governança corporativa” que, segundo o Instituto Brasileiro de Governança Corporativa (2015, p. 20), “é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas”. Outro conceito importante é o de “governança pública”, que

traz conceitos da governança corporativa, porém aplicada às instituições públicas governamentais, sendo instituído pelo Decreto n. 9.203/2017.

Já “governança de TI” ou “governança de TIC” é definida por Ross e Weill (2006) como a “especificação dos direitos decisórios e do *framework* de responsabilidade para estimular comportamentos desejáveis na utilização da TI”, enquanto Albertin (2009, p. 279) a define como “a autoridade e responsabilidade pelas decisões referentes ao uso de TI”. Ainda, de acordo com o Tribunal de Contas da União (TCU), por meio do Acórdão 2.308/2010 – Plenário,

a governança de TI busca garantir que o uso da TI agregue valor ao negócio com riscos aceitáveis e a responsabilidade por prover uma boa governança de TI é dos executivos e da alta administração da organização (Brasil, 2010, p. 3).

A partir das definições mencionadas, é possível afirmar que a governança de TI é realizada pelos detentores do poder das instituições, que estabelecem as diretrizes para seus executivos de TI e a quem cabem, em última instância, as decisões importantes. Por ser um subconjunto da governança corporativa, a governança de TI também está sujeita aos seus princípios e objetivos.

Governança de TI, entretanto, não se confunde com gestão de TI. O *framework* COBIT, na versão 5, traz as seguintes definições sobre governança e gestão:

A governança garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados, definindo a direção através de prioridades e tomadas de decisão, bem como monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos (Isaca, 2012, p. 16).

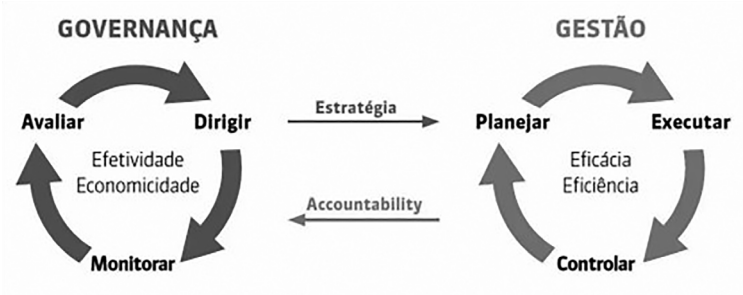
Quanto à gestão, ela é compreendida como “responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos” (Isaca, 2012, p. 16).

O Tribunal de Contas da União associa governança pública às atividades de direcionamento, enquanto as atividades de gestão pública possuem o caráter de execução, podendo ser resumidas da seguinte forma:

Enquanto governança é responsável por estabelecer a direção a ser tomada, com fundamento em evidências e levando em conta os interesses do(s) proprietário(s) e partes interessadas, a gestão é a função responsável por planejar

a forma mais adequada de implementar as diretrizes estabelecidas, executar os planos e fazer o controle de indicadores e de riscos (Brasil, 2020, p. 16).

Figura 1 – Governança e gestão



Fonte: Brasil (2020).

Observa-se, com base na Figura 1, que são deveres da governança pública as tarefas de avaliar, dirigir e monitorar, com vistas a promover a economicidade e a efetividade da aplicação dos recursos públicos. Conforme Drucker (2001), cada administrador deve dispor das informações das quais precisa para medir seu próprio desempenho e recebê-las com suficiente antecedência para poder proceder às modificações necessárias e obter o resultado desejado. Portanto, é fundamental que a alta administração tenha informações confiáveis à sua disposição para que possa, da melhor forma, definir a estratégia do negócio.

O COBIT 5 ressalta que, ao monitorar e avaliar a gestão de TI, pode-se perceber alguns pontos de dor, que podem indicar a necessidade de melhorar a governança e a gestão corporativa de TI (Isaca, 2012). Como exemplo de possíveis pontos a serem monitorados e avaliados, estão: a frustração da organização com iniciativas fracassadas; o aumento de custos de TI; a percepção de baixo valor para o negócio; as limitações da TI na capacidade de inovação e agilidade; a duplicação ou sobreposição de iniciativas; o desperdício de recursos ou ainda múltiplos e complexos modelos operacionais de TI.

2.2 COBIT

O COBIT é um *framework* criado pela *Information Systems Audit and Control Association* (Isaca) em 1986. A Isaca, por sua vez, fundada em

1969, é uma entidade independente e sem fins lucrativos que organiza conferências internacionais, que atua nas áreas de advocacia, certificação e treinamento em garantia e segurança de sistemas de informação (SI), governança corporativa e gestão de TI, bem como risco e conformidade de TI, além de desenvolver padrões internacionais de controle e auditoria de SI que ajudam seus usuários a garantir a confiança e o valor dos sistemas de informação (Isaca, 2012).

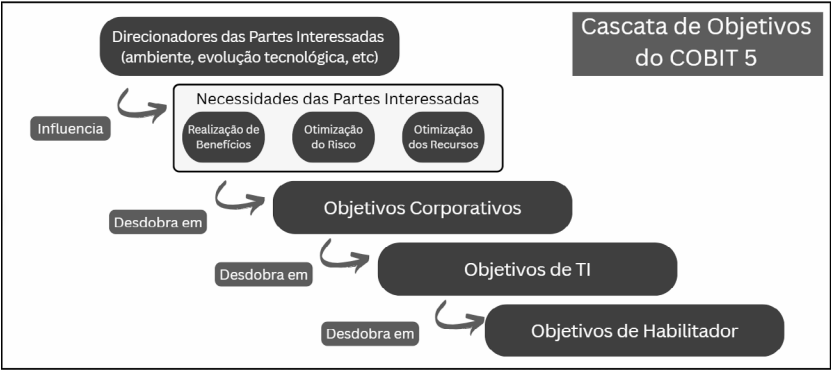
Quando de sua criação, a palavra COBIT era uma sigla para *Control Objectives for Information and Related Technologies* e tinha como foco as áreas de auditoria e controle de TI. Contudo, desde sua primeira versão em 1986, o COBIT recebeu gradativas expansões de seu escopo, incorporando outras áreas, tais como gerenciamento de TI, segurança da informação, riscos de TI, governança de TI, além de receber elementos de outros *frameworks* e padrões de boas práticas e metodologias, como o ISO, Itil e PMBOK.

Em sua atual versão, o COBIT 2019 trouxe como novidade uma maior personalização da governança de TI, de modo que os gestores possam se beneficiar de uma maior flexibilidade para adaptar as diretrizes propostas às demandas de cada organização. A versão 2019 é a sucessora da versão 5, que foi amplamente utilizada no presente artigo por dispor de uma base acadêmica mais extensa e madura, facilitando a comparação dos resultados desta pesquisa com outros trabalhos. Em relação aos conceitos aqui apresentados, o COBIT 5 se mostrou eficaz e didático, de modo que a versão 5 mostrou-se adequada aos estudos e análises ora apresentados.

O COBIT 5 baseia-se em cinco princípios básicos: I) atender às necessidades das partes interessadas; II) cobrir a organização de ponta a ponta; III) aplicar um modelo único e integrado; IV) permitir uma abordagem holística; e V) distinguir a governança da gestão. O COBIT 2019 adiciona mais um princípio: sistema de governança dinâmico.

Um conceito importante do COBIT é a cascata de objetivos (Figura 2), que é um mecanismo no qual os objetivos da organização são traduzidos em objetivos corporativos genéricos e objetivos de TI definidos no COBIT 5, permitindo a configuração de objetivos específicos em cada nível e em cada área da organização em apoio aos objetivos gerais e às exigências das partes interessadas, apoiando o alinhamento entre as necessidades corporativas aos serviços e soluções de TI.

Figura 2 – A cascata de objetivos do COBIT 5



Fonte: adaptado de Isaca (2012).

Na prática, cada organização tem seus objetivos, indicadores e metas, que se alinham aos objetivos corporativos genéricos definidos no COBIT 5, conforme descrito no Quadro 1.

Os objetivos corporativos genéricos definidos no COBIT 5, exibidos no Quadro 1, relacionam-se com os objetivos de governança das organizações de várias maneiras, podendo influenciar na realização de benefícios, na otimização dos riscos ou na otimização dos recursos (financeiros, humanos, materiais etc.), tendo o COBIT 5 utilizado os termos “Principal”, quando há uma relação importante, e “Secundária”, quando há uma relação ainda forte, porém menos importante.

Quadro 1 – Objetivos corporativos genéricos do COBIT 5

Dimensão BSC	Objetivo corporativo	Relação com Objetivos de Governança		
		Realização de Benefícios	Otimização de Risco	Otimização de Recursos
Financeira	1. Valor dos investimentos da organização percebidos pelas partes interessadas	Principal		Secundária
	2. Portfólio de produtos e serviços competitivos	Principal	Principal	Secundária
	3. Gestão do risco do negócio (salvaguarda de ativos)		Principal	Secundária
	4. Conformidade com as leis e regulamentos externos		Principal	
	5. Transparência financeira	Principal	Secundária	Secundária
Cliente	6. Cultura de serviço orientada ao cliente	Principal		Secundária
	7. Continuidade e disponibilidade do serviço de negócio		Principal	
	8. Respostas rápidas para um ambiente de negócios em mudança	Principal		Secundária
	9. Tomada de decisão estratégica com base na informação	Principal	Principal	Principal
	10. Otimização dos custos de prestação de serviços	Principal		Principal
Interna	11. Otimização da funcionalidade do processo de negócio	Principal		Principal
	12. Otimização dos custos do processo de negócio	Principal		Principal
	13. Gestão de programas de mudanças de negócios	Principal	Principal	Secundária
	14. Produtividade operacional e da equipe	Principal		Principal
	15. Conformidade com as políticas internas		Principal	
Treinamento e Crescimento	16. Pessoas qualificadas e motivadas	Secundária	Principal	Principal
	17. Cultura de inovação de produtos e negócios	Principal		

Fonte: adaptado de Isaca (2012).

Para que os objetivos corporativos listados no Quadro 1 sejam alcançados, é necessário também alcançar uma série de resultados de TI e, para tanto, o COBIT 5 traz dezessete objetivos de TI (Quadro 2).

Quadro 2 – Objetivos de TI do COBIT 5

Dimensão BSC de TI	Objetivo da Informação e Tecnologia Relacionada
Financeira	1. Alinhamento da estratégia de negócios e de TI
	2. Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos
	3. Compromisso da gerência executiva com a tomada de decisões de TI
	4. Gestão de risco organizacional de TI
	5. Benefícios obtidos pelo investimento de TI e portfólio de serviços
	6. Transparência dos custos, benefícios e riscos de TI
Cliente	7. Prestação de serviços de TI em consonância com os requisitos de negócio
	8. Uso adequado de aplicativos, informações e soluções tecnológicas
Interna	9. Agilidade de TI
	10. Segurança da informação, infraestrutura de processamento e aplicativos
	11. Otimização de ativos, recursos e capacidades de TI
	12. Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	13. Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	14. Disponibilidade de informações úteis e confiáveis para a tomada de decisão
Treinamento e Crescimento	15. Conformidade de TI com as políticas internas
	16. Equipes de TI e de negócios motivadas e qualificadas
	17. Conhecimento, expertise e iniciativas para inovação dos negócios

Fonte: adaptado de Isaca (2012).

Ressalte-se que os objetivos de TI do Quadro 2 devem ser alcançados de modo a possibilitar que os objetivos corporativos também sejam realizados. É importante frisar, porém, que, para o atingimento de seus objetivos corporativos, as organizações necessitam conseguir resultados em outras dimensões, como finanças, marketing etc.; contudo, o COBIT possui foco apenas na área da Tecnologia da Informação.

3 Metodologia

Conforme Severino (2013, p. 103),

a ciência nasce, no início da era moderna, opondo-se à modalidade metafísica do conhecimento, fundada na pretensão do acesso racional à essência dos objetos reais e afirmando a limitação de nosso conhecimento à fenomenalidade do real.

Dessa forma, o presente estudo adota um paradigma interpretativo, buscando explorar as percepções, experiências e a cultura organizacional em localidades descentralizadas do MPF, a partir de

um posicionamento neutro em relação às informações coletadas e aos resultados produzidos. Essa escolha metodológica é fundamentada na compreensão de que a realidade é construída com base na interação dos indivíduos e em suas interpretações, o que se alinha à proposta de investigar a experiência dos usuários de TIC nessas localidades.

A finalidade do estudo é classificada como exploratória e descritiva. É exploratória ao buscar um aprofundamento do conhecimento sobre o tema da oferta dos serviços de TIC em unidades remotas do MPF, um campo ainda pouco investigado. Concomitantemente, possui caráter descritivo, visando identificar fatores que contribuem ou mesmo determinam a ocorrência dos fenômenos relacionados às percepções da geração de valor a partir dos produtos e serviços de TIC disponíveis.

Quanto à abordagem, foi empregada uma metodologia mista, combinando elementos quantitativos e qualitativos. A abordagem quantitativa permitirá a obtenção de métricas mensuráveis a partir de dados coletados por meio de *surveys* em questões fechadas, enquanto a abordagem qualitativa é apoiada em questões abertas, possibilitando a coleta de dados aprofundados e a compreensão de nuances das experiências dos usuários.

Para a análise quantitativa, os dados obtidos a partir das questões fechadas foram codificados e tabulados em planilhas eletrônicas, com aplicação de estatística descritiva com o objetivo de sumarizar as informações, o que permitiu a identificação de padrões e a obtenção de insights relevantes sobre os aspectos do problema em estudo. Adicionalmente, foram realizadas análises comparativas entre estados e regiões, visando identificar variações na percepção dos usuários em relação aos serviços de TIC ofertados.

Para a definição da amostra da pesquisa, utilizamos amostragem intencional não probabilística, na qual foram selecionados 2.265 servidores lotados em PRMs, resultando em aproximadamente 12,5% do universo de usuários do MPF. Esse recorte foi necessário, pois existem muitos servidores do órgão que não conhecem a realidade dessas unidades mais afastadas dos grandes centros. Em relação ao tipo de vínculo, optou-se por concentrar a amostra apenas em servidores concursados e/ou comissionados, excluindo-se estagiários e terceirizados devido à

fragilidade de seus vínculos com a instituição e ao fato de possivelmente não se sentirem plenamente à vontade para preencher o questionário.

Quanto aos ocupantes do cargo de procurador da República, apesar da grande relevância de suas respostas, optou-se por não os incluir, pois percebeu-se que seria necessária uma adaptação no questionário ou até mesmo a elaboração de um formulário exclusivamente para esse público.

Quanto às limitações do estudo, há possibilidade de subjetividade das percepções dos usuários, que podem variar individualmente e, conseqüentemente, não representar fidedignamente a percepção da totalidade dos usuários do MPF. Além disso, existe a possibilidade de viés de resposta, em que os participantes podem hesitar em expor problemas ou críticas, ou mesmo terem suas respostas influenciadas por preferências ou aversões pessoais.

Com o objetivo de mitigar possíveis problemas relacionados a vieses e subjetividade nas respostas, mesmo com a amostragem determinada, foi dada especial atenção à interpretação dos resultados, observando-se os potenciais valiosos insights que podem apontar melhorias mais alinhadas às necessidades locais e, conseqüentemente, melhorar a geração de valor institucional do MPF, conduzindo indiretamente a instituição a uma atuação mais efetiva em suas diversas localidades.

A análise dos dados qualitativos, provenientes da questão aberta, foi realizada por meio de análise de conteúdo na qual os dados coletados foram submetidos a um processo envolvendo análises em grupos temáticos, em que, com auxílio de recursos de inteligência artificial (IA), foram extraídos pontos relevantes das várias observações realizadas pelos respondentes. Essa categorização possibilitou a identificação e a compreensão das percepções dos usuários, associadas aos aspectos dos serviços de TIC prestados nas unidades descentralizadas.

Quanto ao uso de recursos de inteligência artificial, com o intuito de resguardar a privacidade dos dados, bem como em obediência a orientações internas da instituição (MPF), foi utilizada a IA Google Gemini 2.5, apenas como ferramenta de apoio no processo de análise da pergunta aberta, de modo a facilitar a interpretação das 84 respostas subjetivas recebidas. Ressalte-se ainda que, em observância à

privacidade dos participantes da pesquisa, não foi coletada nenhuma informação que possa identificá-los.

4 Construção do instrumento de levantamento de dados/survey

Para a formulação das perguntas do questionário, tendo como objetivo impulsionar a geração de valor para a instituição MPF, foram listados os objetivos estratégicos do MPF juntamente com os seus indicadores estratégicos, relacionando-os aos objetivos corporativos genéricos do COBIT 5. A partir dos atuais sete objetivos e trinta indicadores estratégicos do MPF, verificou-se que, destes, apenas dois objetivos e cinco indicadores relacionam-se diretamente com as atividades finalísticas das unidades descentralizadas (PRMs) do MPF (Quadro 3).

Quadro 3 – Objetivos estratégicos do MPF e objetivos corporativos genéricos do COBIT 5

Perspectivas da estratégia do MPF	Objetivos Estratégicos do MPF	Indicadores Estratégicos do MPF	Objetivos corporativos do COBIT correlacionados:
Sociedade	Apresentar resultados transparentes para a sociedade em linguagem acessível	Ind04 Índice de satisfação do cidadão - SAC	6. Cultura de serviço orientada ao cliente 7. Continuidade e disponibilidade do serviço de negócio
	Contribuir para a pacificação de conflitos e priorizar a atuação resolutiva	Ind05 Taxa de remanescentes - Cível - Tutela - 1ª instância	8. Respostas rápidas para um ambiente de negócios em mudança
		Ind07 Taxa de remanescentes - Criminal - 1ª Instância	
		Ind09 Tempo mediano de permanência - Cível - Tutela 1ª Instância	
		Ind11 Tempo mediano de permanência - Criminal - 1ª Instância	

Fonte: adaptado pelos autores a partir de trecho da lista de objetivos do Planejamento Estratégico do Ministério Público Federal para o período de 2024 a 2027 (Brasil, 2024).

Os cinco objetivos estratégicos selecionados foram correlacionados a três objetivos corporativos do COBIT: “6. Cultura de serviço orientada ao cliente”, “7. Continuidade e disponibilidade do serviço de negócio” e “8. Respostas rápidas para um ambiente de negócios em mudança”. A partir do conceito de cascata de objetivos do COBIT 5, e utilizando-se o mapeamento dos objetivos corporativos do COBIT 5 em objetivos de TI da Figura 3, pode-se chegar aos objetivos de TI do COBIT 5 que precisam ser trabalhados.

Portanto, seguindo a metodologia do COBIT, a última coluna do Quadro 3 (objetivos corporativos) relaciona-se com os objetivos de TI, conforme a Figura 3.

Figura 3 – Mapeamento dos objetivos corporativos do COBIT 5 em objetivos de TI

		Objetivo Corporativo																	
		Valor dos investimentos em negócio para as partes interessadas																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Objetivo de TI		Financeira				Cliente				Interna				T&C					
Financeira	01	Alinhamento da estratégia de TI e de negócios	P	P	S			P	S	P	P	S	P	S			S	S	
	02	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos			S	P											P		
	03	Compromisso da gerência executiva com a tomada de decisões de TI	P	S	S					S	S		S					S	S
	04	Gestão do risco organizacional de TI				P	S			P	S		P				S	S	
	05	Benefícios obtidos pelo investimento de TI e portfólio de serviços	P	P				S		S		S	S	P		S			S
	06	Transparência dos custos, benefícios e riscos de TI	S		S		P				S	P		P					
Cliente	07	Prestação de serviços de TI em consonância com os requisitos de negócio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adequado de aplicativos, informações e soluções tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidade de TI	S	P	S			S		P			P		S	S		S	P
	10	Segurança da informação, infraestrutura de processamento e aplicativos			P	P			P								P		
	11	Otimização de ativos, recursos e capacidades de TI	P	S						S		P	S	P	S	S			S
	12	Capacitação e apoio dos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	S	P	S			S		S		S	P	S	S	S			S
	13	Entregas de programas fornecendo benefícios, dentro do prazo, orçamento, e atendendo requisitos e padrões de qualidade	P	S	S			S			S		S	S	P				
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão	S	S	S	S			P		P		S						
	15	Conformidade de TI com as políticas internas			S	S											P		
T&C	16	Equipes de TI e de negócios motivadas e qualificadas	S	S	P			S		S						P		P	S
	17	Conhecimento, expertise e iniciativas para a inovação dos negócios	S	P				S		P	S		S		S			S	P
T&C - Treinamento e Crescimento		P: Relacionamento principal entre os objetivos S: Relação secundária entre os objetivos																	

Fonte: adaptado de Isaca (2012).

Considerando apenas o relacionamento primário de objetivos, caracterizados pela letra “P” na Figura 3, tem-se que os objetivos de TI que correspondem aos objetivos corporativos são os de números 1, 4, 7, 9, 10, 14 e 17. É importante discriminar os itens de “objetivos de TI” desejados, pois eles formarão as áreas da tecnologia da informação que precisarão ser trabalhadas para o atingimento dos objetivos institucionais e, com isso, criar valor para a instituição. É também através dos objetivos de TI que são atingidas as métricas dos objetivos de TI e os processos de trabalho do COBIT.

O COBIT 5 traz, ainda, uma matriz com 22 perguntas padronizadas associadas aos 17 objetivos corporativos padronizados e, tomando como referência os objetivos corporativos destacados no Quadro 3 (objetivos corporativos de números 6, 7 e 8), chegou-se a 10 perguntas do COBIT, conforme Quadro 4.

Quadro 4 – Mapeamento das perguntas do COBIT em relação aos objetivos corporativos

Perguntas do COBIT 5 associadas aos objetivos corporativos	Objetivos Corporativos do COBIT 5		
	6. Cultura de serviço orientada ao cliente	7. Continuidade e disponibilidade do serviço de negócio	8. Respostas rápidas para um ambiente de negócios em mudança
Como faço para obter valor com o uso de TI? Os usuários finais estão satisfeitos com a qualidade do serviço de TI?			
Como posso explorar melhor as novas tecnologias para novas oportunidades estratégicas?			
Como faço para criar e estruturar da melhor forma o meu departamento de TI?			
Todos os riscos de TI foram considerados?			
Estou conduzindo uma resiliente e eficiente operação de TI?			
As informações que estou processando estão bem protegidas?			
Como posso melhorar a agilidade dos negócios com um ambiente de TI mais flexível?			
Os projetos de TI falham em entregar o que prometeram – e caso afirmativo, por quê? TI está atrapalhando a execução da estratégia de negócios?			
Quão crítica é a TI para a sustentação da organização? O que fazer se ela não estiver disponível?			
Quanto tempo é necessário para a tomada de decisões importantes de TI?			

Fonte: adaptado de Isaca (2012).

Portanto, apenas considerando o indicador estratégico do MPF “Ind04 – Índice de satisfação do cidadão – SAC”, já seria possível chegar a alguns questionamentos trazidos pelo próprio COBIT 5, sendo que a primeira pergunta – “Como faço para obter valor com o uso de TI? Os usuários finais estão satisfeitos com a qualidade do serviço de TI?” – já nos dá uma direção dos questionamentos necessários.

É importante mencionar que, assim como informado pelo próprio COBIT, a cascata de objetivos não contém a verdade universal, não devendo ser utilizada de maneira puramente mecânica, mas sim como uma diretriz, pois sua metodologia abrange variados tipos de organizações, de portes e setores variados e que têm prioridades diferentes em seus objetivos, podendo essas prioridades, inclusive, mudar com o tempo. Portanto, a cascata de objetivos deve ser utilizada como um arcabouço que pode auxiliar a encontrar as respostas e os caminhos necessários para que os objetivos institucionais sejam satisfeitos.

5 Análise das respostas

A pesquisa foi aplicada no período de 08/09/2025 a 25/09/2025 e, dos 2.265 formulários enviados, foram recebidas 169 respostas, o que corresponde a 7,5% da amostra selecionada.

A primeira pergunta realizada – “1. Em qual unidade da Federação sua unidade municipal (PRM) está localizada?” – foi necessária para que fosse possível delimitar as respostas em termos geográficos, tanto por estados quanto por regiões. Os estados do Acre, Amapá, Espírito Santo, Roraima e Sergipe não participaram da amostra por não terem PRMs em suas estruturas administrativas. A PRM-Araguaína, em Tocantins, com 9 servidores selecionados para a amostra, não teve nenhuma resposta ao questionário.

Tabela 1 – Questionários enviados por estado e modalidade de trabalho

Estado	Questionários enviados	Questionários respondidos (qtd)	Questionários respondidos (%)	Modalidade de trabalho				
				Presencial em uma PRM	Teletrabalho	Híbrido	Presencial em uma PR	Sem resposta
Sem resposta	0	1	-	0	1	0	0	0
Alagoas	22	2	9,1%	2	0	0	0	0
Amazonas	10	2	20,0%	2	0	0	0	0
Bahia	115	6	5,2%	5	1	0	0	0
Ceará	34	3	8,8%	2	0	0	1	0
Goiás	27	3	11,1%	1	0	2	0	0
Maranhão	37	2	5,4%	2	0	0	0	0
Mato Grosso	43	6	14,0%	5	0	1	0	0
Mato Grosso do Sul	64	7	10,9%	4	1	2	0	0
Minas Gerais	189	11	5,8%	6	3	2	0	0
Pará	70	4	5,7%	3	1	0	0	0
Paraíba	41	4	9,8%	2	2	0	0	0
Paraná	236	14	5,9%	11	3	0	0	0
Pernambuco	65	7	10,8%	1	5	1	0	0
Piauí	22	2	9,1%	1	1	0	0	0
Rio de Janeiro	231	22	9,5%	8	9	5	0	0
Rio Grande do Norte	19	3	15,8%	1	2	0	0	0
Rio Grande do Sul	265	17	6,4%	12	4	1	0	0
Rondônia	15	1	6,7%	0	0	1	0	0
Santa Catarina	193	17	8,8%	15	2	0	0	0
São Paulo	558	35	6,3%	13	12	8	1	1
Tocantins	9	0	0,0%	0	0	0	0	0
Totais:	2265	169	7,5%	96	47	23	2	1

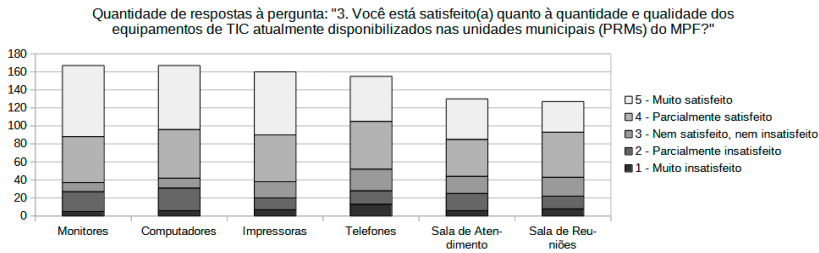
Fonte: elaborado pelos autores com base nos dados de pesquisa coletados por meio do survey.

A Tabela 1 traz os quantitativos gerais dos formulários enviados, formulários respondidos e o percentual de respostas, assim como os resultados da segunda pergunta – “2. Em qual modalidade de trabalho você costuma atuar?”.

Ainda de acordo com a Tabela 1, percebe-se grande variedade na quantidade de pessoal alocado nos estados. Isso ocorre, principalmente, devido ao número de unidades municipais, pois alguns estados têm muitas PRMs enquanto outros têm poucas, havendo também estados com apenas uma ou nenhuma unidade descentralizada. A modalidade de trabalho predominante é a presencial em uma PRM, apontada por 56,8 % (N=96) dos formulários recebidos.

A terceira pergunta aplicada foi do tipo matriz, o que possibilitou coletar as percepções dos usuários a respeito de vários tipos de equipamentos disponibilizados pela TIC nessas localidades (Gráfico 1).

Gráfico 1 – Satisfação dos usuários em relação aos equipamentos disponibilizados



Fonte: elaborado pelos autores.

Em tese, o Gráfico 1 deveria apresentar a mesma altura para todas as colunas, o que seria equivalente a 169 respostas, porém houve um alto índice de respostas “não se aplica” para o item “Sala de atendimento”, com 38 respostas (22,6%), das quais os estados de São Paulo, Rio de Janeiro e Santa Catarina representaram 26,3% (N=10), 21,1% (N=8) e 13,2% (N=5), respectivamente. O mesmo ocorreu com o item “Sala de reuniões”, com 41 (24,3%) respostas “não se aplica”, com liderança dos estados de Rio de Janeiro (26,8%, N=11), São Paulo (24,4%, N=10), Santa Catarina e Rio Grande do Sul (ambos com 9,8%, N=4).

Uma sala de atendimento ao cidadão funcional deve dispor, pelo menos, de um computador e um aparelho telefônico, enquanto uma sala de reuniões, que pode ser utilizada também para a realização de audiências e videoconferências, deve ter à disposição um projetor de vídeo e um computador de mesa ou portátil. Considerando que essa resposta não era obrigatória, sendo possível ter sido deixada em branco, pode-se inferir, entre outras possibilidades, que o volume de respostas “não se aplica” possa significar que esses recursos não estejam disponíveis nessas localidades.

A Tabela 2 lista as médias e o desvio padrão por estado e por região para as notas dos itens referentes aos equipamentos instalados nas unidades.

Tabela 2 – Notas médias e desvio padrão para equipamentos instalados (máx.=5)

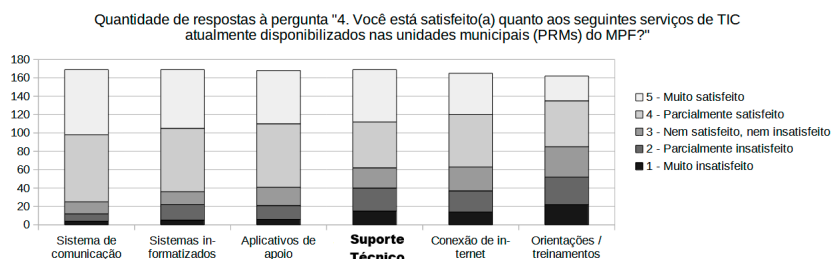
Avaliações por estado (UF)	Computadores		Telefones		Monitores		Impressoras / scanners		Sala de Atendimento ao Cidadão		Sala de Reuniões		Agrupamento dos Equipamentos	
	Média	Desvio Padrão	Média	Desvio Padrão	Média	Desvio Padrão	Média	Desvio Padrão	Média	Desvio Padrão	Média	Desvio Padrão	Média	Desvio Padrão
Goiás - GO	4,7	0,6	4,3	1,2	5,0	0,0	4,0	1,7	4,3	1,2	4,3	1,2	4,4	1,0
Mato Grosso - MT	4,0	1,1	4,0	1,4	3,5	1,5	4,0	1,0	3,6	1,5	3,5	0,8	3,8	1,2
Mato Grosso do Sul - MS	3,9	1,5	4,4	0,8	4,0	1,4	4,4	1,0	3,7	1,4	3,7	1,5	4,0	1,2
Alagoas - AL	4,0	0,0	3,0	0,0	3,0	1,4	2,5	0,7	3,0	0,0	3,0	0,0	3,1	0,7
Bahia - BA	4,5	0,5	4,4	0,5	3,5	1,6	3,6	0,9	3,8	1,1	4,3	0,5	4,0	1,0
Ceará - CE	4,5	0,7	5,0	0,0	5,0	0,0	4,5	0,7	4,0	1,4	4,5	0,7	4,6	0,7
Maranhão - MA	2,5	0,7	2,0	0,0	3,5	2,1	4,5	0,7	4,0	0,0	2,5	2,1	3,2	1,3
Paraíba - PB	3,5	1,9	3,7	2,3	4,0	2,0	3,5	1,9	3,0	2,8	3,0	2,8	3,5	1,9
Pernambuco - PE	4,1	1,5	4,3	0,8	4,1	1,5	4,4	0,8	4,3	1,0	4,2	0,8	4,2	1,0
Piauí - PI	3,5	2,1	3,0	2,8	3,5	0,7	4,5	0,7	5,0	0,0	3,5	0,7	3,8	1,3
Rio Grande do Norte - RN	3,0	1,7	3,7	0,6	3,3	1,5	4,0	1,0	3,3	1,2	3,0	1,7	3,4	1,2
Amazonas - AM	3,0	1,4	3,0	1,4	3,0	1,4	4,5	0,7	2,0		2,0	0,0	3,0	1,2
Pará - PA	3,3	2,1	4,0	1,0	3,8	1,9	4,8	0,5	4,0	1,4	3,5	1,7	3,9	1,5
Rondônia - RO	4,0		4,0		4,0		4,0		4,0		4,0		4,0	0,0
Minas Gerais - MG	3,0	1,3	3,3	1,2	3,8	1,3	3,6	1,3	3,1	1,6	3,0	1,6	3,3	1,4
Rio de Janeiro - RJ	4,1	1,2	3,5	1,3	4,1	1,1	3,9	1,2	3,6	1,3	2,9	1,4	3,8	1,3
São Paulo - SP	4,2	1,0	3,6	1,4	4,3	0,8	3,7	1,3	3,6	1,1	3,8	0,7	3,9	1,1
Paraná - PR	4,1	1,0	3,9	1,2	3,9	1,1	4,5	0,7	4,1	1,0	3,8	0,9	4,1	1,0
Rio Grande do Sul - RS	4,6	0,6	3,7	1,4	4,3	1,2	4,3	1,2	4,1	1,2	4,5	0,9	4,2	1,1
Santa Catarina - SC	3,4	1,2	3,7	1,0	4,2	0,8	4,1	0,9	4,0	1,3	3,8	1,1	3,9	1,1
Centro-Oeste	4,1	1,2	4,3	1,0	4,0	1,4	4,2	1,1	3,8	1,3	3,7	1,2	4,0	1,2
Nordeste	3,9	1,3	3,8	1,3	3,8	1,4	4,0	1,1	3,8	1,1	3,7	1,2	3,8	1,2
Norte	3,3	1,6	3,7	1,0	3,6	1,5	4,6	0,5	3,7	1,4	3,1	1,5	3,7	1,3
Sudeste	4,0	1,2	3,5	1,3	4,1	1,0	3,8	1,3	3,5	1,2	3,5	1,2	3,8	1,2
Sul	4,0	1,1	3,8	1,2	4,2	1,0	4,3	0,9	4,1	1,1	4,1	1,0	4,1	1,1
Brasil	4,0	1,2	3,7	1,2	4,1	1,2	4,0	1,1	3,8	1,2	3,7	1,2	3,9	1,2

Fonte: elaborado pelos autores.

Para o item pesquisado “computadores”, as menores notas dadas pelos usuários foram registradas no estado do Maranhão, com média 2,5. Os estados do Rio Grande do Norte, Amazonas e Minas Gerais receberam dos usuários notas médias 3,0. A região com menores notas nesse quesito foi a Região Norte, com média 3,3.

Em relação aos serviços de TIC disponibilizados nessas unidades, de acordo com o Gráfico 2, o sistema de comunicações, composto por uma solução híbrida que inclui telefonia fixa em nuvem e telefonia via plataforma Zoom, foi muito bem avaliado, com 85% das respostas 4 – Parcialmente satisfeito – ou 5 – Muito satisfeito. Os serviços de suporte técnico, conexão de internet e orientações/treinamentos receberam avaliação 4 ou 5 por, respectivamente, 63,3%, 60,3% e 45,5% das respostas. Para o serviço de suporte técnico, os usuários deram as piores notas para os estados do Piauí (média 1,5), Mato Grosso (média 3,0) e Pernambuco (média 3,1), enquanto o serviço de conexão de internet recebeu as menores notas nos estados do Piauí, Alagoas e Amazonas, todos com média 2,0. O serviço de orientações/treinamentos recebeu menores notas nos estados do Piauí (média 1,5), Rio Grande do Norte (média 1,7) e Alagoas (média 2,0).

Gráfico 2 – Satisfação dos usuários em relação aos serviços disponibilizados nas PRMs



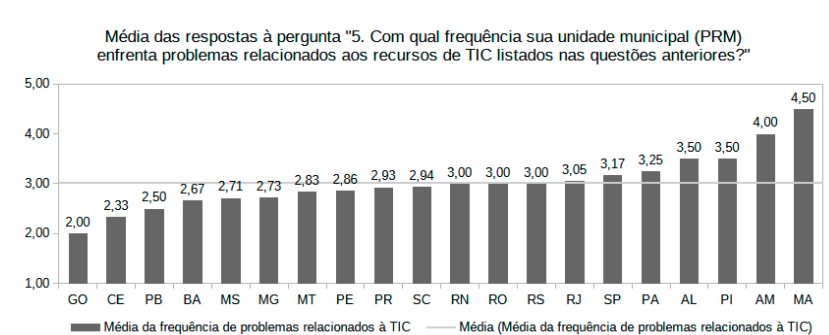
Fonte: elaborado pelos autores.

É importante destacar que as questões 3 e 4 são bem diferentes. A questão 3 avalia os equipamentos que foram instalados nas unidades, disponibilizados pela Coordenadoria de Tecnologia da Informação e Comunicação (CTIC), sediada na capital de seus estados, ao passo que a questão 4 refere-se aos serviços contínuos que chegam àquelas localidades e, na maioria das vezes, são providos nacionalmente.

A quinta pergunta busca avaliar a percepção dos usuários sobre a frequência da ocorrência de problemas relacionados aos recursos de TI apresentados nas questões 3 e 4, em que o número 1 equivale a “nunca” e o número 5 equivale a “muito frequentemente”. Esta pergunta se

refere a ocorrências envolvendo qualquer um dos doze itens, podendo ser equipamento ou serviço. No topo da lista ficaram os estados do Maranhão (4,5), Amazonas (4,0), e Alagoas e Piauí, empatados com avaliação 3,5, o que equivale a “frequentemente”. O Gráfico 3 contempla as notas de todos os estados.

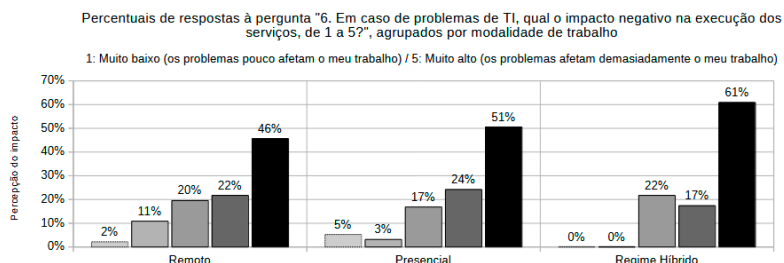
Gráfico 3 – Frequência de problemas envolvendo itens de TIC



Fonte: elaborado pelos autores.

A sexta pergunta aborda o impacto negativo de eventuais problemas envolvendo os recursos de TIC, em que 73,2% das respostas apontaram para impactos do tipo “alto” e “muito alto”. Agrupando-se as respostas por modalidade de trabalho (Gráfico 4), verificou-se que, independentemente da modalidade de trabalho, problemas relacionados aos recursos de TIC afetam sobremaneira a condução dos trabalhos, sendo esse impacto ainda maior para aqueles que trabalham em regime híbrido.

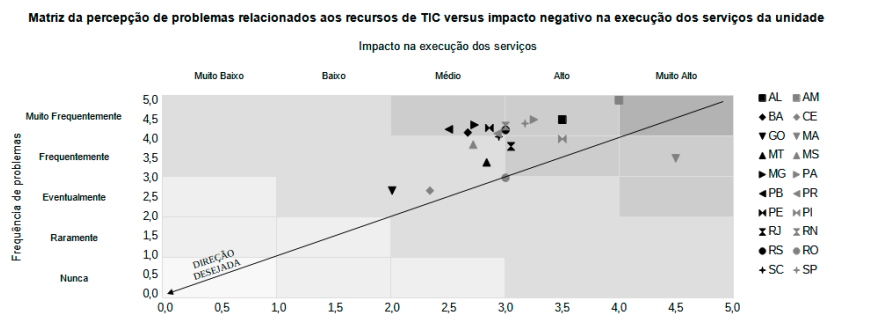
Gráfico 4 – Impacto de problemas envolvendo recursos de TIC



Fonte: elaborado pelos autores.

A partir dos valores coletados nas questões 5 (frequência de problemas) e 6 (impacto negativo dos problemas), foi possível traçar a matriz do Gráfico 5, na qual, de forma análoga a uma matriz de riscos, pode-se avaliar, de forma geral, a percepção dos usuários em relação a problemas de TIC que podem afetar a continuidade das atividades. De acordo com os dados levantados, merecem mais atenção aquelas unidades localizadas nos estados do Amazonas, Alagoas, Maranhão, Pará e Piauí.

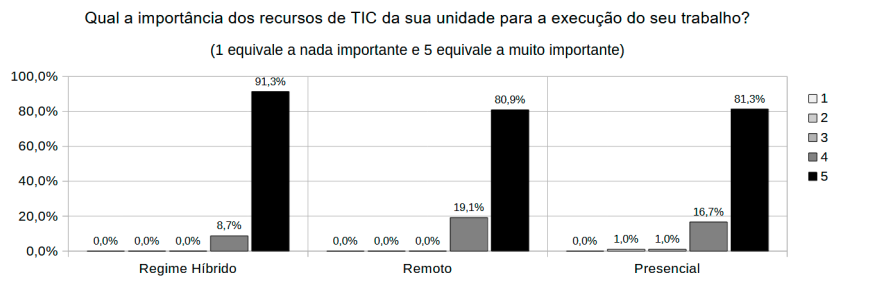
Gráfico 5 – Matriz da percepção do impacto vs. frequência de problemas de TIC



Fonte: elaborado pelos autores.

A sétima pergunta do questionário aborda a importância dos recursos de TIC das unidades descentralizadas. Apesar da resposta aparentar certa obviedade, esse é um questionamento fundamental do COBIT, pois refere-se à criticidade da TI para a continuidade dos negócios. Além do reconhecimento da importância dos recursos de TIC disponibilizados às PRMs, o Gráfico 6 traz essa percepção a partir dos próprios usuários finais, inclusive aqueles em trabalho híbrido ou remoto.

Gráfico 6 – Importância dos recursos de TIC nas unidades



Fonte: elaborado pelos autores.

A oitava pergunta trata dos canais de comunicação utilizados na solicitação de serviços de TIC. Objetivando captar aqueles canais mais utilizados, optou-se por limitar a seleção de até 4 opções como respostas. Conforme demonstrado na Tabela 3, a maioria dos entrevistados (83,9%) abre chamados no Sistema Nacional de Pedidos (SNP), o que é um fator bastante positivo, pois esse é o canal mais adequado para solicitar suporte técnico.

Paralelamente à abertura de chamados no sistema SNP, 46,4% dos usuários afirmaram recorrer a colegas do setor, enquanto 38,7% optam por tentar resolver os problemas sozinhos, em vez de acionarem o suporte técnico. Embora os valores sejam, de certa forma, expressivos, não ficaram claros os motivos prováveis para esse comportamento.

É importante observar que alguns canais disponibilizados estão sendo pouco utilizados, notadamente o MPFBot (5,4%). Outro canal que ficou aquém do esperado, com 7,1%, foi o telefone da Central Nacional de Atendimento (Cenar), que é uma central de atendimento telefônico que resolve alguns problemas e auxilia os usuários a abrir chamados no sistema SNP. A pouca utilização desses canais pode ser um indício de desconhecimento das ferramentas ou da necessidade de evolução do canal, principalmente no caso do MPFBot, por se tratar de uma ferramenta virtual de autoatendimento com recursos de IA. Uma grande vantagem da utilização do chatbot é sua alta disponibilidade, enquanto o atendimento convencional possui limitação do horário do expediente dos atendentes, especialmente num país onde existem vários fusos horários, como é o caso do Brasil.

Tabela 3 – Canais utilizados na solicitação de serviços de TIC

Estado	MPF Bot	Telefone de CENAR	Coordenador de TIC	Técnico de TIC na PR	Técnico de TIC na PRM	Resolver Sozinho	Colegas do setor	Sistema SNP
Alagoas	0,0%	0,0%	0,0%	0,0%	100,0%	0,0%	50,0%	100,0%
Piauí	0,0%	0,0%	0,0%	50,0%	0,0%	0,0%	50,0%	100,0%
Rondônia	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Paraíba	0,0%	0,0%	50,0%	50,0%	25,0%	25,0%	100,0%	100,0%
Minas Gerais	0,0%	0,0%	9,1%	63,6%	18,2%	36,4%	0,0%	100,0%
Amazonas	0,0%	0,0%	50,0%	0,0%	0,0%	50,0%	50,0%	100,0%
Maranhão	0,0%	0,0%	0,0%	0,0%	50,0%	50,0%	0,0%	100,0%
Mato Grosso	0,0%	16,7%	33,3%	50,0%	16,7%	50,0%	16,7%	100,0%
Rio Grande do Norte	0,0%	0,0%	33,3%	33,3%	66,7%	100,0%	33,3%	100,0%
Pernambuco	14,3%	0,0%	0,0%	14,3%	42,9%	21,4%	42,9%	92,9%
Rio de Janeiro	0,0%	4,5%	0,0%	18,2%	54,5%	36,4%	50,0%	86,4%
Pernambuco	14,3%	42,9%	0,0%	14,3%	28,6%	42,9%	85,7%	85,7%
Mato Grosso do Sul	0,0%	0,0%	14,3%	28,6%	14,3%	85,7%	71,4%	85,7%
Bahia	0,0%	0,0%	33,3%	50,0%	16,7%	33,3%	50,0%	83,3%
Santa Catarina	5,9%	11,8%	0,0%	17,6%	70,6%	29,4%	58,8%	82,4%
Pará	0,0%	0,0%	0,0%	75,0%	50,0%	25,0%	50,0%	75,0%
São Paulo	11,4%	14,3%	0,0%	14,3%	40,0%	48,6%	48,6%	74,3%
Rio Grande do Sul	5,9%	0,0%	17,6%	47,1%	35,3%	52,9%	70,6%	70,6%
Goiás	0,0%	0,0%	33,3%	66,7%	0,0%	0,0%	33,3%	66,7%
Ceará	0,0%	0,0%	33,3%	33,3%	0,0%	66,7%	66,7%	66,7%
Totalizadores:	5,4%	7,1%	8,9%	25,0%	39,3%	38,7%	46,4%	83,9%

Fonte: elaborada pelos autores.

A penúltima pergunta, de n. 9, busca conhecer os meios pelos quais os usuários fornecem feedback para a administração. Os resultados listados na Tabela 4 mostram que grande parte dos usuários, 58,3%, opta por fornecer feedback mediante avaliação dos atendimentos de TIC por meio do SNP. No sentido inverso, 27,4% afirmaram não fornecer nenhum tipo de feedback. É importante destacar que o feedback tratado nesta pergunta não se restringe às avaliações dos atendimentos recebidos, procurando também abranger comunicações direcionadas aos gestores administrativos e de TIC. Contudo, poucos respondentes afirmaram fornecer feedback por esses meios.

Tabela 4 – Respostas à pergunta: “Quais tipos de feedback você ou sua PRM costumam fornecer em relação aos serviços e/ou necessidades de TIC?”

Estado	Avalia chamados abertos no SNP	Comunicação à CTIC de seu estado	Comunicação ao Procurador-Chefe do seu estado	Comunicação ao Secret. de TIC ou Secret. Geral	Fornecer feedback informal para o atendente	Não fornece feedback
Amazonas	100,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Mato Grosso do Sul	85,7%	0,0%	0,0%	0,0%	42,9%	14,3%
Paraíba	75,0%	25,0%	0,0%	0,0%	50,0%	25,0%
Pernambuco	71,4%	0,0%	0,0%	0,0%	42,9%	14,3%
São Paulo	68,6%	2,9%	0,0%	0,0%	45,7%	14,3%
Goiás	66,7%	0,0%	33,3%	0,0%	33,3%	0,0%
Mato Grosso	66,7%	0,0%	0,0%	0,0%	33,3%	16,7%
Rio Grande do Sul	58,8%	5,9%	0,0%	0,0%	5,9%	29,4%
Santa Catarina	58,8%	0,0%	0,0%	0,0%	11,8%	35,3%
Paraná	57,1%	21,4%	0,0%	0,0%	28,6%	21,4%
Rio de Janeiro	54,5%	4,5%	0,0%	0,0%	36,4%	40,9%
Piauí	50,0%	0,0%	0,0%	0,0%	50,0%	0,0%
Pará	50,0%	0,0%	0,0%	0,0%	0,0%	50,0%
Minas Gerais	45,5%	0,0%	9,1%	0,0%	27,3%	27,3%
Rio Grande do Norte	33,3%	33,3%	0,0%	0,0%	66,7%	33,3%
Ceará	33,3%	33,3%	0,0%	0,0%	66,7%	33,3%
Bahia	33,3%	33,3%	0,0%	0,0%	16,7%	50,0%
Alagoas	0,0%	50,0%	0,0%	0,0%	100,0%	50,0%
Rorônia	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Maranhão	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%
Totalizadores:	58,3%	7,1%	1,2%	0,0%	31,5%	27,4%

Fonte: elaborada pelos autores.

Por fim, a décima pergunta do questionário, do tipo aberta, possibilitou aos entrevistados acrescentarem informações não abordadas nas questões objetivas. Foram analisados os principais pontos trazidos pelos respondentes, incluindo críticas e elogios.

Em todas as regiões, houve relatos de equipamentos, sobretudo computadores e monitores, defasados, fora de garantia, com necessidades constantes de manutenção ou em quantidades insuficientes. Embora alguns respondentes tenham avaliado esses itens com notas boas, tecendo-lhes elogios pela qualidade, também foram recebidas várias respostas com comentários recorrentes sobre a necessidade de

mais monitores auxiliares e mais computadores no setor, indicando possivelmente a existência de equipamentos parados em decorrência de falta de suporte. Percebe-se pelas respostas uma certa contradição; porém, na prática diária das atividades de suporte, de forma empírica, constata-se em algumas unidades um desequilíbrio interno em relação à distribuição de equipamentos, visto que há setores com equipamentos melhores e em maior quantidade em relação a outros setores.

A falta de técnicos de TI nas unidades foi outra queixa recorrente, pois algumas unidades, principalmente nas Regiões Norte e Nordeste, não possuem esse tipo de profissional em seus quadros, enquanto aquelas que dispunham de técnicos, especialmente nas Regiões Sul e Sudeste, perderam a exclusividade dos seus serviços em virtude da realocação de pessoal para serviços nacionais, como a central de atendimento (Cenar), desenvolvimento de software ou serviços de infraestrutura e segurança de TI.

O serviço de suporte nacional recebeu bastantes comentários, inclusive positivos, nos quais algumas respostas apontaram a qualificação, a paciência e a rapidez dos técnicos de atendimento, demonstrando um reconhecimento dos pesquisados aos servidores de TIC do MPF, inclusive com elogios nominalmente realizados. Contudo, foram recebidas muitas críticas ao modelo de atendimento remoto devido: I) à centralização dos atendimentos de TIC; II) ao desconhecimento das realidades e necessidades locais e, principalmente; III) à impossibilidade de atender aos casos em que haja a necessidade de intervenção presencial, levando os usuários a percepções de insegurança, fadiga e desamparo. Os usuários reclamam por precisarem interromper suas atividades para fazer manobras de cabos de rede ou elétricos, tarefas entendidas como exclusivas dos profissionais de TIC.

Alguns sistemas, como o Único (solução do MPF para a gestão de documentos, procedimentos administrativos e extrajudiciais e processos judiciais) e o Kairós (sistema de controle de jornada), receberam várias críticas. Porém, o sistema de abertura de chamados, denominado Sistema Nacional de Pedidos (SNP), em virtude do foco da pesquisa, recebeu destaque especial, pois, enquanto alguns usuários relataram boas experiências, outros reclamaram de dificuldades para abrir e acompanhar os chamados técnicos, referindo-se ao sistema como “confuso” e “não intuitivo”.

O link de internet das PRMs foi considerado, em geral, lento e instável, fato compatível com as respostas apresentadas no Gráfico 2. Houve comentários sobre a falta de redundância no link de internet e falta de rede Wi-Fi em algumas unidades, fatos não levantados nas perguntas objetivas, embora também sejam recursos importantes, especialmente nas localidades mais distantes. Os usuários pediram ainda a realização de treinamentos que possam auxiliá-los a melhorar o uso dos sistemas e demais recursos de TIC disponibilizados.

A solução de telefonia foi alvo de reclamações, tendo alguns usuários apontado falhas e má qualidade das chamadas via Zoom e dos aparelhos, os quais receberam críticas em virtude de a quantidade instalada ser supostamente insuficiente. Também houve comentários a respeito da falta de fones de ouvido nas unidades, porém, a partir das respostas, não ficou claro se a percepção de má qualidade das chamadas seria devido à falta de distribuição desse item.

6 Considerações finais

Em primeiro lugar, é importante ressaltar a importância do feedback como parte integrante do monitoramento na governança de TI. Assim como destacado na Figura 1, governança inclui avaliar, dirigir e monitorar, sendo esta última parte essencial à retroalimentação do ciclo da governança. No MPF, o monitoramento é realizado por diversos meios, incluindo recursos de *Business Intelligence* (BI), *Data Warehouse*, Ciência de Dados etc., sendo o feedback do usuário apenas mais um componente a somar-se a tantos outros em uso pelo MPF. Todavia, indicadores estratégicos do MPF, como “Ind04 Índice de satisfação do cidadão – SAC”, bem como os indicadores 5, 7, 9 e 11, referentes às taxas de processos remanescentes e ao tempo mediano de permanência de processos, sofrem influência direta dos recursos de TIC disponibilizados às unidades descentralizadas, justificando a importância do feedback desses usuários.

Pelas respostas recebidas, percebe-se que nas unidades descentralizadas há uma grande variação na forma como são entregues os serviços de TIC, pois algumas PRMs são maiores e têm mais usuários e maior quantidade de equipamentos, enquanto outras têm menos recursos à sua disposição, impactando negativamente na satisfação do usuário e na prestação de serviços ao cidadão.

A primeira hipótese levantada (“O fornecimento das soluções de TIC nas diferentes localidades não é suficientemente regular e eficaz, considerando os fatores distância e recursos pessoais e materiais, impactando negativamente na geração de valor institucional”) mostrou-se parcialmente verdadeira, pois o fator distância não teve peso significativo. Contudo, observou-se que, como as PRMs estão subordinadas administrativamente às Procuradorias da República nas capitais, a gestão de TIC dessas unidades cabe às CTICs daqueles estados, vindo estas a confirmarem-se como fundamentais à aplicação da governança de TIC nas unidades descentralizadas. A título de exemplo, mesmo em estados considerados mais abastados ou mais bem localizados geograficamente, existem PRMs sem rede Wi-Fi ou mesmo sala de atendimento ao cidadão, itens considerados básicos. Outro ponto que mereceu atenção foi a falta de itens simples e baratos, como mouses e fones de ouvido. Portanto, confirmou-se a existência de gargalos que dificultaram a correta aplicação das ações de governança e gestão de TIC.

A segunda hipótese (“Em virtude da falta de orientação técnica, há ineficiência no uso dos recursos disponíveis”) se mostrou verdadeira, tendo os respondentes avaliado este item tanto na questão de n. 4 (Gráfico 2) quanto na questão aberta. No grupo de serviços de TIC avaliados na pergunta 4, o quesito “orientações/treinamentos” recebeu as piores notas, tendo destaque os estados do Pará (2,3), Alagoas (2,0), Rio Grande do Norte (1,7) e Piauí (1,5).

A terceira hipótese (“A comunicação nas localidades remotas é ineficiente”) mostrou-se parcialmente verdadeira, mas sem relação direta com o sistema de comunicação em si, pois este serviço obteve mais notas boas dentro do grupo de serviços. Contudo, também recebeu comentários negativos na pergunta aberta, inclusive atrelados a fatores adjacentes, como fones de ouvido ou aparelhos telefônicos. Ressalte-se, todavia, que a qualidade do áudio também sofre interferência direta da conexão de internet.

Portanto, com vistas a uma melhor geração de valor institucional, e em resposta à questão de investigação (“Como a infraestrutura e os serviços de TIC do MPF podem ser otimizados nas diferentes localidades?”), este artigo vem desvendar possíveis gargalos na infraestrutura de TIC nas unidades descentralizadas e propor melhorias alinhadas às demandas locais e aos objetivos estratégicos do MPF.

Tendo por base as respostas obtidas a partir do questionário enviado, é possível citar os seguintes possíveis gargalos: I) necessidade de suporte presencial – foi perceptível a necessidade de várias unidades em relação ao suporte presencial de TIC; II) aperfeiçoamento do sistema SNP – mesmo tendo recebido críticas, percebeu-se que o sistema SNP está bastante consolidado, sendo utilizado por 83,9% dos respondentes, mostrando-se, portanto, a modalidade de abertura de chamados a ser incentivada e continuamente aperfeiçoada; III) falta de acessórios básicos como fones de ouvido; IV) falta de treinamento e/ou orientações aos usuários; e V) problemas na conexão de internet.

Como propostas de melhoria, de forma a contornar e mitigar as lacunas encontradas, é possível citar: I) definição de parâmetros mínimos de qualidade, definidos nacionalmente, de modo a estabelecer critérios técnicos a serem observados pelas CTICs nos estados; II) definição de periodicidade para visitas técnicas às PRMs que não possuem profissional de TIC em seus quadros; III) melhorias no MPFBot – este recurso precisa ser aprimorado continuamente para que os usuários consigam recorrer a essa ferramenta na resolução de problemas mais triviais. Além disso, a ferramenta precisa de treinamento e um maior apoio de IA, de modo que possa sugerir soluções precisas e mais simples para os usuários e, com isso, evitar que os agentes do chatbot sejam meros cadastradores de chamados para os atendentes humanos – e, na impossibilidade de tal correção, considerar a extinção da ferramenta; IV) reavaliação dos parâmetros de qualidade dos links de internet contratados e, se possível, contratação de links de contingência pelo menos para as unidades onde o sinal chega com maior instabilidade.

Dada sua importância, o sistema SNP merece atenção especial, sendo sugeridas as seguintes melhorias: I) construção de uma interface simplificada de abertura de chamados – tendo em vista a existência de uma central de atendimento, torna-se viável o uso de uma interface simplificada, onde o usuário apenas descreve a sua demanda, deixando a categorização a cargo dos agentes de triagem, pois vários usuários relataram dificuldade para selecionar o serviço desejado mais adequado; e II) alteração no sistema de avaliação dos chamados, adotando-se telas sem campos pré-preenchidos e com escalas de Likert de 5 pontos para os quesitos tempo de resolução, qualidade da solução e qualidade de atendimento, bem como restrição da visibilidade da avaliação às chefias para que o solicitante tenha uma maior liberdade para avaliar os chamados.

Ainda sobre o sistema SNP, faz-se necessário que seja utilizado pela totalidade dos clientes de TIC, pois, além da gestão dos atendimentos, seu uso gera dados imprescindíveis para o monitoramento das demandas. Nesse sentido, recomenda-se a edição de normativos e a realização de campanhas educativas com o objetivo de fomentar sua utilização, destacando também a importância da avaliação dos chamados atendidos.

Outra recomendação necessária é a realização de pesquisa para aferir a satisfação dos clientes de TIC das demais unidades do MPF, especialmente se direcionada ao cargo de procurador da República, público não abrangido pelo presente estudo. Com dados mais amplos, é possível realizar análises mais confiáveis e precisas, bem como levantar informações relevantes ao aprimoramento da governança de TIC que, em menor ou maior grau, possam contribuir para uma maior geração de valor para o MPF e a sociedade como um todo.

Devido ao baixo retorno amostral (7,5%), os resultados coletados nesta pesquisa não podem ser extrapolados estatisticamente, podendo não ser totalmente generalizáveis para todas as unidades do MPF, especialmente para os estados que não foram contemplados na amostra por não possuírem PRMs. Desse modo, é possível que os achados sejam mais aplicáveis às unidades descentralizadas (PRMs). Todavia, mesmo com uma baixa taxa de retorno, os dados obtidos mostram indícios que não devem ser desprezados, especialmente se indicam riscos em relação à continuidade e disponibilidade do serviço e do negócio ou da geração de valor institucional.

Tendo em vista que os recursos de TIC disponibilizados às PRMs passam pelas Coordenadorias de TIC nas capitais, e estas atuam como agentes da gestão de TIC, espera-se que uma maior proximidade das CTICs com a alta administração venha a produzir resultados profícuos e valiosos para a instituição, evitando, portanto, que as CTICs locais venham a representar gargalos adicionais para a governança. Para isso, tendo em vista o caráter transformador da educação, sugere-se a realização de palestras e treinamentos específicos para esse público, inclusive sobre temas afeitos à governança de TIC, bem como o estabelecimento de um canal de comunicação direto e contínuo, de modo que as Coordenadorias de Tecnologia da Informação e Comunicação existentes hoje nas capitais dos estados sintam-se e sejam parte da governança de TIC da instituição.

Finalmente, com as considerações aqui trazidas, acredita-se que o presente artigo atingiu o seu objetivo de “analisar a percepção de qualidade da oferta de serviços e equipamentos de TIC nas unidades descentralizadas do MPF sob a perspectiva do usuário final, com vistas à geração de valor institucional”. É importante ressaltar que esta pesquisa não constitui um fim em si, mas um meio de promover a maximização da geração de valor institucional, beneficiando não somente a instituição MPF, mas a sociedade de modo geral.

Referências

AFFELDT, Fabrício Sobrosa; VANTI, Adolfo Alberto. Alinhamento estratégico de tecnologia da informação: análise de modelos e propostas para pesquisas futuras. **Journal of Information Systems and Technology Management**, São Paulo, v. 6, n. 2, p. 203-226, 2009. DOI: <https://doi.org/10.4301/S1807-17752009000200004>.

ALBERTIN, Alberto Luiz. **Administração de informática: funções e fatores críticos de sucesso**. 6. ed. São Paulo: Atlas, 2009.

ALBERTIN, Alberto Luiz; ALBERTIN, Rosa Maria de Moura. Benefícios do uso de tecnologia de informação para o desempenho empresarial. **Revista de Administração Pública**, Rio de Janeiro, v. 42, n. 2, p. 275-302, 2008.

BALBINOT, Jeysonn Isaac; ARAÚJO, Cleber de; LUFT, Renato. Análise dos resultados estratégicos de tecnologia da informação e comunicação no Ministério Público Federal decorrentes do projeto de modernização da gestão administrativa no período 2011-2020. **Brazilian Journal of Development**, Curitiba, v. 7, n. 12, p. 111034-111052, 29 dec. 2021. DOI: <https://doi.org/10.34117/bjdv7n12-063>.

BRASIL. Decreto n. 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF: **Diário Oficial da União**, 23 nov. 2017.

BRASIL. Lei Complementar n. 75, de 20 de maio de 1993. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União. Brasília, DF: **Diário Oficial da União**, 21 maio 1993.

BRASIL. Ministério Público Federal. Portaria PGR/MPF n. 843, de 18 de outubro de 2024. Atualiza o Planejamento Estratégico do Ministério

Público Federal para o período de 2024 a 2027. **Diário do Ministério Público Federal Eletrônico**, Brasília, n. 208, 30 out. 2024.

BRASIL. Tribunal de Contas da União. **Acórdão 2.308/2010-Plenário**. Relator: Aroldo Cedraz. Brasília, DF: Portal TCU, 8 set. 2010. Disponível em: <https://tinyurl.com/3kbjua2p>. Acesso em: 15 out. 2025.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança organizacional**: para organizações públicas e outros entes jurisdicionados ao TCU. 3. ed. Brasília: TCU, Secretaria de Controle Externo da Administração do Estado - SecexAdministração, 2020. 242p.

DRUCKER, Peter F. **O melhor de Peter Drucker**: a administração. São Paulo: Nobel, 2001.

IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015.

ISACA – INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT 5**: modelo corporativo para governança e gestão de TI da organização. Rolling Meadows, IL: ISACA, 2012.

MENDONÇA, Cláudio Márcio Campos de; GUERRA, Lenin Cavalcanti Brito; SOUZA NETO, Manoel Veras de; ARAÚJO, Afrânio Galdino de. Governança de tecnologia da informação: um estudo do processo decisório em organizações públicas e privadas. **Revista de Administração Pública**, Rio de Janeiro, v. 47, n. 2, p. 443-468, abr. 2013. DOI: <https://doi.org/10.1590/S0034-76122013000200008>.

REZENDE, José Francisco de Carvalho; LOUREIRO; José Fiel Faria; RODRIGUES, Pierre Teixeira; MORAES, João Guilherme Calvão. Transformação digital e as métricas de valor de tecnologia da informação sob a perspectiva da teoria neo-institucional. **Journal of Information Systems and Technology Management**, São Paulo, v. 21, out. 2024. DOI: <https://doi.org/10.4301/S1807-177520242100>.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. São Paulo: Cortez, 2013.

WEILL, Peter; ROSS, Jeanne W. **Governança de TI**: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores. São Paulo: Makron Books, 2006.

Avaliação da maturidade digital do Ministério Público Federal: cenário atual e estratégias para potencializar a transformação digital¹

Assessing digital maturity in the Federal Prosecution Service: current scenario and transformation strategies

DOI: https://doi.org/10.63601/978-65-88299-52-4_7

George Antônio Ferreira de Araújo

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Bacharel em Ciência da Computação pelo Instituto Federal de Brasília (IFB). Software Engineer na Solutis Tecnologias. Servidor do Ministério Público Federal (MPF).

Sílvio Simplicio Pinheiro

Mestre em Gestão Pública pela Universidade Federal do Espírito Santo (UFES). Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista na área de gestão, educação e Tecnologia da Informação pelo Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo (IFES). Graduado em Tecnologia em Processos Gerenciais. Servidor do Ministério Público do Trabalho (MPT).

Thiago Russo

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Comunicação e Marketing para Mídias Digitais pela Faculdade Estácio de Sá de Campo Grande. Graduado em Ciência da Computação pela Universidade Anhanguera (Uniderp). Servidor do Ministério Público do Estado de Mato Grosso do Sul (MPMS).

¹ Expressamos nossos sinceros agradecimentos ao Prof. Cleber de Araújo por sua dedicada orientação acadêmica e revisão crítica durante todo o projeto de pesquisa e a elaboração deste trabalho.

Resumo: Os avanços tecnológicos, aliados a fatores sociais, econômicos e organizacionais, têm impulsionado a Transformação Digital (TD) em instituições públicas. Contudo, nem sempre a TD ocorre de forma organizada e com o devido acompanhamento. A pesquisa estrutura-se em três etapas: a seleção e aplicação de um Modelo de Maturidade Digital (MMD), para definir o NMD da instituição; a análise dos resultados e a definição da situação atual do MPF; e a proposição de estratégias de governança e gestão para atacar os pontos fracos identificados e potencializar a TD. Obteve-se como resultado a classificação do MPF em uma escala de NMD, com destaque positivo para dimensões de Serviços ao Cidadão, Liderança e Tecnologia, mas com destaques negativos em Estratégia Digital, Pessoas, Governança e Operações. O estudo indicou a ausência de planejamento estratégico para uso das TDs e a necessidade de capacitação e valorização dos servidores de TIC, além da necessidade de adoção de um projeto de governança capaz de responder de forma rápida às mudanças de que a TD necessita.

Palavras-chave: transformação digital; maturidade digital; estratégia digital; gestão pública.

Abstract: *Technological advances drive Digital Transformation (DT) in public institutions, though often without proper monitoring. This study assesses the Digital Maturity Level (DML) of the Brazilian Federal Prosecution Service (MPF) and proposes strategies to guide its digital evolution. A hybrid assessment model was adopted, combining frameworks from the National Council of the Public Prosecution Service (CNMP) and the Ministry of Management and Innovation (MGI). The research followed three stages: applying a Digital Maturity Model (DMM) to define the DML; analyzing the current scenario; and proposing governance strategies to address identified weaknesses. Results classified the MPF as an intermediate DML, with strengths in Citizen Services, Leadership, and Technology, but gaps in Digital Strategy, People, Governance, and Operations. The findings highlight the absence of a strategic plan for DT, the need for IT personnel training and valuation, and the importance of implementing a governance model capable of responding rapidly to the demands of digital transformation.*

Keywords: *digital transformation; digital maturity; digital strategy; public management.*

1 Introdução

A crescente necessidade de otimização da Administração Pública, impulsionada por pressões sociais, econômicas e pela evolução tecnológica acelerada, tem atuado como catalisador para o avanço da digitalização dos serviços públicos, da implementação do Governo Digital e da adoção das ferramentas motrizes da Transformação Digital (TD) (Albuquerque; Costa, 2025; Haug; Dan; Mergel, 2024).

A TD requer mudanças significativas em múltiplos aspectos da organização, incluindo operações, processos, estrutura, gestão e cadeia de suprimentos. Por essa razão, é fundamental avaliar o Nível de Maturidade Digital (NMD) institucional para assegurar que a TD esteja sendo implementada de forma eficaz e sustentável (Santos *et al.*, 2024).

Visto que a maturidade digital proporciona às organizações evoluírem seu processo de TD (Silva; Vieira; Silva, 2024), a aplicação de um Modelo de Maturidade Digital (MMD) e a consequente definição do NMD da instituição permitem compreender seu estágio de organização e de implementação da TD, com o objetivo de gerar entregas mais efetivas sem comprometer a governança, a segurança da informação ou os princípios da gestão pública. Essa avaliação também possibilita identificar desafios e lacunas a serem superados, além de apontar estratégias que possam apoiar esse processo.

O Ministério Público Federal (MPF) é um dos ramos do Ministério Público da União (MPU) e é composto por mais de 200 unidades distribuídas em todo o território brasileiro (Brasil, 2025). Apesar do porte e relevância da instituição, não foram encontradas publicações anteriores que abordam o NMD do MPF de forma individual. Assim, um estudo dessa natureza pode contribuir significativamente para o diagnóstico de sua transformação digital, fornecendo subsídios valiosos ao Planejamento Estratégico Institucional (PEI) e à governança institucional, orientando estratégias e diretrizes que permitam à instituição alcançar níveis mais elevados de maturidade digital.

Esse estudo tem como objetivo avaliar o NMD do MPF e propor estratégias que possam impulsionar seu avanço, acelerando e sustentando a TD da instituição. A pesquisa está estruturada em três etapas principais: (I) aplicação de um MMD para definir o NMD do MPF; (II) análise dos resultados e identificação de pontos de melhoria; e (III) proposição de estratégias de governança e gestão capazes de potencializar a TD. Com base nisso, o estudo busca responder à seguinte questão de pesquisa (QP):

QP. Qual é o Nível de Maturidade Digital do MPF e quais estratégias podem ser adotadas para impulsionar sua Transformação Digital?

A justificativa para esta pesquisa está relacionada à necessidade estratégica do MPF de aprimorar sua capacidade de transformação

digital, especialmente diante das crescentes demandas sociais por serviços públicos digitais, eficientes e seguros. A avaliação do NMD da instituição permite compreender o cenário atual da TD e mapear as mudanças necessárias para potencializá-la.

Assim, este estudo oferece subsídios técnicos e institucionais à alta gestão e às equipes de Tecnologia da Informação e Comunicação (TIC), contribuindo tanto para o avanço do conhecimento teórico sobre TD quanto para sua aplicação prática no setor público. Espera-se que os achados auxiliem a tomada de decisões, orientem a formulação de políticas internas e apoiem o alcance dos Objetivos Estratégicos Institucionais (OEI).

2 Referencial teórico

Em 2024, o Conselho Nacional do Ministério Público (CNMP) realizou um diagnóstico sobre a destreza digital dos Ministérios Públicos Brasileiros (MPsBr). O modelo e os resultados desse diagnóstico foram publicados por Freitas; Zattar; Silva Júnior; Pedrosa (2024), evidenciando o NMD médio dos MPsBr. “O conceito de destreza digital refere-se à capacidade de uma organização em combinar a abertura ao novo e à disposição para inovar com a efetiva implementação e governança de iniciativas digitais” (CNMP, 2024).

Freitas; Zattar; Silva Júnior; e Pedrosa (2024) estruturam seu MMD em oito dimensões de avaliação: Estratégia Digital; Serviços ao Cidadão; Pessoas; Governança; Liderança; Operações; Cultura e Tecnologia. A soma das pontuações de cada dimensão, dividida pelo total de pontos possíveis, indica o nível de maturidade da instituição. O modelo define sete níveis de maturidade: Não Digital (0-15,99%); Iniciante Digital (16-30,99%); Emergente Digital (31-45,99%); Intermediário Digital (46-60,99%); Avançado Digital (61-75,99%); Líder Digital (76-90,99%) e Visionário Digital (91-100%). O diferencial desse modelo está na adequação ao contexto institucional do Ministério Público, considerando fatores tecnológicos, culturais e estratégicos (Freitas; Pedrosa, 2025).

No âmbito dos modelos desenvolvidos por instituições públicas brasileiras, o governo federal, por meio do Ministério da Gestão e

da Inovação em Serviços Públicos (MGI), elaborou um Modelo de Maturidade de Dados (MMDD). Esse modelo classifica práticas de tratamento de dados dentro das organizações públicas para caracterizar o estado atual do gerenciamento de dados e seus impactos na organização (Brasil, 2024). Na prática, o MMDD atua como um MMD com foco em dados. O Brasil (2024) dividiu seu modelo em 12 dimensões: Análise de Dados; Decisões com Dados; Conhecimento dos Dados; Dados Abertos; Responsabilidade pelos Dados; Uso de Dados; Gerenciamento de Dados; Interoperabilidade; Ética de Dados; Habilidade de Dados; Inteligência Artificial e Qualidade de Dados. Os níveis de maturidade definidos pelo modelo são: Não Iniciado; Iniciado; Emergente; Desenvolvido e Otimizado.

Além dos modelos destacados, existem diversos outros que podem ser empregados na avaliação do NMD por esta pesquisa. Estudos como os de Aras; Büyüközkan (2023); Santos *et al.* (2024); Silva; Vieira; Silva (2024) selecionaram e analisaram diferentes tipos de modelos e abordagens. Os resultados desses estudos foram utilizados para realizar uma análise comparativa com os modelos propostos pelo MGI e pelo CNMP. A análise das dimensões de avaliação revelou que o modelo do CNMP, em conjunto com o do MGI, abrange muitas das dimensões levantadas nos demais estudos citados, o que os torna bons candidatos para a aplicação nesta pesquisa. Adicionalmente, o uso do modelo do CNMP possibilita a comparação dos resultados do MPF com os resultados gerais dos MPsBr, conforme o trabalho de Freitas; Zattar; Silva Júnior; e Pedrosa (2024).

Entretanto, um ponto de limitação no modelo de Freitas; Zattar; Silva Júnior; e Pedrosa (2024) é que a maioria das questões aceitam apenas respostas binárias (sim ou não), o que restringe a profundidade da análise. Outros modelos, como o SANOL (Ünal; Sungur; Yildirim, 2022) e o MMD do Brasil (2024), utilizam escalas graduais de respostas, permitindo uma análise mais precisa sobre a realidade da TD da instituição. O uso de escalas de avaliação se mostra importante, principalmente para instituições de grande porte como o MPF, onde existe uma pluralidade de projetos, soluções e serviços de TIC que são mantidos por diferentes equipes e tecnologias. Dentro desse contexto, respostas binárias são insuficientes para refletir o nível real da maturidade digital, sobretudo em dimensões como tecnologia e operações.

3 Metodologia

A partir da análise realizada e com o objetivo de obter um diagnóstico mais acurado sobre o NMD do MPF, esta pesquisa optou por utilizar um modelo híbrido de avaliação. O MMD do Brasil (2024) foi aplicado integralmente para auxiliar na avaliação da dimensão de Tecnologia e para possibilitar uma visão mais ampla da maturidade de dados da instituição. Para as demais dimensões, foi utilizado o modelo de Freitas; Zattar; Silva Júnior; e Pedrosa (2024), com os seguintes ajustes:

- **Dimensão Governança:** a resposta da questão DGO3 foi transformada de binária para uma escala de avaliação.
- **Dimensão Liderança:** as questões DLI5.1 a DLI5.5 foram movidas para a Dimensão Tecnologia e tiveram suas respostas transformadas de binárias para uma escala gradual. Adicionalmente, foram incluídas outras tecnologias consideradas motrizes da TD no contexto atual. Elas agora equivalem às questões DTI11.1 a DTI11.2.
- **Dimensão Tecnologia:** as questões DTI7 e DTI8, referentes a dados, foram removidas, sendo substituídas pela aplicação do MMDD do MGI. A resposta da questão DT17 será calculada com base nas respostas da dimensão Qualidade de Dados do MMDD. A resposta da questão DT18 será calculada com base nas respostas da dimensão Conhecimento dos Dados do MMDD.

O questionário de Freitas; Zattar; Silva Júnior; e Pedrosa (2024), com as modificações supracitadas, foi segmentado em três instrumentos, visando uma abordagem estratégica: Questionário de Governança (Quadro 1), Questionário das Coordenações de TIC (Quadro 2) e Questionário dos Servidores de TIC (Quadro 3). A divisão foi planejada para:

- **Questionário de Governança:** utilizado para avaliar o NMD do MPF.
- **Questionário das Coordenações de TIC:** possibilitou comparar o quadro geral da instituição (obtido pelo Questionário de Governança) com a realidade operacional de cada coordenação.
- **Questionário dos Servidores de TIC:** buscou realizar um comparativo entre as respostas fornecidas pela área de Governança e a percepção dos servidores de TIC da instituição sobre as questões:

DED1 a DED4 da dimensão Estratégia Digital; DPE3 a DPE6 da dimensão Pessoas e DCT1 a DCT4 da dimensão Cultura.

Adicionalmente, a seção de identificação dos questionários das Coordenações e dos Servidores de TIC incluiu uma questão sobre a unidade de atuação. Essa identificação foi fundamental para realizar uma análise comparativa entre a TIC Nacional do MPF (centralizada na Secretaria de Tecnologia da Informação e Comunicação – STIC, na Procuradoria Geral da República – PGR), a TIC local (centralizada nos Centros de Tecnologia da Informação e Comunicação – CTICs, existentes nas unidades estaduais e regionais) e a estrutura de TIC existente na Secretaria de Perícia, Pesquisa e Análise (SPPEA), que, embora ligada à PGR, opera de forma independente da STIC. Os questionários detalhados são apresentados no Anexo A.

Todos os questionários foram disponibilizados via Google Forms e enviados por e-mail aos seguintes destinatários:

- **Questionário de Governança:** enviado à Assessoria Técnica (Astec) da STIC.
- **Questionário das Coordenações de TIC:** enviado a 31 CTICs, 29 unidades pertencentes à STIC e 5 unidades ligadas à área de TIC da SPPEA.
- **Questionário dos Servidores de TIC:** enviado a 693 servidores da área de TIC de todo o MPF.

Adicionalmente, o Questionário do MMDD do Brasil (2024) foi enviado à Subsecretaria de Dados e Informações Gerenciais (Subdig) da STIC e à Assessoria de Governança de Dados (AGD) da SPPEA.

Uma vez feita a avaliação do NMD do MPF, o resultado da avaliação direcionou a busca e o mapeamento das estratégias que têm potencial para ajudar a melhorar o NMD. Para orientar a busca, foram utilizadas palavras-chave como: Transformação Digital, TI Ambidestra (TI Bimodal), reestruturação organizacional, metodologias ágeis, governança de TIC e *Shadow IT*. Com destaque para autores como: Chaves; Diirr (2025), que propõem um framework que alia as melhores práticas para a TI Bimodal com mecanismos de Governança de TIC; Albuquerque; Costa (2025), que discutem tendências e implicações da transformação digital no setor público global; Haug; Dan; Mergel (2024),

que identificam os fatores organizacionais que impulsionam mudanças digitais no setor público; Kimura; Horita; Rocha (2020), que exploram os impactos da transformação digital na institucionalização de metodologias ágeis, especialmente em contextos com estruturas tradicionais, como é o caso do MPF; e Galvão Junior *et al.* (2024), que constata que a combinação da adoção de metodologias ágeis e da área de Governança de TI forma uma peça importante para auxiliar na mudança cultural e de comunicação necessárias para a TD nas organizações. Por fim, o estudo de Joca (2025), que aborda o *Shadow IT* (o uso de soluções tecnológicas sem aprovação formal da área de TI), enumerando seus riscos e benefícios para a TD.

4 Resultados e discussão

A análise dos dados e a discussão foram divididas em cinco etapas: NMD do MPF; maturidade de dados do MPF; realidade das coordenações; percepção dos servidores; e estratégias para potencializar o TD no MPF.

Após a aplicação do MMD Híbrido, o MPF foi classificado com o NMD Intermediário Digital, obtendo um percentual de 49,33% na avaliação, conforme destacado na Figura 1. Esse valor foi calculado a partir das respostas ao Questionário de Governança e ao Questionário do MMDD pela STIC. Quando comparado com os resultados obtidos por Freitas; Zattar; Silva Júnior; e Pedrosa (2024) e detalhados na Figura 2, o MPF está classificado entre os 13% dos MPsBr com maior NMD.

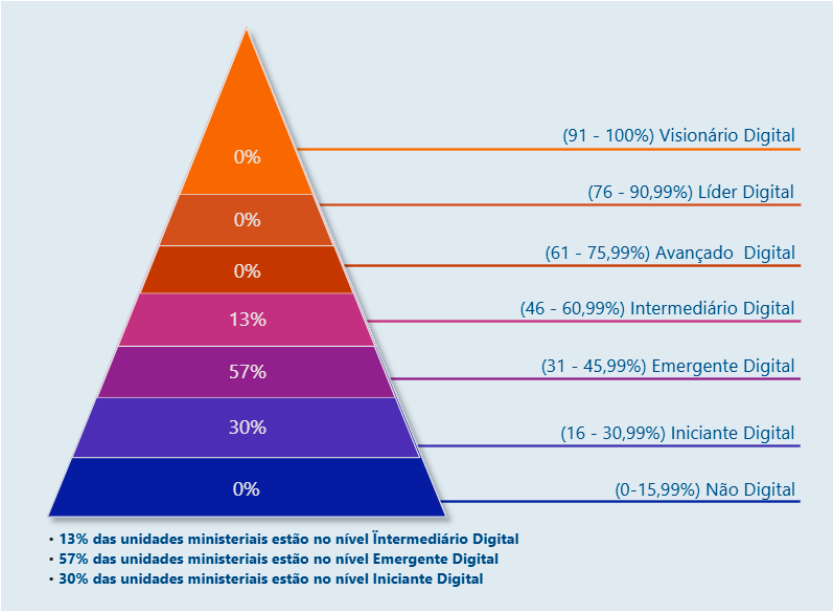
Figura 1 – Nível de maturidade digital do MPF



Fonte: autoria própria, com base nos dados da pesquisa.

Apesar disso, o NMD da instituição ainda se encontra três níveis abaixo do maior NMD na escala do MMD utilizado por esta pesquisa. Quando se analisam de forma separada as dimensões de avaliação (Figura 3), é possível identificar as dimensões mais e menos eficazes em relação à TD. As dimensões de Serviços ao cidadão, Liderança e Tecnologia tiveram um grande destaque positivo para definição do NMD geral do MPF, ficando acima da média obtida pela instituição. Porém, em contraponto, os níveis de maturidade das dimensões Estratégia digital (0,0%), Pessoas (49,98%), Governança (37,50%) e Operações (28,32%) despontaram como um grande destaque negativo desta avaliação, puxando a NMD para baixo.

Figura 2 – Escola Digital dos MPsBr



Fonte: CNMP (2024).

A Estratégia Digital é responsável por definir os objetivos da TD dentro da instituição, alinhados aos Objetivos Estratégicos Institucionais. Um percentual de 0,0% é alarmante, pois demonstra que, embora se tenha investimento em tecnologia e apoio da liderança, não existe um planejamento estratégico para a TD institucional. A ausência de estratégias digitais formalizadas aponta para uma abordagem fragmentada e descoordenada da TD, sugerindo que o MP brasileiro ainda está nos estágios iniciais desse processo (Freitas; Zattar; Silva Júnior; Pedrosa, 2024).

Como destacado pelo CNMP (2024), no nível Intermediário Digital, os colaboradores apresentam um nível intermediário de habilidades digitais, porém é essencial definir uma Estratégia Digital que assegure investimentos em iniciativas integradas e que realmente direcione as ações de gestão. Já para alcançar o próximo nível de maturidade digital, Avançado Digital, é necessária uma Estratégia Digital sólida e bem estruturada, capaz de orientar e impulsionar o processo de TD. As lideranças da organização, seja na área de negócios ou de tecnologia, devem estar cientes de que dependem de uma estratégia de

transformação clara e robusta, incluindo aquelas ligadas à estratégia empresarial e não apenas, ou exclusivamente, à aplicação da tecnologia ao modelo existente (Goes; Costa, 2022).

De acordo com Haug, Dan e Mergel (2024), a TD não é uma consequência direta da implementação da tecnologia; o que é necessário são abordagens que coloquem os atores – e não a tecnologia ou as organizações – no centro dos esforços de mudança. Por isso, é importante capacitar os colaboradores do MPF em relação à TD, criar mecanismos de valorização do pessoal que atua na área de TIC e criar estruturas organizacionais específicas para trabalhar a TD e a inovação. Essa necessidade é evidenciada pela avaliação da dimensão Pessoas abaixo da média geral. Tal problema, contudo, não é uma exclusividade do MPF. Foi identificado que apenas uma unidade ministerial tem um plano de carreira ou incentivos específicos para servidores de TI, o que limita o desenvolvimento profissional, dificulta a retenção de talentos e a atração de novos especialistas, fatores essenciais para a TD (Freitas; Zattar; Silva Júnior; Pedrosa, 2024).

Apesar de os órgãos de controle recomendarem a criação de mecanismos de valorização do pessoal de TIC há anos, o MPF ainda é carente de políticas de valorização específicas para esta categoria de servidores. O Acórdão 1200/2014, do plenário do Tribunal de Contas da União (TCU), faz recomendações para valorização dos servidores de TIC da Administração Pública.

Estabelecer estratégias que visem a minimizar a rotatividade do pessoal efetivo, atuante na área de TI, inclusive com o desenvolvimento de ações voltadas à criação de carreira específica de TI, com remuneração compatível com as atribuições dos respectivos cargos, de modo a tratar as principais causas da evasão de pessoal identificadas (Brasil, 2014).

O Plano Diretor de Tecnologia da Informação (PDTI) do CNMP 2019-2021 destacou como ameaças a TIC, entre outras:

Falta de reconhecimento da TI como área estratégica

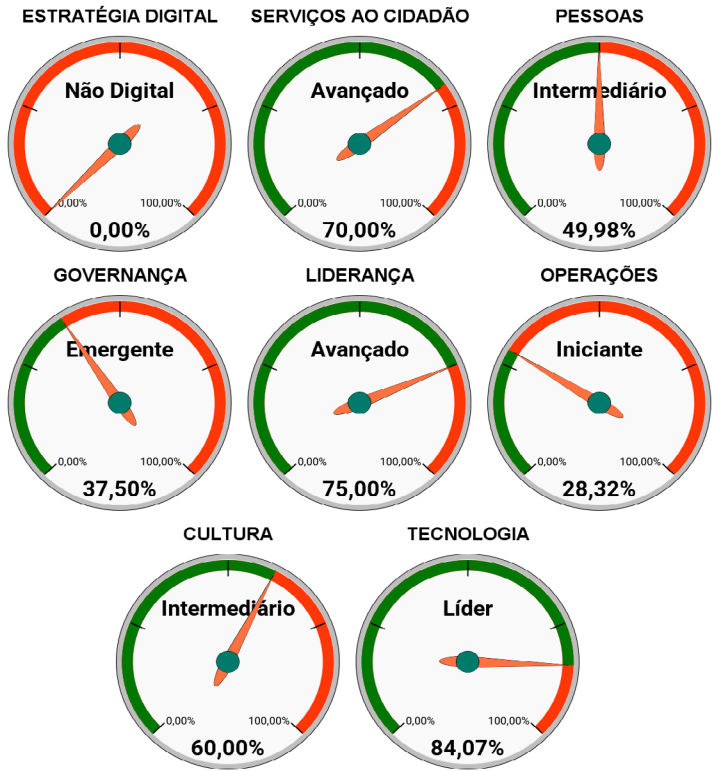
Tomada de decisões que impactam a área técnica sem consulta prévia à Secretaria de Tecnologia da Informação [...]

Ausência de uma política de valorização de especialistas técnicos promovendo a carreira em Y [...]

Rotatividade de servidores frente a carreiras melhores de outros órgãos [...]

Ausência de ações institucionais para motivação dos servidores (CNMP, 2019).

Figura 3 – Dimensões NMD do MPF



Fonte: autoria própria, com base nos dados da pesquisa.

No Fórum Nacional de Gestão do Ministério Público (FNG-MP), organizado pelo CNMP em 2024, o Comitê de Políticas de Tecnologia da Informação (CPTI) publicou a nota técnica “Valorização das equipes de TI dos Ministérios Públicos”. Nessa nota, o CPTI sugere que os MPsBr regulamentem e implementem:

- Gratificação de Tecnologia da Informação e Comunicação (Gatic) para os servidores com cargo de técnico ou analista de TIC, que atuem na área de TIC.
- Regime de teletrabalho, de forma que pelo menos 50% dos servidores com cargo de técnico ou analista de TIC, que atuem na área de TIC, estejam 100% em teletrabalho.

Além da necessidade de fortalecimento de mecanismos de valorização dos servidores de TIC, o MPF ainda caminha no sentido contrário às recomendações dos órgãos de controle e dos estudos sobre TD. A Portaria PGR/MPU n. 216/2024 determinou a extinção gradual do cargo de técnico do MPU/Tecnologia da Informação e Comunicação, que corresponde atualmente a 68,93% dos servidores de TIC de todo o órgão. Essa atitude enfraquece uma categoria de servidores que estão intimamente ligados com os processos de TD.

A Governança é a terceira dimensão desse quarteto vulnerável no NMD do MPF. A Governança é responsável por definir as diretrizes que serão seguidas pela gestão para garantir o *accountability* da instituição. A adoção de boas práticas na gestão e governança de serviços busca a excelência operacional e a satisfação do usuário, além de atender aos requisitos da Lei n. 14.129, art. 47, que exige a implementação e a manutenção de mecanismos e práticas de governança (Freitas; Zattar; Silva Júnior; Pedrosa, 2024).

Uma baixa avaliação na dimensão Governança indica que o MPF necessita de um projeto de governança capaz de responder de forma rápida às mudanças que a TD necessita. Ao analisar as respostas obtidas por Freitas; Zattar; Silva Júnior; Pedrosa (2024) utilizando mineração de dados, Freitas; Pedrosa (2025) identificaram padrões de ocorrência entre atributos institucionais e níveis de maturidade digital. Por exemplo, a existência de governança digital formalizada está fortemente associada à presença de uma estratégia digital clara, reforçando a hipótese de que ações organizadas em torno da governança promovem melhor alinhamento institucional (Freitas; Pedrosa, 2025).

A baixa avaliação da dimensão Governança se deve principalmente aos valores das respostas nos três itens abaixo:

- a ausência de iniciativas estratégicas de automação de processos de trabalho, o que pode trazer diminuição da produtividade e da eficiência do trabalho, aumento de custos e recorrência de erros;
- a falta de indicadores de acompanhamento da utilização das ferramentas digitais oferecidas pela instituição, não permitindo identificar a efetividade das ferramentas desenvolvidas e adquiridas;
- a pouca utilização de metodologias ágeis.

As metodologias ágeis incentivam a melhoria contínua e a inovação, promovendo a otimização de processos e a criação de produtos e serviços mais satisfatórios para os usuários (Freitas; Zattar; Silva Júnior; Pedrosa, 2024). Apesar de pensadas inicialmente como metodologia de gestão de projetos de *software*, as metodologias ágeis são cada vez mais utilizadas como metodologias de gestão de trabalho. O fato de a maioria das metodologias ágeis priorizarem a flexibilidade e a resposta rápida a mudanças as torna uma forte aliada ao processo de TD, que muda constantemente, junto com suas tecnologias motrizes.

Nota-se que a presença de elementos estruturais – como governança digital formalizada, comitês de inovação, equipes de TI capacitadas e planejamento estratégico digital – está fortemente correlacionada com melhores resultados em dimensões como Estratégia, Liderança, Cultura, Tecnologia e Serviços ao Cidadão. Por exemplo, a regra R20 [...] destaca que a presença de equipes e estruturas dedicadas à governança, combinada com a digitalização, está associada à adoção de metodologias ágeis em 90% dos casos (Freitas; Pedrosa, 2025, p. 5).

Por fim, ao analisar o NMD da dimensão Operações, é possível identificar os pontos que levaram a uma avaliação bem abaixo da média da instituição, com destaque para:

- baixo quantitativo de servidores de TIC em relação à quantidade de usuários de serviços de TIC na instituição, 1,17 de 40 pontos possíveis;
- baixo gasto com pessoal de TIC em relação ao total de gasto de pessoal, 1,56 de 40 pontos possíveis;
- baixo gasto destinado a investimentos de TIC, 0,04 de 40 pontos possíveis.

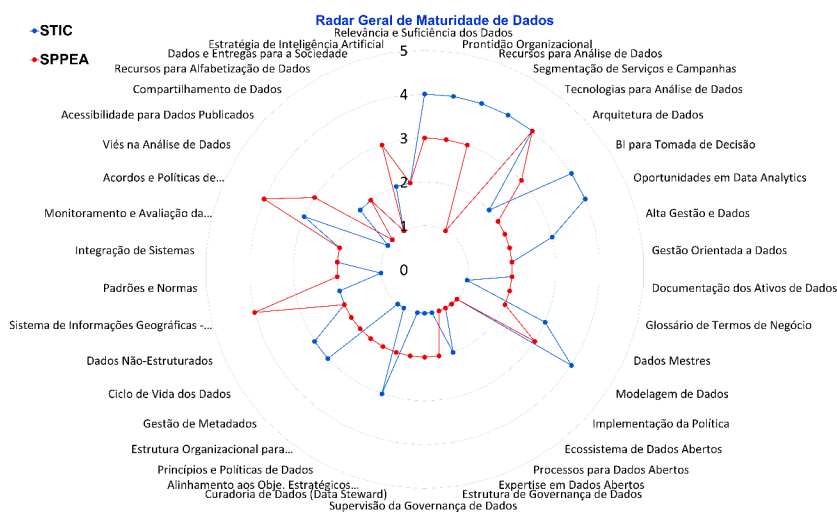
Esses pontos também impactam os resultados da dimensão Pessoas e têm relação com aspectos já citados no PDTI do CNMP 2019-2021 e no Acórdão 1200/2014 do TCU, como: tamanho reduzido do quadro de servidores da TIC; restrição orçamentária; quantidade excessiva de trabalho; e falta de estrutura de pessoal adequada da área de TIC da instituição.

O resultado da aplicação MMDD do Brasil (2024) na STIC e na SPPEA está apresentado na Figura 4. Ao analisar os resultados apontados no gráfico, é possível constatar que a maioria dos tópicos

avaliados, para ambas as unidades, estão no nível 1 (Não iniciado) – ou 2 – Iniciado. Isso demonstra que o Nível de Maturidade de Dados NMDD geral do MPF ainda está no nível inicial e tem muita margem para evolução.

Fazendo um comparativo geral entre as duas unidades, é possível perceber que o NMDD das duas unidades tem pontos de convergência e pontos que apresentam diferentes níveis de maturidade. O fato de os setores de TIC da SPPEA atuarem como uma *Shadow IT* do MPF pode acarretar trabalho duplicado, divisão de mão de obra e esforços e dificultar a estratégia para evolução do NMDD.

Figura 4 – Radar de maturidade de dados do MPF

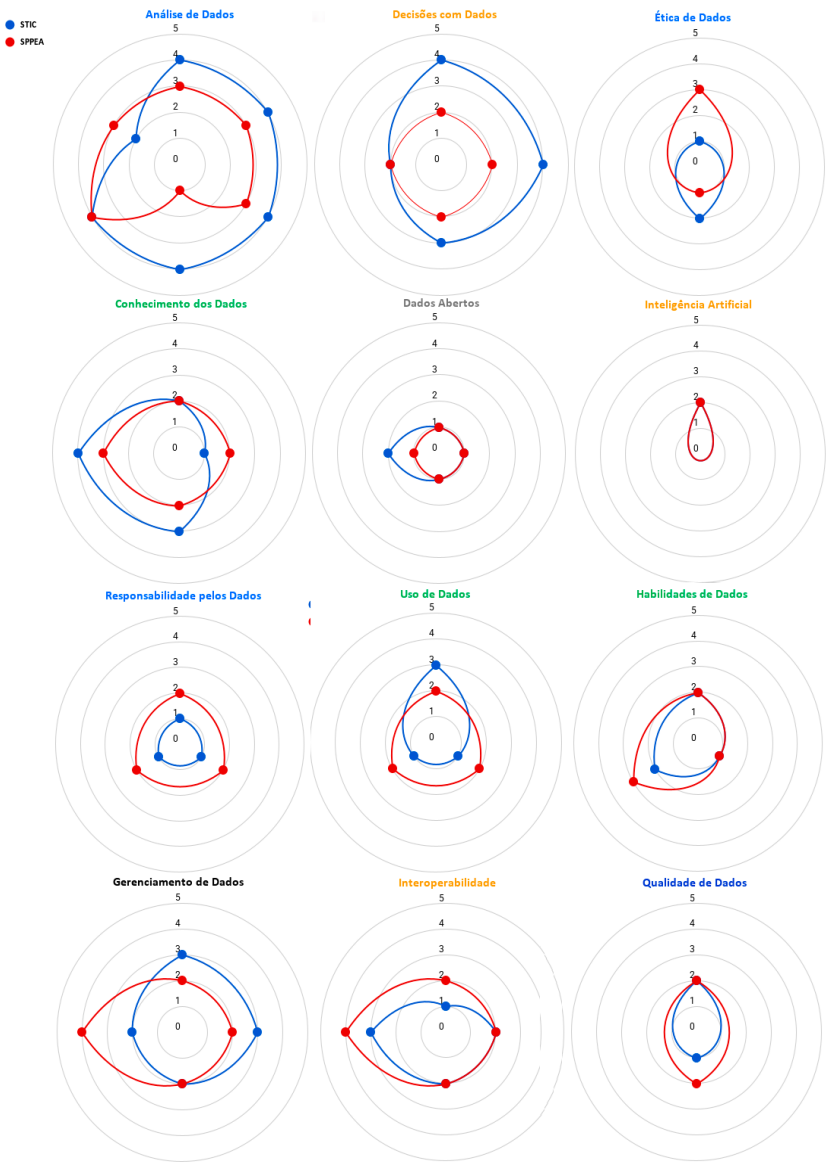


Fonte: autoria própria, com base nos dados da pesquisa.

Ao realizar o comparativo entre o NMDD entre a STIC e a SPPEA, Figura 5, é possível notar que as unidades se complementam em vários tópicos e que uma união de esforços entre as duas unidades tem o potencial de aumentar significativamente o NMDD do MPF. O NMDD da STIC se destaca principalmente nas dimensões Análise de Dados, Decisões com Dados, Conhecimento dos Dados e Gerenciamento de Dados.

A SPPEA, por sua vez, apresenta maior NMDD em Responsabilidade pelos Dados, Uso de dados e Interoperabilidade.

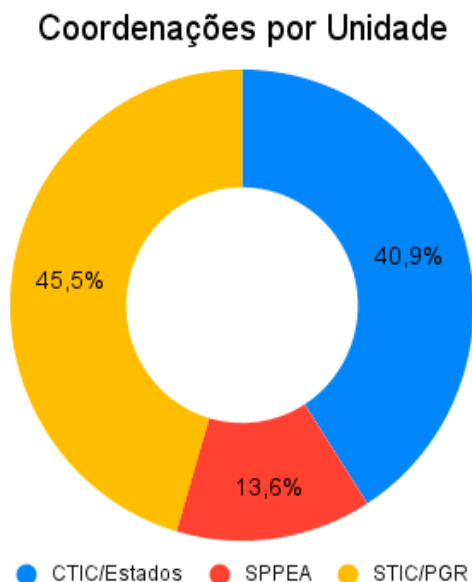
Figura 5 – Comparativo de maturidade de dados STIC e SPPEA



Fonte: autoria própria, com base nos dados da pesquisa.

O Questionário das Coordenações de TIC foi enviado para 31 CTICs, 5 unidades da SPPEA e 29 da STIC. O questionário teve 22 respostas, distribuídas conforme o gráfico da Figura 6, o que demonstra uma representatividade de 33,85% das coordenações de TIC do MPF.

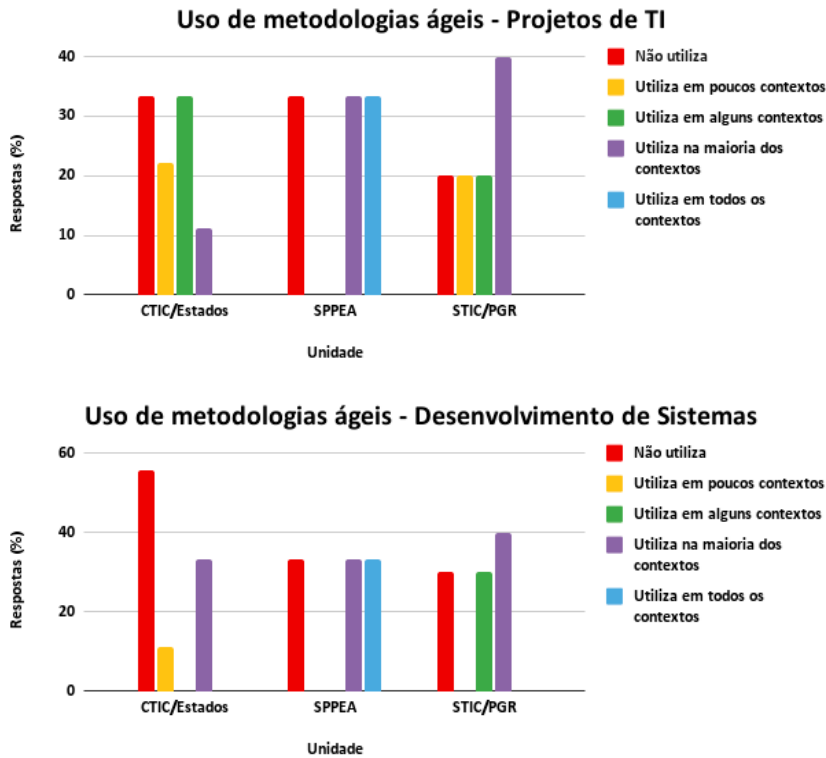
Figura 6 – Percentual de respostas das coordenações por unidade



Fonte: autoria própria, com base nos dados da pesquisa

Ao analisar os gráficos da Figura 7, é possível notar uma grande diferença entre o nível de uso de metodologias ágeis, tanto entre unidades quanto entre diferentes coordenações da mesma unidade. Isso mostra uma falta de alinhamento estratégico que pode ser um impacto da falta de uma estratégia digital bem definida para o MPF, como identificado na dimensão Estratégia Digital.

Figura 7 – Uso de metodologias ágeis por coordenação

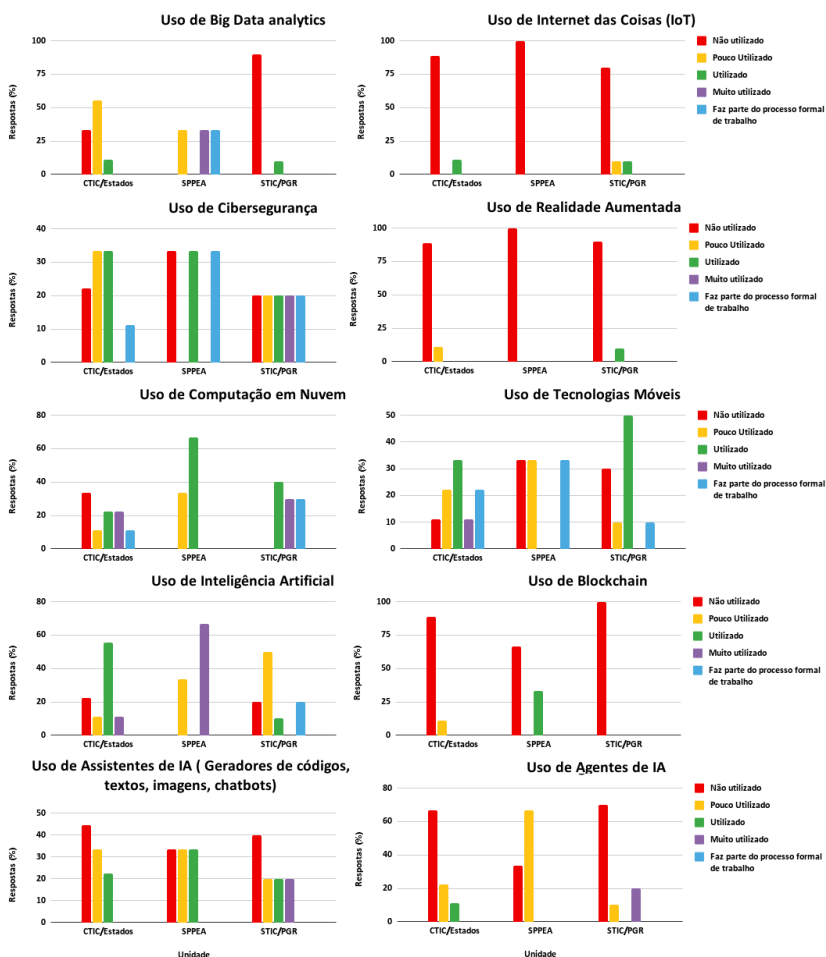


Fonte: autoria própria, com base nos dados da pesquisa.

Em “Projetos de TI”, as unidades da STIC tendem a apresentar níveis mais elevados de adoção, com maior frequência nas categorias “Utiliza na maioria dos contextos” e menor número de respostas em «Não Utiliza». Em «Desenvolvimento de Sistemas», nota-se maior variação entre as unidades, com 55,55% dos CTICs informando que “Não Utiliza” e equilíbrio maior entre STIC e SPPEA.

Ao analisar os gráficos da Figura 8 sobre a utilização de tecnologias motrizes de TD por coordenação, assim como na adoção de metodologias ágeis, é possível notar um descompasso entre o uso das tecnologias pelas unidades. Mais uma vez, na falta de uma orientação que direcione as coordenações, as tecnologias de TD são utilizadas de forma orgânica e pouco organizada, o que evidencia uma divisão de recursos, de conhecimento e força de trabalho.

Figura 8 – Uso de tecnologias de TD por coordenação

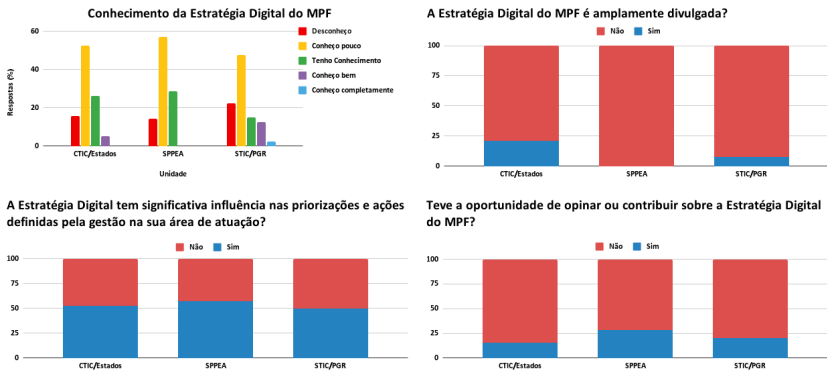


Fonte: autoria própria, com base nos dados da pesquisa.

Os gráficos das Figuras 9 e 10 representam as percepções dos servidores, obtidas pelas respostas ao Questionário dos Servidores de TIC. Ao analisar os gráficos da Figura 9, é possível identificar que os servidores têm dificuldade de entender a estratégia digital do MPF. É possível constatar que a falta da estratégia digital, já identificada no NMD da dimensão de Estratégia Digital e que teve seus efeitos também percebidos na análise dos resultados do Questionário das Coordenações de TIC, é um ponto de dificuldade apontado pelos servidores da área

de TIC do MPF. A falta desse direcionamento estratégico acaba sobre-carregando os servidores, que precisam tomar decisões técnicas e de gestão com base em estratégias heurísticas.

Figura 9 – Percepção dos servidores de TIC sobre a estratégia digital do MPF

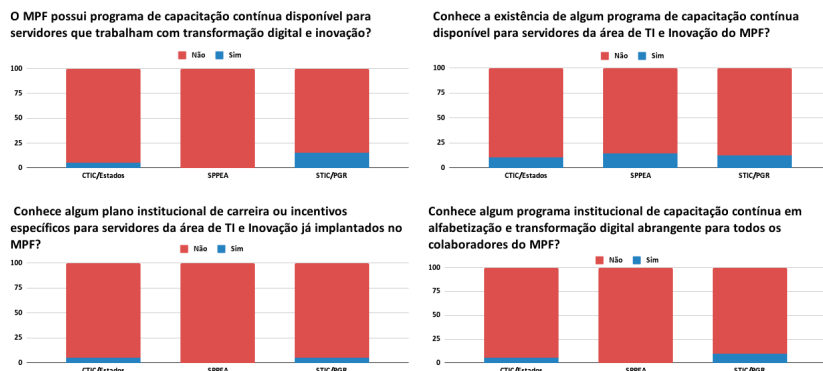


Fonte: autoria própria, com base nos dados da pesquisa.

Nos gráficos da Figura 10, é possível identificar uma percepção negativa dos servidores em relação à falta de programas de capacitação, incentivos e valorização aos servidores de TIC do MPF. Essas respostas, associadas com o NMD das dimensões Governança de TIC, Pessoas e Operações, mostram que essa dificuldade do MPF para alavancar seu NMD com base na valorização dos servidores e no investimento estratégico na área de TIC é evidenciada também pelas respostas dos servidores da área. Além disso, na questão DPE4 do Questionário de Governança, foi informado que o MPF tem um programa de capacitação contínua para servidores de TIC e Inovação. Porém, a grande maioria dos servidores, 87,88%, informou desconhecer tal programa de capacitação, o que demonstra que as capacitações não são devidamente ofertadas e/ou divulgadas.

A partir dos resultados analisados acima, fica claro que o MPF precisa adotar estratégias para elevar o NMD, principalmente para as dimensões Estratégia Digital, Pessoas, Governança e Operações. O MPF não tem uma estratégia digital formalizada, o que demonstra que a instituição tem uma abordagem fragmentada e descoordenada de TD. Essa ausência diminui a capacidade de adaptação às demandas digitais (Freitas; Zattar; Silva Júnior; Pedrosa, 2024).

Figura 10 – Percepção dos servidores de TIC sobre capacitação e incentivos do MPF



Fonte: autoria própria, com base nos dados da pesquisa.

Ao elaborar sua estratégia digital, o MPF tem a oportunidade de utilizar o resultado deste estudo e definir uma estratégia com base em boas práticas que potencializam a TD. A implantação da TI Ambidestra é uma prática base a ser utilizada para a criação dessa estratégia. Na Figura 11, é representado um dos arquétipos de ambidestria mapeados por Chaves; Diirr (2025). Nesse arquétipo, a estrutura de TIC é dividida em TI tradicional (Operação de TI, em rosa), responsável pela operação tradicional de TIC com a sustentação de produtos e serviços de TIC existentes, e em TI de inovação (Projetos e Operação de TI, em laranja), responsável por iniciativas de TD, modernização de tecnologias e desenvolvimento de novos produtos e serviços. A adoção de uma estratégia ambidestra com Modo Ágil permite definir um quadro de servidores alocados especificamente para inovação.

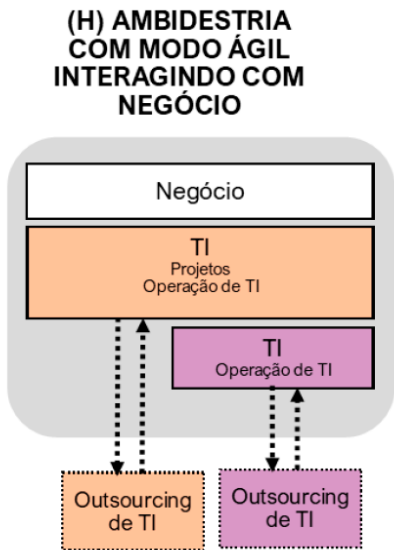
A estratégia digital também deve criar diretrizes para a dimensão de Pessoas e Operações – a criação de um plano de capacitação nacional com alcance e divulgação abrangente que dê suporte a conteúdos tanto para TI tradicional quanto voltados para a TI de inovação –, além da definição de estratégias de valorização dos servidores de TIC do MPF, como:

- a Gratificação de Tecnologia da Informação e Comunicação, sugerida na nota técnica: valorização das equipes de TI dos Ministérios Públicos;

- a gratificação para os servidores que atuam na TI de inovação, responsáveis pela implantação e direcionamento da TD da instituição;
- a reestruturação da carreira de técnicos e analistas de TIC do MPF, unificando-a em uma nova carreira, com remuneração adequada à importância estratégica da TIC.

Para aperfeiçoar os NMD da dimensão Governança, a estratégia digital deve definir diretrizes para a melhoria dos níveis de adoção de metodologias ágeis em projetos institucionais, projetos de TIC e no desenvolvimento de sistemas. Ademais, é preciso definir indicadores de uso de serviços de TIC que devem ser utilizados por todas as ferramentas digitais fornecidas ou utilizadas pelo MPF.

Figura 11 – Arquétipo de ambidestria



Fonte: Chaves, Diirr (2025).

Por fim, a absorção da TIC da SPPEA pela STIC fortaleceria a estrutura formal de TIC do MPF, principalmente a área de dados, como evidenciado pelo MMDD. Além disso, como destacado por Joca (2025), existem riscos significativos na *Shadow IT*, como vazamento de dados; fragilidade na segurança da informação e desconexão entre sistemas,

embora as evidências acadêmicas e práticas apontem que a *Shadow IT* pode potencializar o processo de TD por ser mais flexível que a TIC formal (Joca, 2025). O uso de metodologias ágeis, da TI ambidestra e de um plano de capacitação nacional já seriam suficientes para suplantar as vantagens apontadas.

De forma geral, o MPF encontra-se em um estágio intermediário de maturidade digital, apresentando avanços significativos em tecnologia e serviços digitais, mas com desafios importantes nas áreas de governança, pessoas e estratégia digital. A Figura 3 resume o desempenho por dimensão, evidenciando a necessidade de ações estruturantes e coordenadas para alcançar níveis mais elevados de maturidade.

Os resultados reforçam que a TD não depende apenas de investimentos tecnológicos, mas de uma mudança organizacional e cultural profunda, que envolva planejamento estratégico, liderança digital e valorização de pessoas. Esses achados convergem com as conclusões de Freitas; Zattar; Silva Júnior; Pedrosa (2024); Haug; Dan; Mergel (2024); e Albuquerque; Costa (2025), segundo os quais o sucesso da TD no setor público depende da integração entre estratégia, tecnologia e gestão de pessoas, apoiada por uma governança digital sólida e transparente.

5 Considerações finais

O presente estudo avaliou o Nível de Maturidade Digital (NMD) do Ministério Público Federal (MPF) com base na aplicação de um modelo híbrido de avaliação, que combinou o Modelo do Conselho Nacional do Ministério Público (CNMP) e o Modelo de Maturidade de Dados do Ministério da Gestão e Inovação (MGI). A análise revelou que o MPF se encontra no nível Intermediário Digital, com 49,33% de maturidade, demonstrando avanços significativos em Serviços ao Cidadão, Liderança e Tecnologia, mas fragilidades evidentes nas dimensões Estratégia Digital, Pessoas, Governança e Operações.

Os resultados indicam a ausência de uma estratégia digital formalizada, o que compromete a integração e o alinhamento institucional necessários para consolidar a Transformação Digital (TD). Também ficou evidente a necessidade de valorização e capacitação dos servidores de TIC, bem como de uma estrutura de governança mais ágil, capaz de

responder com eficiência às demandas impostas pela TD. A escassez de investimentos em pessoal e infraestrutura tecnológica reforça a urgência de ações estruturantes e coordenadas.

Diante disso, o estudo propõe as seguintes estratégias para impulsionar a TD no MPF:

1. elaboração de uma Estratégia Digital Nacional do MPF, baseada em princípios de TI Ambidestra (ou bimodal) e metodologias ágeis, assegurando alinhamento entre inovação e governança;
2. implementação de programas de capacitação e valorização profissional, incluindo planos de carreira, incentivos à inovação e políticas de retenção de talentos;
3. fortalecimento da Governança Digital, com definição de indicadores de desempenho e mecanismos de monitoramento contínuo das iniciativas digitais;
4. integração da estrutura de TIC da STIC e da SPPEA, principalmente a estrutura de dados, com vistas à criação de um Comitê de Governança de Dados e Inteligência Artificial para aprimorar a interoperabilidade e o uso estratégico das informações;
5. adoção de mecanismos de comunicação interna voltados à promoção da cultura digital e à conscientização sobre os benefícios da TD.

Conclui-se que, embora o MPF tenha alcançado resultados expressivos em algumas dimensões, ainda há um longo caminho para atingir um nível avançado de maturidade digital. A adoção das estratégias apresentadas neste estudo pode não apenas elevar o NMD institucional, mas também promover maior eficiência, transparência e inovação, fortalecendo o papel do MPF como uma instituição pública moderna, digital e centrada no cidadão.

Como contribuição prática, o estudo oferece subsídios técnicos e estratégicos para o planejamento e gestão da TD no MPF. Como contribuição teórica, amplia a discussão sobre maturidade digital no setor público brasileiro, demonstrando a aplicabilidade de modelos híbridos de avaliação em instituições complexas.

Por fim, recomenda-se a realização de pesquisas futuras voltadas à mensuração dos impactos da TD sobre a eficiência institucional e à

avaliação longitudinal do NMD do MPF, de modo a acompanhar sua evolução ao longo do tempo.

Referências

ALBUQUERQUE, M. R. de; COSTA, L. Transformação digital no setor público: tendências e implicações. **Revista de Gestão e Secretariado**, [s. l.], v. 16, n. 3, p. e4771, 11 mar. 2025. DOI: <https://doi.org/10.7769/gesec.v16i3.4771>.

ARAS, A.; BÜYÜKÖZKAN, G. Digital transformation journey guidance: a holistic digital maturity model based on a systematic literature review. **Systems**, v. 11, n. 4, p. 1-31, abr. 2023. DOI: <https://doi.org/10.3390/systems11040213>.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Modelo de maturidade de dados - MMD**. Brasília, DF: MGI, 2024. Disponível em: <https://tinyurl.com/3a2mwujf>. Acesso em: 1º jul. 2025.

BRASIL. Ministério Público Federal. **Conheça a estrutura do MPF**. Brasília, DF: MPF, 2025. Disponível em: <https://tinyurl.com/47xxzfxe>. Acesso em: 22 out. 2025.

BRASIL. Tribunal de Contas da União. **Acórdão n. 1200/2014**. Relator: Raimundo Carreiro. Brasília, DF, 14 maio 2014. Disponível em: <https://tinyurl.com/3v6hre92>. Acesso em: 23 out. 2025.

CHAVES, V. M. G.; DIIRR, B. Ambidestria em TI nas instituições públicas federais brasileiras. In: CONCURSO DE TESES, DISSERTAÇÕES E TCCS EM SISTEMAS DE INFORMAÇÃO - SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 21., 2025, Recife/PE. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 95-110. DOI: https://doi.org/10.5753/sbsi_estendido.2025.246728.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Diagnóstico de destreza digital do MP brasileiro**: metodologia utilizada para avaliação, pontuação e classificação de cada unidade ministerial. Brasília, DF: CNMP, 25 set. 2024. Disponível em: <https://tinyurl.com/3ywx2tem>. Acesso em: 1º jul. 2024.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Plano Diretor de Tecnologia da Informação 2019/2021**. Brasília: CNMP, 2019.

FREITAS, L. M. de A.; PEDROSA, G. V. Transformação digital no Ministério Público: descobrindo padrões por meio da mineração de dados. *In: LATIN AMERICAN SYMPOSIUM ON DIGITAL GOVERNMENT (LASDiGov)*, 12., 2025, Maceió-AL. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2025. DOI: <https://doi.org/10.5753/lasdigov.2025.9022>. Acesso em: 17 out. 2025.

FREITAS, L. M. de A.; ZATTAR, G. A. P.; SILVA JÚNIOR, P. C. S. da; PEDROSA, G. V. Avaliando a maturidade digital no Ministério Público brasileiro: uma ferramenta para diagnóstico da transformação digital. **Revista de Gestão e Secretariado**, [s. l.], v. 15, n. 9, p. e4213, 2024. DOI: <https://doi.org/10.7769/gesec.v15i9.4213>.

GALVÃO JUNIOR, G. S.; PENHA, R.; VASCONCELOS, V. N. S. A.; SILVA, L. F.; GONÇALVES, M. L. A. Elementos e práticas de gerenciamento de projetos de transformação digital para suportar o business agility uma revisão sistemática da literatura. **International Journal of Innovation**, São Paulo, v. 12, n. 1, p. 1-40, jan./abr. 2024. DOI: <https://doi.org/10.5585/2024.26374>.

GOES, R. S.; COSTA, I. Agile portfolio management and knowledge management in digital transformation: a systematic literature review / Gestão ágil de portfólio e gestão do conhecimento na transformação digital: uma revisão sistemática da literatura. **Brazilian Journal of Development**, [s. l.], v. 8, n. 4, p. 28283-28299, abr. 2022. DOI: <https://doi.org/10.34117/bjdv8n4-361>.

HAUG, N.; DAN, S.; MERGEL, I. Digitally-induced change in the public sector: a systematic review and research agenda. **Public Management Review**, v. 26, n. 7, p. 1963-1987, 2 jul. 2024. DOI: <https://doi.org/10.1080/14719037.2023.2234917>.

JOCA, B. P. Gestão de shadow it: práticas para reduzir riscos e potencializar a inovação. **Revista Contemporânea**, [s. l.], v. 5, n. 6, p. e8342, jun. 2025. DOI: <https://doi.org/10.56083/RCV5N6-037>.

KIMURA, W.; HORITA, F.; ROCHA, V. O impacto da transformação digital na institucionalização de metodologias ágeis. *In: WORKSHOP DE INICIAÇÃO CIENTÍFICA EM SISTEMAS DE INFORMAÇÃO - SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI)*, 16., 2020, Evento Online. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 13-16. DOI: <https://doi.org/10.5753/sbsi.2020.13117>. Acesso em: 3 jun. 2025.

SANTOS, L. G. P.; OLIVEIRA, R. T. S.; FREITAS, V.; FREITAS DE PAULA, V. A. Modelos de maturidade em transformação digital: análise de propostas para pequenas e médias empresas do setor manufatureiro. **P2P e Inovação**, v. 11, n. 1, 5 set. 2024. DOI: <https://doi.org/10.21728/p2p.2024v11n1e-7073>.

SILVA, J. L.; VIEIRA, A. C. L.; SILVA, S. V. Modelos de maturidade digital: um estudo de caracterização baseado na revisão sistemática de literatura. **BBR. Brazilian Business Review**, v. 21, n. 2, 2024. Disponível em: <https://tinyurl.com/mrx55588>. Acesso em: 8 abr. 2026.

ÜNAL, C.; SUNGUR, C.; YILDIRIM, H. Application of the maturity model in industrial corporations. **Sustainability**, v. 14, n. 15, p. 9478, ago. 2022. DOI: <https://doi.org/10.3390/su14159478>.

Anexo A

Quadro 1 – Questionário de Governança

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
5.1.	DIMENSÃO ESTRATÉGIA DIGITAL	
DED1	A instituição possui uma estratégia digital definida e documentada?	Sim / Não
DED2	A estratégia digital da instituição é amplamente divulgada?	Sim / Não
DED3	A estratégia digital tem significativa influência nas prioridades e ações definidas pela gestão?	Sim / Não
DED4	A estratégia digital é continuamente avaliada e adaptada?	Sim / Não
5.2.	DIMENSÃO SERVIÇOS AO CIDADÃO	
DSC1	A instituição disponibiliza serviços digitais ao cidadão?	Sim / Não
DSC1.1	Formulário online para contato direto com os órgãos de execução.	
DSC1.2	Formulário online para contato com a Ouvidoria.	
DSC1.3	Chatbot	
DSC1.4	Aplicativos de mensageria.	
DSC1.5	Serviço de balcão virtual / Atendimento por videoconferência.	
DSC1.6	Consulta de andamento dos atendimentos e dos procedimentos da área-fim.	

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DSC1.7	Envio de documentos (peticionamento externo) para procedimentos.	
DSC1.8	Certidão negativa.	
DSC2	Existem mecanismos para avaliar a satisfação do cidadão com relação aos serviços oferecidos?	Sim / Não
DSC3	A instituição possui um catálogo de serviços indicando quais serviços são digitais e quais são analógicos?	Sim / Não
5.3.	DIMENSÃO PESSOAS	
DPE1	Quantas pessoas atuam com dedicação exclusiva para tratar de temas relacionados à:	0 / 1 / 2 ou mais
DPE1.1	Inovação	
DPE1.2	Transformação digital	
DPE1.3	Governança institucional	
DPE1.4	Governança de TI	
DPE2	Quantas pessoas atuam com dedicação parcial para tratar de temas relacionados à:	0 / 1 / 2 ou mais
DPE2.1	Inovação	
DPE2.2	Transformação digital	
DPE2.3	Governança institucional	
DPE2.4	Governança de TI	
DPE3	A instituição possui programa de capacitação contínua disponível para servidores que trabalham com transformação digital e inovação?	Sim / Não
DPE4	A instituição possui programa de capacitação contínua disponível para servidores da área de TI e Inovação?	Sim / Não
DPE5	Há um plano de carreira ou incentivos específicos para servidores da área de TI e Inovação?	Sim / Não

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DPE6	A instituição possui programa de capacitação contínua em alfabetização e transformação digital abrangente para todos os colaboradores?	Sim / Não
5.4.	DIMENSÃO GOVERNANÇA	
DG01	O planejamento estratégico da instituição possui ações específicas previstas voltadas para o incremento da automação dos processos de negócio e do uso de tecnologias digitais?	Sim / Não
DG02	A instituição possui indicadores que mensuram de forma contínua o uso de ferramentas digitais disponibilizadas aos seus membros e servidores, a fim de aferir o engajamento?	Sim / Não
DG03	A instituição adota alguma metodologia ágil?	Não utilizado / Utiliza em poucos contextos / Utiliza em alguns contextos / Utiliza na maioria dos contextos / Utiliza em todos os contextos
DG03.1	Projetos institucionais	
DG03.2	Projetos de TI	
DG03.3	Desenvolvimento de sistemas	
DG04	A instituição adota boas práticas de mercado para a gestão de serviços?	
DG04.1	Serviços institucionais	Sim / Não
DG04.2	Serviços de TI	Sim / Não
5.5.	DIMENSÃO LIDERANÇA	
DLI1	A alta administração (PGJs, Subs/Vices e SGs) participou de alguma ação de capacitação/sensibilização sobre inovação e transformação digital nos últimos 3 anos?	Sim / Não
DLI2	A alta administração acompanha os resultados pretendidos para a gestão?	Sim / Não

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DLI3	Como está definida a política do teletrabalho/trabalho híbrido para servidores atualmente na instituição?	• Não permitido • Permitido de forma limitada em todas as áreas • Permitido integralmente em algumas áreas
DLI4	Como está definida a política do teletrabalho/trabalho híbrido especificamente para servidores de TI atualmente na instituição?	• Não permitido • Permitido de forma limitada em todas as áreas • Permitido integralmente em algumas áreas
5.6.	DIMENSÃO OPERAÇÕES	
DOP1	Para qual(is) tema(s) a seguir a instituição possui estrutura específica?	
DOP1.1	Inovação	Sim / Não
DOP1.2	Transformação Digital	Sim / Não
DOP1.3	Governança Institucional	Sim / Não
DOP1.4	Governança de TI	Sim / Não
DOP2	Total de servidores efetivos de TI (de carreira).	0
DOP3	Total de servidores de TI (membros, servidores, terceirizados, residentes e estagiários)	0
DOP4	Total de usuários de TI (membros, servidores, terceirizados, residentes, estagiários)	0
DOP5	Orçamento total disponível para a instituição em cada exercício, incluindo os Fundos Especiais (como os Fundos de Reparelhamento)	R\$ 0
DOP6	Orçamento total executado pela instituição em cada exercício, incluindo os Fundos Especiais (como os Fundos de Reparelhamento)	R\$ 0

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DOP7	Do total respondido no item DOP6, quanto foi destinado a gastos com pessoal?	R\$ 0
DOP8	Do total respondido no item DOP7, quanto foi destinado a pessoal lotado na unidade de TI?	R\$ 0
DOP9	Do total respondido no item DOP6, quanto foi destinado a gastos de custeio em todo o MP?	R\$ 0
DOP10	Do total respondido no item DOP9, quanto foi destinado a gastos de custeio de TI, exceto telecomunicações (telefonia fixa e móvel, 4G, internet, redes WAN, redes LAN etc.)?	R\$ 0
DOP11	Do total respondido no item DOP9, quanto foi destinado apenas a gastos de custeio com telecomunicações (telefonia fixa e móvel, 4G, internet, redes WAN, redes LAN etc.)?	R\$ 0
DOP12	Do total respondido no item DOP6, quanto foi destinado a gastos de investimentos de TI?	R\$ 0
DOP13	Do total respondido no item DOP6, quanto foi destinado a gastos de arquitetura e engenharia (aquisições, obras, aluguéis de imóveis etc.)?	R\$ 0
5.7.	DIMENSÃO CULTURA	
DCT1	Há um processo de gestão de mudança mapeado e implementado na instituição?	Sim / Não
DCT2	Os resultados das transformações digitais implementadas são amplamente divulgados DCT2 dentro e fora da instituição?	Sim / Não
DCT3	Há algum programa implementado para que membros e servidores possam propor mudanças ou iniciativas voltadas à inovação?	• Sim - com processo definido de contínua avaliação, aceitação ou rejeição e feedback • Sim - envio de sugestões sem que haja um processo definido de avaliação, aceitação ou rejeição e feedback • Não há programa

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DCT4	Há mecanismos permanentes de reconhecimento ou premiação para iniciativas inovadoras institucionais?	Sim / Não
DCT5	A instituição possui um sistema que foi cedido a outro MP ou utiliza sistema desenvolvido para outro MP?	Sim / Não
5.8.	DIMENSÃO TECNOLOGIA	
DTI1	A unidade possui sistema para tramitação eletrônica dos processos da área-meio?	Sim / Não
DTI2	Esse sistema se integra com outros sistemas?	Sim / Não
DTI3	A unidade possui sistema para tramitação eletrônica dos processos e procedimentos da área-fim?	Sim / Não
DTI4	Esse sistema se integra com outros sistemas?	Sim / Não
DTI5	A instituição possui sistemas de painéis (BIs) para permitir uma atuação baseada em dados na área-meio e/ou área-fim?	Sim / Não
DTI6	A instituição monitora o acesso aos painéis para identificar se eles estão sendo utilizados pelas áreas demandantes?	Sim / Não
DTI9	Existe implementação de projetos com inteligência artificial para as áreas meio ou fim?	Sim / Não
DTI10	A instituição adota tecnologias que possibilitam entregas rápidas voltadas à automação de processos?	Sim / Não
DTI11	Qual é o grau de uso, pela instituição, das seguintes tecnologias?	Não utilizado / Pouco Utilizado / Utilizado / Muito utilizado / Faz parte do processo formal de trabalho
DTI11.1	Big Data analytics	
DTI11.2	Internet das Coisas (IoT)	
DTI11.3	Cibersegurança	
DTI11.4	Realidade Aumentada	

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DTI11.5	Computação em Nuvem	
DTI11.6	Tecnologias Móveis	
DTI11.7	Inteligência Artificial	
DTI11.8	Blockchain	
DTI11.9	Machine Learning, para automatizar tarefas cognitivas e analisar dados	
DTI11.10	Deep Learning	
DTI11.11	Assistentes de IA (geradores de códigos, textos, imagens, chatbots)	
DTI11.12	Agentes de IA	
DTI12	Selecione a opção que se adequa à instituição sobre o planejamento para utilização das seguintes tecnologias	Já utilizamos / Não planejamos usar de forma alguma / Planejamos utilizar em até 2 anos / Poderá ser usado mais tarde
DTI12.1	Big Data analytics	
DTI12.2	Internet das Coisas (IoT)	
DTI12.3	Cibersegurança	
DTI12.4	Realidade Aumentada	
DTI12.5	Computação em Nuvem	
DTI12.6	Tecnologias Móveis	
DTI12.7	Inteligência Artificial	
DTI12.8	Blockchain	
DTI12.9	Machine Learning, para automatizar tarefas cognitivas e analisar dados	
DTI12.10	Deep Learning	
DTI12.11	Assistentes de IA (geradores de códigos, textos, imagens, chatbots)	
DTI12.12	Agentes de IA	

Fonte: Freitas; Zattar; Silva Júnior; Pedrosa (2024).

Quadro 2 – Questionário das Coordenações de TIC

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
1.	IDENTIFICAÇÃO	
ID 1.1	Você é servidor vinculado a qual unidade?	STIC/PGR / CTIC/ Estados / SPPEA / Outro:
ID 1.2	Qual a área de atuação da sua unidade?	Atendimento / Desenvolvimento de Sistemas / Infraestrutura / Contratos e Orçamento / Segurança Cibernética / Gestão de Dados / Governança e Inovação / Outro
5.3.	DIMENSÃO PESSOAS	
DPE2	Quantas pessoas atuam com dedicação parcial para tratar de temas relacionados à:	0 / 1 a 3 / acima de 3
DPE2.1	Inovação	
DPE2.2	Transformação digital	
DPE2.3	Governança institucional	
DPE2.4	Governança de TI	
5.4.	DIMENSÃO GOVERNANÇA	
DG03	A sua equipe adota alguma metodologia ágil? Em qual grau?	Não utiliza / Utiliza em poucos contextos / Utiliza em alguns contextos / Utiliza na maioria dos contextos / Utiliza em todos os contextos
DG03.2	Projetos de TI	
DG03.3	Desenvolvimento de sistemas	
5.8.	DIMENSÃO TECNOLOGIA	
DTI11	Qual é o grau de uso das seguintes tecnologias no dia a dia da sua equipe?	Não utilizado / Pouco utilizado / Utilizado / Muito utilizado / Faz parte do processo formal de trabalho
DTI11.1	Big Data analytics	

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DTI11.2	Internet das Coisas (IoT)	
DTI11.3	Cibersegurança	
DTI11.4	Realidade Aumentada	
DTI11.5	Computação em Nuvem	
DTI11.6	Tecnologias Móveis	
DTI11.7	Inteligência Artificial	
DTI11.8	Blockchain	
DTI11.9	Machine Learning, para automatizar tarefas cognitivas e analisar dados	
DTI11.10	Deep Learning	
DTI11.11	Assistentes de IA (geradores de códigos, textos, imagens, chatbots)	
DTI11.12	Agentes de IA	
DTI12	Selecione a opção que se adequa a sua equipe sobre o planejamento para utilização das seguintes tecnologias	Já utilizamos / Não planejamos usar de forma alguma / Planejamos utilizar em até 2 anos / Poderá ser usado mais tarde
DTI12.1	Big Data analytics	
DTI12.2	Internet das Coisas (IoT)	
DTI12.4	Realidade Aumentada	
DTI12.5	Computação em Nuvem	
DTI12.6	Tecnologias Móveis	
DTI12.7	Inteligência Artificial	
DTI12.8	Blockchain	
DTI12.9	Machine Learning, para automatizar tarefas cognitivas e analisar dados	
DTI12.10	Deep Learning	
DTI12.11	Assistentes de IA (geradores de códigos, textos, imagens, chatbots)	
DTI12.12	Agentes de IA	

Fonte: adaptado de Freitas; Zattar; Silva Júnior; Pedrosa (2024).

Quadro 3 – Questionário dos Servidores de TIC

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
1.	IDENTIFICAÇÃO	
ID 1.1	Você é servidor da área de TIC do MPF?	Sim / Não
ID 1.2	Você é servidor vinculado a qual unidade?	STIC/PGR / CTIC/ Estados / SPPEA / Outro:
ID 1.3	Você tem cargo de chefia ou função de confiança?	Sim / Não
ID 1.4	Você atua na área de Governança ou/e inovação no MPF?	Sim / Não
5.1.*	DIMENSÃO ESTRATÉGIA DIGITAL	
DED1*	Qual seu grau de conhecimento da estratégia digital da instituição?	Desconheço / Conheço pouco / Tenho Conhecimento / Conheço bem / Conheço completamente
DED2*	Na sua opinião, a estratégia digital da instituição é amplamente divulgada?	Sim / Não
DED3*	Na sua opinião, a estratégia digital tem significativa influência nas prioridades e ações definidas pela gestão na sua área de atuação?	Sim / Não
DED4*	Você já teve a oportunidade de opinar ou contribuir sobre a estratégia digital do MPF?	Sim / Não
5.3.	DIMENSÃO PESSOAS	
DPE3	A instituição possui programa de capacitação contínua disponível para servidores que trabalham com transformação digital e inovação?	Sim / Não
DPE4*	Você conhece a existência de algum programa de capacitação contínua disponível para servidores da área de TI e Inovação do MPF?	Sim / Não

CÓDIGO	QUESTÃO	RESPOSTAS POSSÍVEIS
DPE5*	Você conhece algum plano institucional de carreira ou incentivos específicos para servidores da área de TI e Inovação já implantados no MPF?	Sim / Não
DPE6*	Você conhece algum programa institucional de capacitação contínua em alfabetização e transformação digital abrangente para todos os colaboradores do MPF?	Sim / Não
5.7.	DIMENSÃO CULTURA	
DCT1*	Você conhece o processo de gestão de mudança da instituição?	Sim / Não
DCT2*	Você acredita que os resultados das transformações digitais implementadas são amplamente divulgados dentro e fora da instituição?	Sim / Não
DCT3*	Você conhece algum meio onde possa propor mudanças ou iniciativas voltadas à inovação?	Sim - com processo definido de contínua avaliação, aceitação ou rejeição e feedback / Sim - envio de sugestões sem que haja um processo definido de avaliação, aceitação ou rejeição e feedback / Não há programa
DCT4*	Na sua opinião, o MPF tem mecanismos permanentes de reconhecimento ou premiação para iniciativas inovadoras institucionais?	Sim / Não

Fonte: adaptado de Freitas; Zattar; Silva Júnior; Pedrosa (2024).

Governança de TI em escolas de governo: um estudo sobre diretrizes estratégicas para tecnologias críticas

IT governance in government schools: a study on strategic guidelines for critical technologies

DOI: https://doi.org/10.63601/978-65-88299-52-4_8

Henderson Rogers Melo da Silva

Especialista em Docência na Educação Profissional e Tecnológica pelo Instituto Federal do Espírito Santo (IFES). Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Gestão de Instituições Públicas pelo Instituto Federal de Rondônia (IFRO). MBA Profissional em Sistemas de Informação pela Escola Superior Aberta do Brasil (ESAB). Pós-graduando em Didática, Práticas de Ensino e Tecnologias Educacionais pela Universidade Federal dos Vales do Jequitinhonha e Mucuri (UFVJM). Graduado em Análise e Desenvolvimento de Sistemas pela Pitágoras UNOPAR. Servidor do Ministério Público do Estado de Alagoas (MPAL).

Resumo: A transformação digital impôs às escolas de governo do Ministério Público – Escolas Superiores do Ministério Público (ESMPs) e Centros de Estudos e Aperfeiçoamento Funcional (CEAFs) – uma dependência crítica de Ambientes Virtuais de Aprendizagem (AVA) para a continuidade de sua missão institucional de capacitação. No entanto, observa-se frequentemente um descompasso estratégico entre a relevância pedagógica dessas ferramentas e a priorização na alocação de recursos tecnológicos. O objetivo deste estudo foi analisar a interseção entre a governança de TI e a identificação de tecnologias críticas nessas instituições, visando propor diretrizes para mitigar o desalinhamento entre a TI e a área finalística. A metodologia adotou uma abordagem qualitativa de natureza exploratório-descritiva, operacionalizada através de revisão bibliográfica e análise documental dos Planos Diretores de Tecnologia da Informação (PDTI) e portais institucionais de unidades selecionadas do Ministério Público. Os resultados evidenciaram um paradoxo de priorização: embora o AVA (predominantemente Moodle) constitua a tecnologia central para o

negócio das escolas, os mecanismos de governança tendem a direcionar investimentos massivos para infraestrutura de suporte e sistemas administrativos, subestimando a criticidade do ensino a distância. Conclui-se que a eficácia da governança depende do fortalecimento do papel das Diretorias das Escolas e CEAFs, capazes de influenciar a definição do Plano Diretor de Tecnologia da Informação (PDTI). Como contribuição, este estudo apresenta um conjunto de diretrizes estratégicas para orientar os Comitês de TI na reclassificação dos ativos educacionais, assegurando a entrega de valor público.

Palavras-chave: governança em TI; tecnologias críticas; escolas de governo; gestão pública; educação a distância; Moodle.

Abstract: *Digital transformation has imposed on the Government Schools of the Public Prosecutor's Office (ESMPs and CEAFs) a critical dependence on Virtual Learning Environments (VLE) for the continuity of their institutional training mission. However, a strategic mismatch is often observed between the pedagogical relevance of these tools and the prioritization in the allocation of technological resources. The objective of this study was to analyze the intersection between IT Governance and the identification of critical technologies in these institutions, aiming to propose guidelines to mitigate the misalignment between IT and the core business area. The methodology adopted a qualitative, exploratory-descriptive approach, operationalized through a literature review and documentary analysis of Information Technology Master Plans (PDTI) and institutional portals of selected units of the Public Prosecutor's Office. The results evidenced a prioritization paradox: although the VLE (predominantly Moodle) constitutes the central technology for the schools' business, governance mechanisms tend to direct massive investments toward support infrastructure and administrative systems, underestimating the criticality of distance education. It is concluded that governance effectiveness depends on strengthening the role of School Directorates and CEAFs, capable of influencing the definition of the Information Technology Master Plan (PDTI). As a contribution, the work presents a set of strategic guidelines to guide IT Committees in the reclassification of educational assets, ensuring the delivery of public value.*

Keywords: *IT governance; critical technologies; government schools; public management; distance education; Moodle.*

1 Introdução

A Emenda Constitucional n. 19 apresenta instituições de ensino sob o termo “escolas de governo” como responsáveis pela “formação e o aperfeiçoamento dos servidores públicos” da União, dos Estados e do Distrito Federal (Brasil, 1988). A Administração Pública, assim, se vale dessas escolas para a capacitação, qualificação e aperfeiçoamento funcional para aprimorar as habilidades no serviço público de seus

servidores no âmbito do Poder Executivo. Com o mesmo intuito, os poderes Legislativo e Judiciário mantêm instituições similares tais como Escolas de Magistratura e Escolas do Legislativo.

O Ministério Público (MP), órgão fundamental para a Justiça, a quem é atribuída a responsabilidade de defender a ordem jurídica, o regime democrático e os direitos sociais e individuais indisponíveis (art. 127, *caput*, CF 1988), possui autonomia administrativa, funcional e financeira. Não fazendo parte dos três poderes (Executivo, Legislativo e Judiciário), ele é conhecido como “quarto poder” (Macedo Jr., 1999, p. 248) por alguns autores e, do mesmo modo que as instituições dos poderes constitucionais, possui a necessidade de manter a capacitação funcional de seus integrantes, missão que depende cada vez mais de soluções tecnológicas robustas, integradas e seguras.

1.1 O Ministério Público e o papel estratégico das escolas de governo

As escolas de governo (EGs) desempenham um papel fundamental na formação, na valorização do servidor público, no desenvolvimento de suas habilidades, na atualização e aquisição de novos conhecimentos a fim de que o serviço público seja aprimorado periodicamente. Aires *et al.* (2014, p. 1) confirmam ao indicarem que as “escolas de governo têm papel significativo na vida do servidor público, valorizando-o e qualificando-o para a construção de uma nova imagem do serviço público”. Essas instituições são essenciais para capacitar a função pública, agindo como um vetor de resistência a técnicas administrativas ultrapassadas e impulsionando a renovação constante do quadro funcional do Estado.

No âmbito do Ministério Público brasileiro, essa demanda se estende à Escola Superior do Ministério Público (ESMP) e/ou ao Centro de Aperfeiçoamento Funcional (CEAF), responsáveis pela formação contínua de membros e servidores, além de estagiários, voluntários e até da sociedade em geral, para os casos de cursos de extensão, eventos e congêneres. Essas escolas institucionais do MP fortalecem a atuação institucional ao promoverem a qualificação profissional alinhada às exigências contemporâneas, especialmente no contexto de transformação digital e crescente complexidade das funções ministeriais.

1.2 A Transformação Digital

A Transformação Digital (TD) é uma realidade no setor público na busca pelo aprimoramento da qualidade dos serviços prestados à sociedade por meio das Tecnologias da Informação e Comunicação (TICs). Albertin e Albertin (2021, p. 27) ratificam essa informação ao relatarem que “transformação digital pode ser entendida como a aplicação de inovação digital para realizar algo novo, diferente e melhor, gerando valor para a sociedade e para as empresas”. Desse modo, apesar de esse processo não ser promovido apenas com a aplicação da tecnologia, pode-se traduzir que, através da transformação digital, é possível ocorrer uma melhoria na geração de valor para o público-alvo da organização.

Vale ressaltar que a transformação para a era digital envolve, mais do que um *upgrade* na infraestrutura de TI, uma governança eficaz que oriente o uso estratégico dos recursos de Tecnologia da Informação e Comunicação. Como afirma Rogers (2017, p. 8), “transformar-se para a era digital exige que o negócio atualize sua mentalidade estratégica, muito mais que sua infraestrutura de TI”. Essa transformação não requer apenas investimentos em tecnologias, mas também uma governança eficaz que oriente a priorização e o uso estratégico dos recursos de Tecnologia da Informação e Comunicação.

1.3 A governança de TI no setor público

A governança de tecnologia da informação (GTI) está além da gestão de *hardware* e *software*; consiste na liderança, na estrutura e nos processos que assegurem que o uso da TI sustente e amplie os objetivos estratégicos da organização. No contexto do Ministério Público, a Resolução do CNMP n. 171/2017, que institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP), define explicitamente, em seu art. 2º, inciso VI, a governança de TI como um conjunto de elementos que “assegurem que a TI sustente e estenda as estratégias e os objetivos organizacionais, mantendo riscos em níveis aceitáveis e em conformidade com normativos regulatórios internos e externos” (CNMP, 2017b).

Conforme a norma ABNT NBR ISO/IEC 38500:2025 (2025, p. 8, 11), a governança de TI é um “sistema pelo qual o uso atual e futuro da TI é direcionado” e um “subconjunto da governança organizacional”.

Tal perspectiva confere à governança de TI um papel estratégico, bem como um elo, assegurando que os investimentos em TIC sejam capacidades digitais alinhadas ao cumprimento da missão institucional, e não apenas meros gastos.

Assim, a governança de TI é compreendida como um conjunto de processos e estruturas que garantem que a TI sustente e amplie os objetivos estratégicos das organizações, inclusive as do setor público. Heindrickson e Santos Jr. (2014) indicam que essa é uma área de estudos relativamente nova que tem atraído bastante atenção, tendo em vista o papel cada vez mais relevante da TI para as organizações públicas ou privadas, e altamente relevante para a melhoria da prestação de serviços públicos.

Para que os CEAFs e ESMPs possam contribuir de forma efetiva com a missão institucional do Ministério Público, é essencial que disponham de práticas consistentes de governança de TI. A adoção de processos bem definidos, alinhados às necessidades estratégicas da instituição, permite que essas unidades de formação atuem com maior eficiência, inovação e segurança. Com isso, fortalece-se não apenas a capacitação funcional de membros e servidores, mas também a qualidade dos serviços prestados à sociedade.

1.4 Objetivo

Este estudo tem o intuito de analisar como a identificação de tecnologias críticas e a proposição de diretrizes estratégicas podem orientar decisões de governança de TI em escolas de governo, com foco nos CEAFs e nas ESMPs, a fim de apoiar a missão institucional do MP, de modo a preencher uma lacuna na literatura acadêmica.

2 Revisão de literatura

Na literatura, outros termos se aplicam às escolas de governo. O CNMP, por exemplo, as chama de escolas institucionais. Levando em consideração a União, os Estados e o Distrito Federal, os Ministérios Públicos utilizam termos como CEAF – Centro de Aperfeiçoamento Funcional (cerca de 50%), ESMP – Escola Superior do Ministério Público (cerca de 32%) e, em casos específicos, ESMP-CEAF (MPCE),

ou ainda Escola Institucional do MP (MPTO), Escola de Governo (MPRJ) e CESAF¹-ESMP (MPTO).

A entrega finalística das escolas de governo, sejam do Ministério Público, sejam de um dos poderes constitucionais, sempre é a capacitação dos servidores públicos de sua esfera. Isso ocorre por meio de cursos, seminários, capacitações diversas, entre outros eventos, que visam o desenvolvimento dos servidores, quer sejam efetivos, comissionados, ou seus demais colaboradores. Historicamente, tais capacitações sempre ocorreram presencialmente, em auditórios ou salas de aula com infraestrutura tradicional, tais como projetores de vídeo, computadores, quadros etc. Alguns sistemas até poderiam ser usados, sem muita abrangência ou utilização por parte dos discentes.

Com a chegada da pandemia de covid-19, em virtude da necessidade de distanciamento social, o cenário foi drasticamente alterado. A transformação digital foi acelerada, de modo que a modalidade Educação a Distância foi amplamente implementada pelas instituições de ensino de um modo geral, incluindo as escolas institucionais, a fim de que houvesse a continuidade de serviços prestados, de capacitação e desenvolvimento funcional, o que evidenciou cada vez mais a dependência do setor público dos recursos tecnológicos.

Assim, o Ambiente Virtual de Aprendizagem (AVA), também conhecido como LMS (*Learning Management System*) – um sistema baseado em interface *web* que permite a interação entre alunos e professores simulando uma sala de aula virtual, com a capacidade de armazenar e compartilhar materiais digitais, conteúdos de aulas, atividades e avaliações, entre outras ferramentas de ensino-aprendizagem – emergiu como uma tecnologia crítica. Sendo uma plataforma online que simula uma sala de aula virtual, a dependência tecnológica é constante. A entrega finalística da capacitação se torna impossível caso o AVA e/ou as ferramentas auxiliares não estejam no ar. Assim, a disponibilidade, a segurança e a confiabilidade do AVA são vitais para as escolas de governo, tornando esse um dos principais pontos a serem considerados para a governança de TI.

Visando a geração de valor público, entendido, segundo a OCDE (OECD, 2019, p. 27), como aquilo que é valorizado pelo público ou benéfico para a coletividade, avaliado por critérios como transparência e

1 CESAF: Centro de Estudos e Aperfeiçoamento Profissional.

justiça, e capaz de superar interesses individuais em favor de um propósito comum, os CEAFs e ESMPs devem priorizar uma governança de TI voltada à capacidade de entrega e à resiliência desse tipo de plataforma.

2.1 Plano Diretor de Tecnologia da Informação

O órgão do então Ministério do Planejamento, Orçamento e Gestão do Poder Executivo Federal, responsável pela normatização de assuntos de Tecnologia da Informação – Secretaria de Logística e Tecnologia da Informação (SLTI) –, emitiu, em 11 de setembro de 2014, a Instrução Normativa (IN) IN SLTI 04/2014 (Brasil, 2014), que define Plano Diretor de Tecnologia da Informação (PDTI) como

instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período (cap. I, art. 2º, inc. XXVII).

O PDTI consolida-se como o instrumento tático que concretiza a direção estratégica definida pelo Plano Estratégico Institucional (PEI) e pelo Plano Estratégico de TI (PETI). O Plano Diretor de TI emerge, então, como o instrumento tático e operacional que traduz essa direção em um rol de ações concretas e priorizadas. No âmbito do MP, a Resolução CNMP n. 171/2017 (Brasil, 2017b) reitera essa hierarquia, estabelecendo que o PDTI é um desdobramento do PETI e que deve conter as ações necessárias para o alcance dos objetivos estratégicos definidos (arts. 11 e 12).

Assim, o PDTI é uma ferramenta de governança de TI que atende às necessidades de TI em uma organização, por meio de metas, ações e projetos, através do qual poderiam ser analisadas as prioridades de investimento em relação às tecnologias críticas das escolas de governo dos MPs.

2.2 Tecnologias críticas

A noção de tecnologia crítica refere-se a qualquer sistema, infraestrutura ou aplicação que, em caso de falha, interrupção ou comprometimento, tenha o potencial de paralisar as funções essenciais de uma organização, comprometendo a entrega de seu valor e o cumprimento de sua missão institucional. A identificação dessas tecnologias é um passo

fundamental para a governança de TI, em cujo ciclo está inclusa a etapa de priorização de tecnologias/processos ou outros fatores e alocação de recursos, a fim de haver a mitigação de riscos (Prado *et al.*, p. 34006).

Nas Escolas Institucionais do Ministério Público (ESMPs e CEAFs), as tecnologias críticas são aquelas que garantem a continuidade da capacitação funcional, que é o cerne do negócio da escola. Empiricamente, a pesquisa identificou que a Infraestrutura de TI e o Ambiente Virtual de Aprendizagem (AVA) são as tecnologias mais críticas para a entrega de valor. A infraestrutura de rede – incluindo servidores, storage, backups e segurança cibernética – é crítica por ser a base de sustentação de todos os sistemas, incluindo o AVA. O Ambiente Virtual de Aprendizagem, por sua vez, assume a criticidade máxima no cenário de Transformação Digital, atuando como o principal canal de execução da missão pedagógica da escola. A indisponibilidade de um, de outro, ou de ambos inviabiliza a entrega do serviço finalístico da instituição, justificando sua prioridade na governança de TI.

2.3 Governança de TI e a criticidade do AVA

A governança de TI no setor público precisa ser vista como um componente inseparável da missão institucional, garantindo que o uso da tecnologia contribua positivamente para o desempenho da organização (ABNT, 2025, p. 10). Nesse contexto, a identificação e a priorização de tecnologias críticas tornam-se etapas fundamentais de um processo eficaz de governança que, por sua vez, impulsiona o desempenho de TI. Para operacionalizar essa efetividade, Heindrickson e Santos Jr. (2014) destacam a interdependência de três mecanismos clássicos: o Comitê de TI, responsável pela decisão estratégica; o Gestor da Solução de TI, definido como a unidade de negócio que demanda e utiliza a tecnologia; e o Processo de Gestão de Portfólio de Investimentos, que seleciona e prioriza os projetos.

No contexto específico do Ministério Público brasileiro, esses mecanismos teóricos possuem correlações práticas bem definidas. O Comitê de TI materializa-se usualmente como o Comitê Estratégico de Tecnologia da Informação (CETI); o Processo de Gestão de Portfólio de Investimentos concretiza-se na elaboração e execução do Plano Diretor de Tecnologia da Informação (PDTI); e o Gestor da Solução deve ser

representado pelas Diretorias das escolas de governo (CEAFs e ESMPs), visto que são as unidades que detêm o interesse finalístico nas tecnologias educacionais. Segundo o modelo dos autores, a atuação eficaz do Comitê e do Gestor da Solução só gera valor efetivo se mediada por um processo de portfólio robusto.

Portanto, a qualidade desse processo influencia diretamente a capacidade do Comitê e dos Gestores de garantirem a efetividade da governança. A ausência de critérios claros para a priorização do AVA no PDTI pode comprometer os investimentos públicos em TIC, pois a decisão de alocação de recursos deve ser uma tradução direta da criticidade do sistema para a missão institucional. Assim, para o sucesso da governança de TI no MP, é imperativo que a criticidade do AVA esteja explicitamente refletida nos critérios de priorização do PDTI, assegurando que a tecnologia suporte adequadamente a função de capacitação.

2.4 O Conselho Nacional do Ministério Público (CNMP) e as escolas institucionais do MP

O Conselho Nacional do Ministério Público (CNMP), instituído pela Emenda Constitucional n. 45/2004 como órgão responsável pelo controle da atuação administrativa e financeira do Ministério Público e pela fiscalização do cumprimento dos deveres funcionais de seus membros, conforme dispõe o art. 130-A, § 2º (Brasil, 2004), emitiu a Recomendação CN-CNMP n. 2, de 4 de julho de 2017 (Brasil, 2017a), que estabelece diretrizes para a estruturação e a atuação das Escolas Institucionais do Ministério Público brasileiro, definindo parâmetros mínimos para o adequado funcionamento das Escolas Institucionais.

Entre as recomendações apresentadas, é válido destacar, em seu art. 2º, a orientação para que as escolas disponham de auditório, salas de aula, biblioteca e até mesmo veículos necessários para as atividades institucionais. Além disso, sugere-se, em seu art. 3º, a implantação de estrutura organizacional adequada que assegure a autonomia, a eficiência e a democratização nos processos decisórios da instituição, por meio de um corpo técnico composto por especialistas em Pedagogia, Administração, Contabilidade e Tecnologia da Informação. Por fim, o art. 4º recomenda a adoção de estratégias e metodologias voltadas à divulgação das atividades acadêmicas, à difusão cultural e à interação

com a sociedade e a comunidade científica, devendo, para isso, ter uma Assessoria de Comunicação, seja do próprio órgão auxiliar, seja uma disponibilizada pela Administração Superior, bem como criar um periódico, preferencialmente científico, em formato digital e/ou impresso, além de um website institucional.

A recomendação explícita da presença de especialistas em TI e a manutenção de plataformas digitais (como a página na Internet e o periódico digital) reforça a tese central deste estudo: as tecnologias de informação, incluindo desde a infraestrutura de serviços e servidores de rede, computadores e dispositivos portáteis, até o *peopleware* – as pessoas envolvidas em um sistema computacional (usuários, desenvolvedores etc.) –, não são meros suportes, mas sim fazem parte do conjunto funcional de tecnologias críticas para a própria existência e operação das Escolas do MP, demandando, portanto, uma abordagem específica de governança de TI focada em continuidade, segurança e priorização estratégica.

2.5 Lacunas na literatura e contribuições da pesquisa

A literatura especializada sobre governança de TI no setor público, a exemplo de Mendonça *et al.* (2013), embora ofereça uma importante avaliação sobre a participação de gestores de Tecnologia da Informação (TI) no processo decisório estratégico e no alinhamento de TI em organizações públicas e privadas, em geral, evidenciam a ausência de pesquisas sobre a identificação de tecnologias críticas e os critérios de priorização dessas tecnologias em escolas de governo, em especial, do Ministério Público brasileiro.

Uma consulta exploratória nas bases de dados da Capes, Google Scholar e SciELO, utilizando as palavras-chave (“governança de TI” OR “IT Governance”) AND (“Escolas de Governo” OR “Escola de Governo” OR “Government Schools”) AND (“Tecnologias Críticas” OR “Critical Technologies”), não obteve nenhum resultado no SciELO e no Google Scholar, e resultou em um número limitado de 25 artigos entre os anos de 2020 e 2025 no Periódicos Capes.

Desses artigos, dois combinam o tema governança de TI com o contexto do serviço público, focando em avaliação e direcionamento

estratégico, e cinco abordam a contextualização em instituições de ensino públicas. Embora a governança de TI seja amplamente reconhecida como um imperativo estratégico para o sucesso organizacional, sua aplicação eficaz e o foco em prioridades tecnológicas no Setor Público brasileiro representam um campo em desenvolvimento.

Os resultados dessa última pesquisa confirmam essa tendência, indicando um volume crescente de estudos sobre governança de TI em contextos como Universidades Federais e Administração Pública, frequentemente alinhados com diretrizes de órgãos como a Escola Nacional de Administração Pública (Enap). Contudo, percebe-se um hiato significativo na literatura que aborda a convergência entre a governança de TI e a identificação de tecnologias críticas e de diretrizes estratégicas especificamente nas escolas de governo voltadas para a atuação do Ministério Público, como os CEAFs e ESMPs. Como essa ausência pode limitar a compreensão de como a governança de TI se traduz em escolhas concretas sobre a alocação de investimentos e o foco em inovações tecnológicas específicas, um aspecto fundamental para instituições como as escolas de governo dos MPs, a baixa representatividade de trabalhos empíricos e técnicos reforça a originalidade deste estudo e a urgência em propor diretrizes estratégicas.

3 Metodologia

Foram utilizados como instrumentos a análise documental, revisão bibliográfica, de acordo com informações presentes nos meios de comunicação dos CEAFs ou ESMPs e, quando ausentes, dos MPs. A população-alvo compreende os CEAFs e ESMPs do Ministério Público brasileiro. A amostragem é intencional e não probabilística, centrada nas instituições que possuem estrutura formalizada de governança de TI, como a ESMPU, MPDFT, MPAP e MPAC.

A análise comparativa dos dados coletados confere robustez ao estudo, permitindo captar tanto aspectos normativos quanto práticos da governança de TI. A abordagem qualitativa e exploratória é adequada diante do contexto apresentado. A pesquisa tem caráter descritivo e exploratório. Esse arranjo permite cruzar evidências institucionais formais com percepções e práticas comparadas em diferentes escolas do MP.

Foram utilizadas ferramentas de inteligência artificial como apoio para otimização do processo de pesquisa, para a descoberta de literaturas relevantes e fundamentação teórica pelo SciSpace, estruturação de ideias, tradução de obras e artigos, revisão linguística, refinamento de *strings* de pesquisa, a fim de reunir fontes bibliográficas pertinentes ao trabalho e auxiliar no fichamento de artigos científicos para organizar leituras e separar trechos e citações importantes. Foram usadas as seguintes ferramentas: ChatGPT GPT-4o, Claude Sonnet 4, Google Gemini 2.5 Flash, e Google NotebookLM.

Todo resultado do uso das ferramentas de IA foi validado com a checagem da exatidão das informações, incluindo a referência bibliográfica, bem como a realização de uma avaliação detalhada e analítica das informações obtidas por esse meio. Ademais, não foram compartilhados dados sensíveis, e o texto adquirido foi devidamente revisado e editado antes de seu uso na pesquisa, além de não terem sido utilizados dados primários gerados por tais ferramentas.

4 Apresentação e discussão dos resultados

Foi realizado o levantamento inicial nos 26 Ministérios Públicos Estaduais (MPes) e no MPDFT, que revelou o cenário da tecnologia crítica para capacitação, além da Escola Superior do MPU, conforme o Quadro 1.

Quadro 1 – Escolas Institucionais do MP, AVAs e PDTI

MP	NOMENCLATURA DA ESCOLA	AVA (LINKS)	DOCUMENTAÇÃO (PDTI ETC.)
MPAC	CEAF-MPAC	Moodle: https://eventos.mpac.mp.br/	PDTI: https://www.mpac.mp.br/wp-content/uploads/PDTI-MPAC-171-2022-2024-CETI-v-Final-p.-assinatura5D-assinado-1-1.pdf
MPAL	ESMP	Moodle: https://ead.mpal.mp.br/	Inexistente

MP	NOMENCLATURA DA ESCOLA	AVA (LINKS)	DOCUMENTAÇÃO (PDTI ETC.)
MPAP	CEAF	Moodle: https://www3.mpap.mp.br/educ/login/index.php	PDTI: https://diqwlbtn1ltnj.cloudfront.net/Portal%20da%20TI/npQ1SQiamvxnoGKg5RjdKgx1BclZgSIpnF1bTnv.pdf
MPAM	CEAF	Moodle: https://ead.mpam.mp.br/	Regimento: https://www.mpam.mp.br/images/CEAF/Regimento_Interno_183.2005.pdf Regimento Revista Jurídica: https://www.mpam.mp.br/images/CEAF/reg_revista.pdf
MPBA	CEAF	Site institucional: https://ceaf.mpba.mp.br/ Moodle: https://ead.mpba.mp.br/	PDTI não encontrado
MPCE	ESMP-CEAF	Moodle: https://cursos.mpce.mp.br/	PDTI não encontrado
MPDFT	MPDFT EaD	Moodle: https://www.mpdft.mp.br/ead/login/index.php	PETI do MPDFT: https://www.mpdft.mp.br/portal/images/pdf/gestao_estrategica/peti/PETI_2021_2026.pdf PDTI 2025: https://www.mpdft.mp.br/portal/images/pdti_2025.pdf
MPES	CEAF	CEAF Cursos (não é Moodle): https://ceafcursos.mpes.mp.br/	PGA MPES: https://mpes.mp.br/wp-content/uploads/2025/04/relatorio_PGA_24-25_v5.pdf Relatório de Gestão: https://mpes.mp.br/wp-content/uploads/2025/04/Relatorio_Gestao_2024_v0.pdf

MP	NOMENCLATURA DA ESCOLA	AVA (LINKS)	DOCUMENTAÇÃO (PDTI ETC.)
MPGO	ESMP	Site ESMP: https://www.mpggo.mp.br/portal/pagina/escola-superior-do-ministerio-publico Moodle: https://esump.mpggo.mp.br/	PDTI não encontrado
MPMA	ESMP	Site: https://www.mpma.mp.br/escola-superior-mpma/ Moodle: https://esmp.mpma.mp.br/	PDTI (2015-2016): https://cdn-0.mpma.mp.br/publicacoes/17531/03155f02032b19690476fccd67defb9b.pdf
MPMT	CEAF	Site: https://ceaf.mpmpt.mp.br/ Moodle: https://ceafead.mpmpt.mp.br/login/index.php	PDTI não encontrado
MPMS	ESMP	Site: https://escola.mpms.mp.br/ Moodle: https://ead.mpms.mp.br/	PDTI (2020-2022): https://mpms.mp.br/anexo/MDExMDU3MjAzNjE3NTdhNDY5M2JlMTlkNDYlZjAzZTgzYTUwYWUzMWYzMzMtMDI4
MPMG	CEAF	Site: https://www.mpmg.mp.br/portal/menu/conheca-o-mpmg/centro-de-estudos-e-aperfeicoamento-funcional/ Moodle: https://moodle-ceaf.mpmg.mp.br/	Política de governança de TI: https://mpnormas.mpmg.mp.br/files/1/1/1-1-CB30-28-res_pgj_09_2019.pdf
MPPA	CEAF	AVA (não é Moodle): https://ceaf.mppa.mp.br/app/login	PDTI não encontrado

MP	NOMENCLATURA DA ESCOLA	AVA (LINKS)	DOCUMENTAÇÃO (PDTI ETC.)
MPPB	CEAF	Site: https://www.mppb.mp.br/index.php/pt/mppb/orgaos-auxiliares/ceaf Moodle: http://moodle.mppb.mp.br/	PDTI não encontrado
MPPR	ESMP	Site: https://site.mppr.mp.br/escolasuperior https://sites.google.com/mppr.mp.br/trilhas-de-aprendizagem/ Moodle: https://ead.mppr.mp.br/login/index.php	Citado no site, mas não encontrado
MPPE	ESMP	Site: https://portal.mppe.mp.br/escola-superior Moodle: https://ead.mppe.mp.br/	Citado no site, mas não encontrado.
MPPI	CEAF	Site: https://www.mppi.mp.br/internet/ceaf/ Eventos: https://aplicativos3.mppi.mp.br/eventosceaf/publico/login.xhtml Moodle: https://moodle.mppi.mp.br/login/index.php	Citado no site, mas não encontrado.
MPRJ	Escola de Governo	Site: https://ierbb.mprj.mp.br/ Moodle: https://ierbb-ead.mprj.mp.br/login/index.php	Citado no site, mas não encontrado.

MP	NOMENCLATURA DA ESCOLA	AVA (LINKS)	DOCUMENTAÇÃO (PDTI ETC.)
MPRN	CEAF	Site: https://www.mprn.mp.br/paginas/centro-de-estudos-e-aperfeicoamento-funcional/ Moodle: https://ava.mprn.mp.br/	Citado no site, mas não encontrado.
MPRS	CEAF	Site: https://www.mprs.mp.br/ceaf/ AVA (Não é Moodle): https://gestaoeducacional.mprs.mp.br/softexpert/login	Não encontrado
MPRO	ESMP	Site: https://www.mpro.mp.br/pages/conheca-mp/orgaos-auxiliares/empro AVA (não é Moodle): https://empro.mpro.mp.br/	Não encontrado
MPRR	CEAF	AVA (não é Moodle): https://ceaf.mprr.mp.br/	Não encontrado
MPSC	CEAF	Site: https://www.mpsc.mp.br/centro-de-estudos-e-aperfeicoamento Moodle: https://ead.mpsc.mp.br/	PDTI: https://www.mpsc.mp.br/atos-e-normas/detalhe?id=4063
MPSP	ESMP	Site: https://www.mpsp.mp.br/esmp AVA (não é Moodle): https://lector.live/esmp/subscribe/login	Citado no site, mas não encontrado.

MP	NOMENCLATURA DA ESCOLA	AVA (LINKS)	DOCUMENTAÇÃO (PDTI ETC.)
MPSE	ESMP	Site: https://www.mpse.mp.br/index.php/portal-da-escola-superior/ Inscrições: https://sistemas.mpse.mp.br/4.5/EventosESMP/Login.aspx	Não encontrado
MPTO	CESAF-ESMP	Site: https://mpto.mp.br/cesaf Moodle: https://eadcesaf.mpto.mp.br/login/index.php	Não encontrado
MPU	ESMPU	Site: https://escola.mpu.mp.br/ Moodle: https://ead.escola.mpu.mp.br/login/index.php	PDTI 2024-2025: https://escola.mpu.mp.br/a-escola/legislacao-e-regulamentos/pdti/pdti-2024-2025/PDTI_2024_2025.pdf

Fonte: próprio autor – pesquisa em sites institucionais dos Ministérios Públicos e escolas institucionais dos MPs (2025).

4.1 Análise descritiva do Quadro 1

O Quadro 1 é resultante da pesquisa realizada e lista a nomenclatura das escolas institucionais dos MPs (ESMP ou CEAF), o link do Ambiente Virtual de Aprendizagem como uma tecnologia crítica, o link da documentação referência para a análise, o Plano Diretor de Tecnologia da Informação (PDTI), ou o indicativo de que não foi encontrado, ou outra documentação relevante para a pesquisa.

Percebe-se, inicialmente, que, na maioria dos casos, não há PDTI na escola institucional do MP. Todavia, sendo um órgão auxiliar da instituição, a pesquisa incluiu os sites das próprias unidades dos MPs. Ademais, há casos em que o PDTI é disponibilizado, tal como no MPAC; há outros casos em que o PDTI foi citado no site institucional do MP ou em outra documentação disponibilizada pela instituição, mas não foi

encontrado, seja na página web, seja disponível para download, como no caso do MPPE. Ainda, há situações em que o MP não elaborou a documentação, tal como o MPAL, e há casos em que o PDTI é antigo.

Parece haver uma alta incidência de PDTIs não encontrados. Apesar da grande importância desse plano, ele é ocultado, propositalmente ou não, ou arquivado de forma inadequada, aparentemente indo contra o princípio da Lei de Acesso à Informação (LAI). É possível que, nos casos em que o documento é citado em outros documentos, mas não disponibilizado no site em sua íntegra, haja o cuidado com a segurança da informação. Nesse caso, seria esperado que, a fim de manter conformidade com a transparência, os Ministérios Públicos publicassem versões executivas do PDTI, focadas no alinhamento estratégico, nas metas de transformação digital e na estimativa de resultados, excluindo detalhes técnicos sensíveis (inventário de ativos, topologia de rede, planos de mitigação de vulnerabilidades específicas etc).

4.1.1 AVA predominante

O diagnóstico empírico ressalta como AVA predominante o Moodle, sigla para Modular Object-Oriented Dinamic Learning Environment (Ambiente de Aprendizagem Dinâmico Modular e Orientado a Objetos), uma plataforma de ensino-aprendizagem de código aberto, iniciada em 1999 (Moodle, 2025), que se tornou o sistema de gerenciamento de aprendizado mais utilizado no mundo, inclusive por mais de 78% das escolas de governo dos Ministérios Públicos brasileiros (Quadro 1). Em outros casos, Ambientes Virtuais de Aprendizagem personalizados foram desenvolvidos para a instituição, como no caso do CEAF do MPRS, ou ainda, foi desenvolvido um sistema intermediário, que faz a interface com o usuário para cadastro e acesso inicial, integrado ao Moodle, que disponibiliza as ferramentas de gestão de educação, como no caso da Escola do MPSP.

4.2 Análise dos PDTIs e discussão

Percebeu-se relevante para a governança de TI a alta incidência de PDTIs não encontrados (70,3%) ou não vigentes (7,4%). Isso indica uma lacuna de transparência e, mais criticamente, uma potencial deficiência

na gestão e no planejamento formal dos recursos de TI que dão suporte à finalidade educacional dos MPs.

Para aprofundar a análise sobre a priorização de tecnologias críticas, foram selecionados os documentos disponíveis de quatro Escolas/MPs: ESMPU, MPDFT, MPAC e MPAP. A escolha das quatro instituições foi intencional, orientada por critérios que garantissem a consistência da comparação proposta. A presença de PDTIs atualizados e acessíveis ao público foi o fator principal e decisivo, já que muitas organizações consultadas não disponibilizavam esses documentos, o que inviabilizaria a análise.

Optou-se também por uma composição equilibrada da amostra, formada por 50% de instituições federais (ESMPU e MPDFT) e 50% de estaduais (MPAC e MPAP), permitindo comparar realidades administrativas e orçamentárias distintas. Além disso, considerou-se a diversidade das estratégias de infraestrutura tecnológica adotadas, que variam desde o investimento em soluções de nuvem até a priorização de redundância física ou o fortalecimento de sistemas internos.

Esse conjunto de características oferece um panorama suficientemente heterogêneo para examinar como cada instituição trata suas tecnologias consideradas críticas para o ensino. O foco da análise recaiu sobre o tratamento dado às escolas de governo dos MPs e às tecnologias críticas para capacitação (AVA) dentro dos seus Planos de Ação e Orçamento.

Quadro 2 – Análise comparativa dos PDTIs

PDTI	MENTÃO EXPLÍCITA À ESCOLA/CEAF	PROJETOS RELACIONADOS À CAPACITAÇÃO	TECNOLOGIAS CRÍTICAS PRIORIZADAS	ORÇAMENTO DA ESCOLA EM TI (PDTI)	COERÊNCIA CRÍTICO-ESTRATÉGICA
ESMPU (2024-2025)	Sim, ESMPU é o foco.	Implícito (Projetos genéricos, como “Integração das bases de dados de Atividades”)	Redes/Segurança (76% dos contratos ativos) e Oracle (92% de progresso)	Não detalhado (o documento é da Escola)	Foco em infraestrutura de TI (Redes/Segurança/Oracle) e terceirização de serviços, com projetos de melhoria do AVA diluídos ou ausentes no portfólio.
MPDFT (2025)	Sim, “MPDFT EaD” é um ponto no Mapa Estratégico.	Direto (IN22: Promover treinamentos sobre o uso de IA; IN18: Atualizar o Moodle)	Inteligência Artificial (JARVIS, ALFRED, Luminar1A, TINTENDO) e Processo Eletrônico	Não detalhado (PDTI da STI)	Foco em IA e Processo Eletrônico (atividade-fim) e IN22 e IN18 (Capacitação/AVA). Há ações de <i>Aprimoramento e Inovação</i> , mas sem a criticidade orçamentária do core do MP.

PDTI	MENTÃO EXPLÍCITA À ESCOLA/CEAF	PROJETOS RELACIONADOS À CAPACITAÇÃO	TECNOLOGIAS CRÍTICAS PRIORIZADAS	ORÇAMENTO DA ESCOLA EM TI (PDTI)	COERÊNCIA CRÍTICO-ESTRATÉGICA
MPAP (2024-2025)	Não (Apenas “Capacitação” em Iniciativas)	Implícito (“Promover a capacitação dos profissionais de TI”)	Nuvem (24,1% do investimento do DTI) e Segurança da Informação (medida: 70%)	Não detalhado (PDTI do DTI/CIII)	Reconhece a Capacitação como objetivo, mas os projetos de TI priorizam a migração para a Nuvem e Segurança Cibernética (necessidades globais do MP), sem alocar projetos específicos de desenvolvimento do AVA.
MPAC (2022-2024)	Sim, CEAF é mencionado como área de treinamento.	Direto (“Implementar o plano de capacitação de usuários e técnicos”)	Datacenter Secundário (Redundância) e SAJ/MP	Detalhado no QDD (Quadro de Detalhamento da Despesa)	O foco principal é o Datacenter Secundário e a redundância (prioridade máxima para a continuidade), que beneficia o AVA indiretamente. O AVA/CEAF é citado em ações de treinamento, mas não de infraestrutura crítica.

Fonte: próprio autor – análise dos PDTIs do MPAC (2022-2024), MPAP (2024-2025), MPDFT (2025) e ESMPU (2024-2025).

A análise dos PDTIs presente no Quadro 2 demonstra que todas as instituições reconhecem o Comitê de TI (ou órgão similar) e o alinhamento ao Planejamento Estratégico Institucional como essenciais, o que é um ponto forte da governança de TI. Todos os planos demonstram o reconhecimento da capacitação como um objetivo estratégico institucional, seja mencionando o AVA explicitamente (MPDFT), seja incluindo iniciativas de treinamento e estruturação da Escola (MPAP). As prioridades de investimento demonstram focos distintos. Enquanto o MPDFT alinha a TI da Escola com a inovação de ponta (IA e atualização do Moodle), sugerindo um alto grau de integração da área de ensino com a estratégia da TI; o MPAP, por ter recentemente migrado para a nuvem, concentra seu foco e recursos na segurança e resiliência da nova infraestrutura (Sustentação), o que, embora prudente, dilui o investimento em plataformas de ensino.

Em suma, a análise reforça que o PDTI, embora presente e formalizado, carece de um critério de ponderação específico que relacione o impacto da paralisação do AVA (tecnologia crítica de negócio) diretamente com a pontuação de prioridade, garantindo que o motor de entrega da escola receba o investimento compatível com sua importância estratégica. Em particular, o MPDFT se destaca por incorporar de forma ativa projetos de inteligência artificial e pela atualização do Moodle (AVA) em seu plano, mostrando um interesse proativo em relação às tecnologias emergentes. Essa orientação reforça o compromisso institucional com a modernização de seus ambientes digitais e com a ampliação das capacidades tecnológicas voltadas ao suporte das atividades educacionais e administrativas.

4.2.1 ESMPU (2024-2025)

A análise documental do Plano Diretor de Tecnologia da Informação (PDTI) 2024-2025 da ESMPU demonstra formalmente o alinhamento de seus objetivos de TI com a missão institucional de capacitação. Enquanto a Secretaria de TI da ESMPU possui como visão “ser reconhecida como unidade inovadora no uso da TI, especialmente nos aspectos educacionais”, a análise SWOT presente no documento apresenta como Oportunidades a “transformação digital”, “educação

híbrida” e “ecossistema educacional”, evidenciando o reconhecimento do papel das tecnologias educacionais, nesse caso, do AVA.

O portfólio de projetos de TI (anexo I do PDTI) em andamento com o maior progresso de execução confirma a priorização da infraestrutura, além de que a proposta orçamentária detalhada para 2024 ratifica a alocação de altos valores para sistemas de base, como o suporte ao SGBD Oracle (R\$ 526.500,00) e a renovação de garantia de *switches* de acesso e *core* (R\$ 300.000,00). Sabe-se que esses investimentos beneficiam o AVA indiretamente, ao garantir a estabilidade da infraestrutura, mas vale ressaltar que se percebe a ausência de uma rubrica de alto valor diretamente destinada à evolução, customização ou evolução do AVA.

Por sua vez, com relação aos contratos continuados, lista de monitoramento presente no anexo II do PDTI, percebe-se que 19 (76%) dos 25 contratos são voltados a redes e segurança, o que corrobora com a priorização de outras tecnologias críticas da ESMPU, evidenciando a boa governança de tecnologia da informação.

4.2.2 MPDFT (2025)

Apesar de não haver um PDTI específico para a Escola do MPDFT, o plano da instituição reconhece o Moodle como tecnologia de mercado relevante. A iniciativa IN18 – “Prospectar, adotar e manter sistemas externos e soluções de mercado” – prevê a ação A18.14 Moodle (“atualizar solução”). O plano ainda classifica essa ação como porte P, o que mostra que a priorização orçamentária e de esforço humano é menor em comparação a outros projetos. A instituição se destaca por incorporar ativamente projetos de IA e a atualização do Moodle (AVA) em seu plano, mostrando um interesse proativo em relação às tecnologias emergentes.

Entretanto, a ausência de uma métrica explícita e quantificável que relacione o impacto da paralisação do AVA diretamente com a prioridade de investimento sugere que o PDTI ainda carece de um critério de priorização específico para tecnologias críticas relacionadas à missão da escola de governo. A tendência observada é valorizar a infraestrutura e a atividade-fim do MP (processo eletrônico, forense), em detrimento da relevância do AVA, objeto de valor da escola.

4.2.3 MPAC (2022-2024)

No âmbito estadual do MP, semelhante ao MPDFT, não há PDTI na escola institucional do MPAC. Nos “Níveis de Prioridade para Ações de Governança – Anexo C”, como resposta ao CNMP, a instituição lista “CAPACITAÇÃO (treinamento de membros e servidores)” como extremamente prioritário. Apesar de não identificar o AVA como uma tecnologia crítica, a previsão de ação Implantação em Datacenter Secundário beneficia indiretamente a plataforma de gestão da educação. No entanto, a alta prioridade dada ao Datacenter Secundário (como uma tecnologia crítica de infraestrutura) em detrimento de um projeto de mesmo peso para o AVA (a tecnologia crítica de negócio) indica que a priorização visa o risco para toda a instituição do MPAC (indisponibilidade dos serviços).

4.2.4 MPAP (2024-2025)

Após a migração dos sistemas e aplicativos do MPAP para a nuvem, o investimento concentrou-se em estabilidade, segurança cibernética, escalabilidade, flexibilidade, automação e conectividade. Essa prioridade de investimento em infraestrutura, apesar de indiretamente beneficiar a escola institucional, não está descrito o investimento na tecnologia crítica que garante a entrega final da escola do MPAP. Além disso, o PDTI revela um investimento mínimo em capacitações: apenas 1,4% dos valores contratados foram em capacitações e, ainda assim, voltadas para a área de TI. Isso é evidenciado ainda mais quando o plano prevê investimentos em capacitações específicas e não em atividades de ensino, pesquisa e extensão promovidas para os integrantes do MP, o que demonstra um paradoxo de priorização, subestimando a criticidade do AVA.

4.3 Diretrizes estratégicas propostas

A governança de TI nas escolas de governo do Ministério Público prevê o alinhamento estratégico com segurança, infraestrutura e AVA operante. No entanto, a análise comparativa revelou uma oportunidade de aprimoramento no PDTI para garantir que o Ambiente Virtual de Aprendizagem (AVA) receba a prioridade compatível com sua natureza

de tecnologia crítica de negócio. As diretrizes a seguir visam apoiar os Comitês Estratégicos de TI (CETI) dessas instituições a traduzir a criticidade do AVA em ações de investimento concretas, elevando a qualidade do serviço educacional em consonância com as melhores práticas de governança de TI.

Sugere-se, portanto, que as escolas de governo do MP busquem adotar, ou avaliem a possibilidade de colocar em prática, de acordo com cada contexto, diretrizes e medidas voltadas ao fortalecimento da governança de tecnologia da informação com foco na continuidade e entrega dos serviços de capacitação. Primeiramente, ressalta-se a importância da elaboração de um processo formal e periódico para avaliar ou reavaliar a criticidade das tecnologias utilizadas nas escolas institucionais, considerando o surgimento de necessidades educacionais da escola e o impacto nos objetivos institucionais de ensino, pesquisa, extensão, entre outras, com o uso de métricas bem definidas para a avaliação, tais como a taxa de indisponibilidade tolerável do AVA.

Ademais, propõe-se a criação de um Comitê de governança de TI, contendo profissionais de múltiplas áreas, tais como: TI, Pedagogia, Administração e Contabilidade, conforme recomendação do CNMP, além de membro da Diretoria da Escola ou CEAf e de usuários selecionados, de modo a promover constante discussão sobre a priorização de investimentos que reflitam o alinhamento pedagógico e o valor estratégico dos projetos de TI.

Sugere-se, também, que a priorização de tecnologia e investimentos seja baseada na análise que considere risco financeiro, operacional e reputacional, e no impacto direto na capacidade de entrega de valor educacional, em consonância com os objetivos da escola de governo do MP. Por fim, destaca-se a importância do investimento contínuo em infraestrutura e segurança do AVA, reconhecendo-o como tecnologia crítica cuja estabilidade e desempenho devem ser permanentemente assegurados.

5 Considerações finais

A presente pesquisa buscou preencher uma lacuna notável na literatura, investigando a intersecção entre a governança de TI e a priorização de tecnologias críticas no contexto específico das escolas de

governo do Ministério Público (ESMPs e CEAFs). A análise detalhada dos PDTIs e da revisão de literatura demonstrou o papel estratégico dessas escolas no fortalecimento das capacidades estatais, missão que se tornou totalmente dependente das tecnologias de informação e comunicação no contexto da transformação digital.

O levantamento empírico, baseado na análise dos Planos Diretores de Tecnologia da Informação, identificou o Ambiente Virtual de Aprendizagem, em especial, a plataforma Moodle, como a tecnologia crítica central para a continuidade do negócio das escolas de governo do MP. Contudo, foi evidenciado um paradoxo de priorização na governança de TI dos MPs em geral: enquanto a capacidade de entrega da Escola depende do AVA, os recursos orçamentários e o foco dos projetos priorizam predominantemente a infraestrutura de suporte de TI do MP e os sistemas de atividade-fim. Isso sugere que a governança de TI, ao alocar recursos, tende a mitigar o risco geral da instituição, mas subestima a criticidade direta e contínua da plataforma de ensino, relegando a evolução do AVA a projetos de menor peso orçamentário.

A priorização dos investimentos revelou-se um elo mediador crucial na governança analisada. Observou-se que a eficácia dos mecanismos decisórios e de gestão depende intrinsecamente da qualidade do Plano Diretor de Tecnologia da Informação. A subestimação da criticidade do AVA nesse documento compromete a capacidade da governança de TI de gerar valor para a Escola de Governo do MP de forma otimizada, evidenciando que a atuação isolada de comitês ou gestores não é suficiente sem um método robusto de priorização que considere o impacto no negócio educacional.

Nessa linha, o presente artigo procedeu ao levantamento do arcabouço teórico que alicerça o estudo, realçando a importância do foco em processos críticos e apontando diretrizes concretas para aprimorar o Processo de Portfólio de Investimento, visando o alinhamento com a missão institucional. As diretrizes estratégicas sugeridas buscam ser o arcabouço prático do trabalho, oferecendo aos gestores de TI um conjunto de recomendações para que a governança de TI implemente uma cultura de priorização das tecnologias críticas das Escolas.

Em conclusão, a pesquisa demonstrou que a governança de TI nas Escolas do MP tem a oportunidade de evoluir, superando a

priorização implícita e adotando critérios explícitos que reflitam a criticidade e o impacto direto na missão de capacitação. A aplicação das diretrizes propostas reafirma o interesse do estudo e a sua contribuição para que as escolas institucionais do Ministério Público alcancem a excelência em gestão pública e a nota máxima na entrega de valor à sociedade, demonstrando, assim, a plena adequação aos objetivos acadêmicos.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 38500:2025**: Tecnologia da informação – Governança da TI para a organização. Rio de Janeiro: ABNT, 2025.

AIRES, Renan Felinto de Farias *et al.* Escolas de governo: o panorama brasileiro. **Revista de Administração Pública**, Rio de Janeiro, v. 48, n. 4, p. 1007-1027, jul./ago. 2014. DOI: <http://dx.doi.org/10.1590/0034-76121689>.

ALBERTIN, A; ALBERTIN, R. Transformação digital: gerando valor para o “novo futuro”. **GV-executivo**, v. 20, n. 1, jan./mar. 2021. Disponível em: <https://tinyurl.com/3dys448r>. Acesso em: 16 jun. 2025.

BRASIL. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. **Casa Civil**, Brasília-DF, 1988. Disponível em: <https://tinyurl.com/yc8rrdk5>. Acesso em: 3 set. 2025.

BRASIL. Emenda Constitucional n. 19, de 4 de junho de 1998. **Casa Civil**, Brasília-DF, 1998. Disponível em: <https://tinyurl.com/4zzy33dd>. Acesso em: 2 set. 2025.

BRASIL. Emenda Constitucional n. 45, de 30 de dezembro de 2004. **Casa Civil**, Brasília-DF, 1998. Disponível em: <https://tinyurl.com/yyd9yxz4>. Acesso em: 3 dez. 2025.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação (SLTI). Instrução Normativa n. 4, de 11 de setembro de 2014. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal. **Diário Oficial da União**: Seção 1, Brasília-DF, p. 96-99, 12 set. 2014. Disponível em: <https://tinyurl.com/4v6zw9nm>. Acesso em: 5 set. 2025.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Recomendação CN-CNMP n. 2, de 4 de julho de 2017. Estabelece diretrizes para a estruturação e a atuação das Escolas Institucionais do Ministério Público brasileiro. **Diário Oficial da União**: seção 1, Brasília-DF, n. 128, p. 126-127, 6 jul. 2017a. Disponível em: <https://tinyurl.com/3cyv6yfc>. Acesso em: 17 out. 2025.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Resolução n. 171, de 27 de junho de 2017. Institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP). **Portal CNMP**, Brasília, jun. 2017b. Disponível em: <https://tinyurl.com/yppadzjv>. Acesso em: mar. 2026.

HEINDRICKSON, Gelson; SANTOS JR., Carlos D. Governança de TI em organizações públicas: como a efetividade percebida se relaciona com três mecanismos clássicos. **JISTEM** – Journal of Information Systems and Technology Management, São Paulo, v. 11, n. 2, p. 297-326, maio/ago. 2014. DOI: <https://doi.org/10.4301/S1807-17752014000200005>.

MACEDO JUNIOR, Ronaldo Porto; VIGLIAR, José Marcelo Menezes (org.). **Ministério Público II: Democracia**. São Paulo: Atlas, 1999.

MENDONÇA, Cláudio Márcio Campos de *et al.* Governança de tecnologia da informação: um estudo do processo decisório em organizações públicas e privadas. **Revista de Administração Pública**, Rio de Janeiro, v. 47, n. 2, p. 483-503, mar./abr. 2013. Disponível em: <https://tinyurl.com/3vw39dxz>. Acesso em: 14 set. 2025.

MOODLE. Sobre nós. **Moodle**, Perth-Austrália, 2026. Disponível em: <https://tinyurl.com/4jrspbme>. Acesso em: 30 set. 2025.

OECD. **Public value in public service transformation**: working with change. Paris: OECD Publishing, 2019. DOI: <https://doi.org/10.1787/47c17892-en>.

PRADO, Edmir Parada Vasques *et al.* Governança de TI em organizações do setor de saúde: um estudo de caso de aplicação do COBIT. **Brazilian Journal of Development**, Curitiba, v. 6, n. 6, p. 34002-34022, jun. 2020. DOI: <http://dx.doi.org/10.34117/bjdv6n6-086>.

ROGERS, David L. **Transformação digital**: repensando o seu negócio para a era digital. Belo Horizonte: Autêntica Business, 2017. E-Book Kindle.

Da manutenção tradicional ao BIM: reformulação de contratos públicos de operação e manutenção predial

From traditional maintenance to BIM: reformulation of public building operation and maintenance contracts

DOI: https://doi.org/10.63601/978-65-88299-52-4_9

Italo Yure Braga Arruda

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Servidor do Ministério Público Federal (MPF). Analista e Perito de Engenharia Elétrica.

Wagner Pinheiro da Silva

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Engenheiro de automação e controle. Pesquisador em Building Information Modeling (BIM). Servidor do Ministério Público Federal (MPF).

Resumo: Este estudo investigou a aplicação do Building Information Modeling (BIM) em contratos públicos de manutenção predial, visando sua incorporação na fase de operação e manutenção das edificações. A pesquisa baseou-se em uma revisão da literatura e na análise de quatro contratos vigentes, identificando práticas contratuais e comparando-as com recomendações teóricas e evidências empíricas. Os resultados indicam que a adoção do BIM requer ajustes em diversos tópicos contratuais como objeto, justificativa, equipe técnica, qualificação, treinamento, definição de serviços, gestão de materiais, sistemas eletrônicos, entregáveis, prazos, base normativa, fiscalização e habilitação técnica. As propostas apresentadas mostram que o BIM aprimora a rastreabilidade da informação, a fiscalização contratual, a transparência e a gestão do patrimônio público, configurando uma agenda estratégica para a transformação digital do setor público, apesar dos desafios técnicos, orçamentários e organizacionais existentes.

Palavras-chave: Modelagem da Informação da Construção; BIM; contratos públicos; gerenciamento das instalações; operação e manutenção; transformação digital.

Abstract: *This study investigated the application of Building Information Modeling (BIM) in public building maintenance contracts, aiming to integrate this methodology into the operation and maintenance phase of facilities. The research was based on a literature review and the analysis of four active contracts, identifying current practices and comparing them with theoretical recommendations and empirical evidence. The results indicate that BIM adoption requires adjustments in several contractual aspects such as scope, justification, technical team, qualification, training, service definition, material management, maintenance systems, deliverables, schedules, legal framework, inspection, and technical qualification. The proposed improvements show that BIM enhances information traceability, contract oversight, transparency, and public asset management, representing a strategic agenda for the digital transformation of the public sector, despite existing technical, financial, and organizational challenges.*

Keywords: *Building Information Modeling; BIM; public contracts; facility management; operation and maintenance; digital transformation.*

1 Introdução

O Building Information Modeling (BIM) tem-se consolidado como uma das mais relevantes inovações tecnológicas na forma como os edifícios são concebidos, construídos e gerenciados (Azhar; Khalfan; Maqsood, 2012). Seu uso é amplamente reconhecido nas fases de planejamento, projeto e construção de edifícios (Li *et al.*, 2018). Contudo, embora a fase de operação e manutenção (O&M) represente a maior parcela dos custos do ciclo de vida de uma edificação (Hu *et al.*, 2018), a aplicação do BIM nesse estágio do empreendimento permanece limitada e restrita a poucas de suas funcionalidades (Gao; Pishdad-Bozorgi, 2019; Li *et al.*, 2018). Diante dessa lacuna, o presente estudo propõe-se a discutir meios para a modernização dos contratos públicos de manutenção predial, a fim de incorporar a metodologia BIM na fase de O&M das edificações.

O Decreto n. 11.888/2024 define o BIM ou a Modelagem da Informação da Construção como o

conjunto integrado de processos e tecnologias que permite criar, utilizar, atualizar e compartilhar, colaborativamente, modelos digitais de uma construção, de forma a servir potencialmente a todos os participantes do empreendimento durante o ciclo de vida da construção.

O BIM permite que todos os aspectos, disciplinas e sistemas de uma instalação sejam inseridos em uma única representação digital, melhorando a comunicação e a colaboração de todas as partes interessadas (proprietários, arquitetos, engenheiros, empreiteiros, subcontratados e fornecedores) (Azhar; Khalfan; Maqsood, 2012). Mais do que uma metodologia de projeto, o BIM constitui um modelo de gestão baseado em dados, capaz de integrar informações multidisciplinares ao longo de todo o ciclo de vida das edificações (Abuhussain *et al.*, 2024).

Na manutenção e operação das infraestruturas, o BIM permite gestão, análise e utilização mais eficientes dos dados da construção, resultando em melhorias na manutenção, gestão energética, segurança e desempenho geral das instalações (Cao; Kamaruzzaman; Aziz, 2022; Gao; Pishdad-Bozorgi, 2019). A implementação do BIM permite a redução de custos, aumento da eficiência e melhoria no gerenciamento do tempo, resultando em um paradigma inovador na indústria da Arquitetura, Engenharia e Construção (AEC) (Azhar; Khalfan; Maqsood, 2012).

A aplicação do BIM ainda apresenta desafios quando se trata da adaptação de edificações existentes que não foram originalmente projetadas ou executadas com base nessa metodologia (Hossan; Yeoh, 2018), além dos obstáculos tecnológicos e organizacionais envolvidos, tais como, falta de capacitação de pessoal para o correto uso da metodologia e suas ferramentas computacionais; problemas com gerenciamento de dados e informações; e dificuldades na interoperabilidade, comunicação e integração de ferramentas e equipes (Arrotéia; Freitas; Melhado, 2021).

A implementação do BIM em instituições públicas é um processo complexo e que deve ser realizado em várias etapas de forma estruturada: iniciar com a realização do diagnóstico da organização, identificando barreiras e os meios de superação para introdução da metodologia (Rodrigues; Andrade; Griz, 2023); desenvolver o planejamento estratégico da instituição, estabelecendo metas, formando comitês e definindo diretrizes e padrões (Cheng; Lu, 2015); realizar ações para formação e capacitação de pessoal, promover mudanças culturais e incentivar o trabalho colaborativo e compartilhamento de informações (Boumann; Tavares; Vasconcelos, 2024); integrar o BIM aos processos de compras e aquisições da instituição (Cheng; Lu, 2015); por fim, monitorar o processo para manter a aprendizagem e melhoria contínua na implementação da metodologia (Chowdhury *et al.*, 2024).

Compreender como adaptar os processos e procedimentos do BIM à realidade dos contratos de operação e manutenção de edificações públicas, especificamente no âmbito do Ministério Público Federal (MPF), respeitando suas especificidades e restrições, representa um aperfeiçoamento para a institucionalização da metodologia no setor público, contribuindo para a melhoria da governança e o aprimoramento da gestão dos ativos prediais. A relevância deste estudo reside no fato de abordar um cenário real e desafiador: a necessidade de implementação do BIM na operação e manutenção das infraestruturas prediais do MPF, com foco na superação das limitações impostas pelo legado construtivo não digitalizado.

A pertinência temática do projeto é reforçada pelo recente marco regulatório brasileiro, como o Decreto n. 11.888/2024, que estabelece a Estratégia Nacional de Disseminação do BIM no Brasil com o objetivo de promover um ambiente adequado ao investimento em BIM e a sua difusão no país. Esse normativo evidencia a crescente exigência de que instituições públicas adaptem suas práticas à nova realidade tecnológica e promovam a digitalização e a modernização dos processos de gestão patrimonial.

O problema investigado pode ser sintetizado na seguinte questão: como estruturar um modelo de contrato de operação e manutenção baseado na metodologia BIM, adaptado aos edifícios do MPF? A investigação central deste projeto consiste, portanto, em explorar a literatura existente e buscar sistematizar um modelo replicável que viabilize a adoção do BIM em edificações já construídas pertencentes ao MPF.

Parte-se da hipótese de que os seguintes fatores inviabilizaram, até o momento, a implementação do BIM na gestão da operação e manutenção dos ativos do MPF: o desconhecimento da metodologia pela alta administração; a inexistência de um *framework* replicável e adaptado à realidade dos edifícios do MPF; a ausência de padronização nos processos; e a falta de capacitação das equipes acerca da metodologia BIM.

O objetivo geral deste artigo é investigar e propor adaptações nos contratos existentes para implementar a O&M dos edifícios do MPF baseada na metodologia BIM, considerando os desafios técnicos e normativos da aplicação do BIM em construções que não foram originalmente projetadas com essa tecnologia. Para atingir esse propósito, foram estabelecidos os seguintes objetivos específicos: 1) levantar e analisar os contratos vigentes de manutenção das instalações prediais da Procuradoria-Geral

da República (PGR); 2) pesquisar a literatura científica a fim de identificar padrões, conceitos, funções, responsabilidades e práticas associadas à metodologia BIM; 3) propor melhorias para implementação do BIM nos contratos de manutenção das instalações prediais da PGR.

No âmbito institucional, este estudo busca promover a melhoria da gestão predial, com maior controle e rastreabilidade dos ativos e sistemas das edificações; o aperfeiçoamento do controle de custos operacionais por meio da digitalização de processos de manutenção preventiva e corretiva; a ampliação da transparência administrativa, com informações centralizadas, acessíveis e auditáveis; o fortalecimento da governança institucional; e o alinhamento à política pública federal de disseminação do BIM.

No âmbito acadêmico, pretende-se contribuir com o avanço do conhecimento técnico e científico sobre aplicações do BIM na operação e manutenção de instalações prediais; a exploração de metodologias de digitalização de edifícios existentes; e o fomento à interdisciplinaridade entre engenharia, arquitetura, tecnologia da informação e administração pública.

Este estudo está organizado em cinco capítulos. O primeiro capítulo, dedicado à introdução, apresenta a relevância e pertinência do tema, contextualiza a problemática, formula a questão de investigação, define as hipóteses, os objetivos geral e específicos, justifica a pesquisa e descreve a estrutura do trabalho. O segundo capítulo descreve a metodologia adotada, detalhando os procedimentos da pesquisa empírica, os instrumentos empregados e o processo de coleta de dados. O terceiro capítulo expõe o referencial teórico, abordando os conceitos utilizados, as aplicações do BIM, suas ferramentas, desafios, experiências e consolidada evidências extraídas da produção científica. O quarto capítulo trata da análise e discussão dos resultados, apresentando e examinando os dados à luz dos objetivos do estudo e do referencial teórico. Por fim, o quinto capítulo apresenta as considerações finais.

2 Metodologia

A pesquisa insere-se no paradigma interpretativo, pois busca compreender como a metodologia BIM pode ser aplicada à realidade do MPF na gestão da operação e manutenção de seus edifícios. Esse enfoque

permite analisar os significados atribuídos pelas instituições às suas práticas, considerando o contexto organizacional e a complexidade dos processos institucionais (Coutinho, 2014). Complementarmente, incorpora elementos do paradigma sociocrítico, em virtude de seu caráter propositivo e transformador (Coutinho, 2014), ao indicar o aperfeiçoamento de contratos públicos e favorecer mudanças institucionais. O estudo possui natureza exploratória, por investigar um fenômeno ainda pouco sistematizado no setor público – a aplicação do BIM na gestão de edificações existentes, – e caráter descritivo, ao sistematizar práticas atuais e sugerir modificações em cláusulas contratuais (Coutinho, 2014).

O principal instrumento de coleta de dados foi a pesquisa documental (Padua, 2000), realizada por meio do levantamento de contratos de manutenção das instalações prediais da PGR, obtidos no Portal da Transparência do MPF¹, utilizando como critério de busca a palavra-chave “manutenção” no campo do objeto contratual. A consulta retornou 46 contratos, dos quais foram selecionados, por amostragem intencional, quatro Termos de Contrato (TCs) diretamente relacionados à manutenção predial, representativos de diferentes áreas técnicas. A análise qualitativa dos documentos foi orientada pela análise de conteúdo (Bardin, 2011), com as cláusulas organizadas em categorias temáticas ou tópicos contratuais, a fim de estruturar a etapa subsequente da coleta de dados.

A revisão da literatura foi conduzida em duas etapas. A primeira teve como objetivo a conceituação e a definição da metodologia BIM, incluindo seus usos, benefícios, barreiras, desafios, tendências recentes, lacunas e oportunidades. Para operacionalizar a busca, foi elaborada uma estratégia específica (Snyder, 2019), aplicada em bases de dados como Web of Science, Scopus, SciELO, DOAJ e Google Scholar. Utilizou-se inicialmente a seguinte *string* de pesquisa: (“*Building Information Modeling*” OR “*BIM*”) AND (“*operation and maintenance*” OR “*O&M*” OR “*facility management*” OR “*asset management*”) AND (“*implementation process*” OR “*adoption process*” OR “*deployment*” OR “*integration*” OR “*digit* transformation*” OR “*digitalization*”) AND (“*public building*” OR “*government building*” OR “*institutional infrastructure*” OR “*public infrastructure*”) AND (“*workflow*” OR “*process*” OR “*procedure*” OR “*strategy*” OR “*framework*”) NOT (“*design phase*” OR “*construction only*”). Essa *string*

¹ Disponível em: <https://transparencia.mpf.mp.br/>.

serviu como ponto de partida para a busca, sendo posteriormente refinada em múltiplas iterações, a fim de aumentar sua precisão, ampliar a recuperação de estudos relevantes e eliminar resultados irrelevantes. A pesquisa privilegiou estudos publicados entre 2019 e 2024, a fim de identificar o estado atual da produção científica, sem deixar de considerar trabalhos anteriores relevantes para o embasamento teórico. As buscas foram restritas aos idiomas português e inglês, priorizando publicações que abordassem a integração do BIM na gestão da operação e manutenção, estudos de caso em edifícios legados ou existentes, metodologias, processos e ferramentas de aplicação, além de trabalhos com potencial de replicação ou que discutissem desafios técnicos e soluções de interoperabilidade. Foram excluídos os estudos que tratavam exclusivamente da fase de projeto ou construção, sem vínculo com a etapa operacional.

Na segunda etapa, investigou-se a literatura científica com o objetivo de reunir evidências para fundamentar propostas de melhoria na reformulação das cláusulas contratuais. Seguindo as orientações de Snyder (2019), elaborou-se um plano metodológico estruturado capaz de sintetizar resultados de pesquisas teóricas e empíricas de forma ampla e interdisciplinar, característica pertinente a campos emergentes e interdisciplinares, como a aplicação do BIM à manutenção predial em contratos públicos. O propósito não foi esgotar a produção científica existente, mas integrar perspectivas diversas e extrair evidências úteis para embasar recomendações práticas. Como parte desse plano, foram formuladas perguntas norteadoras específicas para cada tópico contratual. No caso da “equipe técnica”, por exemplo, indagou-se: “Quais profissionais devem ser contratados para a implantação da metodologia BIM em contratos de manutenção e operação de instalações?” e “Quais são as funções e papéis existentes na metodologia BIM?”. Essas questões delimitaram o escopo da pesquisa em três dimensões: tema (BIM), contexto (manutenção e operação de edificações) e foco (estrutura da equipe técnica). A busca pelas respostas foi realizada em plataformas digitais como Consensus e SciSpace, e a seleção da literatura considerou a pertinência das respostas às perguntas formuladas, a atualidade das publicações, a disponibilidade em português ou inglês e a viabilidade temporal da pesquisa (dois meses). Por fim, os artigos escolhidos foram sistematizados em uma matriz de evidências, reunindo trechos diretamente relacionados aos tópicos de investigação.

Para potencializar a busca, leitura, compreensão e fichamento dos artigos, bem como ampliar a capacidade interpretativa da análise documental, foram utilizadas ferramentas de Inteligência Artificial (IA) e sistemas baseados em IA, como Semantic Scholar, SciSpace, Consensus, ChatGPT-5 e Gemini 2.5 Flash. Essas ferramentas atuaram como instrumentos auxiliares na otimização das *strings* de pesquisa, categorização dos achados e identificação de lacunas contratuais em relação às exigências do BIM. Ressalta-se, contudo, que a IA não substituiu o julgamento crítico dos pesquisadores, funcionando apenas como apoio metodológico. Esse uso está alinhado a estudos que validam a aplicação da IA em pesquisas qualitativas, sobretudo em tarefas de conceituação, análise temática e de conteúdo, desde que observadas rigorosamente diretrizes éticas (Christou, 2023).

2.1 Coleta de dados

Na etapa de levantamento documental, foram selecionados quatro TCs da PGR, representativos de diferentes áreas técnicas de manutenção predial: o TC n. 39/2024, referente à manutenção dos sistemas de ar-condicionado, automação predial, detecção, alarme e combate a incêndio, refrigeração, portões automáticos e manuais, plataforma elevatória, aquecimento de água, ventilação mecânica, exaustão e ar comprimido; o TC n. 66/2024, relativo à manutenção civil; o TC n. 44/2023, referente à manutenção das instalações elétricas e da infraestrutura passiva de rede estruturada; e o TC n. 74/2024, voltado à manutenção dos sistemas hidrossanitários, gás liquefeito de petróleo (GLP), irrigação automatizada, poço semiartesiano e sistema de combate a incêndio. A análise desses contratos permitiu a definição de tópicos contratuais que estruturaram a investigação e orientaram a revisão da literatura, organizando as cláusulas em categorias analíticas que contemplam os principais elementos de um contrato de manutenção predial: objeto, justificativa da contratação, equipe técnica, qualificação da equipe técnica, treinamento e capacitação, definições, descrição dos serviços, gestão de materiais, entregáveis e relatórios, sistema eletrônico para gestão da manutenção, prazos e cronogramas, base legal e normativa, fiscalização e acompanhamento, Instrumento de Medição de Resultado (IMR), habilitação técnica e composição dos custos.

A análise revela que a definição do objeto dos contratos concentra-se na manutenção física e operacional dos sistemas prediais. Os contratos descrevem a execução de serviços de manutenção preventiva, corretiva e preditiva, assegurando o funcionamento das instalações elétricas, civis, hidrossanitárias e de climatização e automação, sem previsão de uso de ferramentas digitais integradas. As justificativas apresentadas vinculam-se à necessidade de manter a continuidade operacional das edificações e de atender às demandas de segurança, conforto e eficiência dos usuários, não havendo referência a ferramentas digitais ou metodologias inovadoras de gestão.

No que tange à equipe técnica, os dispositivos analisados estabelecem a alocação de profissionais residentes e não residentes, além de supervisores e responsáveis técnicos com emissão de Certidões de Acervo Técnico (CATs) e Atestados de Capacidade Técnica (ACTs). As qualificações exigidas mantêm-se vinculadas às práticas tradicionais de manutenção, voltadas essencialmente para a execução física e supervisão direta das atividades de manutenção predial, incluindo experiência em sistemas elétricos, hidrossanitários, civis e de climatização, conforme a natureza de cada contrato. As exigências de treinamento concentram-se no cumprimento de normas regulamentadoras de segurança, como NR-10, NR-33 e NR-35, acrescidas de cursos específicos ligados às atividades-fim, como instalação e manutenção de redes estruturadas.

As definições e descrições de serviços estão dirigidas para um contexto de manutenção predial tradicional e detalham as modalidades de manutenção (preditiva, preventiva e corretiva), os serviços extraordinários ou sob demanda, os regimes de execução, regras de subcontratação, procedimentos operacionais e exigências para relatórios. A gestão de materiais organiza-se em categorias clássicas (consumo, reposição, adaptação e ressarcimento) com mecanismos de controle físico-financeiro. Quanto aos entregáveis e relatórios, apresentam um formato predominantemente documental e descritivo, estruturado para atender a obrigações legais, de fiscalização e de acompanhamento técnico-administrativo. Esses relatórios contemplam itens como registros de manutenção preventiva e corretiva, laudos técnicos específicos, cronogramas, listas de materiais, cadastros em software de manutenção e Anotações de Responsabilidade Técnica (ARTs). O suporte tecnológico previsto exige o uso de um sistema eletrônico de gestão da manutenção (software) voltado para gestão

administrativa e técnica tradicional, contemplando a emissão de ordens de serviço, registro de histórico, controle de estoque, relatórios e, em alguns casos, previsão estatística de corretivas.

No tocante aos prazos e cronogramas, os contratos disciplinam a execução dos serviços, o fornecimento de materiais e a gestão administrativa, estabelecendo marcos de acompanhamento. As bases legais e normativas apresentam normas e legislações que abrangem tanto a execução física quanto a segurança do trabalho, em uma relação abrangente de normas técnicas da ABNT, regulamentações trabalhistas (Normas Regulamentadoras), resoluções do CONFEA/CAU, exigências de concessionárias, portarias ministeriais e até referências a normas internacionais reconhecidas, como ASHRAE e SMACNA. A fiscalização e o acompanhamento ficam a cargo de fiscais técnicos e administrativos e gestor administrativo, designados pela contratante, responsáveis pelo controle documental, acompanhamento da execução, registro de ocorrências, emissão de notificações, aplicação de sanções e validação de pagamentos. O Instrumento de Medição de Resultado (IMR) está presente em todos os contratos como ferramenta de aferição da qualidade da prestação de serviços, com tabelas de pontuação para falhas e desconformidades, resultando em descontos proporcionais no valor mensal.

Por fim, as exigências de habilitação técnica mantêm-se alinhadas ao contexto tradicional, com a requisição de CATs e ACTs específicos às disciplinas de cada contrato (elétrica, civil, climatização/automação e hidrossanitária). A composição de custos organiza-se em tabelas que discriminam mão de obra, materiais, serviços sob demanda, ressarcimentos e assistência ao empregado.

3 Revisão de literatura

3.1 Conceituação

O BIM tem-se consolidado como uma metodologia que integra tecnologias digitais e práticas colaborativas para fornecer uma representação virtual das características físicas e funcionais de uma edificação, servindo como uma base de dados compartilhada para decisões ao longo de todo o ciclo de vida do ativo, da concepção à demolição (Azhar; Khalfan; Maqsood, 2012). As dimensões do BIM evoluem além

da modelagem 3D, incorporando 4D (tempo), 5D (custos), 6D (sustentabilidade) e 7D (gerenciamento das instalações) (Charef; Alaka; Emmitt, 2018), esta última dedicada à fase mais longa e custosa do ciclo de vida das edificações (Katić; Tadić, 2023; Obradović; Alić; Čulo, 2024).

O uso do BIM na fase de operação e manutenção permite o gerenciamento inteligente de sistemas prediais, como os sistemas mecânicos, elétricos e hidráulicos (MEP), por meio de modelos *as-built* otimizados com dados operacionais (Hu *et al.*, 2018). Esse modelo digital melhora o acesso à informação, reduz perdas e aumenta a eficiência na execução das atividades de manutenção (Gao; Pishdad-Bozorgi, 2019). O BIM, ao centralizar informações e facilitar sua interoperabilidade, representa um recurso estratégico para a manutenção de edificações, especialmente aquelas não concebidas originalmente com essa metodologia (Hossan; Yeoh, 2018).

Contudo, a integração do BIM em edifícios existentes requer a adoção de processos específicos que possibilitem a captura, modelagem e incorporação de informações relevantes à operação e manutenção. Esse processo inicia com o levantamento das condições reais do edifício para a criação de modelos digitais *as-built* (Hossan; Yeoh, 2018). Em seguida, o modelo do edifício deve ser carregado com dados funcionais e operacionais, considerando os Elementos Fonte de Manutenção (ESM), a fim de estruturar informações úteis para as tarefas de inspeção, limpeza, correção e substituição (Carvalho *et al.*, 2023). A interoperabilidade com sistemas de gerenciamento é viabilizada por padrões como o *Construction-Operations Building information exchange* (COBie), que facilitam a exportação e reutilização dos dados do modelo BIM em plataformas de *Facility Management* (FM) (Gao; Pishdad-Bozorgi, 2019). Fluxos de trabalho integrados, que associam o BIM a metodologias de programação digital, viabilizam o planejamento eficiente de cronogramas e custos na manutenção dos componentes construtivos (Chen; Tang, 2019). Esses processos representam a ponte entre o modelo tridimensional e a gestão contínua do edifício.

Apesar desses benefícios, persistem desafios de natureza técnica, operacional e econômica. Do ponto de vista técnico, a geração do modelo *as-built* é um processo complexo, demorado e oneroso, em especial quando a documentação original é incompleta ou inconsistente (Hossan; Yeoh, 2018). Além disso, informações sobre os equipamentos

MEP registrados em documentos não estruturados exigem a realização de esquemas de agrupamento e rotulagem específicos para viabilizar a extração e a transformação automatizada desses dados em formatos compatíveis com ambientes BIM (Hu *et al.*, 2018). A integração do BIM às rotinas de operação e manutenção enfrenta entraves como a falta de padronização das informações e a necessidade de adaptação dos modelos para refletir elementos e sistemas antigos, muitas vezes incompatíveis com os padrões atuais de interoperabilidade, como os definidos pelo *Industry Foundation Classes* (IFC) e COBie (Carvalho *et al.*, 2023; Gao; Pishdad-Bozorgi, 2019). No enfoque econômico, os custos elevados associados à modelagem e à digitalização de ativos preexistentes dificultam a adoção do BIM, especialmente em contextos de organizações públicas ou com restrições orçamentárias, nos quais os investimentos em tecnologias de digitalização ainda competem com prioridades mais imediatas (Abuhussain *et al.*, 2024; Arrotéia; Freitas; Melhado, 2021).

Estudos de caso, entretanto, demonstram que superar os desafios para aplicação do BIM na operação e manutenção de edifícios existentes proporciona benefícios tangíveis. O estudo de Carvalho *et al.* (2023) propõe um modelo BIM adaptado às necessidades de manutenção, estruturado com base em seis atos principais (inspeção, limpeza, medidas proativas, correção, substituição e termos de uso), organizados conforme os ESMs, o que facilita a interoperabilidade com sistemas de FM. Hu *et al.* (2018), por sua vez, relatam o desenvolvimento de um sistema inteligente de gerenciamento para sistemas MEP em edifícios existentes, utilizando modelos *as-built* carregados com dados operacionais, demonstrando ganhos na resposta a emergências e na execução de tarefas rotineiras de O&M. No setor público, a pesquisa de Boumann, Tavares e Vasconcelos (2024) evidencia que a integração bem-sucedida do BIM depende fortemente de estratégias de capacitação, mudança cultural e padronização dos processos, sendo essencial o envolvimento precoce de todos os atores no ciclo de vida do ativo.

Como tendências recentes, soluções emergentes focam na integração de tecnologias digitais e na adoção de *frameworks* colaborativos para superar as limitações técnicas e operacionais ao realizar a modelagem retroativa. A fotogrametria digital, o Laser Scanner Terrestre (TLS) e o Radar de Penetração no Solo (GPR) são tecnologias utilizadas para a coleta automatizada de dados espaciais e operacionais, que alimentam

os modelos *as-built* com maior precisão e rapidez (Hossan; Yeoh, 2018). A interoperabilidade tem sido impulsionada pelo desenvolvimento e uso de padrões como o IFC e o COBie, permitindo que dados relevantes de operação e manutenção sejam integrados de forma estruturada ao modelo digital (Carvalho *et al.*, 2023; Gao; Pishdad-Bozorgi, 2019). *Frameworks* de gestão do ciclo de vida enfatizam o benefício da aplicação contínua do BIM desde o projeto até a demolição, promovendo a colaboração entre *stakeholders* e assegurando a atualização e usabilidade dos modelos durante toda a vida útil da edificação (Abuhussain *et al.*, 2024).

Apesar dos avanços na aplicação do BIM em edifícios existentes, persistem lacunas que limitam sua adoção plena na fase de operação e manutenção. Assim, abrem-se oportunidades para aprofundamento teórico e prático. Linhas de pesquisa emergentes podem investigar as deficiências na interoperabilidade entre modelos BIM e sistemas de gestão patrimonial, com ênfase na padronização e na qualidade dos dados necessários para a efetividade da gestão das instalações (Gao; Pishdad-Bozorgi, 2019). Há oportunidades para a realização de estudos voltados para a avaliação do retorno sobre o investimento (ROI) da implementação do BIM em edifícios existentes, em razão das dificuldades para justificar economicamente a adoção da tecnologia (Sadek, 2022). Trabalhos futuros podem abordar a ausência de diretrizes para definir o tipo de informação necessária para uso pela equipe de FM durante a fase de O&M e como transferir essas informações perfeitamente para os sistemas de FM existentes (Matarneh *et al.*, 2019). A falta de maturidade digital e a carência de capacitação técnica como barreiras persistentes em órgãos públicos demonstram a necessidade de desenvolver *frameworks* educacionais e estratégicos voltados à transformação digital institucional (Boumann; Tavares; Vasconcelos, 2024).

A revisão da literatura evidencia que a integração do BIM à gestão da operação e manutenção de edifícios existentes é um campo em expansão, marcado por avanços significativos, mas também por desafios persistentes. Foram abordados conceitos fundamentais como a modelagem digital *as-built*, a interoperabilidade via padrões como IFC e COBie e a conexão com sistemas de gestão da manutenção. A literatura também aponta para a importância de processos específicos, como o levantamento das condições reais do edifício, a estruturação das informações em ESM e a adoção de tecnologias de captura digital.

Apesar dos benefícios relatados em estudos de caso, questões técnicas, econômicas e organizacionais ainda dificultam a adoção plena do BIM em edifícios preexistentes. Esses achados se alinham aos objetivos deste estudo ao destacar a necessidade de desenvolver processos específicos para viabilizar essa integração.

3.2 Evidências para proposição de melhorias

A partir da coleta e análise dos contratos de manutenção das instalações prediais da PGR e da definição dos tópicos contratuais, a pesquisa avançou para a investigação da literatura científica relacionada a cada um desses tópicos. Essa etapa possibilitou aprofundar a compreensão acerca da forma como os elementos contratuais têm sido abordados no contexto do BIM, além de identificar os ajustes necessários para sua aplicação adequada em contratos de operação e manutenção.

No que se refere à aplicação do BIM ao objeto do contrato, a literatura destaca a necessidade de adaptar contratos tradicionais para contemplar responsabilidades, níveis de informação, ambiente comum de dados e interoperabilidade (Chong *et al.*, 2017; Erpay; Sertyesilisik, 2021; Pérez-García; Martín-Dorta; Aranda, 2021). Também aponta a inclusão de entregas específicas, como modelos *as-built*, planilhas COBie, relatórios de manutenção e integração com sistemas de gestão de ativos (Matos; Cruz; Branco, 2024; Pishdad-Bozorgi *et al.*, 2018; Wijeratne *et al.*, 2023). Além disso, ressaltam-se planos de execução BIM que definem objetivos, padrões e estratégias de colaboração, consolidando o objeto contratual como instrumento de clareza, qualidade e eficiência nas contratações públicas (Abdelalim *et al.*, 2024; Brito; Ferreira; Costa, 2021; Inojosa *et al.*, 2024; Lin *et al.*, 2016).

Entre as justificativas para contratação de serviços ou sistemas baseados em BIM, destacam-se as capacidades do BIM na gestão da segurança e emergência, manutenção e reparo, gestão da energia, apoio para *retrofit* e renovação, gestão de espaços e ativos prediais (Cao; Kamaruzzaman; Aziz, 2022). A integração da *Building Condition Assessment* (BCA) com o BIM melhora processos de manutenção, aumentando eficiência, qualidade e velocidade (Salzano *et al.*, 2023). O BIM oferece representação digital da edificação, facilita colaboração entre *stakeholders*, reduz

despesas, promove sustentabilidade e aumenta produtividade e inovação (Abuhussain *et al.*, 2024). Também permite a construção digital precisa, detecção precoce de erros, estimativas acuradas e maior coordenação, reduzindo custos (Pérez-García; Martín-Dorta; Aranda, 2021). Outro benefício é a substituição dos métodos convencionais por ambientes digitais integrados, apoiando decisões, gestão de riscos, licitações, monitoramento e modelos *as-built* (Matos; Cruz; Branco, 2024). O BIM permite integrar modelos digitais com sistemas de gestão de ativos, promovendo economia, manutenção preventiva, conformidade e segurança (Wijeratne *et al.*, 2023). Por fim, destaca-se sua capacidade de centralizar informações de sistemas, materiais e histórico de manutenção, facilitando o planejamento e o monitoramento, além de oferecer uma visão holística para apoiar decisões na gestão predial (Inojosa *et al.*, 2024).

A equipe técnica deve ser formada por diferentes perfis profissionais, com atribuições bem definidas e integradas ao longo do ciclo de vida do projeto (Kassem; Raoff; Ouahrani, 2018; Lin *et al.*, 2016; Pishdad-Bozorgi *et al.*, 2018). Os principais cargos incluem Gerente de BIM, responsável pelo gerenciamento estratégico do BIM, coordenação de disciplinas, auditoria de modelos e dados, controle de qualidade, detecção de conflitos, gestão de informações e treinamento da equipe interna (Davies; Wilkinson; McMeel, 2017; Habib *et al.*, 2022; Lin *et al.*, 2016; Sampaio; Azevedo; Gomes, 2023); Coordenador de BIM, atuando na detecção de conflitos, integração de modelos multidisciplinares, verificação de conformidade com padrões e protocolos BIM, comunicação com *stakeholders* e supervisão de processos e entregáveis (Davies; Wilkinson; McMeel, 2017; Habib *et al.*, 2022; Jacobsson; Merschbrock, 2018; Matos; Cruz; Branco, 2024; Nguyen; Dau-Thi; Dao, 2020); e Modelador de BIM, responsável pelo desenvolvimento de modelos 3D, elaboração de desenhos, integração de informações, controle de qualidade do modelo e suporte à equipe em tarefas técnicas (Habib *et al.*, 2022; Matos; Cruz; Branco, 2024; Nguyen; Dau-Thi; Dao, 2020). A literatura ressalta a importância de definir claramente funções e entregas de cada membro, garantindo que recursos especializados sejam alocados adequadamente e que a equipe seja totalmente integrada, evitando silos de informação e promovendo colaboração ao longo de todas as fases do projeto (Lin *et al.*, 2016; Matos; Cruz; Branco, 2024; Pishdad-Bozorgi *et al.*, 2018).

Sobre a qualificação da equipe técnica, estudos destacam a necessidade de desenvolver competências como habilidades em BIM, conhecimento de normas e padrões, compartilhamento de dados, visão estratégica e treinamento (Dakhil; Underwood; Shawi, 2019). O mercado de trabalho exige, de forma recorrente, habilidades em softwares BIM, conhecimento de conceitos e padrões, domínio de regulamentações, experiência prática, competências interpessoais, idiomas e comportamentos profissionais adequados (Nguyen; Dau-Thi; Dao, 2020). Essa visão é ampliada ao considerar que a competência não se restringe ao domínio tecnológico, mas envolve gestão de mudanças, planejamento estratégico, finanças, liderança, comunicação, compreensão do ciclo de vida do projeto e domínio das legislações contratuais (Shahrudin; Zairul; Haron, 2021). As competências podem ser classificadas em essenciais, comuns e específicas por cargo, variando conforme funções como gerente de projeto BIM, coordenador BIM ou modelador, com destaque para a exigência de experiência profissional acumulada (Uhm; Lee; Jeon, 2017).

Acerca do treinamento e capacitação, a literatura indica que a aquisição de competências em BIM envolve habilidades técnicas, educacionais e organizacionais, essenciais tanto para profissionais quanto para clientes que lideram a adoção do BIM (Dakhil; Underwood; Shawi, 2019). Funções específicas, como as de coordenador BIM e gerente BIM, exigem a capacidade de “treinar e ensinar outros” como parte das competências fundamentais para a execução adequada do projeto (Uhm; Lee; Jeon, 2017). Atribuições operacionais também incluem a condução de treinamentos, assegurando a proficiência no uso de ferramentas, protocolos de troca de dados e controle de qualidade (Davies; Wilkinson; McMeel, 2017). Além disso, profissionais em atividade devem aprimorar continuamente suas habilidades para acompanhar as transformações do setor da construção civil, sendo a responsabilidade pela educação em BIM compartilhada entre indústria e academia (Papuraj; Izadyar; Vrcelj, 2025; Sampaio; Azevedo; Gomes, 2023). Programas de aprendizagem baseados em projetos e ambientes colaborativos têm demonstrado eficácia na aquisição de conhecimento e competências práticas, permitindo aplicação direta no desenvolvimento de carreiras (Ismail *et al.*, 2019). Para assegurar uma implementação estruturada e sustentável do BIM, recomenda-se a elaboração de BEP que inclua programas de treinamento formais, aprendizagem contínua

e capacitação em novas tecnologias, garantindo que todas as partes interessadas estejam aptas a operar de acordo com as diretrizes e melhores práticas do BIM (Abdelalim *et al.*, 2024; Matos; Cruz; Branco, 2024).

Em relação aos tópicos contratuais que tratam da definição de termos e da descrição dos serviços, a literatura evidencia que os contratos devem incluir uma seção de definições abrangendo abreviações, nomenclaturas e conceitos essenciais, como objetivos do BIM, usos, níveis de desenvolvimento (LOD), níveis de informação (LOI) e requisitos de informação (Abdelalim *et al.*, 2024; Erpay; Sertyesilisik, 2021; Lin *et al.*, 2016; Pérez-García; Martín-Dorta; Aranda, 2021; Pishdad-Bozorgi *et al.*, 2018). A definição clara do escopo e das funções de cada parte envolvida é indispensável para assegurar que as responsabilidades e direitos sejam compreendidos e juridicamente vinculativos (Chong *et al.*, 2017; Erpay; Sertyesilisik, 2021; Lin *et al.*, 2016). Os contratos devem detalhar procedimentos de interoperabilidade entre sistemas BIM e ferramentas de gestão de instalações, como sistema de gestão da manutenção (CMMS) e sistema de gestão de *facilities* (CAFM), garantindo a integridade, padronização e segurança dos dados ao longo de todo o ciclo de vida do projeto (Matos; Cruz; Branco, 2024; Pishdad-Bozorgi *et al.*, 2018; Wijeratne *et al.*, 2023). A descrição dos serviços deve abranger a criação, atualização e manutenção de modelos BIM, a gestão de informações para operação e manutenção, a elaboração do BEP, a definição de entregáveis como modelos *as-built*, documentação de manutenção, nuvens de pontos, cartografia, relatórios, certificações e matrizes de conflitos, bem como a utilização de fluxos de trabalho, padrões de modelagem e protocolos de segurança digital (Abdelalim *et al.*, 2024; Erpay; Sertyesilisik, 2021; Inojosa *et al.*, 2024; Pérez-García; Martín-Dorta; Aranda, 2021; Pishdad-Bozorgi *et al.*, 2018). Além disso, o detalhamento de funções, fluxos de trabalho, níveis de desenvolvimento, sistemas de classificação, entregáveis e medidas de segurança digital promove confiabilidade, rastreabilidade e qualidade das informações, garantindo que os contratos funcionem como instrumentos eficazes para suportar a implementação do BIM (Abdelalim *et al.*, 2024; Lin *et al.*, 2016; Matos; Cruz; Branco, 2024; Pishdad-Bozorgi *et al.*, 2018; Wijeratne *et al.*, 2023).

Em relação à gestão de materiais, práticas como a criação de listas de inventário de ativos BIM (Pishdad-Bozorgi *et al.*, 2018) e o uso de modelos *as-built* para fundamentar certificados de medição e controlar

quantidades (Matos; Cruz; Branco, 2024) demonstram a importância de estruturar informações sobre equipamentos, sistemas e materiais de construção de forma padronizada e interoperável, assegurando a rastreabilidade e a correta utilização dos recursos, enquanto a integração de informações BIM com padrões como COBie permite que dados sobre manutenção preventiva sejam incorporados e atualizados de forma consistente, garantindo que os modelos sirvam como base para a gestão do ciclo de vida dos ativos (Lin *et al.*, 2016; Matos; Cruz; Branco, 2024). Quanto aos sistemas eletrônicos para gestão da manutenção, os estudos indicam que a implementação de plataformas digitais, como CMMS ou CAFM, integradas aos modelos BIM, facilita o acesso e a análise de informações, reduzindo erros e duplicação de trabalho (Pishdad-Bozorgi *et al.*, 2018; Wijeratne *et al.*, 2023), enquanto a utilização de ambientes comuns de dados (CDE) e protocolos de segurança para armazenamento, compartilhamento e interoperabilidade das informações se mostra crítica para o sucesso da operação e manutenção das instalações (Arshad *et al.*, 2019; Chong *et al.*, 2017; Erpay; Sertyesilisik, 2021; Pérez-García; Martín-Dorta; Aranda, 2021). Além disso, a integração de diferentes *softwares* e ferramentas, como Autodesk Revit, Navisworks e IBM Maximo, permite consolidar dados do modelo 3D com bancos de dados de ativos, oferecendo uma visão detalhada de localização, acessibilidade e manutenibilidade dos equipamentos, e viabilizando um gerenciamento mais eficiente e seguro das instalações (Pishdad-Bozorgi *et al.*, 2018; Wijeratne *et al.*, 2023).

Com base nas evidências extraídas da literatura científica, sobre o tópico “Entregáveis e Relatórios”, os contratos devem prever a entrega de modelos BIM *as-built*, acompanhados de relatórios de coordenação 3D, documentação técnica, manuais, garantias, planilhas detalhadas, matrizes de colisão, mapas COBie e arquivos nos formatos nativos e abertos (IFC, BCF, COBie, CityGML, gbXML) (Erpay; Sertyesilisik, 2021; Matos; Cruz; Branco, 2024; Pishdad-Bozorgi *et al.*, 2018). Além disso, os entregáveis incluem o BEP, que centraliza responsabilidades, processos, gestão, aspectos técnicos e análise de riscos do projeto (Abdelalim *et al.*, 2024; Erpay; Sertyesilisik, 2021; Inojosa *et al.*, 2024; Matos; Cruz; Branco, 2024; Pérez-García; Martín-Dorta; Aranda, 2021). A documentação deve contemplar *checklists*, marcos e tabelas detalhadas para inspeção e atualização do modelo BIM, assegurando a precisão, integridade

e rastreabilidade das informações (Lin *et al.*, 2016; Pishdad-Bozorgi *et al.*, 2018). Os procedimentos de gestão da informação englobam criação, compartilhamento, arquivamento, *backup* e restauração dos dados do modelo BIM, além de estabelecer normas e fluxos para transferência ao operador durante a fase de operação e manutenção (Erpay; Sertyesilisik, 2021; Lin *et al.*, 2016). Por fim, a definição clara dos entregáveis e relatórios é fundamental para assegurar a interoperabilidade entre os modelos BIM, o CMMS e os requisitos contratuais, promovendo eficiência, transparência e suporte à tomada de decisão na gestão predial (Brito; Ferreira; Costa, 2021; Pérez-García; Martín-Dorta; Aranda, 2021).

A literatura demonstra que os prazos e cronogramas das atividades de manutenção predial podem ser aprimorados com a implementação da metodologia BIM, especialmente por meio do uso de BEP. Esses planos permitem organizar detalhadamente as fases e marcos do projeto, definindo funções, responsabilidades, entregas e estratégias de execução, além de estruturar cronogramas de troca de informações e reuniões entre as partes interessadas (Abdelalim *et al.*, 2024; Erpay; Sertyesilisik, 2021). A integração de modelos 3D ao planejamento contratual possibilita a simulação 4D, conectando o cronograma da obra aos modelos BIM, permitindo identificar tarefas adiantadas ou atrasadas, e gerando animações e relatórios para acompanhamento e análise (Matos; Cruz; Branco, 2024). Durante a operação e manutenção, o desenvolvimento de *checklists*, marcos, pontos de verificação e roteiros detalhados garante o monitoramento contínuo do progresso das atividades e a redução de erros na aplicação dos modelos BIM (Lin *et al.*, 2016). Além disso, a utilização de fluxogramas e tabelas derivados do Plano de Execução BIM facilita a visualização do sistema de manutenção, organizando as etapas aplicáveis e apoiando a análise do estado das instalações e elementos do edifício (Inojosa *et al.*, 2024).

Com base nas evidências extraídas da literatura científica, observa-se que a implementação da metodologia BIM em contratos de manutenção predial demanda a incorporação de disposições legais e normativas específicas. Estudos destacam que, apesar do crescente interesse pelo BIM, as questões jurídicas ainda são pouco exploradas, sendo necessário esclarecer papéis, responsabilidades, direitos autorais e segurança dos dados digitais no âmbito contratual (Chong *et al.*, 2017; Erpay; Sertyesilisik, 2021; Pérez-García; Martín-Dorta; Aranda, 2021).

A adaptação da estrutura dos contratos tradicionais aos requisitos do BIM envolve a inclusão de cláusulas que garantam a conformidade com normas internacionais e regionais, como ISO 19650, ISO 12006, COBie e IFC, bem como a integração dos Requisitos de Troca de Informação (EIR) e do BEP (Abdelalim *et al.*, 2024; Matos; Cruz; Branco, 2024). Além disso, a legislação nacional estabelece obrigações específicas para a utilização do BIM, como exemplificado pelo Decreto n. 10.306/2020, que torna obrigatório o uso do BIM na gestão e manutenção de empreendimentos a partir de 2028 (Inojosa *et al.*, 2024).

Acerca dos processos de fiscalização e acompanhamento e do Índice de Medição de Resultados (IMR), a literatura científica destaca que o BEP deve detalhar funções e responsabilidades da equipe, incluindo gerentes e coordenadores BIM, além de estabelecer métodos de monitoramento da execução, como avaliação de quantidades, simulações 4D e relatórios de coordenação 3D (Matos; Cruz; Branco, 2024; Pérez-García; Martín-Dorta; Aranda, 2021). Inspeções sistemáticas do modelo BIM, verificando informações, localização e integridade dos elementos, aliadas à documentação de alterações e *checklists*, são essenciais para o acompanhamento das atividades de manutenção (Lin *et al.*, 2016). A criação de bancos de dados padronizados com histórico de manutenção, manifestações patológicas e métodos de reparo, bem como a geração de cronogramas e relatórios, constitui um instrumento efetivo de medição de resultados (Inojosa *et al.*, 2024). Auditorias regulares, mecanismos de feedback e métricas de desempenho sobre cronogramas, custos, qualidade das entregas e satisfação das partes interessadas permitem avaliar continuamente o sucesso da implementação do BIM (Abdelalim *et al.*, 2024; Erpay; Sertyesilisik, 2021; Pishdad-Bozorgi *et al.*, 2018).

No que concerne à habilitação técnica, os requisitos contratuais relacionados à adoção do BIM podem incluir a qualificação técnica em compras públicas, além de métodos e ferramentas para verificar a qualidade dos entregáveis e componentes BIM (Brito; Ferreira; Costa, 2021). A integração do BIM ao edital deve exigir dos licitantes, além das propostas técnica e comercial tradicionais, uma proposta BIM específica, contendo documentação pré-contratual como o BEP, Plano Mestre de Entrega de Informações (MIDP), avaliação de risco e comprovação da capacidade e competência da equipe e da empresa (Matos; Cruz; Branco, 2024). Essa proposta deve apresentar currículos da equipe

técnica, organogramas, certificados de treinamento, portfólios de projetos anteriores e detalhamento de *softwares* e *hardwares* utilizados, além de definir claramente funções e responsabilidades da equipe, demonstrando a capacidade de implementação da metodologia BIM e de gestão da qualidade em todas as suas fases. Ademais, destaca-se a necessidade de pré-qualificação dos fornecedores, avaliando competência em BIM e capacidade de gerenciamento de riscos, de modo a garantir que apenas licitantes tecnicamente aptos sejam considerados para execução do projeto (Erpay; Sertyesilisik, 2021).

Na composição de custos dos contratos públicos de manutenção predial que utilizam a metodologia BIM, as propostas licitatórias devem contemplar preços fixos e não revisáveis e apresentar de forma clara os insumos e os recursos necessários (Matos; Cruz; Branco, 2024). Além disso, embora o BIM traga benefícios, sua implementação envolve gastos significativos, tais como licenças de *software*, atualização de *hardware*, infraestrutura tecnológica, treinamento de pessoal, consultorias e manutenção dos modelos BIM, todos diretamente relacionados à formação de planilhas de custos detalhadas (Criminale; Langar, 2017; Mohamed *et al.*, 2024). Os custos iniciais representam barreiras à adoção do BIM, sendo recomendada a criação de planos governamentais e institucionais para reduzir esses impactos (Hyarat; Hyarat; Kuisi, 2022). Ainda, em países em desenvolvimento, o fator custo aparece como barreira significativa para a implementação do BIM, diferentemente de países desenvolvidos, onde pode representar economia (Haron; Soh; Harun, 2017).

4 Análise dos resultados

O levantamento dos contratos de manutenção das instalações prediais da PGR evidenciou uma estrutura contratual consolidada e relativamente homogênea, organizada em tópicos recorrentes que abrangem objeto, justificativa da contratação, equipe técnica, qualificação, treinamentos, definições, descrição dos serviços, gestão de materiais, entregáveis e relatórios, sistema eletrônico de gestão, prazos e cronogramas, base legal e normativa, fiscalização, IMR, habilitação técnica e composição de custos. Observa-se que os contratos mantêm um viés tradicional, com ênfase na comprovação de capacidade técnica por meio de CATs e ACTs, definição de profissionais residentes e não residentes

e exigências de treinamento voltadas principalmente à conformidade com normas de segurança regulamentadoras. Os serviços contemplam rotinas clássicas de manutenção (preventiva, preditiva e corretiva), acompanhadas de mecanismos de controle físico-financeiro e sistemas eletrônicos voltados ao registro e acompanhamento das manutenções e ordens de serviço. Destaca-se a presença do IMR como ferramenta sistemática de avaliação de desempenho, vinculada a penalidades financeiras em caso de falhas. Por outro lado, não se identificaram menções à integração digital de modelos de informação, interoperabilidade de dados ou entregas baseadas em BIM. A análise dos contratos evidencia, portanto, um arcabouço ainda ancorado em práticas convencionais, sem incorporar de forma explícita elementos ligados à digitalização ou ao uso de modelos BIM.

A revisão da literatura científica evidencia que a aplicação da metodologia BIM em contratos de operação e manutenção predial amplia de forma significativa o escopo contratual tradicional. Os estudos ressaltam a necessidade de definição clara do objeto, abrangendo usos, entregas e responsabilidades, além da adaptação das cláusulas contratuais para contemplar interoperabilidade, ambiente comum de dados e níveis de informação. Entre os principais avanços identificados estão a inclusão de entregas digitais específicas, como modelos *as-built*, planilhas COBie, relatórios digitais e a exigência de planos de execução BIM para padronizar objetivos, processos e estratégias de colaboração. Além disso, a literatura associa o BIM a benefícios como maior eficiência, redução de custos, sustentabilidade, rastreabilidade dos ativos e apoio à tomada de decisão, destacando sua integração com sistemas de gestão de manutenção e *facilities*. Observa-se também a valorização da equipe técnica qualificada, com funções claramente definidas (gerente, coordenador e modelador BIM), e o treinamento contínuo como fator crítico de sucesso. Outros elementos recorrentes incluem a necessidade de cláusulas normativas e jurídicas adaptadas ao contexto digital, o fortalecimento dos mecanismos de fiscalização e medição de resultados, a exigência de propostas BIM específicas em licitações e a incorporação de custos associados a *softwares*, *hardwares* e capacitação. Nesse sentido, destaca-se que, embora o BIM possa gerar ganhos de eficiência e economia no longo prazo, os custos iniciais de implantação representam uma barreira significativa, sobretudo em

países em desenvolvimento, onde investimentos em tecnologia, *software* e treinamento podem constituir entraves.

Com base no diagnóstico das práticas contratuais atualmente utilizadas e nas recomendações consolidadas pela literatura científica, abre-se espaço para a proposição de melhorias. As cláusulas contratuais, reunidas em categorias temáticas, são aqui repensadas e reestruturadas com vistas a sua adequação à metodologia BIM.

No que se refere ao objeto dos contratos de manutenção predial, observa-se a necessidade de superação da abordagem tradicional, centrada exclusivamente na execução de serviços físicos de manutenção preventiva, corretiva e preditiva. Propõe-se que o objeto contratual passe a incorporar a metodologia BIM como instrumento estruturante, de modo a incluir não apenas a realização dos serviços, mas também a elaboração, atualização e utilização de modelos digitais integrados da edificação.

Em relação à justificativa para contratação, recomenda-se que as cláusulas contratuais deixem de se restringir apenas à continuidade operacional das edificações, ao atendimento das demandas dos usuários e às necessidades de conforto e segurança, e incorporem fundamentos que expressem o valor estratégico da adoção do BIM na operação e manutenção predial. A justificativa deve explicitar que o BIM contribui para a eficiência e a qualidade dos serviços; amplia a sustentabilidade dos empreendimentos públicos; fortalece a gestão de ativos ao longo de todo o ciclo de vida da edificação, integra processos de manutenção com modelos digitais para maior precisão e agilidade; centraliza informações em ambientes comuns de dados, garantindo rastreabilidade e transparência; auxilia o suporte à tomada de decisão baseada em informações confiáveis; permite a integração com sistemas de gestão de ativos (CMMS/CAFM); e promove a inovação institucional alinhada às políticas públicas de digitalização e disseminação do BIM.

As cláusulas contratuais relativas à equipe técnica devem incorporar a exigência de profissionais especializados e qualificados para operar com a metodologia BIM. Recomenda-se a inclusão de funções como gerente, coordenador e modelador BIM, devendo-se definir claramente as atribuições, responsabilidades, entregas e níveis de participação de cada profissional.

A qualificação da equipe técnica deve incorporar competências específicas para atuação em ambiente BIM. Recomenda-se incluir requisitos de capacitação em *softwares* e ferramentas BIM, conhecimento de normas e padrões nacionais e internacionais e habilidades em interoperabilidade e gestão de informações digitais. Além da dimensão tecnológica, deve-se prever competências em gestão de mudanças, planejamento estratégico, liderança, comunicação e domínio das legislações aplicáveis. A qualificação também deve ser estruturada de forma diferenciada por função, contemplando competências essenciais, comuns e específicas para cada cargo. Por fim, recomenda-se a exigência de comprovação de capacitação específica em BIM por meio de certificados, portfólios e experiências anteriores, a fim de certificar que a equipe atenda aos padrões de qualidade e às exigências do BIM.

O treinamento e a capacitação devem ser estendidos para além do atendimento a normas regulamentadoras de segurança e cursos pontuais vinculados às atividades técnicas e introduzir a exigência de conteúdos BIM específicos adaptados ao nível de interação de cada função com a metodologia, garantindo que todos os profissionais compreendam seu papel dentro de um fluxo de manutenção digital e integrado. As atribuições do gerente BIM e do coordenador BIM devem incluir a responsabilidade de treinar e orientar equipes, assegurando a disseminação do conhecimento e a integração das práticas digitais. Sugere-se a inserção de mecanismos de aprendizagem contínua que permitam a adaptação constante às inovações do setor. Por fim, recomenda-se que os contratos exijam a comprovação da realização de capacitações periódicas e que o BEP contemple estratégias de formação, garantindo a sustentabilidade da adoção da metodologia ao longo de todo o ciclo contratual.

As cláusulas contratuais referentes a definições e descrição dos serviços devem ser ampliadas e prever a criação de uma seção de definições padronizadas, contemplando abreviações, nomenclaturas e conceitos centrais, como objetivos do BIM, usos, LOD, LOI e EIR. A descrição dos serviços deve prever, de forma detalhada, a criação, atualização e manutenção de modelos BIM, a elaboração e o cumprimento do BEP, a definição de entregáveis digitais (modelos *as-built*, planilhas COBie, nuvens de pontos, relatórios de manutenção, certificações, matrizes de conflitos) e a integração com sistemas de gestão como CMMS e CAFM. Além disso, é necessário especificar protocolos de interoperabilidade,

padrões de modelagem, fluxos de trabalho colaborativos e medidas de segurança digital, assegurando confiabilidade, rastreabilidade e integridade dos dados. Por fim, sugere-se explicitar as funções e responsabilidades de cada parte, tornando os direitos e obrigações juridicamente vinculativos e garantindo que o contrato se consolide como instrumento efetivo de suporte à implementação e sustentabilidade do BIM.

A gestão de materiais e os sistemas eletrônicos para gestão da manutenção devem superar o enfoque tradicional limitado ao controle físico-financeiro e ao uso de *softwares* administrativos isolados, incorporando práticas alinhadas à metodologia BIM que assegurem rastreabilidade, padronização e interoperabilidade das informações. Recomenda-se que os contratos prevejam a criação de inventários digitais de ativos vinculados a modelos *as-built*, capazes de correlacionar resultados de medição, controlar quantidades e apoiar decisões de manutenção preventiva. Essas informações devem ser estruturadas em conformidade com padrões internacionais, como COBie, assegurando padronização, interoperabilidade, rastreabilidade, consistência e atualização contínua dos dados de equipamentos e materiais. Paralelamente, os contratos devem exigir a utilização de sistemas eletrônicos de manutenção (CMMS ou CAFM) integrados ao modelo BIM e operando em um ambiente comum de dados, observando protocolos de segurança, armazenamento e compartilhamento. A integração entre *softwares* especializados, como Autodesk Revit, Navisworks e IBM Maximo, deve ser prevista para consolidar dados tridimensionais e bancos de ativos, viabilizando uma gestão mais detalhada da localização, informações e manutenibilidade dos equipamentos.

As cláusulas contratuais que tratam de entregáveis e relatórios devem passar a exigir, além dos relatórios tradicionais, a entrega de modelos digitais *as-built* atualizados, vinculados a sistemas de gestão da manutenção. Devem ser incluídos entregáveis específicos, como relatórios de coordenação 3D, planilhas COBie, matrizes de conflitos, documentação técnica, manuais, garantias e mapas digitais em formatos nativos e abertos (por exemplo, IFC, BCF, gbXML), possibilitando a integração plena com ambientes comuns de dados e sistemas CMMS/CAFM. Recomenda-se a obrigatoriedade da apresentação do BEP como documento de referência central, consolidando responsabilidades, fluxos de trabalho, protocolos de qualidade e estratégias de mitigação de

riscos. A documentação deve contemplar *checklists*, marcos de verificação e cronogramas de atualização do modelo. Finalmente, os contratos devem prever regras de criação, compartilhamento, arquivamento, restauração de dados digitais e integridade da informação.

As disposições sobre prazos e cronogramas devem estabelecer prazos para elaboração do BEP que detalhem fases, marcos, responsabilidades, entregas e estratégias de execução. Devem também ser incluídos mecanismos de controle como *checklists*, pontos de verificação e fluxogramas derivados do BEP, que assegurem rastreabilidade, precisão e qualidade na execução das tarefas de operação e manutenção.

A base legal e normativa deve incluir, além da referência às normas sobre manutenção predial, segurança do trabalho e regulamentações profissionais, normativos específicos para a metodologia BIM. Alguns deles são: ABNT NBR 15965 (Sistema de classificação da informação da construção); ABNT NBR ISO 19650 (Organização e digitalização da informação sobre edifícios e obras de engenharia civil); ABNT NBR ISO 12006-2 (Organização de informação da construção); ABNT NBR ISO 16739 (Industry Foundation Classes – IFC); e COBie (padrão de interoperabilidade). As cláusulas precisam tratar de aspectos jurídicos, como definição clara dos papéis e responsabilidades das partes, direitos autorais sobre os modelos digitais, propriedade e segurança de dados.

As cláusulas contratuais que tratam da fiscalização e acompanhamento e do IMR devem incorporar mecanismos digitais, prevendo que a fiscalização seja realizada diretamente no modelo BIM, com inspeções sistemáticas que verifiquem a integridade, a localização e a atualização das informações, apoiadas por *checklists* e documentação de alterações. O IMR deve contemplar glosas contratuais vinculadas a falhas digitais, como ausência de atualização do modelo, inserção de informações incompletas ou divergentes, falta da inclusão de relatórios e laudos e desconformidades na integração entre os sistemas.

A habilitação técnica deve incluir requisitos específicos para comprovação da capacidade da empresa e de sua equipe para implementação da metodologia BIM. Recomenda-se que os editais exijam, além das propostas técnica e comercial, comprovação da qualificação da equipe, certificados de capacitação em BIM e atestados que demonstrem experiência no uso do BIM.

A composição de custos deve incluir os custos relacionados a *softwares* e licenças, atualização de *hardware*, infraestrutura tecnológica, consultorias especializadas, treinamento contínuo da equipe e manutenção evolutiva dos modelos digitais. Devem ser previstos custos adicionais com contratação de profissionais especializados, por exemplo, gerente, coordenador e modelador BIM. Recomenda-se que os editais prevejam a apresentação de planilhas de custos detalhadas, com a devida discriminação dos insumos tecnológicos, recursos humanos e capacitação, de modo a garantir transparência e viabilidade econômica da proposta.

O Quadro 1 apresenta a consolidação dos tópicos contratuais analisados, das práticas atualmente vigentes e das propostas de melhorias formuladas a partir da revisão documental e da literatura científica.

Quadro 1 – Práticas vigentes e propostas de melhorias contratuais

TÓPICO CONTRATUAL	PRÁTICAS VIGENTES	PROPOSTAS DE MELHORIAS
Objeto do contrato	Concentram-se na manutenção física e operacional dos sistemas prediais. Descreve a execução dos serviços de manutenção sem prever o uso de ferramentas digitais integradas.	Extrapolar a execução de serviços físicos de manutenção e incorporar a metodologia BIM como instrumento estruturante.
Justificativa para contratação	Restringem-se à necessidade de manter a continuidade operacional das edificações e de atender às demandas de segurança, conforto e dos usuários.	Incluir a adoção do BIM como fundamento estratégico, destacar ganhos em eficiência, sustentabilidade, qualidade, gestão de ativos, integração com sistemas digitais, transparência e alinhamento às políticas públicas de inovação.
Equipe técnica	Estabelecem a alocação de profissionais residentes e não residentes, além de supervisores e responsáveis técnicos com emissão de CATs e ACTs.	Exigir profissionais qualificados em BIM (gerente, coordenador e modelador), com atribuições, responsabilidades e entregas claramente definidas.

TÓPICO CONTRATUAL	PRÁTICAS VIGENTES	PROPOSTAS DE MELHORIAS
Qualificação da equipe técnica	Dirigidas às práticas tradicionais de manutenção, voltadas à execução física e supervisão direta das atividades de manutenção predial, incluindo experiência conforme natureza de cada contrato.	Acrescentar competências específicas em BIM, incluindo domínio de <i>softwares</i> e normas. As exigências devem ser diferenciadas por função e comprovadas por certificados ou experiências prévias.
Treinamento e capacitação	Concentram-se no cumprimento de normas regulamentadoras de segurança, como NR-10, NR-33 e NR-35, acrescidas de cursos específicos ligados às atividades-fim.	Adicionar conteúdos BIM adaptados à função profissional. Supervisores devem treinar e orientar equipes. Prever mecanismos de aprendizagem contínua e capacitação periódica.
Definições e descrição dos serviços	Orientadas para um contexto de manutenção predial tradicional, detalham as modalidades de manutenção, os serviços extraordinários ou sob demanda, os regimes de execução, regras de subcontratação, procedimentos operacionais e exigências para relatórios.	Incluir conceitos centrais do BIM, detalhar uso de modelos digitais e integração de sistemas, definir protocolos de interoperabilidade, padrões de modelagem e medidas de segurança digital, explicitar funções e responsabilidades, assegurar clareza jurídica e suporte à implantação do BIM.
Entregáveis e relatórios	Voltadas para atendimento documental das obrigações contratuais. Apresentação de relatórios mensais, registros de manutenção, laudos técnicos, cronogramas, listas de materiais, cadastros em software e ARTs.	Exigir a realização do BEP, modelos digitais <i>as-built</i> integrados a sistemas de manutenção, relatórios digitais automáticos, planilhas COBie e arquivos em formatos abertos.
Gestão de materiais e sistema eletrônico para gestão da manutenção	Organizam os materiais em categorias, com mecanismos de controle físico-financeiro. Exigem o uso de software que contemple a emissão de ordens de serviço, gestão de ativos e registro e planejamento de manutenções.	Prever inventários digitais vinculados a modelos <i>as-built</i> , estruturados em padrões como COBie e IFC. Integrar softwares ao modelo BIM em ambiente comum de dados, com protocolos de segurança e interoperabilidade.

TÓPICO CONTRATUAL	PRÁTICAS VIGENTES	PROPOSTAS DE MELHORIAS
Prazos e cronogramas	Disciplinam a execução dos serviços, o fornecimento de materiais e a gestão administrativa, estabelecendo marcos de acompanhamento.	Exigir a elaboração do BEP com fases, marcos, responsabilidades e estratégias de execução, prever mecanismos de controle como checklists, pontos de verificação e fluxogramas.
Base legal normativa	Relacionam normas técnicas da ABNT, regulamentações trabalhistas, resoluções dos conselhos profissionais, exigências de concessionárias, portarias ministeriais e normas internacionais.	Acrescentar normas e regulamentos específicos ao BIM, como ABNT NBR 15965, ABNT NBR ISO 19650, ABNT NBR ISO 12006-2, ABNT NBR ISO 16739 (IFC) e COBie.
Fiscalização e acompanhamento e IMR	Realizam controle documental, acompanhamento da execução, registro de ocorrências, emissão de notificações, aplicação de sanções, validação de pagamentos e aferição da qualidade do serviço por meio do IMR.	Prever inspeções no modelo BIM, realizar glosas em razão da falta de atualização do modelo, informações incompletas, ausência de relatórios e problemas de integração entre os sistemas.
Habilitação técnica	Requisitam CATs e ACTs específicos às disciplinas de cada contrato (elétrica, civil, climatização/automação e hidrossanitária).	Comprovar qualificação profissional e capacitação da empresa mediante atestados de execução de serviços com uso do BIM.
Composição de custos	Organizam tabelas que discriminam mão de obra, materiais, serviços sob demanda, ressarcimentos e assistência ao empregado.	Contemplar custos com softwares, hardware, infraestrutura tecnológica, consultorias, capacitação contínua e profissionais especializados em BIM.

Fonte: elaborado pelos autores (2025).

5 Considerações finais

O presente artigo buscou analisar cláusulas contratuais de manutenção predial no âmbito da PGR, identificando suas práticas e propondo melhorias alinhadas à metodologia BIM. O estudo partiu da definição do problema e da questão de pesquisa, estruturou objetivos e utilizou revisão da literatura e análise documental como métodos de investigação. A partir dessa abordagem, foi possível compreender como os contratos vigentes ainda se concentram na execução física dos serviços, carecendo de instrumentos adequados para a gestão digital da informação.

Os principais achados indicam que a implementação do BIM em contratos públicos de manutenção exige ajustes em diversos tópicos contratuais. As propostas apresentadas evidenciam que a incorporação da metodologia contribui para a centralização e o gerenciamento das informações dos ativos, fortalece a fiscalização e o acompanhamento dos serviços prestados pelas empresas contratadas, amplia a transparência e a rastreabilidade no uso dos recursos públicos, além de fornecer dados e análises que apoiam a tomada de decisão e a melhoria contínua da manutenção.

As contribuições deste estudo se apresentam em duas dimensões principais. No campo prático, oferecem recomendações aplicáveis à formulação de editais e contratos, com potencial para apoiar gestores e instituições públicas na condução da transformação digital de suas atividades. No campo acadêmico, a pesquisa reforça a relevância da integração entre BIM e contratações públicas, ampliando o debate sobre as implicações jurídicas, técnicas e operacionais dessa metodologia.

Entretanto, o estudo apresenta limitações. O foco em quatro contratos específicos restringe a generalização dos resultados, assim como a ausência de aplicação prática das recomendações em um caso real limita a verificação de sua efetividade. Além disso, a pesquisa concentrou-se na perspectiva contratual, não se aprofundando em questões tecnológicas, financeiras e culturais que também influenciam a adoção do BIM.

A partir dessas limitações, surgem perspectivas para futuras pesquisas, como a aplicação prática das cláusulas propostas em contratos-piloto, a análise comparativa entre diferentes órgãos da Administração

Pública, a investigação sobre custos e benefícios da implementação e o estudo de estratégias de capacitação para consolidar o BIM como padrão em contratações.

Em conclusão, a pesquisa reforça que a adoção da metodologia BIM nos contratos públicos de manutenção predial representa uma agenda estratégica para o setor público brasileiro. Sua implementação tem potencial para aprimorar a prestação dos serviços, aumentar a transparência no uso dos recursos e melhorar a gestão do patrimônio público. Portanto, os benefícios potenciais incentivam a superação dos desafios técnicos, orçamentários e organizacionais existentes.

Referências

ABDELALIM, A. M. *et al.* Developing standard BIM execution plans for complex construction projects. **Applied Sciences**, Basil, v. 14, n. 15, p. 6614, jul. 2024. DOI: <https://doi.org/10.3390/app14156614>.

ABUHUSSAIN, M. A. *et al.* Integrating Building Information Modeling (BIM) for optimal lifecycle management of complex structures. **Structures**, [s. l.], v. 60, p. 105831, fev. 2024. DOI: <https://doi.org/10.1016/j.istruc.2023.105831>.

ARROTÉIA, A. V.; FREITAS, R. C.; MELHADO, S. B. Barriers to BIM adoption in Brazil. **Frontiers in Built Environment**, [s. l.], v. 7, p. 520154, mar. 2021. DOI: <https://doi.org/10.3389/fbuil.2021.520154>.

ARSHAD, M. F. *et al.* Contractual risks of Building Information Modeling: toward a standardized legal framework for design-bid-build projects. **Journal of Construction Engineering and Management**, [s. l.], v. 145, n. 4, p. 04019010, abr. 2019. DOI: [https://doi.org/10.1061/\(ASCE\)CO.1943-7862.0001617](https://doi.org/10.1061/(ASCE)CO.1943-7862.0001617).

AZHAR, S.; KHALFAN, M.; MAQSOOD, T. Building Information Modeling (BIM): now and beyond. **Australasian Journal of Construction Economics and Building**, [s. l.], v. 12, n. 4, p. 15-28, 2012. DOI: <https://doi.org/10.5130/AJCEB.v12i4.3032>.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BOUMANN, P. S. C.; TAVARES, R. F. E.; VASCONCELOS, B. M. Analysis of critical factors and strategies for implementing and using BIM in the public

sector. **International Journal of Business Administration**, [s. l.], v. 15, n. 1, p. 21, 22 fev. 2024. DOI: <https://doi.org/10.5430/ijba.v15n1p21>.

BRITO, D. M.; FERREIRA, E. A. M.; COSTA, D. B. An investigation of contractual requirements for BIM adoption in the Brazilian Public Sector. *In*: TOLEDO SANTOS, Eduardo; SCHEER, Sergio (orgs.). **Proceedings of the 18th International Conference on Computing in Civil and Building Engineering**. Cham: Springer International Publishing, v. 98 p. 395-408, 2021. (Lecture Notes in Civil Engineering Series). DOI: https://doi.org/10.1007/978-3-030-51295-8_28.

CAO, Y.; KAMARUZZAMAN, S. N.; AZIZ, N. M. Building Information Modeling (BIM) capabilities in the operation and maintenance phase of green buildings: a systematic review. **Buildings**, Basel, v. 12, n. 6, p. 830, 14 jun. 2022. DOI: <https://doi.org/10.3390/buildings12060830>.

CARVALHO, A. T. *et al.* BIM model to support O&M tasks. **Journal of Information Technology in Construction**, [s. l.], v. 28, p. 322-331, 5 maio 2023. DOI: <https://doi.org/10.36680/j.itcon.2023.016>.

CHAREF, R.; ALAKA, H.; EMMITT, S. Beyond the third dimension of BIM: a systematic review of literature and assessment of professional views. **Journal of Building Engineering**, [s. l.], v. 19, p. 242-257, set. 2018. DOI: [10.1016/j.jobbe.2018.04.028](https://doi.org/10.1016/j.jobbe.2018.04.028).

CHEN, C.; TANG, L. BIM-based integrated management workflow design for schedule and cost planning of building fabric maintenance. **Automation in Construction**, [s. l.], v. 107, p. 102944, nov. 2019. DOI: <https://doi.org/10.1016/j.autcon.2019.102944>.

CHENG, J. C. P.; LU, Q. A review of the efforts and roles of the public sector for BIM adoption worldwide. **Journal of Information Technology in Construction**, v. 20, p. 442-478, out. 2015. Disponível em: <http://www.itcon.org/2015/27>. Acesso em: 13 abr. 2026.

CHONG, H. *et al.* Preliminary contractual framework for BIM-enabled projects. **Journal of Construction Engineering and Management**, [s. l.], v. 143, n. 7, p. 04017025, mar. 2017. DOI: [https://doi.org/10.1061/\(ASCE\)CO.1943-7862.0001278](https://doi.org/10.1061/(ASCE)CO.1943-7862.0001278).

CHOWDHURY, M. *et al.* Comprehensive analysis of BIM adoption: from narrow focus to holistic understanding. **Automation in Construction**, [s. l.], v. 160, p. 105301, abr. 2024. DOI: <https://doi.org/10.1016/j.autcon.2024.105301>.

CHRISTOU, P. How to use artificial intelligence (AI) as a resource, methodological and analysis tool in qualitative research? **The Qualitative Report**, Florida, 31 jul. 2023. DOI: <https://doi.org/10.46743/2160-3715/2023.6406>.

COUTINHO, C. P. **Metodologia de investigação em ciências sociais e humanas: teoria e prática**. 2. ed. Coimbra: Almedina, 2014.

CRIMINALE, A.; LANGAR, S. Challenges with BIM implementation: a review of literature. *In: ASC ANNUAL INTERNATIONAL CONFERENCE PROCEEDINGS*, 53., 2017, Washington. **Proceedings** [...]. Mississippi: University of Southern Mississippi, 2017. p. 329-335.

DAKHIL, A.; UNDERWOOD, J.; SHAWI, M. A. Critical success competencies for the BIM implementation process: UK construction clients. **Journal of Information Technology in Construction (ITcon)**, [s. l.], v. 24, p. 80-94, fev. 2019.

DAVIES, K.; WILKINSON, S.; MCMEEL, D. A review of specialist role definitions in BIM guides and standards. **Journal of Information Technology in Construction (ITcon)**, [s. l.], v. 22, p. 185-203, out. 2017.

ERPAY, M. Y.; SERTYESILISIK, B. Preliminary checklist proposal for enhancing BIM-based construction project contracts. **Journal of Information Technology in Construction (ITcon)**, [s. l.], v. 26, p. 341-365, jul. 2021. DOI: <https://doi.org/10.36680/j.itcon.2021.019>.

GAO, X.; PISHDAD-BOZORGI, P. BIM-enabled facilities operation and maintenance: a review. **Advanced Engineering Informatics**, [s. l.], v. 39, p. 227-247, jan. 2019. DOI: <https://doi.org/10.1016/j.aei.2019.01.005>.

HABIB, U. E. H. *et al.* BIM roles and responsibilities in developing countries: a dedicated matrix for design-bid-build projects. **Buildings**, Basel, v. 12, n. 10, p. 1752, 20 out. 2022. DOI: <https://doi.org/10.3390/buildings12101752>.

HARON, N. A.; SOH, R. P. Z. A. R.; HARUN, A. N. Implementation of Building Information Modelling (BIM) in Malaysia: a review. **Pertanika Journal of Science and Technology**, Malaysia, v. 25, n. 3, p. 661-674, jul. 2017.

HOSSAN, M. A.; YEOH, J. K. W. BIM for existing buildings: potential opportunities and barriers. **IOP Conference Series**, [s. l.], v. 371, p. 012051, jun. 2018. DOI: <https://doi.org/10.1088/1757-899X/371/1/012051>.

HU, Z. *et al.* BIM-based integrated delivery technologies for intelligent MEP management in the operation and maintenance phase. **Advances**

in Engineering Software, [s. l.], v. 115, p. 1-16, jan. 2018. DOI: <https://doi.org/10.1016/j.advengsoft.2017.08.007>.

HYARAT, E.; HYARAT, T.; KUISI, M. A. Barriers to the implementation of Building Information Modeling among Jordanian AEC companies. **Buildings**, Basel, v. 12, n. 2, p. 150, 31 jan. 2022. DOI: <https://doi.org/10.3390/buildings12020150>.

INOJOSA, L. da S. P. *et al.* BIM execution plan for building maintenance systems. **Revista Delos**, São José dos Pinhais-PR, v. 17, n. 60, p. e2186, out. 2024. DOI: <https://doi.org/10.55905/rdelosv17.n60-053>.

ISMAIL, A. I. *et al.* Enhancing the graduates' employability and career development through Building Information Modelling intensive training. **International Journal of Built Environment and Sustainability**, Malaysia, v. 6, n. 1-2, p. 91-99, abr. 2019. DOI: <https://doi.org/10.11113/ijbes.v6.n1-2.387>.

JACOBSSON, M.; MERSCHBROCK, C. BIM coordinators: a review. **Engineering, Construction and Architectural Management**, [s. l.], v. 25, n. 8, p. 989-1008, 20 set. 2018. DOI: <https://doi.org/10.1108/ECAM-03-2017-0050>.

KASSEM, M.; RAOFF, N. L. A.; OUAHRANI, D. Identifying and analyzing BIM specialist roles using a competency-based approach. In: CREATIVE CONSTRUCTION CONFERENCE, 2018, Ljubljana. **Proceedings [...]**. Ljubljana: Budapest University of Technology and Economics, 2018. DOI: <https://doi.org/10.3311/CCC2018-135>.

KATIĆ, D.; TADIĆ, M. Life cycle cost analysis of an office building. **E-Zbornik, elektronički zbornik radova Građevinskog fakulteta**, v. 13, n. 26, p. 1-8, dez. 2023. DOI: <https://doi.org/10.47960/2232-9080.2023.26.13.1>.

LI, J. *et al.* A review of currently applied building information modeling tools of constructions in China. **Journal of Cleaner Production**, [s. l.], v. 201, p. 358-368, 10 nov. 2018. DOI: <https://doi.org/10.1016/j.jclepro.2018.08.037>.

LIN, Y. *et al.* Development of BIM execution plan for BIM model management during the pre-operation phase: a case study. **Buildings**, Basel, v. 6, n. 1, p. 8, 17 fev. 2016. DOI: <https://doi.org/10.3390/buildings6010008>.

MATARNEH, S. T. *et al.* BIM for FM: Developing information requirements to support facilities management systems. **Facilities**, [s. l.], v. 38, n. 5/6, p. 378-394, nov. 2019. DOI: <https://doi.org/10.1108/F-07-2018-0084>.

MATOS, B. C.; CRUZ, C. O.; BRANCO, F. B. Digitalization and procurement in construction projects: an integrated BIM-based approach. **Journal of Information Technology in Construction (ITcon)**, [s. l.], v. 29, p. 400-423, may 2024. DOI: <https://doi.org/10.36680/j.itcon.2024.019>.

MOHAMED, H. *et al.* Assessing cost and benefit attributes of Building Information Modelling (BIM) implementation in Malaysian public agency: PLS-SEM approach. **Journal of Information Technology in Construction (ITcon)**, [s. l.], v. 29, p. 308-323, abr. 2024. DOI: <https://doi.org/10.36680/j.itcon.2024.015>.

NGUYEN, T.; DAU-THI, N.; DAO, T. Human resources for BIM jobs in the AEC industry in Vietnam: an investigation on job positions and requirements. **IOP Conference Series: Materials Science and Engineering**, Belgorod, v. 945, n. 1, p. 012037, 1º out. 2020. DOI: <https://doi.org/10.1088/1757-899X/945/1/012037>.

OBRADOVIĆ, D.; ALIĆ, M. B.; ČULO, K. The issue of estimating the maintenance and operation costs of buildings: a case study of a school. **Eng**, v. 5, n. 3, p. 1209-1231, 27 jun. 2024. DOI: <https://doi.org/10.3390/eng5030066>.

PADUA, E. M. M. de. **Metodologia da pesquisa**: abordagem teórico-prática. 6. ed. Campinas: Papirus, 2000.

PAPURAJ, X.; IZADYAR, N.; VRCELJ, Z. Integrating building information modelling into construction project management education in Australia: a comprehensive review of industry needs and academic gaps. **Buildings**, Basel, v. 15, n. 1, p. 130, jan. 2025. DOI: <https://doi.org/10.3390/buildings15010130>.

PÉREZ-GARCÍA, A.; MARTÍN-DORTA, N.; ARANDA, J. A. BIM requirements in the spanish public tender – analysis of adoption in construction contracts. **Buildings**, Basel, v. 11, n. 12, p. 594, 29 nov. 2021. DOI: <https://doi.org/10.3390/buildings11120594>.

PISHDAD-BOZORGI, P. *et al.* Planning and developing facility management-enabled building information model (FM-enabled BIM). **Automation in Construction**, [s. l.], v. 87, p. 22-38, mar. 2018. DOI: <https://doi.org/10.1016/j.autcon.2017.12.004>.

RODRIGUES, I.; ANDRADE, M.; GRIZ, C. BIM implementation on the public sector of state of Pernambuco: a comparative study between state enterprises of PET-GOV extension project. *In*: INTERNATIONAL CONFERENCE OF THE IBEROAMERICAN SOCIETY OF DIGITAL GRAPHICS, 26.,

2022, Lima. **Proceedings** [...]. Lima: Blucher, abr. 2023. DOI: https://doi.org/10.5151/sigradi2022-sigradi2022_150.

SADEK, A. W. Return on investment of building information modeling adoption in the construction industry in developing countries. **Saudi Journal of Engineering and Technology**, Dubai, v. 7, n. 9, p. 525-532, out. 2022.

SALZANO, A. *et al.* Existing assets maintenance management: optimizing maintenance procedures and costs through BIM tools. **Automation in Construction**, [s. l.], v. 149, p. 104788, may 2023. DOI: <https://doi.org/10.1016/j.autcon.2023.104788>.

SAMPAIO, A. Z.; AZEVEDO, G.; GOMES, A. BIM manager role in the integration and coordination of construction projects. **Buildings**, Basel, v. 13, n. 8, p. 2101, 19 ago. 2023. DOI: <https://doi.org/10.3390/buildings13082101>.

SHAHRUDDIN, S.; ZAIRUL, M.; HARON, A. T. Redefining the territory and competency of architectural practitioners within a BIM-based environment: a systematic review. **Architectural Engineering and Design Management**, v. 17, n. 5-6, p. 376-410, nov. 2021. DOI: <https://doi.org/10.1080/17452007.2020.1768506>.

SNYDER, H. Literature review as a research methodology: an overview and guidelines. **Journal of Business Research**, [s. l.], v. 104, p. 333-339, nov. 2019. DOI: <https://doi.org/10.1016/j.jbusres.2019.07.039>.

UHM, M.; LEE, G.; JEON, B. An analysis of BIM jobs and competencies based on the use of terms in the industry. **Automation in Construction**, [s. l.], v. 81, p. 67-98, set. 2017. DOI: <https://doi.org/10.1016/j.autcon.2017.06.002>.

WIJERATNE, P. U. *et al.* BIM enabler for facilities management: a review of 33 cases. **International Journal of Construction Management**, [s. l.], v. 24, n. 3, p. 251-260, 17 jul. 2023. DOI: <https://doi.org/10.1080/15623599.2023.2222962>.

Governança de tecnologia da informação no Ministério Público Federal: estratégias para resposta a incidentes de cibersegurança

Information technology governance in the Federal Prosecution Service: strategies for responding to cybersecurity incidents

DOI: https://doi.org/10.63601/978-65-88299-52-4_10

Leonardo Pereira Orrico

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Graduado em Ciência da Computação na Universidade Federal da Bahia. Servidor do Ministério Público Federal (MPF) na Divisão de Segurança de Equipamentos de Usuários (DSEU/STIC) da Subsecretaria de Segurança Cibernética (SUBSEC/STIC).

Marcos Daniel Vaz Cavalcante Ramos

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Graduado em Sistemas de Informação no Instituto Luterano de Ensino Superior de Porto Velho – ILES/ULBRA. Servidor do Ministério Público do Estado de Rondônia (MPRO), com atuação na Diretoria de Tecnologia da Informação (DTI).

Resumo: A governança de tecnologia da informação (TI) é um conjunto estruturado de políticas, normas e processos implementados em uma organização para a melhor utilização dos recursos de TI, mantendo alinhamento com o planejamento estratégico da instituição. Os incidentes de cibersegurança são um problema global crítico, que ameaçam organizações, indivíduos e governos. Objetivou-se investigar se a governança de TI surtiu o efeito desejado no apoio à resposta a incidentes de segurança no âmbito do Ministério Público Federal (MPF). Tem-se como motivação central desta pesquisa a expectativa de que a governança de TI promova um ganho na atuação proativa nas respostas a incidentes, tradicionalmente caracterizadas por uma abordagem predominantemente reativa. Inicialmente, realizou-se

revisão bibliográfica para fundamentar a relevância da cibersegurança e o papel da governança de TI no setor público e privado. A partir deste referencial, definiu-se uma metodologia de abordagem qualitativa, exploratória e descritiva. Com base nisso, passou-se à análise de forma contextualizada entre a governança de TI e a resposta a incidentes no MPF. Na sequência, mapearam-se as estratégias e diretrizes em vigor, avaliando o nível de maturidade institucional. Esse diagnóstico permitiu examinar a integração dessas estratégias aos processos de resposta a incidentes. Então, de modo a verificar o efetivo apoio da governança de TI à cibersegurança, correlacionaram-se normativos internos às evidências dos relatórios de gestão. Por fim, discutem-se os resultados apresentados. Esta pesquisa evidenciou importantes resultados estratégicos e melhorias na segurança do MPF, porém constatou falta de publicidade de estatísticas dos incidentes de segurança.

Palavras-chave: governança; TI; cibersegurança; incidentes; MPF.

Abstract: *Information Technology (IT) governance is a structured set of policies, standards, and processes implemented within an organization to ensure optimal use of IT resources while maintaining alignment with the institution's strategic planning. Cybersecurity incidents are a critical global problem that threatens organizations, individuals, and governments. The objective was to investigate whether IT governance had the desired effect in supporting security incident response within the Federal Prosecution Service (MPF). The central motivation for this research is the expectation that IT governance will promote improved proactive incident response, traditionally characterized by a predominantly reactive approach. Initially, a literature review was conducted to substantiate the relevance of cybersecurity and the role of IT governance in the public and private sectors. Based on this framework, a qualitative, exploratory, and descriptive methodology was defined. Based on this, a contextualized analysis of IT governance and incident response within the MPF was conducted. Next, the current strategies and guidelines were mapped, assessing the level of institutional maturity. This diagnosis allowed us to examine the integration of these strategies into incident response processes. To verify IT governance's effective support for cybersecurity, internal regulations were correlated with evidence from management reports. Finally, the presented results are discussed. This research evidenced important strategic results and improvements in the security of the MPF, but found a lack of public disclosure of statistics on security incidents.*

Keywords: *governance; IT; cybersecurity; incidents; Federal Prosecution Service.*

1 Introdução

Nas últimas décadas, a tecnologia da informação passou a desempenhar um papel fundamental nas organizações públicas brasileiras. Isso fica evidente no processo de transformação digital que ocorre em muitas

dessas instituições (Reck; Hübner, 2021). Nesse contexto, a governança de TI é necessária para que os recursos tecnológicos se alinhem aos objetivos estratégicos da organização, proporcionando eficiência, aderência às normas e leis e, principalmente, priorizando a segurança da informação.

Entretanto, é importante que as instituições públicas brasileiras disponham não apenas de mecanismos reativos, que são essenciais aos incidentes de segurança da informação, mas também de uma estrutura de governança de TI capaz de abarcar a segurança da informação e integrá-la aos objetivos estratégicos da organização (Cunha; Faria; Marins, 2024). Estratégias de governança de TI bem implementadas podem apoiar e influenciar diretamente a resposta a incidentes de segurança da informação, ao definir papéis, responsabilidades, determinar o processo decisório e a priorização de recursos, além de avaliar e monitorar os resultados.

Considerando esse cenário, apresenta-se o seguinte problema de pesquisa: “Como as estratégias de governança de TI adotadas pelo Ministério Público Federal estão estruturadas para apoiar sua atuação diante de incidentes de cibersegurança?”

Este artigo tem como motivação verificar de que modo as estratégias de governança de TI adotadas no MPF influenciaram os processos de resposta a incidentes de segurança da informação, evidenciando em que medida a governança de TI contribuiu para o apoio a essas respostas no âmbito do MPF. A análise parte da premissa de que a governança de TI pode favorecer um ganho com uma postura mais proativa perante incidentes cibernéticos, campo tradicionalmente caracterizado pela reatividade.

Diante do aumento sem precedentes de incidentes cibernéticos refinados e sofisticados (Qudus, 2025), os quais ameaçam a confidencialidade, a integridade e a disponibilidade dos dados públicos de milhares de cidadãos, o zelo com a segurança da informação é algo que não se pode ignorar, sobretudo em instituições com a importância do MPF, que lidam com informações sigilosas e processos jurídicos de grande relevância que afetam a vida de milhares de pessoas. Responder de forma imediata e eficaz a incidentes de segurança da informação é algo mandatório em instituições da natureza do MPF, devido a seu papel de combate à corrupção e sua atuação como defensor de direitos coletivos e de políticas públicas (Kerche; Viegas, 2024).

Os achados desta pesquisa são similares aos de Qudus (2025), uma vez que as tendências do crime cibernético, incluindo incidentes de *ransomware*, ressaltam a urgência de estruturas de governança robustas para mitigar riscos e proteger infraestruturas críticas. Os achados desta pesquisa também coadunam com a pesquisa de Lima e Palheta (2024), pois mostram que o desempenho da governança de TI concorre para uma redução de riscos e promove a segurança dos dados, elementos fundamentais para a administração pública, diminuindo o número de incidentes de segurança da informação. Esta pesquisa contribui com esses estudos, já que, diferentemente desses, inclui dados e análises do MPF.

Neste artigo, primeiramente, a revisão bibliográfica situa a importância da cibersegurança, bem como o valor que a governança de TI propicia ao setor público e privado, dando credibilidade aos resultados alcançados.

Considerando o referencial obtido na revisão bibliográfica e as limitações decorrentes dos tipos de dados públicos disponíveis, explana-se a metodologia adotada, a qual utiliza o paradigma interpretativo, com abordagem qualitativa, de natureza exploratória e descritiva, que possibilitou uma compreensão aprofundada e contextualizada da governança de TI e da resposta a incidentes de segurança no MPF. A metodologia utilizada, pesquisa documental e exploratória, utilizou análise de conteúdo para expor as relações de causa e efeito das práticas institucionais.

Na sequência, identificaram-se as estratégias e diretrizes de governança de TI atualmente adotadas no MPF na área de cibersegurança e verificou-se se elas realmente refletem o nível de maturidade do órgão. Adiante, analisou-se como as estratégias de governança de TI do MPF estão integradas aos processos de resposta a incidentes de segurança da informação e, também, as ações e os resultados relativos a essa integração.

Correlacionaram-se então as ações de normativos internos, como Instruções Normativas (INs), Planejamento Estratégico de Tecnologia da Informação (PETI) e Plano Diretor de Tecnologia da Informação (PDTI), com as suas efetivas execuções apontadas nos relatórios de gestão do MPF, de modo a apurar o apoio da governança de TI à cibersegurança.

Por fim, apresentou-se a discussão dos resultados, considerando o objetivo de pesquisa proposto e as particularidades da resposta a incidentes de segurança no contexto do MPF.

2 Revisão bibliográfica

A governança de TI é um instrumento essencial para alinhar recursos tecnológicos aos objetivos institucionais e assegurar a criação de valor em paralelo à mitigação de riscos, incluindo, entre outras ações, o apoio à resposta a incidentes de cibersegurança. Segundo Elazhary *et al.* (2023), ela envolve alinhar as metas de TI às metas de negócio, de forma a demonstrar o valor agregado e, ao mesmo tempo, minimizar riscos. Nesse mesmo sentido, Weill e Ross (2004) complementam que a governança de TI consiste em especificar direitos de decisão e estruturas de responsabilização capazes de induzir comportamentos desejáveis no uso da tecnologia. Por conseguinte, a governança funciona como um sistema de direção que assegura equilíbrio entre a criação de valor e a redução de riscos relacionados à TI.

No contexto da segurança cibernética, esse equilíbrio se torna ainda mais relevante diante da crescente complexidade das ameaças. Incidentes de segurança cibernética se configuram como ações maliciosas originadas no ciberespaço que visam causar impactos negativos em instituições, expondo dados sensíveis e comprometendo operações (Hassanzadeh *et al.*, 2020). Além do efeito direto sobre a continuidade dos serviços, estima-se que o cibercrime tenha provocado perdas globais na ordem de 8 trilhões de dólares em 2023 (Qudus, 2025). A interconexão crescente de sistemas, potencializada por tecnologias emergentes como a Internet das Coisas (IoT), amplia a superfície de ataque e aumenta a criticidade da proteção (Krumay; Bernroider; Walser, 2018). Nesse cenário, a ausência de estratégias de governança específicas para riscos advindos dessas inovações, somada a abordagens predominantemente reativas, representa um desafio para a cibersegurança (Qudus, 2025).

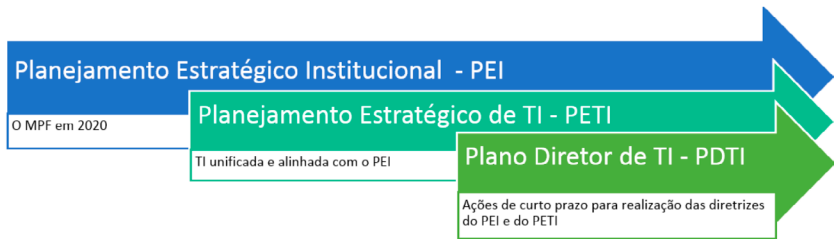
A governança de TI, portanto, mostra-se essencial para apoiar a tomada de decisões e assegurar que ativos tecnológicos e processos estejam alinhados às estratégias organizacionais. Bianchi, Sousa e Pereira (2021) ressaltam que sua função é garantir que as ações e os recursos em TI sejam conduzidos em sintonia com os objetivos estratégicos e táticos. Do mesmo modo, Tarouco e Graeml (2011) destacam que a governança de TI deve considerar visões de negócio, infraestrutura, pessoas e processos, de modo a assegurar a contribuição efetiva da TI para o alcance dos resultados institucionais.

No caso do MPF, a governança é estruturada por um conjunto de práticas, estruturas e processos que visam orientar a gestão estratégica e

assegurar a legitimidade das decisões. Enquanto a governança finalística é exercida por instâncias colegiadas, como o Conselho Superior e as Câmaras de Coordenação e Revisão, a governança dos aspectos estruturantes recai sobre o procurador-geral da República, apoiado pela Secretaria-Geral e demais instâncias previstas em seu Regimento Interno (Portaria PGR/MPF n. 357/2015). Essa configuração institucional garante mecanismos de transparência, delimitação de responsabilidades e prestação de contas.

Entre os instrumentos que direcionam a gestão no MPF, destaca-se o Planejamento Estratégico Institucional (PEI), que funciona como referência para outros planos estratégicos e planos táticos, a exemplo do PETI e do PDTI, conforme Figura 1. O Objetivo Estratégico 4 (OE4) – “Prover soluções de tecnologia da informação e comunicação alinhadas com a estratégia” – impulsionou a elaboração do PETI (Balbinot; Araújo; Luft, 2021). Assim, as diretrizes do PEI e seus desdobramentos orientam a estruturação das estratégias de governança de TI do órgão.

Figura 1 – Relação entre PEI, PETI e PDTI



Fonte: Relatório de Prestação de Contas do MPF 2017 (Brasil, 2017a).

Nessa ótica, *frameworks* se apresentam como referenciais para estruturar tanto a governança de TI quanto as respostas a incidentes de cibersegurança. O COBIT, por exemplo, apresenta um conjunto de objetivos de controle e processos voltados à governança de TI, fornecendo flexibilidade para adaptação às diferentes realidades organizacionais (Marques; Santana, 2023). Já no campo da cibersegurança, o NIST SP 800-61 Rev. 3 oferece orientações para integrar a resposta a incidentes ao gerenciamento de riscos, propondo terminologia padronizada que favorece a comunicação institucional (Nelson *et al.*, 2025). Além disso, estudos recentes demonstram o potencial da inteligência artificial para fortalecer práticas de cibersegurança em alinhamento ao *framework* do NIST (Charfeddine *et al.*, 2024).

Outros referenciais, como o NIST *Cybersecurity Framework* (CSF), destacam-se por oferecer uma abordagem abrangente para gerenciar riscos cibernéticos em consonância com os objetivos de negócio (Egho-Promise *et al.*, 2024; Delgado *et al.*, 2021). Esse *framework* auxilia na priorização de ações e no alinhamento entre políticas, tecnologia e práticas organizacionais, enquanto sua aplicabilidade técnica favorece o tratamento de registros, controles e incidentes (Sulistyowati; Handayani; Suryanto, 2020). Não menos relevante, o CIS *Controls* v8, desenvolvido pelo *Center for Internet Security* (CIS), é uma publicação constituída por um conjunto de boas práticas de segurança cibernética com o objetivo de auxiliar organizações na proteção de seus ativos de tecnologia da informação. Essas boas práticas são estruturadas em controles prioritários e condutas que visam reduzir a superfície de ataque, mitigar riscos e fortalecer a resiliência contra ameaças digitais. Amplamente reconhecidos internacionalmente, os CIS *Controls* oferecem uma abordagem prescritiva e acessível, facilitando a implementação de medidas essenciais de defesa, especialmente em instituições que buscam melhorar rapidamente sua postura de segurança. Eles fornecem orientações práticas por meio de 18 controles que abrangem desde a gestão de ativos até a resposta a incidentes, servindo como guia para equipes de TI na implementação de medidas eficazes de proteção de sistemas e dados (Tanjung; Nurhayati; Wibowo, 2024).

Dessa forma, observa-se que os *frameworks* de governança e segurança, quando integrados às estratégias institucionais, fornecem uma base sólida para estruturar processos de resposta a incidentes e para assegurar a resiliência organizacional. No caso do MPF, a articulação entre diretrizes estratégicas, mecanismos de governança e boas práticas de cibersegurança revela-se fundamental para garantir que a tecnologia atue como suporte eficaz à missão institucional e à proteção contra ameaças digitais.

Contudo, um ponto crítico da literatura é a falta de estudos que contemplem especificamente o MPF. A presente pesquisa busca complementar os conhecimentos, analisando como as estratégias de governança de TI adotadas no MPF influenciam os processos de resposta a incidentes de segurança da informação.

3 Metodologia

A presente pesquisa está inserida no paradigma interpretativo, com abordagem qualitativa, de natureza exploratória e descritiva. Tal escolha

metodológica se justifica pela necessidade de compreender os fenômenos relacionados à governança de TI e à resposta a incidentes de segurança da informação, considerando o contexto institucional do MPF. A abordagem qualitativa possibilita a análise contextualizada de significados, práticas e registros institucionais referentes ao objeto de estudo.

A finalidade principal deste estudo é explicativa, buscando identificar relações de causa e efeito entre a estrutura e o funcionamento da governança de TI e a capacidade institucional de resposta a incidentes de segurança da informação. Busca-se, ainda, identificar fatores determinantes para uma resposta mais eficaz – ou não – a tais incidentes, no âmbito do MPF.

Adota-se uma abordagem qualitativa, com ênfase na interpretação de dados históricos institucionais. Embora dados quantitativos sejam utilizados como apoio, sua função é subsidiar a análise qualitativa dos documentos coletados, reforçando a compreensão das relações analisadas.

O método de pesquisa documental e exploratória foi a opção escolhida, tendo como ponto de análise o Ministério Público Federal. A análise documental adotada, que conforme Cellard (2008) auxilia na compreensão dos significados, contextos e informações presentes nos registros institucionais, constitui um procedimento fundamental para aprofundar a investigação do fenômeno estudado. Esse método envolve a seleção criteriosa das fontes, sua crítica quanto à autenticidade, coerência e relevância, bem como a interpretação sistemática de seu conteúdo, permitindo situá-las em seu contexto de produção e uso.

A escolha do MPF justifica-se por sua relevância na estrutura do Estado brasileiro e pela evolução de sua maturidade de governança de TI.

A população de interesse engloba gestores de TI de órgãos públicos federais e membros de comitês de governança de TI. Entretanto, a presente pesquisa não envolve a realização de entrevistas com esses atores, limitando-se à análise de documentos por eles produzidos ou referenciados. A amostra é composta por documentos institucionais, normativos internos, relatórios públicos e bases de dados acessíveis. A técnica de amostragem utilizada é não probabilística por critérios, sendo previamente definidos os tipos de documentos, os períodos e os órgãos cujos registros serão analisados.

Os dados foram coletados por meio de pesquisa documental, a partir de fontes institucionais do MPF e de outras fontes públicas. Prioritariamente, foi utilizado o site do Repositório Institucional do MPF¹, buscando-se por documentos relacionados à segurança da informação e governança de TI. Foram reunidos documentos constantes desse repositório e de outras fontes abertas como atas de reuniões, normas internas, resoluções, decretos, instruções normativas, leis, portarias, relatórios e demais registros relacionados à governança de TI e à segurança da informação.

Além da técnica de análise documental, aprofundou-se a pesquisa com a análise de conteúdo, identificando categorias e relações (Bardin, 2016) e procedendo com a interpretação crítica de registros escritos. Essa análise de conteúdo buscou identificar padrões, práticas institucionais, diretrizes normativas, indicadores de desempenho e evidências de respostas a incidentes.

Esta pesquisa foi desenvolvida com base em dados públicos e acessíveis, em conformidade com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Não foram utilizados dados pessoais ou sensíveis, nem realizadas entrevistas com indivíduos. Por esse motivo, não se fez necessária a submissão do projeto ao Comitê de Ética em Pesquisa.

As principais limitações deste estudo se referem ao recorte institucional, restrito a um único órgão público, e à ausência de entrevistas com gestores ou servidores diretamente envolvidos nas ações de governança. Além disso, a dependência de registros documentais pode limitar a compreensão de aspectos subjetivos ou implícitos que influenciam a resposta a incidentes de segurança da informação. Ressalta-se também que muitos dados relativos à cibersegurança geralmente envolvem algum grau de sigilo, o que impossibilitou o acesso a muitas informações do MPF, dificultando uma análise mais minuciosa.

4 Governança de TI e a resposta a incidentes de cibersegurança no MPF

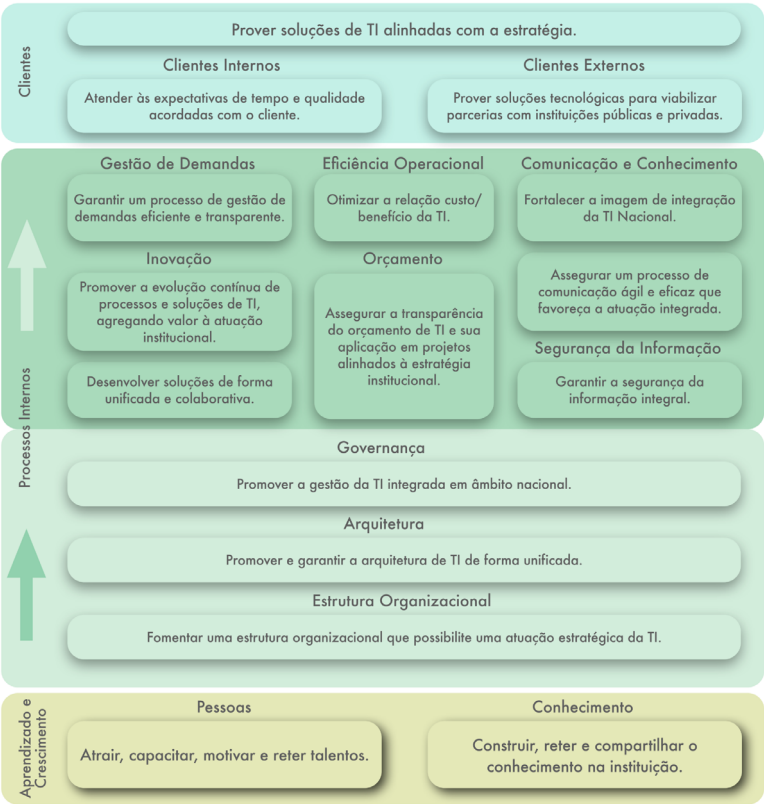
A governança de TI no MPF evoluiu de um planejamento estratégico de longo prazo para um conjunto de políticas, estruturas

¹ Disponível em: <https://tinyurl.com/2za9n8zt>. Acesso em: 20 mar. 2026.

organizacionais e ações práticas que buscam alinhar os recursos tecnológicos com a missão institucional, incluindo um escopo na segurança da informação e na capacidade de resposta a incidentes de cibersegurança.

O Planejamento Estratégico de Tecnologia da Informação (PETI) 2012-2020 (Brasil, 2013c), instituído pela Portaria PGR/MPF n. 560/2013, estabeleceu as bases para uma atuação de TI nacional unificada e estratégica. Um de seus objetivos estratégicos, o OETI 11 – “Garantir a segurança da informação integral” – (vide Figura 2), definiu a meta de difundir e implantar as melhores práticas para a preservação da continuidade dos serviços e da confidencialidade e integridade das informações, promovendo a criação de políticas específicas de segurança (Brasil, 2013c, 2013d).

Figura 2 – Mapa Estratégico de Tecnologia da Informação



Fonte: Planejamento Estratégico de Tecnologia da Informação – 2012/2020 (Brasil, 2011a).

De suma importância, o Plano de Segurança Institucional do MPF (Portaria PGR/MPF n. 417/2013) foi desenvolvido para abordar a segurança de forma ampla, dedicando um capítulo à “Segurança da Informação nos Meios de Tecnologia da Informação”. Este plano estabeleceu medidas concretas para segurança de redes, uso de recursos de TI, controle de acesso e auditoria, servindo como um guia para a implementação das diretrizes do PETI. O Plano de Segurança Institucional (PSI), no que tange aos incidentes de segurança da informação, definiu a necessidade da identificação e do mapeamento de sistemas e serviços cuja interrupção cause dano ou prejuízo à instituição. Também definiu um planejamento de contingência, que consiste em “uma série de ações a serem realizadas para diminuir ou neutralizar o impacto de um incidente de segurança [da informação], buscando manter os sistemas e serviços funcionando de forma integral ou buscando alternativas, de modo a reduzir os danos e prejuízos de toda ordem” ao MPF (Brasil, 2013b), restabelecendo a continuidade dos processos através da combinação de ações preventivas e de recuperação. Outro fator relevante, a segurança em contratos envolvendo sigilo, também foi abordado pelo PSI. A orientação é que, nesses contratos, se estabeleçam cláusulas que contemplem a criação de medidas de gestão de incidentes de segurança da informação, estipulando procedimentos a serem adotados pelas partes para notificação e tratamento de incidentes de segurança.

A estrutura de governança é complementada por instâncias consultivas e deliberativas, como a Comissão Estratégica de Tecnologia da Informação (CETI), que tem a competência de emitir pareceres sobre políticas, diretrizes, planos diretores e prioridades de investimento em TI (Brasil, 2015b). Operacionalmente, a Secretaria de Tecnologia da Informação e Comunicação (STIC) é a unidade responsável por implantar, acompanhar e gerir o PETI, o PDTI e a governança de TI em todo o MPF (Brasil, 2013d, 2015a).

5 Estratégias e diretrizes de governança de TI no MPF

A estratégia de governança de TI é detalhada e operacionalizada por meio de instruções normativas (INs) que estabelecem políticas claras para as áreas críticas da cibersegurança, a exemplo da Política de Controle de Acesso e Segurança de Rede (Instrução Normativa SG/

MPF n. 38/2023), que estipula diretrizes para garantir a segurança, a confidencialidade, a integridade e a disponibilidade no acesso às redes do MPF. Suas principais estratégias incluem a segregação de redes para isolar domínios críticos, a autenticação individualizada e multifator (MFA) para todos os usuários, o monitoramento contínuo dos acessos para fins de auditoria e detecção de incidentes, e o controle de dispositivos pessoais e do uso de ferramentas não institucionais (Brasil, 2023c). Essa instrução normativa aborda a resposta a incidentes de cibersegurança, determinando a comunicação imediata da ocorrência através de canais apropriados que devem existir previamente. Também determina que o monitoramento de rede forneça evidências, no caso de incidente de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei.

A Política de Cópia de Segurança (backup) e Restauração de Dados (Instrução Normativa SG/MPF n. 3/2023) visa auxiliar a continuidade dos serviços de TI e minimizar os reflexos da perda de dados decorrente de falhas, desastres ou ataques cibernéticos. Suas diretrizes estratégicas incluem a realização de no mínimo duas cópias de segurança em mídias distintas (online e *off-line*), o armazenamento de backups de serviços críticos em formato *off-site* (localidade diversa), a criptografia dos dados tanto em repouso (*data at rest*) quanto em trânsito (*data in transit*) e a realização de testes periódicos de restauração para garantir a confiabilidade dos backups (Brasil, 2023b).

Já a Política de Gestão de Continuidade de Serviços de Tecnologia da Informação e Comunicação (TIC) (Instrução Normativa SG/MPF n. 39/2023) busca minimizar riscos e enfrentar ameaças que possam causar interrupções, focando na capacidade do MPF de continuar a entrega de serviços em um nível aceitável após um incidente de segurança da informação. A estratégia central da IN n. 39 é a identificação formal dos serviços de TIC críticos e a elaboração de Planos de Continuidade de Serviços de TIC (PCSTIC) para cada um deles. Esses planos incluem a definição de *Recovery Time Objective* (RTO) e a elaboração de Planos de Recuperação de Desastres (PRDTIC) (Brasil, 2023d), que diminuam o impacto pós-incidente de cibersegurança.

Instituído pela Instrução Normativa SG/MPF n. 33/2025, o Plano de Gerenciamento de Crises de Tecnologia da Informação e Comunicação

(PGC) visa minimizar o impacto de uma crise ou ameaça no contexto da TIC de forma rápida e organizada, proporcionando o retorno à normalidade no menor tempo possível. A relevância do PGC para a governança reside na sua abordagem objetiva, que fundamenta o protocolo de atuação em indicadores e gatilhos pré-definidos, garantindo uma resposta estruturada e menos reativa. O PGC define claramente o que constitui uma crise de TIC: a manifestação de risco em um serviço de TIC crítico, com impacto classificado como significativo ou máximo. A classificação do nível de crise está diretamente ligada ao potencial de impacto e ao tipo de recuperação de desastre necessária.

O Plano de Comunicação de Tecnologia da Informação e Comunicação (PCOM), instituído pela Instrução Normativa SG/MPF n. 34/2025, complementa o PGC, definindo a forma como a instituição se comunica durante uma crise de TIC. A diretriz fundamental do PCOM é a transparência, excetuando-se os casos em que a divulgação de informações possa comprometer a cibersegurança do MPF ou expor dados pessoais protegidos por legislação específica. Esse princípio reforça o alinhamento da governança de TI com a conformidade legal (LGPD), que exige a proteção dos dados pessoais. O método de divulgação dos comunicados é determinado pelo público-alvo e pelo nível da crise, utilizando canais como o serviço de troca de mensagens instantâneas, o correio eletrônico institucional, a página da intranet e os perfis do MPF nas redes sociais. O PCOM também prevê o uso de meios alternativos, como o *Short Message Service* (SMS), caso os meios de comunicação primários estejam indisponíveis, garantindo a difusão da informação em momentos críticos. A execução da comunicação cabe à Secretaria de Comunicação Social (Secom).

Não menos importante, a Política de Emissão de Certificados Digitais (Instrução Normativa SG/MPF n. 5/2022) normatiza e disciplina o processo de emissão de certificados digitais, que são documentos eletrônicos para comprovar a identidade de pessoas, equipamentos e aplicações em transações eletrônicas. A estratégia visa incrementar a segurança da informação no acesso a serviços e permitir a assinatura digital com presunção de validade jurídica, fortalecendo a autenticidade e a integridade das comunicações (Brasil, 2022). Isso dificulta de forma imensa o acesso de pessoas e equipamentos estranhos ao ambiente que possam expor o MPF a incidentes de cibersegurança.

Faz-se relevante frisar que essas instruções normativas consideram as boas práticas de segurança de tecnologia da informação, notadamente as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 e os *frameworks*, destacadamente, *NIST Cybersecurity Framework Subcategory* e *CIS Critical Security Controls*.

6 Processos de resposta a incidentes de cibersegurança

A governança de TI no MPF está intrinsecamente integrada aos processos de resposta a incidentes, direcionando a prevenção, a detecção, a resposta e a recuperação de incidentes. Essa integração se mostra peremptoriamente no modo como os normativos se complementam e se reforçam. A prevenção e a detecção são consolidadas pela IN n. 38/2023, que define o controle de acesso e o monitoramento da rede como linhas de defesa primárias. A exigência de MFA, por exemplo, dificulta o acesso não autorizado, que é um vetor comum para incidentes de segurança. O monitoramento contínuo e o registro de todos os acessos fornecem as evidências necessárias para auditorias e para a identificação de atividades maliciosas, que são os primeiros sinais de um incidente de segurança (Brasil, 2023c).

Quando um incidente ocorre, a capacidade de resposta e recuperação é diretamente apoiada pelas políticas de continuidade e backup. A IN n. 39/2023 define “incidente” como um evento que pode permitir acesso não autorizado, interrupção ou alteração nas operações e estabelece a necessidade de Planos de Gerenciamento de Crises e Planos de Recuperação de Desastres de TIC (PRDTIC). Esses planos são os guias práticos para a equipe de resposta a incidentes de segurança da informação (Brasil, 2023d). A IN n. 3/2023 é a ferramenta operacional mais crítica para a recuperação. Em um cenário de ataque de *ransomware*, por exemplo, a existência de backups *off-line* e *off-site*, conforme determinado pela política, é o que garante a possibilidade de restaurar os dados sem ceder a extorsões. A definição de RPO (*Recovery Point Objective*) e RTO (*Recovery Time Objective*) nos planos de backup ajuda a gerenciar as expectativas e a priorizar a restauração dos serviços mais críticos. Os testes de restauração periódicos garantem que, em uma crise real, as equipes técnicas estejam aptas a executar os procedimentos de recuperação de forma precisa (Brasil, 2023b).

Considerando um momento de crise de TIC, a IN n. 33/2025 e a IN n. 34/2025 são elementos primordiais na tradução dos objetivos de governança de TI para a prática operacional de resposta a incidentes de segurança da informação. O PGC estabelece dois níveis de crise (grave e crítico), relacionando-os diretamente com as estratégias de recuperação de desastres. A resposta imediata é garantida pela instituição do grupo gestor de crise. A composição do grupo gestor para crises de nível crítico é digna de nota, pois inclui a participação da alta administração, como o secretário-geral ou seu adjunto, o secretário de TI e Comunicação ou seu adjunto, e o secretário de Comunicação Social ou seu adjunto. Em ambos os níveis, se o serviço envolver o tratamento de dados pessoais, a Unidade de Proteção de Dados Pessoais (UPDP) do MPF deve indicar um integrante para o grupo gestor.

As reuniões de tratamento de crise, iniciais e regulares, visam confirmar a manifestação do risco, avaliar a extensão do impacto, decidir sobre o acionamento do PRDTIC ou de ações extras e preparar informações básicas para os públicos interno e externo. Após a conclusão bem-sucedida do PRDTIC ou das ações extras, o grupo gestor se reúne para registrar o término da crise e elaborar um relatório de encerramento que detalha o motivo, a duração, as ações tomadas e propostas para modificação do PRDTIC e de outros planos pertinentes (Brasil, 2025a). Já o PCOM é acionado em momentos definidos pelo PGC, em resposta aos eventos previstos nas crises de nível grave e crítico, garantindo que a comunicação, um aspecto imprescindível em crises de cibersegurança, seja transparente e coordenada pela alta administração com o suporte da Secom (Brasil, 2025b).

A evolução da estrutura organizacional do MPF reflete uma integração ainda mais profunda entre a governança de TI e os processos de resposta a incidentes de cibersegurança. A criação da Assessoria Nacional de Segurança da Informação (Anasi) e, mais recentemente, da Subsecretaria de Segurança Cibernética (Subsec), por meio da Portaria SG/MPF n. 1.194/2024, evidencia a priorização da cibersegurança na alta gestão. A Subsec possui uma estrutura dedicada à resposta a incidentes, incluindo a Coordenadoria de Defesa e Monitoramento de Segurança Cibernética e a Divisão de Resposta a Incidentes, formalizando e centralizando a capacidade de reação a ameaças cibernéticas (Brasil, 2024b).

7 Apoio da governança de TI à cibersegurança

A análise dos relatórios de gestão e atividades do MPF demonstra a correlação direta entre o planejamento estratégico, os normativos de governança e os resultados práticos obtidos. O PETI 2012-2020 não foi apenas um documento, mas um impulsionador de ações concretas, como o desenvolvimento do Sistema Único, a implementação do processo eletrônico, a criação de Centros de Serviços Compartilhados e Centros de Excelência, e a padronização de políticas de TIC (Balbinot; Araújo; Luft, 2021). O PETI contribuiu de forma decisiva com a resposta a incidentes de segurança da informação através de suas iniciativas estruturantes, mais especificamente com o mecanismo de melhoria contínua na gestão do MPF, através da iniciativa de estruturação do grupo de resposta a incidentes de segurança da informação (Brasil, 2013c).

A maturidade da governança de TI do MPF foi reconhecida externamente.

O Tribunal de Contas da União (TCU) calcula regularmente o Índice de Governança de Tecnologia da Informação (iGovTI), que é o resultado de levantamentos que abordam práticas de governança e de gestão de TI na Administração Pública Federal previstas em leis, regulamentos, normas técnicas e modelos internacionais de boas práticas. O levantamento [...], realizado em 2016, conferiu ao MPF o nível máximo de capacidade nas dimensões de liderança, estratégias e planos, informações, pessoas e resultados e, na dimensão referente aos processos, conferiu o nível intermediário. Ainda segundo o iGovTI2016, a Instituição obteve o 1º lugar no grupo “Ministério Público” e o 11º lugar geral, entre 368 entidades avaliadas. Sua nota média foi de 0,81, sendo que a média geral ficou em 0,49 (Brasil, 2017b, p. 111-112).

Já em sua avaliação de 2018, o TCU classificou o MPF com um índice de governança de TI (iGovTI) de 89%, posicionando a instituição em um estágio aprimorado e à frente de outras grandes organizações públicas (Brasil, 2019). Essa avaliação externa valida a eficácia das políticas e estruturas de governança implementadas.

Como referência para a criação de estratégias relativas a incidentes de cibersegurança no MPF, vale destacar a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP), criada pelo Conselho Nacional do Ministério Público (CNMP) através da Resolução n. 294, de 28 de maio de 2024 (Brasil, 2024a), que regulamenta a cibersegurança no âmbito de todos os ramos do Ministério Público.

A PNCiber-MP estabelece princípios, diretrizes e o sistema de governança mínimo para nortear o planejamento, as ações e o controle da cibersegurança no âmbito das unidades e ramos do Ministério Público. Seus princípios orientadores incluem a atuação preventiva e proativa a incidentes cibernéticos, a confiabilidade dos ativos (disponibilidade, integridade, confidencialidade e autenticidade) e a articulação das ações de cibersegurança com a proteção de dados. Dentre seus objetivos, destaca-se fomentar a criação de uma rede nacional de cooperação entre as unidades e os ramos do Ministério Público para prevenção, tratamento e resposta a incidentes cibernéticos. Para operacionalizar esses objetivos, a PNCiber-MP estabelece o Sistema Nacional de Cibersegurança do Ministério Público (SNCiber-MP), que adota uma metodologia cooperativa sob a coordenação do CNMP. Esse sistema é composto pelo Comitê Gestor Nacional de Cibersegurança do Ministério Público (CGNCiber-MP), responsável pela coordenação, cooperação e articulação das ações em todo o MP; pelo Comitê de Gerenciamento de Crises, ativado em incidentes cibernéticos relevantes que comprometam o funcionamento regular das unidades; e pela Rede Nacional de Cooperação em Cibersegurança do Ministério Público (REDECiber-MP), que promove o compartilhamento de informações sobre ameaças e incidentes. As unidades do MP devem, por sua vez, instituir Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), que servirão como canais de interação com a REDECiber-MP. O MPF já tem o seu ETIR instituído e atuante.

A relevância da PNCiber-MP se evidencia em instrumentos do MPF, como a IN n. 33/2025 e a IN n. 34/2025, que a citam nos seus considerandos. Isso comprova a magnitude da PNCiber-MP como diretriz regulatória e instrumento que auxilia a governança de TI nas práticas de cibersegurança na gestão de crises no MPF.

Os relatórios de gestão também evidenciam a execução das estratégias de segurança da informação, incluindo resposta a incidentes de cibersegurança. O Relatório de Atividades da Procuradora-Geral da República de 2017-2018 destaca que, graças aos esforços diários de manutenção da segurança, como a atualização de equipamentos e softwares antivírus, o MPF não foi atingido por ataques de *ransomware*, demonstrando a efetividade das medidas preventivas e de resposta (Brasil, 2018). A modernização da infraestrutura de rede, a adoção de tecnologias em nuvem e a criptografia de bancos de dados são exemplos

de projetos executados que fortalecem diretamente a segurança e a resiliência (Brasil, 2019).

A criação da Central Nacional de Atendimento e Relacionamento (Cenar) em 2023, como resultado do processo de nacionalização da TIC, mostra como a governança tem otimizado recursos e padronizado serviços, o que também impacta a segurança ao centralizar e uniformizar procedimentos de suporte (Brasil, 2023a).

O apoio da governança de TI vai além da cibersegurança, viabilizando projetos finalísticos como o “Amazônia Protege” e o “Conexão Água”, que dependem de infraestrutura tecnológica segura para operar (Brasil, 2019). O mesmo foi demonstrado por Dias, Silva e Dias (2021), que encontraram uma correlação positiva entre a qualidade da governança e gestão de TI e os resultados finalísticos (a prestação de serviços públicos com qualidade e eficiência) das organizações públicas.

8 Discussão dos resultados

Na vasta documentação pesquisada, não há menção explícita à realização de exercícios e simulações regulares de resposta a incidentes de cibersegurança para testar a eficácia dos planos, identificar lacunas na coordenação e no conhecimento das equipes e refinar os procedimentos de resposta. Um exercício regular de *Red Team/Blue Team* seria de grande valia para o MPF. Esse exercício é um confronto entre duas equipes de profissionais de segurança cibernética altamente treinados: uma equipe vermelha que se comporta como hackers na tentativa de comprometer o ambiente, e uma equipe azul que consiste na equipe de resposta a incidentes de cibersegurança, a qual trabalha no órgão para identificar, avaliar e responder à intrusão.

Esses exercícios ajudam as organizações a identificar pontos de vulnerabilidade em relação a pessoas, tecnologias e sistemas, assim como determinar melhorias nos processos de resposta a incidentes em todas as suas fases. As descobertas do *Red Team* fornecem insights valiosos que permitem ao *Blue Team* fortalecer ainda mais as suas defesas. Implementar uma estratégia de *Red Team/Blue Team* permite que as organizações testem ativamente suas defesas em um ambiente de baixo risco. Ao envolver esses dois grupos, é possível evoluir continuamente a estratégia de segurança cibernética com base nas fraquezas e

vulnerabilidades específicas do MPF. Essa interação contínua cria um ciclo de melhoria da segurança, pois o *Blue Team* pode implementar as correções com base nos ataques simulados.

Por que o MPF adota predominantemente estratégias reativas e não proativas, conforme sugerido por Baladari (2021) com os testes de *Red Team/Blue Team*? Testes contínuos e validações de segurança permitem que as organizações permaneçam um passo à frente das ameaças cibernéticas.

Outra iniciativa proveitosa para o MPF seria a divulgação de mais dados quantitativos da governança de TI sobre a cibersegurança. Embora exista indicador no PETI para a segurança da informação, não existem métricas de desempenho dedicadas à resposta a incidentes de cibersegurança como tempo médio para detecção (MTTD), tempo médio para contenção (MTTC), tempo médio para reparo (MTTR), criticidade, percentual de incidentes resolvidos dentro do SLA, entre outras. Definir e monitorar indicadores-chave de desempenho (KPIs) específicos para a eficácia da resposta a incidentes de cibersegurança permitiria a avaliação contínua e a otimização dos processos a ela relacionados. Dar publicidade a esses dados, considerando o nível de sigilo adequado, facilitaria e melhoraria a qualidade de futuras pesquisas sobre o tema da cibersegurança no MPF e no setor público.

Adicionalmente, um ponto de extrema importância para o MPF, não percebido de forma contundente em todo o material pesquisado, é a necessidade de fortalecer a cultura de cibersegurança e fortalecer ainda mais a comunicação, não só para as equipes de TI. Apesar da recente IN n. 34/2025 (Brasil, 2025b), que implementou o PCOM, o qual tem uma utilização muito particular em momentos de crise, cabe ao MPF intensificar os programas de treinamento e conscientização sobre cibersegurança para todos os membros, servidores, estagiários e terceirizados, em todos os momentos, garantindo que as políticas sejam compreendidas e aplicadas de forma consistente em todo o MPF.

A comunicação e o fortalecimento da cultura de cibersegurança devem ser feitos de forma contínua, considerando as peculiaridades de cada público e sempre monitorando a efetividade e a abrangência dessas comunicações. Notadamente, o elemento humano tem um papel substancial nos riscos de segurança cibernética. Com o uso cada dia mais refinado da engenharia social, os cibercriminosos usam técnicas

sempre mais sofisticadas para induzir as pessoas a favorecer, mesmo que inadvertidamente, o comprometimento de dados e sistemas dentro das organizações. Garantir que todos tenham as informações e o conhecimento para uma defesa melhor contra esses ataques é algo basilar.

Os resultados desta pesquisa revelam como as estratégias de governança de TI implementadas de modo eficiente apoiam a resposta a incidentes de segurança da informação no MPF. Considerando os dados obtidos a partir das fontes institucionais do MPF e de outros órgãos, foi possível identificar um conjunto de boas práticas impulsionadas pela governança de TI. É evidente o alinhamento estratégico com a clara conexão entre o PEI, o PETI e os normativos específicos, garantindo que as ações de cibersegurança estejam alinhadas aos objetivos maiores da instituição (Balbinot; Araújo; Luft, 2021), o que denota o total apoio das estratégias de governança de TI à resposta de incidentes de cibersegurança. A existência de instruções normativas detalhadas para áreas críticas como backup, continuidade, gerenciamento de crises, comunicação e controle de acesso salienta uma formalização de políticas que torna a gestão da segurança da informação consistente e auditável (Brasil, 2023b, 2023c, 2023d, 2025a, 2025b).

A criação de estruturas dedicadas como a Subsec, com equipes para a gestão de segurança cibernética e com uma divisão específica para resposta a incidentes, demonstra um alto nível de comprometimento do MPF e de sua governança de TI no apoio a incidentes em cibersegurança (Brasil, 2024b). Aspectos de segurança utilizados no MPF como múltiplos fatores de autenticação (MFA), criptografia, backups *off-line* com definições de RPO/RTO e testes periódicos evidenciam o esforço com a prevenção de incidentes de cibersegurança e, também, com a resiliência para a rápida recuperação no pós-incidente (Brasil, 2023b, 2023c).

9 Considerações finais

Em suma, a presente pesquisa documental e exploratória alcançou o objetivo geral de analisar as estratégias de governança de TI adotadas no MPF e sua influência na resposta a incidentes de segurança da informação. A análise revelou que, embora o MPF possua diretrizes e

normativos bem estabelecidos, a governança de TI ainda se concentra em uma abordagem predominantemente reativa, conforme identificado no cenário atual da governança de TI e a Resposta a Incidentes de Cibersegurança no MPF. Os resultados obtidos no mapeamento das estratégias e diretrizes de governança no MPF indicam que a transição para uma postura mais proativa, essencial para a maturidade em cibersegurança, exige a integração de métricas de risco, a publicização de estatísticas detalhadas sobre incidentes e a realização de exercícios regulares de resposta a incidentes de cibersegurança. Dessa forma, o problema de pesquisa “Como as estratégias de governança de TI adotadas pelo Ministério Público Federal estão estruturadas para apoiar sua atuação diante de incidentes de cibersegurança?” é respondido com a conclusão de que a estrutura atual oferece um excelente suporte reativo, mas necessita de uma evolução no nível de maturidade da governança para garantir uma resposta mais eficiente e preventiva, o que constitui a principal contribuição deste estudo.

Esta pesquisa apresentou como limitações o fato de ter se concentrado exclusivamente no MPF como objeto de estudo e a falta de dados quantitativos mais expressivos. Ainda assim, considerando a abrangência nacional do MPF, entende-se que contribuiu de forma significativa para a análise da importância dos mecanismos de governança de TI no apoio à resposta a incidentes de cibersegurança e no alcance dos objetivos estratégicos. Para estudos futuros, recomenda-se ampliar o escopo da investigação a outros órgãos públicos.

Referências

BALADARI, Venkata. Red team vs. blue team: assessing cybersecurity resilience through simulated attacks. **European Journal of Advances in Engineering and Technology**, Shriganganagar, v. 8, n. 4, p. 82-87, 2021. DOI: <https://doi.org/10.5281/zenodo.15044438>.

BALBINOT, Jeysonn Isaac; ARAÚJO, Cleber de; LUFT, Renato. Análise dos resultados estratégicos de tecnologia da informação e comunicação no Ministério Público Federal decorrentes do projeto de modernização da gestão administrativa no período 2011-2020. **Brazilian Journal of Development**, Curitiba, v. 7, n. 12, p. 111034-111052, dez. 2021. DOI: <https://doi.org/10.34117/BJDV7N12-063>.

BARDIN, Laurence. **Análise de conteúdo**. Tradução de Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2016.

BIANCHI, Isaías Scalabrin; SOUSA, Rui Dinis; PEREIRA, Ruben. Information technology governance for higher education institutions: a multi-country study. **Informatics**, Basel, v. 8, n. 2, abr. 2021. DOI: <https://doi.org/10.3390/informatics8020026>.

BRASIL. Conselho Nacional do Ministério Público. **Resolução n. 294, de 28 de maio de 2024**. Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências. Brasília, DF: CNMP, 2024a. Disponível em: <https://tinyurl.com/n6rk9k6t>. Acesso em: 6 ago 2025.

BRASIL. Ministério Público Federal. **Diálogo, integração e efetividade**: Procuradoria-Geral da República. Relatório da gestão set./2019 – set./2023. Brasília, DF: MPF, 2023a. Disponível em: <https://tinyurl.com/4xzmz5je>. Acesso em: 23 mar. 2026.

BRASIL. Ministério Público Federal. **Governança, gestão, inovação e resultados**: biênio 2011-2013. Brasília, DF: MPF, 2013a. Disponível em: <https://tinyurl.com/4a8drcz3>. Acesso em: 23 mar. 2026.

BRASIL. Ministério Público Federal. **Mapa estratégico do MPF**. Brasília, DF: Procuradoria-Geral da República, 2011a.

BRASIL. Ministério Público Federal. **Planejamento Estratégico 2012-2020**. Brasília, DF: MPF, 2011b.

BRASIL. Ministério Público Federal. **Portaria PGR/MPF n. 417, de 5 de julho de 2013**. Dispõe sobre o Plano de Segurança Institucional do Ministério Público Federal. Brasília, DF: MPF, jul. 2013b. Disponível em: <https://tinyurl.com/4nhp3x5e>. Acesso em: 29 jul. 2025.

BRASIL. Ministério Público Federal. **Planejamento Estratégico de Tecnologia da Informação (PETI)**: 2012/2020. Brasília, DF: MPF, 2013c.

BRASIL. Ministério Público Federal. **Relatório de atividades da Procuradora-Geral da República**: set. 2017 – set. 2018. Brasília, DF: MPF, 2018. Disponível em: <https://tinyurl.com/3huue4ca>. Acesso em: 23 mar. 2026.

BRASIL. Ministério Público Federal. **Relatório de gestão da Procuradoria-Geral da República**: set. 2017 – set. 2019. Brasília, DF: MPF, 2019.

BRASIL. Ministério Público Federal. **Relatório de gestão do Ministério Público da União**: 2020. Brasília, DF: MPF, 2021. Disponível em: <https://tinyurl.com/3fn5anpn>. Acesso em: 23 mar. 2026.

BRASIL. Ministério Público Federal. **Relatório de Prestação de Contas do Ministério Público Federal no exercício de 2017**. Brasília: MPF, 2017a.

BRASIL. Ministério Público Federal. **Relatório de resultados do procurador-geral da República**: diálogo, unidade, transparência, profissionalismo, efetividade: 2015-2017. Brasília: MPF, 2017b. Disponível em: <https://tinyurl.com/mr2dy39>. Acessado em: 1º set. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Instrução Normativa SG/MPF n. 5, de 10 de junho de 2022**. Dispõe sobre o processo de emissão de certificados digitais para os membros, servidores, equipamentos e aplicações do Ministério Público Federal. Brasília, DF: MPF, 2022. Disponível em: <https://tinyurl.com/5chaavk3>. Acesso em: 14 ago. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Instrução Normativa n. 3, de 6 de março de 2023**. Dispõe sobre a institucionalização da Política de cópia de segurança (backup) e restauração de dados digitais no âmbito do Ministério Público Federal. Brasília, DF: MPF, 2023b. Disponível em: <https://tinyurl.com/45339jze>. Acesso em: 29 jul. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Instrução Normativa n. 38, de 21 de novembro de 2023**. Institui a Política de Controle de Acesso e Segurança de Rede no âmbito do Ministério Público Federal. Brasília, DF: MPF, 2023c. Disponível em: <https://tinyurl.com/2dcyuu27>. Acesso em: 29 jul. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Instrução Normativa n. 39, de 7 de novembro de 2023**. Dispõe sobre a institucionalização da Política de Gestão de Continuidade de Serviços de Tecnologia da Informação e Comunicação do Ministério Público Federal. Brasília, DF: MPF, 2023d. Disponível em: <https://tinyurl.com/yc5p6xhy>. Acesso em: 29 jul. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Instrução Normativa SG/MPF n. 33, de 23 de setembro de 2025**. Institui o Plano de Gerenciamento de Crises de Tecnologia da Informação e Comunicação do Ministério Público Federal. Brasília, DF: MPF, 2025a. Disponível em: <https://tinyurl.com/yp74n7pr>. Acesso em: 2 out. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Instrução Normativa SG/MPF n. 34, de 18 de setembro de 2025**. Institui o Plano de Comunicação de Tecnologia da Informação e Comunicação do Ministério Público Federal. Brasília, DF: MPF, 2025b. Disponível em: <https://tinyurl.com/y45nhzxs>. Acesso em: 2 out. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Portaria n. 382, de 5 de maio de 2015**. Aprova o Regimento Interno Administrativo do Ministério Público Federal. Brasília, DF: MPF, 2015a. Disponível em: <https://tinyurl.com/6csbnz6a>. Acesso em: 25 ago. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Portaria PGR/MPF n. 560, de 14 de agosto de 2013**. Institui o Planejamento Estratégico de Tecnologia da Informação do Ministério Público Federal para o período 2012-2020. Brasília, DF: MPF, 2013d. Disponível em: <https://tinyurl.com/5fmcmbhv>. Acesso em: 19 ago. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Portaria PGR/MPF n. 357, de 5 de maio de 2015**. Aprova o Regimento Interno Diretivo do Ministério Público Federal. Brasília, DF: MPF, 2015b. Disponível em: <https://tinyurl.com/3fvtecu4>. Acesso em: 25 ago. 2025.

BRASIL. Ministério Público Federal. Secretaria Geral. **Portaria SG/MPF n. 1.194, de 19 de novembro de 2024**. Estabelece a estrutura organizacional da Secretaria de Tecnologia da Informação e Comunicação do Ministério Público Federal. Brasília, DF: MPF, 2024b. Disponível em: <https://tinyurl.com/2v8tfv36>. Acesso em: 28 jul. 2025.

CELLARD, André. A análise documental. In: POUPART, Jean-Pierre *et al.* **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. Tradução de Ana Cristina Nasser. Petrópolis: Vozes, 2008.

CHARFEDDINE, Maha; KAMMOUN, Habib M.; HAMDAOUI, Bechir; GUIZANI, Mohsen. ChatGPT's security risks and benefits: offensive and defensive use-cases, mitigation measures, and future implications. **IEEE Access**, v. 12, p. 30263-30310, 2024. DOI: <https://doi.org/10.1109/ACCESS.2024.3367792>.

CUNHA, Vanice Canuto; FARIA, Alexandre Magno de Melo; MARINS, Joyce Aline de Oliveira. iESGo como guia estratégico para impulsionar a governança de TI em instituições públicas brasileiras. **Caderno Pedagógico**, Curitiba, v. 21, n. 13, e12385, 18 dez. 2024. DOI: <https://doi.org/10.54033/cadpedv21n13-330>.

DELGADO, Maurice Frayssinet; ESENARRO, Doris; REGALADO, Francisco Fernando Juárez; REÁTEGUI, Mónica Díaz. Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. **3C TIC: Cuadernos de Desarrollo Aplicados a las TIC**, Logronho, v. 10, n. 2, p. 123-141, jun./sep. 2021. DOI: <https://doi.org/10.17993/3ctic.2021.102.123-141>.

DIAS, Claudia Marcia Vasconcelos e Mello; SILVA, Jorge Ferreira da; DIAS, Augusto Cesar Arenaro e Mello. Impacto da governança e gestão de TI nos resultados das organizações brasileiras. **Revista Ibero-Americana de Estratégia**, São Paulo, v. 20, p. 1-30, 30 mar. 2021. DOI: <https://doi.org/10.5585/riae.v20i1.17117>.

EGHO-PROMISE, Ehigiator; LYADA, Emmanuel; ASANTE, George; AINA, Folayo. Towards improved vulnerability management in digital environments: a comprehensive framework for cyber security enhancement. **International Research Journal of Computer Science**, Tamil Nadu, v. 11, n. 5, p. 441-449, may 2024. DOI: <https://doi.org/10.26562/irjcs.2024.v11i05.01>.

ELAZHARY, Moustafa; POPOVIČ, Aleš; BERMEJO, Paulo Henrique de Souza; OLIVEIRA, Tiago. How information technology governance influences organizational agility: the role of market turbulence. **Information Systems Management**, Londres, v. 40, n. 2, p. 148-168, 2023. DOI: <https://doi.org/10.1080/10580530.2022.2055813>.

HASSANZADEH, Amin; RASEKH, Amin; GALELLI, Stefano; AGHASHAHI, Mohsen; TAORMINA, Riccardo; OSTFELD, Avi; BANKS, M. Katherine. A review of cybersecurity incidents in the water sector. **Journal of Environmental Engineering**, Cincinnati, v. 146, n. 5, feb. 2020. DOI: <https://doi.org/10.48550/arXiv.2001.11144>.

KERCHE, Fábio; VIEGAS, Rafael Rodrigues. O Ministério Público Federal: de defensor de direitos a combatente da corrupção (1988-2018). **Revista Direito GV**, São Paulo, v. 20, e2408, 2024. DOI: <https://doi.org/10.1590/2317-6172202408>.

KRUMAY, Barbara; BERNROIDER, Edward W. N.; WALSER, Roman. Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST cybersecurity framework. **Secure IT Systems**, Oslo, LNCS, v. 11252, p. 369-384, nov. 2018. DOI: https://doi.org/10.1007/978-3-030-03638-6_23.

LIMA, Raysa Freitas de; PALHETA, Raphael Ribeiro. A importância da governança de tecnologia da informação e comunicação no desempenho organizacional do Poder Judiciário do Estado do Amazonas. **Revista Políticas Públicas e Cidades**, Curitiba, v. 13, n. 2, e1379, 3 dez. 2024. DOI: <https://doi.org/10.23900/2359-1552v13n2-335-2024>.

MARQUES, Thyago Carvalho; SANTANA, Adriano César. Diagnóstico da importância da governança em TI e o seu impacto no desempenho da gestão das empresas. **Latin American Journal of Development**, Curitiba, v. 5, n. 3, p. 893-910, dez. 2023. DOI: <https://doi.org/10.46814/lajdv5n3-002>.

NELSON, Alex; REKHI, Sanjay; SOUPPAYA, Murugiah; SCARFONE, Karen. Incident response recommendations and considerations for cybersecurity risk management: a CSF 2.0 community profile. **National Institute of Standards and Technology**, Gaithersburg, apr. 2025. DOI: <https://doi.org/10.6028/NIST.SP.800-61r3>.

QUDUS, Lawal. Cybersecurity governance: strengthening policy frameworks to address global cybercrime and data privacy challenges. **International Journal of Science and Research Archive**, Maharashtra, v. 14, n. 1, p. 1146-1163, 30 jan. 2025. DOI: <https://doi.org/10.30574/ijrsra.2025.14.1.0225>.

RECK, Janriê Rodrigues; HÜBNER, Bruna Henrique. A transformação digital do Estado: digitalização do governo e dos serviços públicos no Brasil. **Revista Eletrônica Direito e Política**, Itajaí, v. 16, n. 3, p. 1075-1096, 20 dez. 2021. Disponível em: <https://tinyurl.com/535w8hd4>. Acesso em: 20 mar. 2026.

SULISTYOWATI, Diah; HANDAYANI, Fitri; SURYANTO, Yohan. Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. **International Journal on Informatics Visualization**, Padang, v. 4, n. 4, p. 225-230, 18 dez. 2020. DOI: <http://dx.doi.org/10.30630/joiv.4.4.482>.

TANJUNG, Dio Febrilian; NURHAYATI, Oky Dwi; WIBOWO, Adi. Design information security in electronic-based government systems using

NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS Control. **International Journal of Innovative Science and Research Technology**, Jaipur, v. 9, n. 6, p. 523-530, jun. 2024. DOI: <https://doi.org/10.38124/ijisrt/IJISRT24JUN1212>.

TAROUCO, Hiury Hakim; GRAEML, Alexandre Reis. Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas usuárias. **Revista de Administração**, São Paulo, v. 46, n. 1, p. 7-18, 2011.

WEILL, Peter David; ROSS, Jeanne W. **IT governance**: how top performers manage IT decision rights for superior results. Boston: Harvard Business School Press, 2004.

Desenvolvimento e avaliação de um chatbot agêntico multimodelo baseado em RAG para facilitar o acesso do cidadão aos serviços do Ministério Público da União e seus ramos

Development and evaluation of an agentic RAG-based chatbot to facilitate citizen access to the services of the Prosecution Service of the Union and its branches

DOI: https://doi.org/10.63601/978-65-88299-52-4_11

Thiago Coelho Vieira

Mestre em Informática pela Universidade de Brasília (UnB). Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Servidor do Ministério Público Federal (MPF), com atuação no desenvolvimento de soluções baseadas em inteligência artificial, IA generativa e processamento de linguagem natural aplicadas ao setor público.

Luana da Silva Ferreira

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Tecnóloga em Análise e Desenvolvimento de Sistemas. Servidora do Ministério Público Federal (MPF), com atuação na área de suporte, design, análise de requisitos e negócios no MPF.

Resumo: Este estudo propõe o desenvolvimento e a avaliação de um chatbot agêntico multimodelo baseado em *Retrieval-Augmented Generation* (RAG), com consulta automatizada à sua base de conhecimento e a sites de notícias institucionais, como instrumento de inovação no atendimento ao cidadão no Ministério Público da União (MPU) e seus ramos. No contexto da transformação digital da Administração Pública brasileira, a pesquisa avalia o potencial dessa tecnologia para melhorar o acesso à informação, otimizar fluxos de atendimento e fortalecer a eficiência

institucional. Adota-se uma abordagem metodológica mista com integração sequencial exploratória, com análise documental, entrevistas com servidores, testes de usabilidade e questionários aplicados a usuários do chatbot. Em experimento com servidores, obteve-se CSAT 4,49 e CES 6,23, com taxa de sucesso de 99,7% e tempo médio de resposta de 21s. Os resultados preliminares indicam que agentes conversacionais inteligentes podem contribuir para reduzir a sobrecarga de trabalho, aumentar a satisfação dos usuários e promover a transparência administrativa. A pesquisa oferece subsídios práticos para a adoção responsável de soluções de inteligência artificial no setor público, com foco na usabilidade, integração institucional e replicabilidade, fornecendo base para futuras implementações em órgãos de justiça.

Palavras-chave: chatbot; inteligência artificial; RAG; inovação no setor público; governança digital.

Abstract: *This study proposes the development and evaluation of a multi-model agentic chatbot based on (Retrieval-Augmented Generation (RAG), with automated queries to its knowledge base and institutional news websites, as an innovation instrument for citizen service at the Prosecution Service of the Union (MPU) and its branches. Within the context of digital transformation in Brazilian public administration, the research assesses this technology's potential to improve access to information, streamline service workflows, and strengthen institutional efficiency. A mixed-methods approach with an exploratory sequential design is adopted, combining document analysis, interviews with civil servants, usability testing, and user questionnaires. In an experiment with staff, the chatbot achieved CSAT 4.49 and CES 6.23, a 99.7% success rate, and an average response time of 21s. Preliminary results indicate that intelligent conversational agents can help reduce workload, increase user satisfaction, and promote administrative transparency. The study provides practical guidance for responsible adoption of AI solutions in the public sector, focusing on usability, institutional integration, and replicability, and offers an empirical basis for future deployments in justice institutions.*

Keywords: chatbot; artificial intelligence; RAG; public sector innovation; digital governance.

1 Introdução

Este estudo trata do desenvolvimento e da avaliação de um chatbot agêntico multimodelo baseado em *Retrieval-Augmented Generation* (RAG), chamado ChatMPU, com o objetivo de facilitar o acesso do cidadão aos serviços do Ministério Público da União (MPU) e de seus ramos. A pesquisa insere-se no contexto dos desafios enfrentados pela Administração Pública brasileira para ampliar a qualidade, a acessibilidade e a eficiência do atendimento ao cidadão, especialmente diante do crescimento das demandas informacionais e da limitação de recursos humanos.

Com o avanço das tecnologias de inteligência artificial (IA) e a consolidação de políticas públicas voltadas à transformação digital, ferramentas automatizadas como chatbots têm sido cada vez mais utilizadas para mediar a relação entre Estado e sociedade. No setor público, essas soluções apresentam potencial para ampliar o acesso à informação, reduzir custos operacionais e melhorar a experiência do usuário, desde que alinhadas aos princípios de governança digital, transparência e foco no cidadão.

Assistentes virtuais baseados em IA vêm-se consolidando como instrumentos relevantes na modernização dos serviços públicos, contribuindo para otimizar fluxos de atendimento e aumentar a satisfação dos usuários (Bruno, 2024). No entanto, apesar do crescimento dessas iniciativas, ainda são limitados os estudos empíricos que avaliam criticamente o uso de chatbots em instituições jurídicas e de controle, como o Ministério Público, cuja atuação envolve temas sensíveis e de elevado impacto social.

Sob a perspectiva da governança digital e da inovação pública orientada ao cidadão, este estudo busca preencher essa lacuna ao analisar, de forma empírica, a adoção de um chatbot agêntico baseado em RAG no contexto do Ministério Público Federal (MPF). A pesquisa dialoga com diretrizes da Estratégia de Governo Digital e com instrumentos institucionais de planejamento de tecnologia da informação, ao investigar como as soluções de IA podem ser incorporadas de forma responsável e eficaz ao atendimento informacional ao cidadão.

Diante desse cenário, este estudo é orientado pela seguinte pergunta de pesquisa: *Em que medida um chatbot agêntico multimodelo baseado em RAG pode melhorar a experiência do usuário (satisfação e esforço percebido) no atendimento informacional do MPU, e quais gargalos técnicos e organizacionais condicionam sua eficiência e sua escalabilidade?* Como desdobramento, investigam-se, também, os mecanismos de controle (filtro de escopo, pedidos de esclarecimento e rastreabilidade por evidências) que contribuem para reduzir ambiguidades e aumentar a transparência do atendimento.

As contribuições da pesquisa são três: I) *contribuição empírica*: apresenta evidências quantitativas e qualitativas sobre uso de um chatbot RAG em ambiente institucional, combinando indicadores de experiência (CSAT e CES) com métricas operacionais derivadas de *logs* (tempo,

sucesso e gargalos); II) *contribuição metodológica*: propõe um desenho avaliativo replicável para serviços públicos, articulando métodos mistos e triangulação entre percepção do usuário e observabilidade do pipeline; e III) *contribuição prática e gerencial*: sistematiza lições de implementação para adoção responsável de IA no setor público (delimitação de escopo, governança da base de conhecimento, auditabilidade e integração com fluxo de atendimento humano), oferecendo subsídios para replicação em órgãos do sistema de justiça e em serviços públicos informacionais.

2 Referencial teórico

O referencial teórico fundamenta-se nos conceitos de inovação no setor público (Mulgan; Albury, 2003), governança digital (Santos, 2021) e inteligência artificial aplicada aos serviços públicos (Davenport; Ronanki, 2018). A articulação desses conceitos permite analisar não apenas a funcionalidade técnica do chatbot, mas também seus impactos organizacionais, sua aceitação pelos usuários e sua aderência aos princípios que orientam a atuação do MPU, conforme evidenciado nos estudos de Bruno (2024) e Monteiro (2023).

A digitalização de serviços públicos tem buscado ampliar acesso, reduzir fricção e aumentar a capacidade de resposta do Estado, com crescente ênfase em canais digitais e automação de atendimentos informacionais. No contexto brasileiro, a governança digital envolve não apenas tecnologia, mas também desenho de serviços, gestão da informação e capacidade institucional de sustentar canais confiáveis e auditáveis para o cidadão (Santos, 2021). Em paralelo, diretrizes internacionais tratam a estratégia de governo digital como componente estruturante para melhorar prestação de serviços e *accountability*, destacando interoperabilidade, foco no usuário e transparência como princípios orientadores (Larsen; Følstad, 2024).

Chatbots em governo podem atuar como “porta de entrada” para serviços, triagem e orientação, com potencial de reduzir carga sobre canais tradicionais e melhorar a experiência do usuário quando o escopo é bem delimitado e a informação é confiável. Revisões e estudos em *e-government* indicam crescimento do uso de chatbots, mas também apontam desafios recorrentes: qualidade do conteúdo, governança de dados, desenho conversacional, vieses e expectativas de respostas

“jurídicas” ou decisórias que extrapolam atendimentos informacionais (Cortés-Cediel *et al.*, 2023). Trabalhos sobre entrega de valor em serviços mediados por chatbots sugerem que o valor público depende de fatores como utilidade percebida, clareza do escopo, transparência sobre limitações e capacidade de escalonamento para atendimento humano quando necessário (Makasi *et al.*, 2020). Evidências qualitativas sobre provisão de serviços mostram que a adoção efetiva também se relaciona à confiança e à percepção de legitimidade do canal, variando conforme o tipo de serviço e o perfil do usuário (Larsen; Følstad, 2024).

A literatura aponta que a aceitação de IA em serviços públicos tende a ser condicionada por percepções de benefício (como, por exemplo, rapidez e conveniência), mas também por fatores de risco (como perda de controle, erro e falta de explicação). Estudos experimentais sugerem que a confiança em chatbots de IA no setor público é sensível à transparência do sistema e ao alinhamento entre expectativa e capacidade real de resposta (Aoki, 2020). De modo complementar, pesquisas sobre adoção de serviços públicos com IA destacam que intenção de uso pode aumentar quando há clareza de propósito, explicações compreensíveis e percepção de que o cidadão mantém opções e controle sobre o atendimento (Geske; Leyer, 2022).

Chatbots baseados em modelos de linguagem podem produzir respostas plausíveis, porém incorretas quando não ancorados em evidências, o que é especialmente crítico em contextos públicos. Arquiteturas de *Retrieval-Augmented Generation* (RAG) buscam reduzir esse risco ao combinar recuperação de trechos relevantes em uma base de conhecimento com geração condicionada às evidências recuperadas (Lewis *et al.*, 2020). Em aplicações governamentais, esse desenho pode ser associado a requisitos de transparência e auditabilidade: registrar quais fontes foram consultadas e como a resposta foi construída é parte do controle organizacional e do monitoramento de qualidade. Assim, além do componente de recuperação semântica (base vetorial + *embeddings* + *chunking*), estratégias de orquestração podem adicionar etapas de qualificação de consulta (ex.: checagem de escopo e pedido de esclarecimentos) para reduzir ambiguidades e orientar o usuário a formular demandas compatíveis com o objetivo do serviço.

No contexto do setor público, a avaliação de chatbots deve ser interpretada à luz do *valor público* e da *qualidade do serviço*. Diferentemente de

aplicações estritamente comerciais, ganhos como redução de fricção, aumento de previsibilidade do atendimento e maior acesso a informações confiáveis afetam diretamente dimensões de equidade, transparência e eficiência institucional. Assim, medidas de satisfação e esforço não devem ser lidas apenas como “preferência do usuário”, mas como sinais indiretos de qualidade do desenho do serviço, adequação do escopo e capacidade do canal digital de resolver demandas informacionais com clareza e confiabilidade.

Para além da qualidade textual, avaliações de chatbots de serviço comumente incorporam medidas de experiência e esforço do usuário. Métricas como CSAT (satisfação) e CES (esforço percebido) permitem capturar dimensões complementares da interação. O CES, por exemplo, é usado para estimar quão fácil foi resolver a demanda pelo canal (Dixon; Freeman; Toman, 2010). A combinação dessas métricas com indicadores operacionais (tempo de resposta, taxa de sucesso e *logs* por etapa) tende a produzir diagnóstico mais acionável, pois conecta percepção subjetiva a gargalos técnicos e escolhas arquiteturais.

3 Metodologia

Este estudo adota abordagem metodológica mista, com desenho sequencial exploratório, combinando análise documental e implementação de protótipo com avaliação por usuários (Creswell; Clark, 2013). O enquadramento epistemológico é interpretativo com base construtivista, adequado para investigações em que a compreensão dos fenômenos depende do contexto institucional, das percepções dos participantes e dos significados atribuídos às interações com a tecnologia (Denzin; Lincoln, 2006). Como estratégia de investigação, emprega-se estudo de caso único, voltado à análise aprofundada do desenvolvimento e uso de um chatbot agêntico baseado em RAG no contexto do Ministério Público da União.

3.1 Contexto, artefato e delineamento do estudo

O objeto empírico é o ChatMPU, um chatbot agêntico multimodelo que utiliza Retrieval-Augmented Generation (RAG) para responder perguntas do cidadão sobre serviços do MPU e seus ramos, com devolutivas fundamentadas em evidências recuperadas de uma base de

conhecimento e, quando necessário, em fontes institucionais externas. A solução foi projetada para atender a demandas informacionais e de encaminhamento, com mecanismos de filtragem de escopo e solicitações de esclarecimentos para reduzir ambiguidades, mantendo registro de evidências utilizadas na resposta (Lewis *et al.*, 2020).

O estudo contempla: I) construção e configuração do artefato (pipeline agêntico + base vetorial + observabilidade); II) experimentos com usuários internos para aferir satisfação, esforço percepção e utilidade; e III) análise de *logs* do orquestrador para verificar desempenho, taxa de sucesso e gargalos operacionais, complementando os resultados perceptivos com métricas objetivas de execução.

3.2 Implementação do protótipo e ambiente de execução

A arquitetura do ChatMPU combina interface conversacional, orquestração de agentes e persistência de conhecimento. O *front-end* é disponibilizado via interface web (Openwebui, 2025), e o encadeamento das etapas é coordenado por um orquestrador de fluxos, que registra eventos e permite visualização da execução por nós e etapas (N8N, 2025). A base de conhecimento é indexada em repositório vetorial, permitindo busca semântica por similaridade e recuperação de trechos relevantes para compor o contexto do modelo gerador (Qdrant, 2025). Os modelos de linguagem utilizados foram desenvolvidos pela Maritaca AI (Maritaca.AI, 2025), laboratório brasileiro de pesquisa e inovação em modelos de linguagem abertos. Foram empregados os modelos *Sabiá 3.1* e *Sabiázinho 3*, que oferecem suporte nativo ao português brasileiro e apresentam alta eficiência de execução local, sendo utilizados para interpretar perguntas, acionar ferramentas e gerar respostas contextualizadas.

A arquitetura combina um pipeline RAG (*Retrieval-Augmented Generation*) com agentes autônomos e ferramentas de busca externas. O fluxo central é controlado pelo orquestrador, que atua como motor principal de execução e observabilidade, permitindo registrar *logs* e resultados intermediários de cada nó do pipeline. A Figura 1 apresenta o pipeline lógico com os agentes de preparação (Simples, Escopo e Esclarecimentos) e o Agente Principal que orquestra as ferramentas (RAG, Extract News e Search), além dos pontos de telemetria.

O agente principal, denominado *ChatMPU Agent*, é responsável por decidir o uso das ferramentas conforme o tipo de consulta: o *Agente RAG Qdrant* para recuperar informações estáticas das cartas de serviços e o *Search Agent Tool*, baseado em busca web via API, para buscas dinâmicas em portais de notícias institucionais.

Para reduzir alucinações e manter respostas focadas no cidadão, a solução adota uma orquestração multiagente com papéis bem definidos antes do agente principal: I) um *Agente Simples*, voltado para atender interações iniciais de apresentação, apoiar o mecanismo da interface do chatbot na geração das perguntas de acompanhamento, títulos e *tags* das conversas; II) um *Agente de Escopo (Filtro/Guardrails)*, que classifica a consulta como dentro ou fora do escopo com fundamento na base de conhecimento e no tipo de demanda (serviços do MPU, canais, notícias institucionais); e III) um *Agente de Esclarecimentos*, acionado apenas quando a pergunta é vaga/incompleta, para pedir dados faltantes (ramo/órgão, tipo de serviço, localidade, datas) antes de acionar ferramentas. Essa etapa pré-RAG melhora a precisão, reduz o uso desnecessário de busca e torna o fluxo auditável.

A camada de armazenamento vetorial foi implementada com o *Qdrant*, escolhido por sua performance em recuperação semântica e compatibilidade com *embeddings* densos. O modelo de *embeddings* utilizado é o *EmbeddingGemma* quantizado (Vera et al., 2025), executado via Ollama (Ollama, 2026) em ambiente ARM, devido à sua alta eficiência e ao seu suporte multilíngue, com excelente desempenho para o português-brasileiro. Essa configuração garante precisão semântica com baixo custo de inferência. Já o reranqueamento das respostas é realizado pelo modelo *Cohere Multilingual Reranker v3* (Cohere, 2025), que melhora a relevância dos trechos recuperados.

Os experimentos e coletas foram realizados em ambiente Linux (Ubuntu), com instância computacional de 4 vCPU (ARM), 24 GB de RAM e 50 GB de armazenamento, com persistência e registro de execuções em banco relacional para apoiar rastreabilidade e auditoria do pipeline (Postgresql, 2025). Para geração e composição de respostas, o sistema utiliza modelos de linguagem configurados no *back-end*, com parametrizações de temperatura e limites de *tokens* ajustados para equilibrar consistência das respostas e latência operacional.

3.3 Base de conhecimento e estratégia de RAG

A base de conhecimento foi construída a partir de documentos institucionais e páginas oficiais, selecionados por relevância para as perguntas mais frequentes sobre atuação e serviços do MPU. O conteúdo é segmentado em unidades textuais (*chunks*) com sobreposição controlada, visando preservar continuidade semântica e reduzir perda de contexto em consultas longas. Cada *chunk* é representado por *embeddings* e indexado para recuperação semântica. Na etapa de resposta, o orquestrador realiza: I) interpretação da intenção do usuário; II) checagem de escopo e necessidade de esclarecimentos; III) recuperação dos trechos mais relevantes; e IV) geração final com citação das evidências recuperadas (Lewis *et al.*, 2020).

A ingestão dos documentos na base vetorial foi realizada com o uso do modelo de *embeddings EmbeddingGemma* (Vera *et al.*, 2025), que gera representações textuais densas de 768 dimensões, adequadas para aplicações multilíngues e de alta precisão semântica. O particionamento dos textos seguiu a estratégia de *recursive chunking*, configurada com tamanho médio de 1500 caracteres e sobreposição de 200, parâmetros considerados ideais para documentos administrativos de média complexidade e estrutura variada, como as cartas e guias de serviços do MPU.

O processo resultou em 458 *chunks*, com comprimento médio de 1121,87 caracteres, mínimo de 186 e máximo de 1500 caracteres, garantindo equilíbrio entre granularidade e preservação de contexto. Cada *chunk* foi armazenado com metadados associados, incluindo nome do documento original, URL de origem, ramo institucional inferido a partir do nome do arquivo e o texto integral correspondente.

3.4 Participantes e procedimentos de coleta

A seleção dos participantes ocorreu por *amostragem por conveniência*, a partir de convites enviados a servidores com diferentes perfis de atuação, buscando diversidade de contexto e evitando concentração em uma única unidade. Antes da interação, foi apresentado aos participantes um breve enquadramento sobre o objetivo do protótipo, seu *escopo informacional* e suas *limitações* (incluindo a orientação de que o chatbot não substitui

atendimento jurídico, análise de caso concreto ou decisões administrativas). A interação foi realizada em duas modalidades: I) *tarefas orientadas*, em que o participante executou demandas típicas de encaminhamento e busca de serviços (por exemplo: localizar o canal adequado para registrar uma demanda; identificar unidade/ramo competente; obter requisitos e documentos para um serviço específico); e II) *perguntas livres*, dentro do escopo do sistema, permitindo avaliar naturalidade e utilidade prática.

Ao final, os participantes responderam a questionário estruturado contendo itens de *CSAT* (escala 1–5) e *CES* (escala 1–7), além de questões sobre tempo percebido de resposta, intenção de reutilização e comparação subjetiva com canal humano, complementadas por campo aberto para comentários. Para assegurar consistência, respostas incompletas foram tratadas por exclusão apenas do item específico (sem descarte do respondente), mantendo o tamanho amostral em cada métrica conforme disponibilidade de respostas.

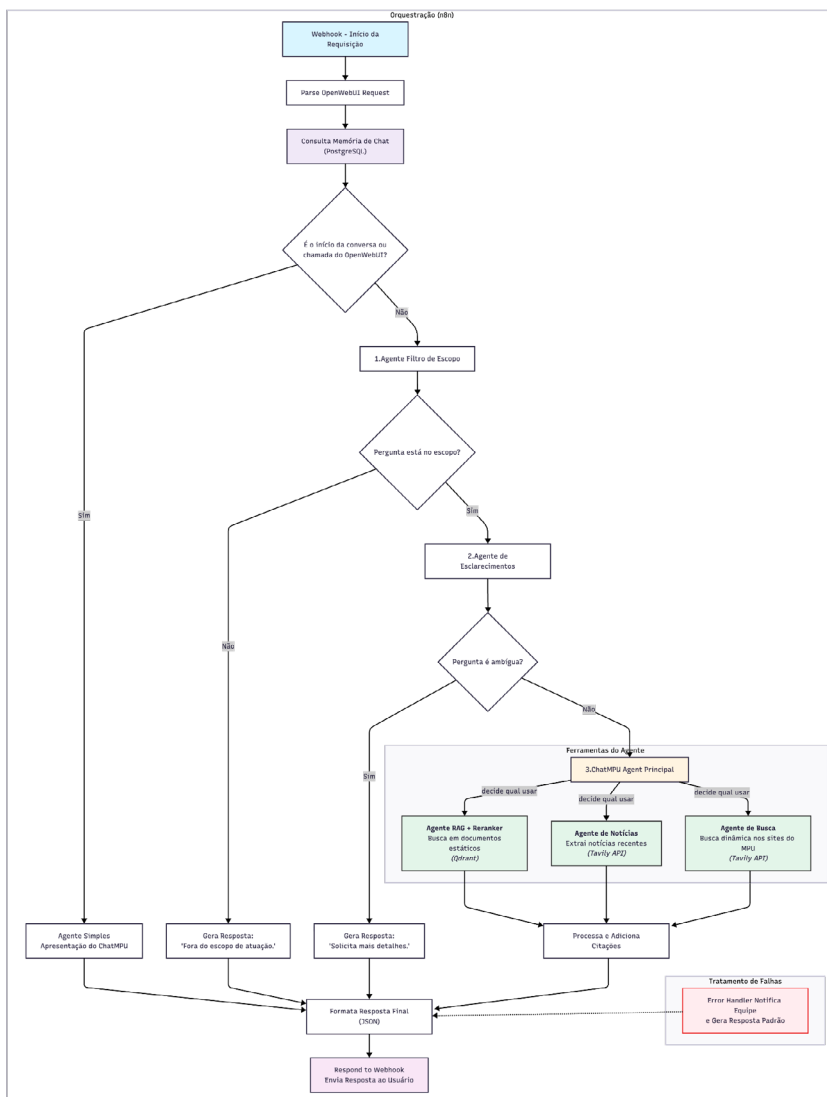
Para complementar a avaliação, foram coletados *logs* do orquestrador, registrando cada execução e seus resultados (sucesso/erro), latência total, latência por etapa e tipologia de interações (ex.: perguntas diretas, pedidos de esclarecimento, consultas fora do escopo). Esses dados foram utilizados para triangulação entre percepção do usuário e desempenho observável do sistema.

3.5 Instrumentos e métricas

A avaliação quantitativa utilizou: I) *CSAT* (*Customer Satisfaction Score*) em escala de 1 a 5 para medir satisfação global com o atendimento; II) *CES* (*Customer Effort Score*) em escala de 1 a 7 para estimar esforço percebido pelo usuário ao resolver sua necessidade via chatbot; III) percepção de tempo de resposta; IV) intenção de reutilização; e V) comparação subjetiva com canal humano (Dixon; Freeman; Toman, 2010). Para interpretação, foram calculadas estatísticas descritivas, intervalos de confiança e medidas de concentração (ex.: Top-2-Box) para facilitar a leitura gerencial (Farris *et al.*, 2010).

Na dimensão qualitativa, as respostas abertas foram analisadas por análise temática, permitindo organizar percepções em categorias (pontos fortes, limitações, sugestões e riscos percebidos), com codificação iterativa e consolidação das temáticas emergentes (Braun; Clarke, 2006).

Figura 1 – Fluxo lógico de orquestração dos agentes e ferramentas do ChatMPU



Fonte: elaboração própria.

3.6 Aspectos éticos, privacidade e tratamento de dados

O estudo priorizou a minimização de dados pessoais e anonimização das informações coletadas. O chatbot foi avaliado com foco em

demandas informacionais e de encaminhamento, sem coleta de dados sensíveis como requisito para resposta. As interações e questionários foram tratados de forma agregada, com supressão de identificadores diretos e indiretos, atendendo princípios de necessidade e finalidade previstos na legislação brasileira de proteção de dados (Brasil, 2018).

A participação no experimento ocorreu de forma voluntária, mediante consentimento informado, com possibilidade de desistência a qualquer momento. Os registros de interação foram utilizados exclusivamente para fins de pesquisa e melhoria do protótipo, com acesso restrito à equipe do projeto e sem associação a identificadores pessoais. Adicionalmente, por se tratar de atendimento informacional, o chatbot reforça limitações de escopo e orienta o usuário a buscar canais institucionais adequados quando houver necessidade de análise de caso concreto, reduzindo risco de uso indevido e alinhando a solução a princípios de responsabilidade e transparência.

4 Resultados e discussão

4.1 Arquitetura técnica e observabilidade

A solução foi estruturada para combinar robustez de recuperação (RAG) e controle de execução via orquestração de agentes. O fluxo operacional inicia com interpretação da consulta e checagem de escopo; quando necessário, solicita esclarecimentos para refinar a intenção do usuário e reduzir ambiguidades. Em seguida, realiza recuperação semântica na base vetorial e gera resposta final ancorada em trechos recuperados, com indicação explícita de evidências utilizadas. Essa organização busca mitigar alucinações e aumentar rastreabilidade, favorecendo transparência na interação (Lewis *et al.*, 2020).

O sistema foi projetado para funcionar em infraestrutura híbrida (local e em nuvem), exigindo desempenho estável, baixo tempo de resposta e segurança no tratamento dos dados. Entre os requisitos principais estão a *compatibilidade com o idioma português-brasileiro*, a *integração com múltiplas fontes de informação* (documentos institucionais, sites oficiais e notícias recentes) e a *observabilidade completa das execuções dos agentes*. Essas diretrizes motivaram a adoção de ferramentas com

suporte nativo a fluxos visuais e *logs* detalhados, em vez de frameworks emergentes, cuja curva de implementação seria mais longa e de menor transparência operacional para auditorias.

Durante a fase de implementação, diversos desafios técnicos foram identificados e solucionados de forma iterativa. Um dos principais desafios esteve relacionado à otimização do uso de recursos computacionais, especialmente de CPU e memória, devido às demandas elevadas do serviço de *embeddings* e do banco de dados. Para contornar esse problema, o banco de dados foi migrado de um ambiente diferente de nuvem para o mesmo ambiente dos demais serviços. Foi realizada também uma configuração customizada dos limites e reservas de recursos para cada serviço, garantindo o equilíbrio entre desempenho e estabilidade. O serviço de *embeddings* recebeu a maior alocação de recursos para assegurar a rapidez das buscas, enquanto o banco de dados foi otimizado com parâmetros específicos para leitura e escrita em ambiente de nuvem. Essa otimização refletiu-se em menor latência de resposta e maior disponibilidade do sistema.

Do ponto de vista da inteligência artificial, um desafio recorrente foi assegurar que o agente de IA utilizasse consistentemente as ferramentas de agente RAG (*Retrieval-Augmented Generation*) e identificasse quando usar o agente de busca nos sites institucionais. A solução encontrada envolveu a experimentação com modelos de linguagem mais “obedientes”, como o Sabia 3.1, que demonstraram maior propensão a seguir as instruções de uso das ferramentas designadas. Outros obstáculos técnicos foram os diversos ajustes e testes no script de ingestão de dados da base de conhecimento. Entre eles, pode-se citar a correção de falhas para corrigir a inclusão dos metadados e estratégias de *chunk* (particionamento dos textos).

A formatação das citações no texto gerado, visando integrá-las ao padrão nativo à interface do chatbot com o usuário, apresentou-se como um desafio complexo, levando a modificações diretas no código-fonte da interface e à criação de um pipeline alternativo para testar a injeção de referências *inline* (diretamente ao lado da frase de resposta), embora os resultados iniciais não tenham sido plenamente satisfatórios. Por fim, para aumentar a confiabilidade do sistema, foi implementado um nó dedicado ao tratamento de erros, que fornece uma resposta padrão

ao usuário em caso de falha e notifica a equipe técnica por e-mail, melhorando significativamente a robustez da solução.

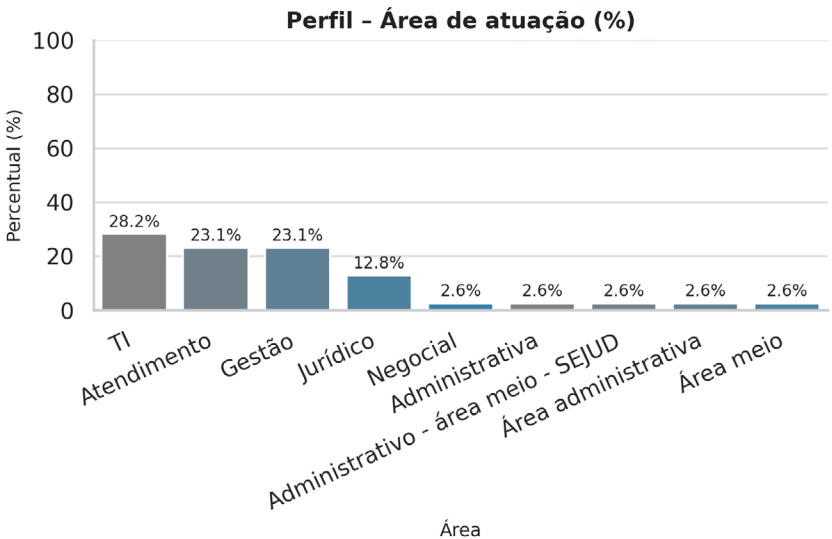
No que se refere às estratégias de recuperação de informação, a implementação inicial concentrou-se no uso exclusivo de *embeddings* densos, gerados pelo modelo *EmbeddingGemma* (Vera *et al.*, 2025), que combina alto desempenho em tarefas multilíngues e sua natureza computacionalmente eficiente mesmo em versões quantizadas, características ideais para a aplicação no setor público. Essa abordagem demonstrou desempenho satisfatório em termos de precisão semântica e tempo de resposta. Entretanto, o planejamento de evolução da arquitetura prevê a adoção de uma busca híbrida, combinando *embeddings* densos e esparsos com técnicas de pré-busca (*prefetch*) e fusão de classificação recíproca (*reciprocal rank fusion* – RRF), visando melhorar ainda mais a precisão e a cobertura da recuperação de informações. Essa segunda fase representa uma evolução natural da arquitetura e está alinhada com as boas práticas contemporâneas em sistemas de RAG de alta performance.

Em síntese, a análise da arquitetura e da implementação do ChatMPU demonstra que a combinação entre modularidade, otimização de recursos e integração entre ferramentas de orquestração, inferência e persistência de dados foi determinante para o sucesso da solução. As decisões de design, como o uso de infraestrutura containerizada e o foco em pipelines auditáveis e reproduzíveis, garantiram escalabilidade e confiabilidade ao sistema. Os desafios enfrentados ao longo do desenvolvimento permitiram aprimorar a maturidade técnica do projeto, consolidando o ChatMPU como uma base sólida para futuras aplicações de agentes conversacionais no setor público.

4.2 Experimentos com usuários

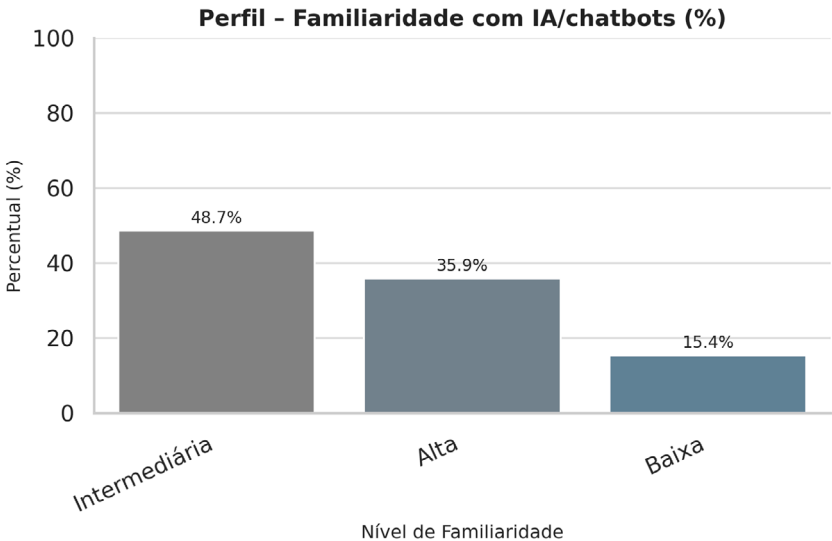
Participaram 39 respondentes com servidores de diferentes áreas de atuação institucional, garantindo diversidade de contextos de uso e demandas (*vide* Figura 2) e predominantemente familiarizadas com chatbot, conforme Figura 3.

Figura 2 – Área de atuação



Fonte: elaboração própria.

Figura 3 – Familiaridade com IA/Chatbots



Fonte: elaboração própria.

4.2.1 Resultados quantitativos

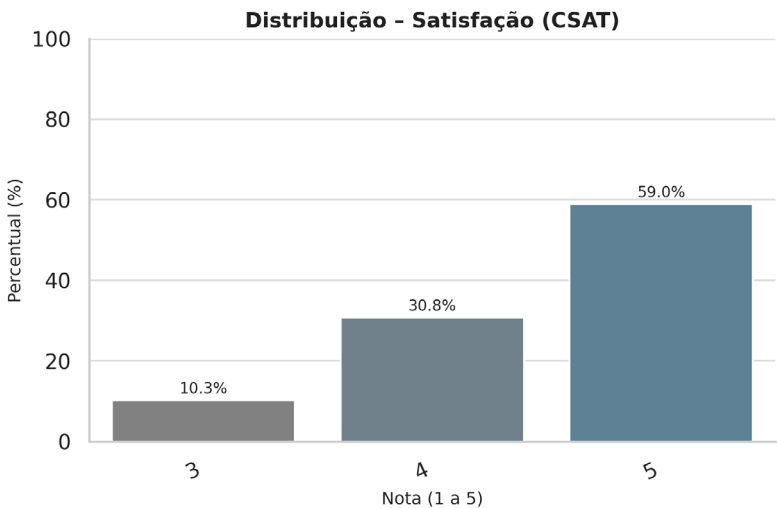
A média de satisfação (CSAT, escala 1–5) foi de 4,49 (IC95% [4,27; 4,71], n=39), indicando avaliação muito positiva. Em termos de concentração, o Top-2-Box (notas 4-5) atingiu 89,7%, sugerindo elevada aceitação do chatbot como canal informacional (*vide* Figura 4).

A média de esforço percebido (CES, escala 1–7) foi 6,23 (IC95% [5,88; 6,58], n=39), com Top-2-Box (notas 6-7) de 82,1%, sinalizando que a maioria considerou fácil resolver sua necessidade com o ChatMPU (Dixon; Freeman; Toman, 2010), conforme Figura 5.

A percepção de tempo de resposta foi positivamente avaliada, com média 3,97/5 (Figura 6), sugerindo que o desempenho foi considerado adequado para o contexto de uso, embora existam oportunidades de otimização em cenários de maior carga.

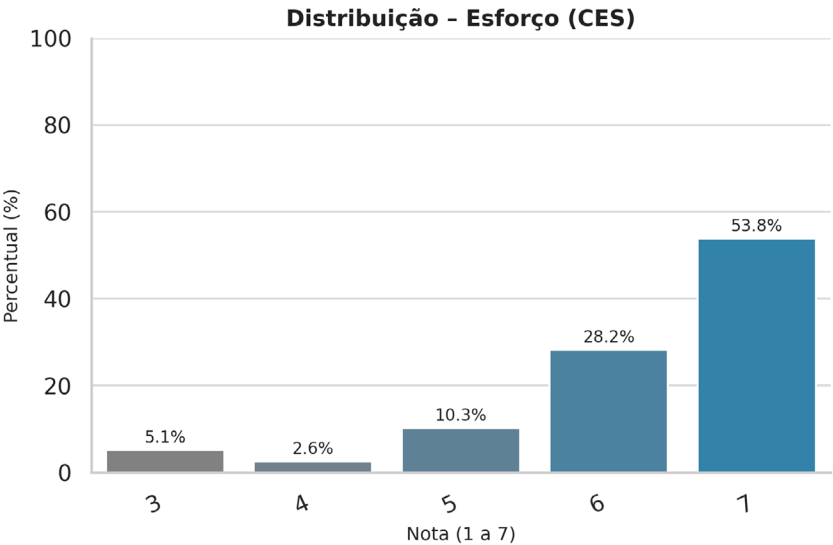
A intenção de reutilização foi elevada (89,7% responderam que usariam novamente e 10,3% “talvez”), indicando potencial de adoção recorrente (Figura 7). Na comparação com atendimento humano, predominaram avaliações de equivalência ou superioridade do chatbot para demandas informacionais de encaminhamento e orientação, com ressalvas quando a demanda exige análise contextual complexa.

Figura 4 – Distribuição CSAT



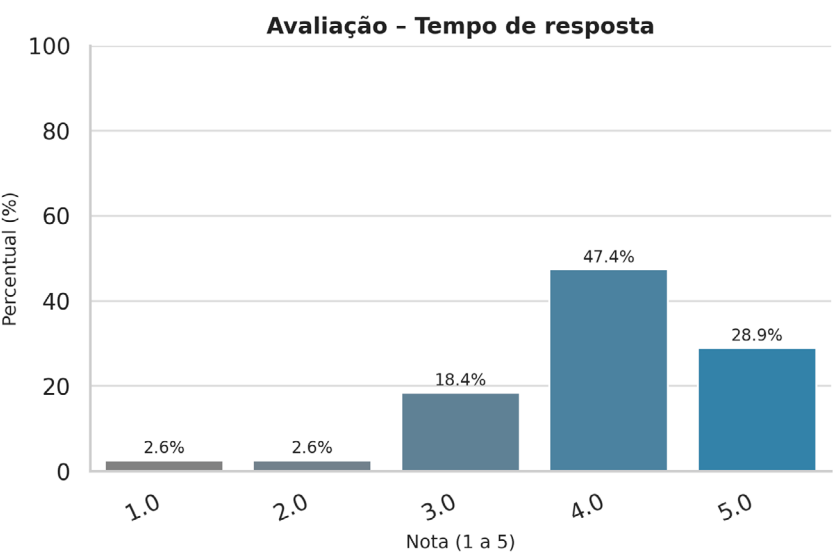
Fonte: elaboração própria.

Figura 5 – Distribuição CES



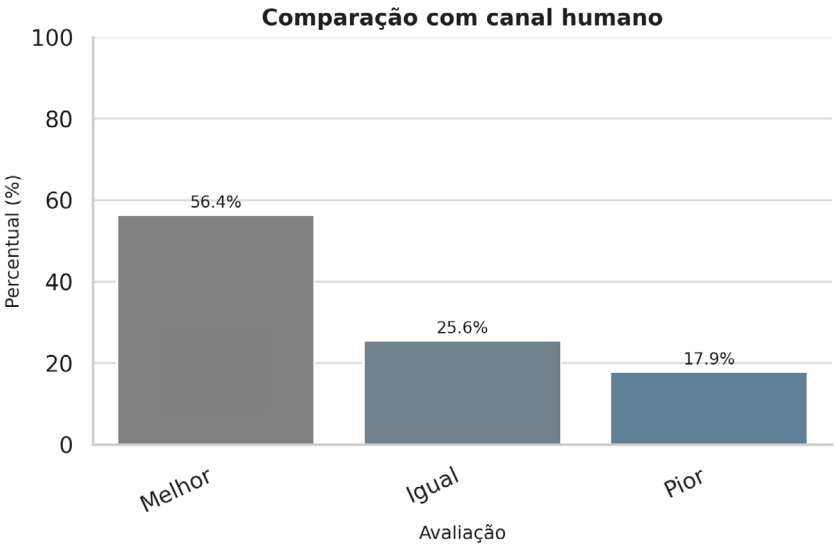
Fonte: elaboração própria.

Figura 6 – Tempo de resposta



Fonte: elaboração própria.

Figura 7 – Comparação com canal humano



Fonte: elaboração própria.

Em conjunto, os resultados quantitativos sugerem que o ChatMPU atende a um conjunto relevante de demandas informacionais com alta aceitação, baixo esforço percebido e percepção de tempo satisfatória, o que é consistente com o papel de chatbots como porta de entrada para triagem e orientação, desde que o escopo seja claramente delimitado.

4.2.2 Resultados qualitativos

A análise temática das respostas abertas (Braun; Clarke, 2006) evidenciou quatro eixos principais:

1. Clareza e utilidade prática: participantes relataram que o chatbot fornece orientação objetiva e facilita encontrar o setor competente, reduzindo tempo de busca em páginas institucionais dispersas.
2. Confiança e fundamentação: a presença de evidências e referências recuperadas foi apontada como elemento relevante para aumentar confiabilidade e permitir verificação da informação.
3. Limitações e escopo: surgiram pedidos para ampliar cobertura de conteúdos e melhorar tratamento de perguntas ambíguas; também

houve sinalização de que o chatbot deve reforçar limites para não substituir orientação jurídica ou decisões administrativas.

4. Sugestões de melhoria: destacaram-se melhorias no desempenho (redução de latência), maior consistência na formatação de respostas e maior robustez em casos de consulta fora do escopo (com encaminhamento explícito para canal humano).

Esses achados qualitativos reforçam que a aceitação depende não apenas de “acerto factual”, mas também de explicitar limites, manter linguagem clara e oferecer caminhos de escalonamento quando a demanda ultrapassa o escopo do sistema.

4.3 Análise das interações no pipeline do orquestrador (logs)

Foram analisadas 2.597 execuções no pipeline do orquestrador, das quais 375 (14,4%) corresponderam a interações reais, enquanto o restante, 2.222 (85,6%), foram de interações internas automáticas do próprio chatbot. Essas execuções internas são responsáveis por tarefas auxiliares, como a geração automática de títulos, perguntas de acompanhamento e tags, compondo o comportamento autônomo do agente Simples.

O tempo total acumulado de processamento foi de 12.897,73 segundos (aproximadamente 3,58 horas). O desempenho geral foi estável, onde a taxa de sucesso de execução do pipeline foi de 99,73%, o tempo médio de resposta foi de 21,23s nas interações reais, o tempo médio nas chamadas auxiliares foi de 1,03s e o tempo máximo observado foi de 164s (*outlier* de requisições compostas).

Cabe ressaltar que a taxa de sucesso reportada refere-se ao sucesso técnico de execução do pipeline (fluxo concluído sem falha/*timeout*), e não necessariamente à “resolução completa” da demanda em todos os casos. Por essa razão, a análise combina métricas técnicas com medidas de experiência do usuário (CSAT/CES) e comentários qualitativos, permitindo distinguir estabilidade operacional de efetividade percebida no atendimento.

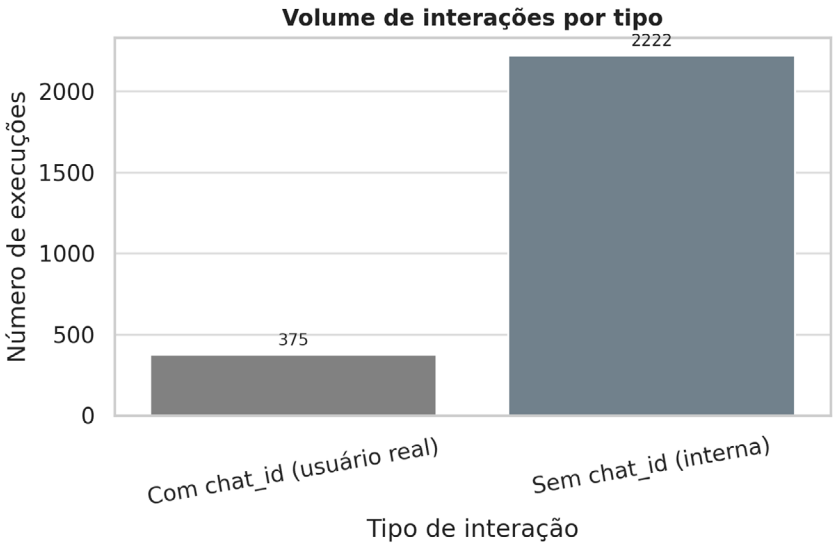
A Figura 8 ilustra o volume de interações por tipo, enquanto a Figura 9 demonstra a taxa de sucesso quase integral das execuções. A distribuição dos resultados (sucesso, erro, *timeout*) encontra-se na Figura 10 e o tempo médio por categoria é mostrado na Figura 11.

Como padrão, as etapas com maior custo de tempo concentraram-se em chamadas sequenciais a múltiplos agentes e na consolidação final da resposta com formatação e citações. Em termos de engenharia, esse diagnóstico sugere que otimizações podem ser obtidas por: I) paralelização de agentes independentes; II) cache semântico para respostas repetidas; III) redução do volume de contexto enviado ao modelo por filtragem mais agressiva dos trechos recuperados; e IV) ajustes de temperatura/*tokens* para reduzir variabilidade e custo computacional em consultas simples.

Ao detalhar o pipeline, verificou-se que 87,23% do tempo total de execução é consumido por agentes baseados em modelos de linguagem (LLMs), especialmente nos nós “ChatMPU Agent”, “Filtro de Escopo” e “Esclarecimentos”. O “ChatMPU Agent” foi o maior gargalo, respondendo por 24,6% do tempo total, com tempo médio de 11,7s por execução.

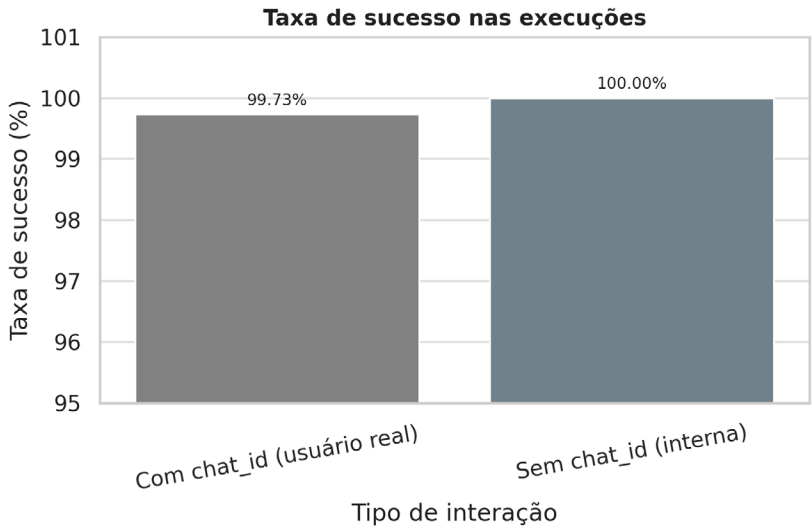
A Figura 12 apresenta o tempo médio por tipo de ferramenta, destacando que o “Search Agent Tool” (buscas externas) e o “Agente RAG Qdrant” são os componentes mais sensíveis à latência.

Figura 8 – Volume de interações por tipo



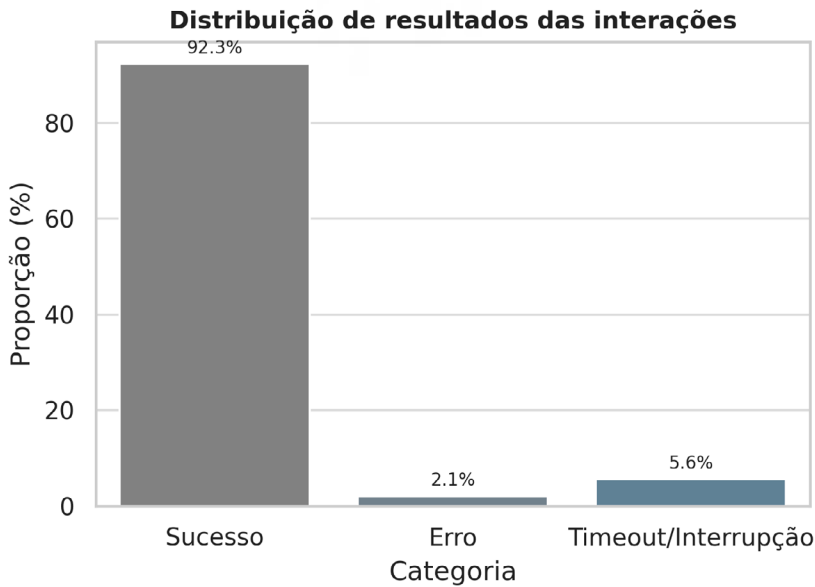
Fonte: elaboração própria.

Figura 9 – Taxa de sucesso nas execuções



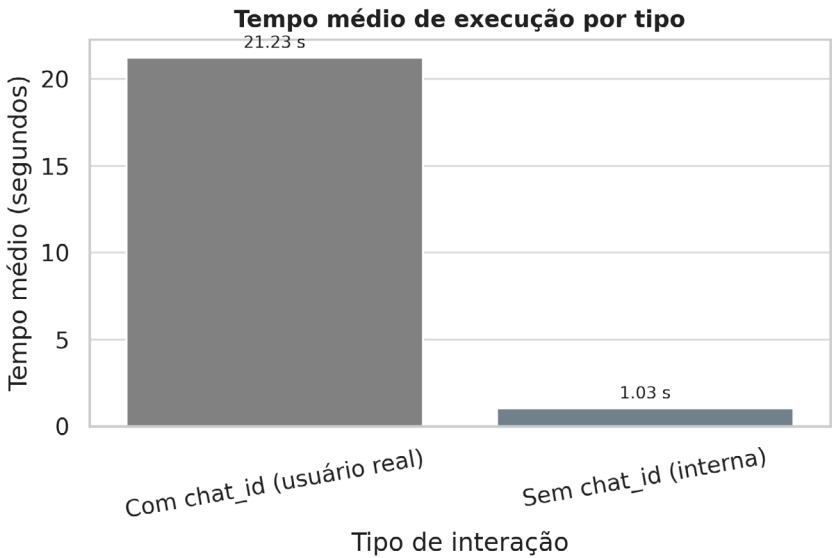
Fonte: elaboração própria.

Figura 10 – Distribuição de resultados das interações



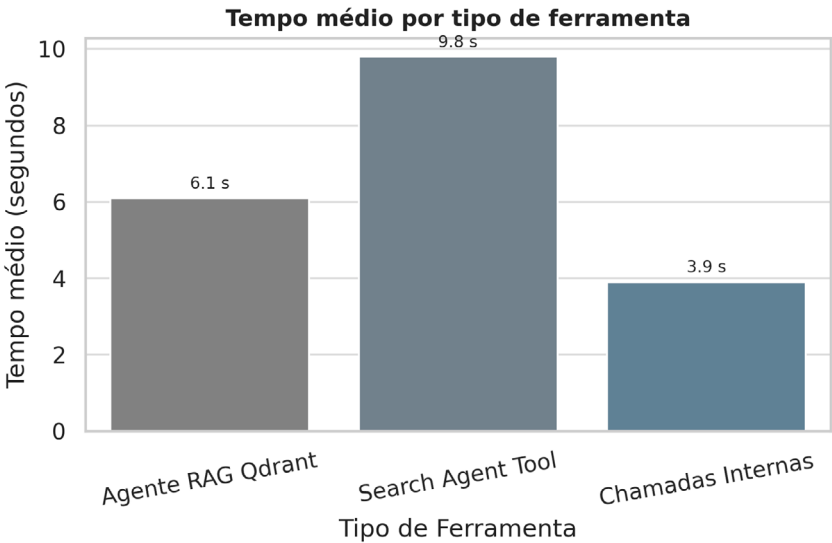
Fonte: elaboração própria.

Figura 11 – Tempo médio de execução por tipo de interação



Fonte: elaboração própria.

Figura 12 – Tempo médio por tipo de nó



Fonte: elaboração própria.

4.4 Análise dos agrupamentos da base de conhecimento

Com o objetivo de compreender a estrutura semântica da base vetorial e avaliar a consistência dos *chunks* gerados, realizou-se uma análise de agrupamento utilizando os vetores armazenados no Qdrant. Os *embeddings* foram projetados em duas dimensões por meio do algoritmo *t-SNE* e agrupados por *K-Means*, resultando em cinco *clusters* principais, com melhor pontuação de *Silhouette* igual a 0,108 para $k=5$, *Davies–Bouldin* de 3,53 e *Calinski–Harabasz* de 19,96 (Kaufman; Rousseeuw, 2009; Davies; Bouldin, 1979; Calinski; Harabasz, 1974). Esses indicadores sugerem que os *chunks* apresentam coesão temática moderada, ainda que com sobreposição entre tópicos correlatos, o que é esperado em documentos institucionais com terminologia compartilhada entre os ramos do MPU (Calinski; Harabasz, 1974; Kaufman; Rousseeuw, 2009).

Em termos práticos, a análise de agrupamentos permite detectar: I) clusters coesos, sugerindo temas bem representados e recorrentes; e II) clusters heterogêneos, que podem indicar necessidade de refinamento no *chunking*, inclusão de documentos ou revisão de taxonomias. Essa etapa não substitui avaliação de qualidade de resposta, mas contribui para governança do conhecimento e para melhoria incremental do RAG.

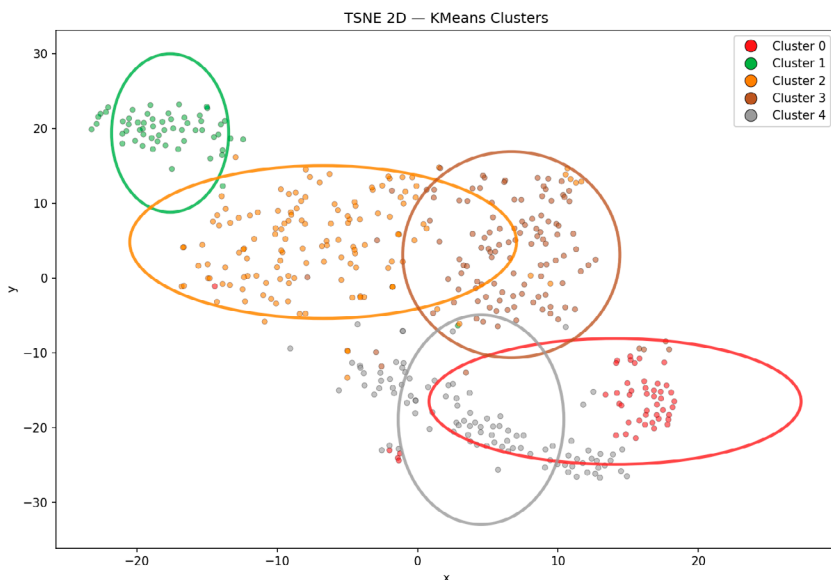
A análise de agrupamento (*clustering*) sobre os vetores semânticos da base Qdrant permitiu identificar padrões de similaridade entre os *chunks* textuais extraídos dos documentos do MPU. A Figura 13 apresenta a projeção bidimensional (*t-SNE*) dos vetores semânticos da base de conhecimento do ChatMPU, agrupados pelo algoritmo *K-Means* em 5 clusters principais. Cada ponto representa um *chunk* (pedaço) textual de um documento institucional, e as elipses destacam as regiões de maior densidade temática.

A análise combinou as palavras-chave predominantes de cada agrupamento, obtidas via TF-IDF, e o documento mais frequente identificado, de modo a avaliar a coerência e a diversidade de conteúdos. Essa análise revelou padrões semânticos bem definidos, com variações na coesão e na diversidade dos conteúdos.

O Cluster 0, com 81,2% de seus trechos provenientes do arquivo *carta-servicos-mpt.pdf*, apresentou estrutura densa e homogênea, concentrando fragmentos administrativos e de identificação institucional do Ministério Público do Trabalho (MPT).

O Cluster 1 destacou-se pela menor dispersão entre todos os grupos, sendo formado quase integralmente por textos da *carta-de-servicos-esmpu.pdf* (94,8%). Suas palavras-chave (*esmpu*, *carta*, *atendimento* e *escola*) evidenciam foco em serviços educacionais e relacionamento com o usuário, configurando um domínio altamente específico e bem delimitado.

Figura 13 – Distribuição bidimensional dos clusters (t-SNE + K-Means)



Fonte: elaboração própria.

O Cluster 2, por sua vez, foi o mais heterogêneo, com apenas 40% de trechos provenientes de um único arquivo, *carta-servicos-mpdft.pdf*. Essa diversidade reflete a sobreposição entre conteúdos do MPF e do MPDFT, reunindo tópicos sobre atendimento ao cidadão, canais de ouvidoria e informações gerais, caracterizando um agrupamento transversal e de linguagem mais genérica.

O Cluster 3 manteve composição semelhante, também ancorado no mesmo documento (39,7%), mas com vocabulário marcadamente institucional, incluindo termos como *ministério público*, *justiça*, *militar* e *federal*, associados a descrições jurídico-administrativas e à atuação junto à Justiça Militar.

Por fim, o Cluster 4 mostrou-se altamente coeso, com 96% de seus trechos oriundos do MPT. As palavras predominantes (*trabalho, ofícios e fiscalização*) confirmam a consistência temática do grupo, voltado às atribuições e aos procedimentos internos da instituição.

De modo geral, os resultados indicam que os clusters C1 e C4 possuem a menor diversidade interna, representando domínios bem definidos, enquanto o C2 exibe a maior variação temática, abrangendo conteúdos comuns a diferentes ramos do MPU. Essa distribuição demonstra que o modelo de *embeddings* preserva adequadamente a estrutura semântica dos textos e que a base vetorial reflete tanto a especialização institucional quanto as regiões de interseção entre serviços e áreas de atendimento ao público.

Esses resultados reforçam a eficácia do modelo *EmbeddingGemma* em preservar as relações semânticas e a adequação da estratégia de *recursive chunking* na manutenção de coesão temática. A presença de agrupamentos coerentes, porém com graus distintos de diversidade, indica que o pipeline de ingestão e indexação do ChatMPU captura tanto a especificidade de cada ramo quanto as interseções linguísticas entre eles, característica essencial para o desempenho do sistema RAG na recuperação contextual de informações.

Em termos metodológicos, a distribuição observada sugere que futuras otimizações podem focar no balanceamento da base vetorial, sobretudo reduzindo a predominância de documentos do MPT e do MPDFT e incorporando mais exemplos de outros ramos e serviços.

4.5 Implicações para a gestão pública e replicabilidade

Os achados sugerem implicações práticas para adoção de chatbots baseados em IA no setor público, especialmente em serviços com alta demanda informacional e necessidade de rastreabilidade. Em primeiro lugar, a delimitação explícita de escopo e a existência de um mecanismo de esclarecimentos reduzem ambiguidades e evitam o acionamento desnecessário de buscas externas, favorecendo a eficiência e a previsibilidade do atendimento. Em segundo lugar, a resposta ancorada em evidências recuperadas e a manutenção de trilhas de execução (*logs* por etapa) contribuem para auditabilidade, facilitando a supervisão, a melhoria contínua e a prestação de contas.

Do ponto de vista operacional, os resultados indicam que a observabilidade do pipeline permite transformar “qualidade percebida” em medidas acionáveis de gestão, ao revelar onde se concentram os custos de tempo e variabilidade. Para replicação, destacam-se as recomendações: I) adotar um conjunto mínimo de indicadores combinando experiência do usuário (CSAT/CES) e desempenho do serviço (latência, taxa de erro e taxa de esclarecimentos); II) priorizar governança da base de conhecimento (curadoria, atualização, padronização de fontes e metadados); III) estabelecer regras claras de encaminhamento para canal humano quando a demanda extrapolar o escopo; e IV) tratar o chatbot como componente de um serviço, com rotinas de monitoramento, ciclos de melhoria e documentação técnica compatível com auditorias.

4.6 Limitações e trabalhos futuros

Este estudo possui limitações típicas de estudos de caso: amostra não probabilística, avaliação em contexto institucional específico e potencial viés de seleção por participação voluntária. Além disso, o período de observação e o volume de interações reais, embora relevantes para diagnóstico inicial, não capturam todas as variabilidades de uso em larga escala.

Como estudos futuros, recomenda-se: I) ampliar testes com públicos mais diversos, incluindo usuários externos; II) implementar experimentos A/B para avaliar impactos de diferentes estratégias de *chunking*, *embeddings* e número de trechos recuperados; III) incluir avaliação automática de qualidade de respostas em tarefas com referência, quando aplicável (ex.: pertinência, fidelidade a evidências e cobertura de contexto); IV) reduzir latência por paralelização, cache semântico e otimização do agente consolidador; e V) aperfeiçoar governança da base, com processos de atualização periódica e auditoria de conteúdos sensíveis.

5 Considerações finais

Este estudo teve como objetivo desenvolver e avaliar um chatbot agêntico multimodelo baseado em RAG para facilitar o acesso do cidadão aos serviços e informações do Ministério Público da União e seus ramos. A pesquisa partiu do desafio de centralizar informações

dispersas e melhorar a eficiência do atendimento informacional em um contexto de crescente demanda e limitação de recursos humanos.

Os resultados demonstraram a viabilidade técnica da solução proposta e sua adequação ao contexto institucional analisado. A arquitetura multiagente, aliada ao uso de RAG e à ênfase em observabilidade, mostrou-se capaz de fornecer respostas consistentes, auditáveis e alinhadas aos princípios de governança digital. A solução apresentou elevados índices de satisfação e facilidade de uso, além de alta taxa de sucesso técnico, indicando equilíbrio entre desempenho e aceitabilidade.

Do ponto de vista organizacional, o artigo oferece evidências empíricas de que chatbots baseados em inteligência artificial podem contribuir para a modernização do atendimento ao público, reduzindo a sobrecarga de trabalho humano e ampliando o acesso à informação, o que corrobora estudos como o de Izzo *et al.* (2021). A abordagem adotada, baseada em componentes de código aberto, reforça o potencial de replicabilidade e adaptação da solução em outros órgãos do sistema de justiça e da Administração Pública.

Entre as limitações do estudo, destacam-se o recorte em um único contexto organizacional e a amostragem não probabilística (Marconi; Lakatos, 2017), que restringem a generalização dos resultados. Ainda assim, os achados fornecem subsídios relevantes para futuras implementações e pesquisas.

Como estudos futuros, apontam-se o aprofundamento da avaliação com usuários externos; a incorporação de métricas automáticas de qualidade das respostas; estudos comparativos entre diferentes modelos e estratégias de RAG, bem como a ampliação da base de conhecimento; e a integração com outros sistemas institucionais. Dessa forma, a pesquisa contribui para o avanço do debate sobre o uso responsável e eficaz da inteligência artificial no setor público, com foco na inovação centrada no cidadão.

Como reforço à replicabilidade, pretende-se disponibilizar os principais *artefatos técnicos* do estudo em repositório público, incluindo scripts de ingestão (sem dados sensíveis), estrutura de métricas, parâmetros de *chunking/embeddings* e versões anonimizadas dos fluxos de orquestração, de modo a permitir reprodução do pipeline em contextos semelhantes e facilitar comparações futuras entre estratégias de RAG e modelos.

Referências

AOKI, Naomi. An experimental study of public trust in AI chatbots in the public sector. **Government Information Quarterly**, London, v. 37, n. 4, 2020. DOI: <https://doi.org/10.1016/j.giq.2020.101490>.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral da Proteção de Dados Pessoais (LGPD). Brasília-DF: Presidência da República, ago. 2018.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology. **Qualitative Research in Psychology**, v. 3, n. 2, p. 77-101, 2006. DOI: <https://doi.org/10.1191/1478088706qp063oa>.

BRUNO, Alysson Martins. **Desenvolvimento de um chatbot com inteligência artificial para atendimento aos cidadãos pela Justiça Eleitoral do Tocantins**. 2024. Dissertação (Mestrado em Modelagem Computacional e Sistemas) – Universidade Federal do Tocantins, Palmas, 2024. Disponível em: <https://tinyurl.com/4xs4a7c5>. Acesso em: 15 out. 2025.

CALINSKI, Tadeusz; HARABASZ, J. A dendrite method for cluster analysis. **Communications in Statistics**, v. 3, n. 1, p. 1-27, 1974. DOI: <https://doi.org/10.1080/03610927408827101>.

COHERE. Cohere Multilingual Reranker v3. **Cohere API**, 2025. Disponível em: <https://tinyurl.com/3ce9uutm>. Acesso em: 15 out. 2025.

CORTÉS-CEDIEL, María. E. *et al.* Trends and challenges of e-government chatbots: advances in exploring open government data and citizen participation content. **Government Information Quarterly**, London, v. 40, n. 4, 2023.

CRESWELL, John W.; CLARK, Vicki L. Plano. **Pesquisa de métodos mistos**. 2. ed. Porto Alegre: Penso, 2013.

DAVENPORT, Thomas H; RONANKI, Rajeev. **Artificial intelligence for the real world**: don't start with moon shots. Boston: Harvard Business Review, 2018.

DAVIES, David L.; BOULDIN, Donald W. A Cluster separation measure. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 1, n. 2, p. 224-227, 1979. DOI: <https://doi.org/10.1109/TPAMI.1979.4766909>.

DENZIN, Norman K.; LINCOLN, Yvonna S. **O planejamento da pesquisa qualitativa**: teorias e abordagens. 2. ed. Porto Alegre: Artmed, 2006.

DIXON, Matthew; FREEMAN, Karen; TOMAN, Nicholas. Stop trying to delight your customers. **Harvard Business Review**, Massachusetts, 2010.

FARRIS, Paul W. *et al.* **Marketing metrics**: the definitive guide to measuring marketing performance. 2 ed. New Jersey: Pearson, 2010.

GESK, Tanja Sophie; LEYER, Michael. Artificial intelligence in public services: when and why citizens accept its usage. **Government Information Quarterly**, London, v. 39, 2022. DOI: <https://doi.org/10.1016/j.giq.2022.101704>.

IZZO, Beatriz Balestro *et al.* O uso de chatbot para inovação no atendimento em gestão de pessoas no Senado Federal. *In: ENCONTRO BRASILEIRO DE ADMINISTRAÇÃO PÚBLICA (EBAP)*, 8., 2021, Brasília. **Sociedade Brasileira de Administração Pública**, GT 6 Inovação e Empreendedorismo no Setor Público, Brasília-DF, 2021.

KAUFMAN, Leonard; ROUSSEUW, Peter J. **Finding groups in data**: an introduction to cluster analysis. New York: John Wiley & Sons, 2009.

LARSEN, Anna Grøndahl; FØLSTAD, Asbjørn. The impact of chatbots on public service provision: a qualitative interview study with citizens and public service providers. **Government Information Quarterly**, London, v. 41, n. 2, 2024. DOI: <https://doi.org/10.1016/j.giq.2024.101927>.

LEWIS, Patrick *et al.* Retrieval-augmented generation for knowledge-intensive NLP tasks. **NIPS'20: Proceedings of the 34th International Conference on Neural Information Processing Systems**, San Diego, USA, 2020. DOI: <https://doi.org/10.48550/arXiv.2005.11401>.

MAKASI, Tendai *et al.* Chatbot-mediated public service delivery: a public service value-based framework. **First Monday**, Chicago, v. 25, n. 12, 2020. DOI: <https://doi.org/10.5210/fm.v25i12.10598>.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MARITACA.AI. **Modelos de linguagem Sabiá 3 e Sabiázinho 3**: LLMs abertos em português. São Paulo: Maritaca AI, 2025. Software. Disponível em: <https://tinyurl.com/3wv3jx76>. Acesso em: 16 out. 2025.

MONTEIRO, Andréa Silva. **A transformação digital da comunicação na administração pública**: uma análise da viabilidade do uso de um chatbot na Secretaria de Recursos Humanos da Universidade Federal de Campina

Grande. 2023. Dissertação (Mestrado Profissional em Administração Pública) – Universidade Federal de Campina Grande, Sousa, PB, 2023.

MULGAN, Geoff; ALBURY, David. **Innovation in the public sector**. London: Strategy Unit, Cabinet Office, 2003.

N8N.IO. **n8n (v. 1.112.3)**: ferramenta de automação e orquestração de fluxos. n8n GmbH, 2025. Software. Disponível em: <https://tinyurl.com/5dwczt8>. Acesso em: 15 out. 2025.

OLLAMA. Ollama (v. 0.12.x): local inference engine for large language models. **Ollama**, 2025. Software. Disponível em: <https://tinyurl.com/bdftsscu>. Acesso em: 15 out. 2025.

OPENWEBUI. OpenWebUI (v. 0.6.30): interface de código aberto para modelos de linguagem. **Portal GitHub**, 2025. Software. Disponível em: <https://tinyurl.com/26c8b7pc>. Acesso em: 15 out. 2025.

POSTGRESQL. PostgreSQL: open-source relational database system. **PostgreSQL**, v. 16, 2025. Software. Disponível em: <https://tinyurl.com/nedyhmx7>. Acesso em: 15 out. 2025.

QDRANT. Qdrant (v. 1.15.x): vector database for semantic search and retrieval. **Qdrant Tech**, 2025. Software. Disponível em: <https://tinyurl.com/zjr2h63t>. Acesso em: 15 out. 2025.

SANTOS, Matheus Henrique de Souza. Aspectos da governança digital da Administração Pública Federal do Brasil sob a luz das orientações da OCDE. **Revista Tempo do Mundo**, Brasília, n. 25, p. 331-355, 2021.

VERA, Henrique S. *et al.* **EmbeddingGemma**: powerful and lightweight text representations. ArXiv – preprint arXiv:2509.20354, v. 3, 2025. DOI: <https://doi.org/10.48550/arXiv.2509.20354>. Acesso em: 15 out. 2025.

Blockchain, uma visão de futuro para o Ministério Público Federal

Blockchain, a vision for the future of the Federal Prosecution Service

DOI: https://doi.org/10.63601/978-65-88299-52-4_12

Rodrigo Barreto da Silva

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Graduado em Tecnologia de Segurança da Informação pelo Centro Universitário Icesp (Unicesp). Servidor do Ministério Público Federal (MPF).

Sóstenes P. Leite Junior

MBA em Gestão de Tecnologia da Informação pelo Instituto de Gestão e Tecnologia da Informação. Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Direito Constitucional e Administrativo pelo Centro Universitário Uniftec. Bacharel em Direito pela Universidade Federal do Amazonas. Servidor do Ministério Público Federal (MPF).

Resumo: A transformação digital impulsiona a Administração Pública brasileira na busca por inovações, como demonstrado pelas iniciativas Drex e Rede Blockchain Brasil (RBB). Nesse ambiente, a tecnologia *blockchain* se destaca pela capacidade de oferecer transparência, imutabilidade e auditabilidade para o setor público. Investigam-se aqui fatores que influenciam o processo de adoção da *blockchain* no Ministério Público Federal (MPF), visando propor uma matriz de implementação. Esta contribuição é vital, pois a adoção tecnológica se alinha diretamente à sua missão constitucional de promover a justiça, exigindo o aprimoramento contínuo de mecanismos de controle. A pesquisa iniciou com a revisão conceitual da tecnologia da *blockchain*, correlacionando-a com o planejamento estratégico do Ministério Público Federal. A metodologia empregada é a revisão sistemática da literatura, seguindo as orientações do protocolo PRISMA 2020. Os estudos selecionados foram analisados sob o framework TOE (*Technology, Organization, Environment*) para categorizar os fatores críticos de adoção, riscos e oportunidades. Como resultados

e discussão, fez-se o comparativo entre as características da *blockchain* e os valores estratégicos do MPF, mapearam-se possíveis casos de uso; entretanto, foram identificadas limitações metodológicas relacionadas à carência de dados empíricos específicos sobre o seu uso em órgãos públicos. A conclusão é que, embora exista aderência entre a tecnologia e os valores do MPF, a falta de dados empíricos específicos prejudica a mensuração dos resultados relacionados ao custo-benefício da adoção da *blockchain* pelo MPF, sendo necessários mais estudos para viabilizar uma proposta de matriz de implementação validada por métricas.

Palavras-chave: *blockchain*; Administração Pública; Ministério Público Federal; transformação digital; eficiência.

Abstract: *Digital transformation is driving Brazilian Public Administration in its pursuit of innovation, as demonstrated by the Drex and Rede Blockchain Brasil (RBB) initiatives. In this environment, blockchain technology stands out for its ability to offer transparency, immutability, and auditability to the public sector. This study investigates factors influencing the adoption of blockchain in the Federal Prosecution Service (MPF), aiming to propose an implementation matrix. This contribution is vital because technological adoption aligns directly with its constitutional mission of promoting justice, requiring the continuous improvement of control mechanisms. The research began with a conceptual review of blockchain technology, correlating it with the strategic planning of the Federal Prosecution Service. The methodology employed is a systematic literature review, following the guidelines of the PRISMA 2020 protocol. The selected studies were analyzed under the TOE (Technology, Organization, Environment) framework to categorize critical adoption factors, risks, and opportunities. As a result and discussion, a comparison was made between the characteristics of blockchain and the strategic values of Brazilian Federal Prosecution Service (MPF), and possible use cases were mapped. However, methodological limitations were identified related to the lack of specific empirical data on its use in public bodies. The conclusion is that, although there is alignment between the technology and the values of MPF, the lack of specific empirical data hinders the measurement of the results related to the cost-benefit of adopting blockchain by MPF, and further studies will be necessary to enable a proposal for an implementation matrix validated by metrics.*

Keywords: *blockchain*; Public Administration; Federal Prosecution Service; digital transformation; efficiency.

1 Introdução

A transformação digital tornou-se uma necessidade premente para governos e organizações, impulsionando a busca por tecnologias que otimizem a prestação de serviços e a gestão pública. No Brasil, esse movimento tem sido marcado por iniciativas como o projeto de moeda digital do Banco Central (Drex) e a criação da Rede Blockchain Brasil (RBB).

Paralelamente, o Tribunal de Contas da União (TCU), por meio do Acórdão n. 1613/2020, realizou um levantamento sobre o uso da tecnologia *blockchain* no setor público, identificando seu potencial para otimizar serviços, bem como alertando sobre os riscos inerentes à sua adoção.

A tecnologia *blockchain* é valorizada por atributos intrínsecos como transparência, descentralização, imutabilidade e auditabilidade. Essas características são amplamente reconhecidas por sua capacidade de enfrentar desafios crônicos da Administração Pública, como a ineficiência, a burocracia, a falta de transparência e a corrupção.

Nesse contexto, esta pesquisa busca contribuir para o avanço do conhecimento em gestão pública e tecnologia da informação, ao investigar o processo de adoção da tecnologia *blockchain* com foco no Ministério Público Federal (MPF). Sua principal contribuição consiste em avaliar de que forma as características da *blockchain* se alinham às necessidades operacionais e estratégicas do órgão.

A busca por um serviço público mais íntegro, eficiente e orientado à inovação constitui a principal motivação deste estudo. A relevância da pesquisa é justificada pela própria missão institucional do MPF: promover a justiça em benefício da sociedade e em defesa do Estado Democrático de Direito. Esse propósito demanda o aprimoramento contínuo de seus processos, em consonância com as demandas da chamada “cibersociedade”. A adoção da *blockchain* não representa apenas uma tendência tecnológica, mas sim uma nova fronteira dos direitos digitais.

Assim, o objetivo central desta pesquisa é investigar quais fatores influenciam o processo de adoção da tecnologia *blockchain* no Ministério Público Federal, com o intuito de gerar conhecimento prático e fornecer subsídios para a criação de uma matriz de implementação da tecnologia.

A tecnologia *blockchain* gerou um *hype* significativo nos círculos políticos, levando à crescente experimentação, implementação de projetos-piloto e a uma intensa produção acadêmica nas mais diversas áreas, inclusive na Administração Pública (Clifton, 2023).

Nesse panorama, destaca-se novamente o Acórdão n. 1.613/2020 do TCU. Outro estudo relevante, intitulado “Uso da tecnologia *blockchain* nas contratações públicas sustentáveis de obras rodoviárias”, analisou 25 processos licitatórios do Departamento Nacional de Infraestrutura de

Transportes (DNIT) no Paraná, entre 2017 e 2020. A pesquisa propôs a integração da tecnologia *blockchain* ao Portal Nacional de Contratações Públicas (PNCP), reforçando seu potencial de aplicação no setor público (Giamberardino, G. G.; Gadda, T. M. C.; Nagalli, 2024).

No cenário internacional, destaca-se o editorial *Bridging the chasm between “what could be” and “what is”: the impact of blockchain technologies on public service management*, publicado na *International Journal of Public Sector Management*. O artigo ressalta a necessidade de superar a fase conceitual e alcançar impactos práticos da tecnologia *blockchain* na Administração Pública (Tan; Dan; Shahzad, 2025). A coletânea enfatiza a importância de estudos que integrem teoria e prática na Administração Pública, aplicando perspectivas das ciências gerenciais e organizacionais, sustentadas por evidências empíricas de casos reais.

Esses estudos anteriores não apenas corroboram a pertinência da presente investigação, como também evidenciam a necessidade de aprofundamento empírico. A originalidade desta pesquisa reside no esforço de transpor o conhecimento conceitual sobre a *blockchain* para sua aplicação prática no contexto específico do Ministério Público Federal, o que demarca sua contribuição inédita em relação aos trabalhos existentes.

A pesquisa estrutura-se em uma abordagem sequencial que inicia pela revisão conceitual da *blockchain* e do planejamento estratégico com objetivo de articular os conceitos que servirão de base teórica para análise futura. Em seguida, descreve-se a metodologia PRISMA utilizada como critério para seleção dos artigos, bem como as limitações encontradas relacionadas à qualidade do material selecionado. Ao final, é apresentada a discussão sobre os achados da pesquisa sob a ótica do *Framework* TOE, avaliando-se a compatibilidade da tecnologia *blockchain* com os valores intrínsecos do Ministério Público Federal e, por fim, elencando casos de usos práticos para aplicação institucional.

2 Revisão conceitual

Em um cenário marcado pela convergência entre a tecnologia e o arcabouço jurídico-institucional, torna-se necessário aprofundar a compreensão sobre conceitos-chave que balizam a transformação digital no setor público.

Nesse sentido, a revisão conceitual se desdobrará em duas vertentes principais, que possuem um vínculo de causalidade e potencial de sinergia no contexto da modernização institucional: a tecnologia *blockchain* e o planejamento estratégico institucional do Ministério Público Federal.

Logo no início, serão revisados os conceitos da tecnologia *blockchain*, detalhando sua arquitetura, os mecanismos de consenso subjacentes e as características intrínsecas que a qualificam como um instrumento de descentralização, imutabilidade e transparência. Serão exploradas algumas de suas aplicações, com foco nas implicações para a gestão de dados, a segurança da informação e a rastreabilidade em processos formais. A compreensão aprofundada da *blockchain* é crucial, pois ela representa um paradigma de infraestrutura digital com potencial disruptivo para redefinir as relações de confiança e a eficiência operacional das organizações.

Em seguida, o foco se deslocará para o Planejamento Estratégico Institucional (PEI), que é definido como um processo gerencial formal e sistemático, de natureza cíclica e abrangência de longo prazo, cuja principal finalidade é formular um conjunto de estratégias que promovam o alinhamento de todos os recursos humanos, financeiros e tecnológicos da organização com sua identidade estratégica (Missão, Visão e Valores), em resposta às mudanças e incertezas do ambiente externo (Schotten, P. C. *et al.*, 2020).

A articulação desses conceitos se configura como elemento central para a construção de um discurso sobre a aplicabilidade da tecnologia da *blockchain* ao Ministério Público Federal. Os conceitos aqui estabelecidos servirão como referencial teórico para a análise que será desenvolvida nos capítulos posteriores.

2.1 Tecnologia *blockchain*

A crise financeira global de 2008, ou crise do subprime, teve sua origem nos Estados Unidos. Ela foi desencadeada por práticas comerciais que inflaram artificialmente os preços dos imóveis, impulsionados pela ampla disponibilidade de crédito hipotecário com juros baixos. O subsequente aumento das taxas de juros levou a um crescimento da inadimplência e à queda abrupta no valor dos imóveis, resultando em

perdas substanciais para os bancos, que não conseguiam recuperar o montante dos empréstimos mesmo após a retomada dos bens. A falência do banco Lehman Brothers, ocasionada pela crise, intensificou o sentimento de desconfiança no setor, propagando-o por todo o mercado financeiro global (Trevisan, 2018).

Nesse contexto de desconfiança do mercado e dos bancos, foi publicado o *white paper* “Bitcoin: a peer-to-peer electronic cash system” (Bitcoin: um sistema de dinheiro eletrônico ponto a ponto, em tradução livre) propondo um sistema de dinheiro eletrônico descentralizado e de código aberto para se opor ao modelo financeiro tradicional, que não necessita de intermediários e utiliza as tecnologias de criptografia e *hash* para criar registros únicos e irreversíveis e evitar gastos duplos (Nakamoto, 2008).

O criador do Bitcoin, sob o pseudônimo de Satoshi Nakamoto, não utiliza o termo *blockchain* explicitamente, mas define a rede como um registro público e descentralizado de transações digitais, organizado em uma cadeia de blocos com marcação de tempo, em que cada bloco é interligado ao anterior por um sistema de *hashes* encadeados, formando uma sequência imutável. O mecanismo de consenso garante a segurança, a ordem e a confiança da rede através de um esforço computacional denominado de prova de trabalho, *Proof-of-Work* (PoW) (Nakamoto, 2008).

Embora a *blockchain* tenha alcançado proeminência como infraestrutura primária para o Bitcoin e demais criptoativos, seu potencial transcende a esfera monetária. Essencialmente, a *blockchain* é uma Tecnologia de Registro Distribuído – *Distributed Ledger Technology* (DLT) –, que provê um mecanismo imutável para registrar qualquer tipo de dado. Sua aplicação é vasta, abrangendo o registro de ativos físicos, como imóveis e veículos, a gestão de cadeias de suprimentos, o controle de identidade digital e acesso, cadeia de custódia, bem como sistemas de votação eletrônica.

O diferencial fundamental reside em sua arquitetura nativamente distribuída, transparente e descentralizada. Tais características possibilitam a auditoria dos registros em tempo real e, fundamentalmente, asseguram a integridade e a validade das transações para todos os participantes da rede, mitigando a necessidade de intermediários.

Em 2013, Vitalik Buterin, pesquisador do ecossistema Bitcoin, identificou uma limitação fundamental na arquitetura dessa *blockchain*. O criador do Bitcoin restringiu deliberadamente a complexidade da linguagem de script que poderia ser executada na *blockchain*, uma medida de segurança para evitar a sobrecarga computacional da rede.

Para Vitalik, a tecnologia poderia ir muito além do que registrar e validar transações financeiras. A ideia seria criar uma *blockchain* capaz de rodar aplicações mais sofisticadas, descentralizando o processamento de informações e criando um computador mundial distribuído capaz de executar qualquer lógica programável. Para concretizar essa visão, Vitalik criou uma nova *blockchain* denominada Ethereum (Buterin, 2014).

Com a programabilidade inserida na rede Ethereum, foi possível a implementação do conceito de contratos inteligentes (*Smart Contracts*) formalizado por Nick Szabo, que definiu contratos inteligentes como um protocolo de transação informatizado que executa os termos de um contrato. Para Szabo, um contrato inteligente pode ser caracterizado pelo atingimento de quatro objetivos principais: observabilidade, verificabilidade, privacidade e obrigatoriedade (Szabo, 1994).

O avanço da rede Ethereum e a introdução de sua *Ethereum Virtual Machine* (EVM), juntamente com a funcionalidade dos contratos inteligentes, estabeleceram o arcabouço tecnológico para a criação de representações digitais de valor. Esses ativos digitais, denominados tokens, são definidos por meio de padrões de contrato *Ethereum Request for Comment* (como ERC-20 e ERC-721), permitindo a tokenização de uma vasta gama de ativos. Tais tokens podem representar desde valores fungíveis (moedas, tokens de governança e ativos financeiros) até valores não fungíveis (obras de arte, direitos autorais e frações de propriedades reais), redefinindo a gestão, a liquidez e a acessibilidade dos ativos no ambiente digital.

A classificação das redes *blockchain* é determinada, sobretudo, pelo seu modelo de acesso (público ou privado) e pelo seu mecanismo de permissão (permissionada ou não permissionada), o que define a sua governança e o seu modelo de consenso.

O modelo de *blockchain* pública e não permissionada representa a arquitetura original exemplificada pelas redes Bitcoin e Ethereum. É caracterizado pela ausência de barreiras de entrada, permitindo que

qualquer participante (nó) possa ingressar na rede, verificar o histórico de transações, enviar transações e participar ativamente do processo de validação e consenso (mineração ou *staking*). A confiança é estabelecida por criptografia e pelo incentivo econômico, e não por autoridades centrais.

O modelo de *blockchain* pública e permissionada, também conhecido como *blockchain* consorciada, representa um modelo híbrido, em que qualquer indivíduo pode entrar, verificar o histórico de transações (mantendo a transparência pública). No entanto, apenas um conjunto pré-selecionado e autorizado de nós (membros de um consórcio, por exemplo) possui a permissão e a responsabilidade de transacionar e validar blocos. Esse modelo é frequentemente adotado quando se busca um equilíbrio entre descentralização e conformidade regulatória. Exemplos de plataformas que suportam este modelo incluem *Hyperledger Fabric* e *Hyperledger Besu*.

Já no modelo privado e permissionário, a rede é controlada por uma organização; o acesso, a verificação e a validação são estritamente restritos a participantes previamente identificados e autorizados. Embora ainda utilizem a imutabilidade do DLT, o grau de descentralização é baixo, pois a confiança é estabelecida apenas nas entidades controladoras.

2.2 Planejamento estratégico do Ministério Público Federal

O Planejamento Estratégico Institucional (PEI), cujo ciclo inaugural compreendeu o decênio 2011-2021, fundamentou-se na tríade conceitual composta por missão, visão e valores cujo objetivo foi nortear a governança e o desempenho organizacional, sendo posteriormente atualizado para o ciclo vigente de 2022-2027 a fim de assegurar a continuidade do alinhamento estratégico da instituição.

A missão institucional definida naquele ciclo estratégico era “Promover a realização da justiça, a bem da sociedade e em defesa do Estado Democrático de Direito” (Brasil, 2011). Esta declaração sintetiza o propósito fundamental do MPF, focando no seu papel constitucional de zelar pelos interesses sociais e pela ordem jurídica.

A visão representava o estado futuro e aspiracional que o MPF almejava atingir até o final do plano. A meta era “até 2020, ser reconhecido, nacional e internacionalmente, pela excelência na promoção

da justiça, da cidadania e no combate ao crime e à corrupção” (Brasil, 2011). A ênfase na excelência, na promoção da cidadania e, principalmente, no combate à corrupção balizou grande parte dos 25 objetivos estratégicos do período.

Os valores estratégicos estabeleceram os princípios éticos e comportamentais inegociáveis que deveriam permear a conduta de membros e servidores, garantindo a integridade e a identidade da instituição. Os valores adotados foram: autonomia institucional, compromisso, transparência, ética, independência funcional, unidade, a qual reflete a ideia de que os membros do MPF constituem uma só instituição, iniciativa que define a capacidade de a instituição agir independentemente de provocação e efetividade que pauta a atuação focada no alcance de resultados positivos para a sociedade.

Já para o ciclo de 2022 a 2027, a missão institucional passa a ser a defesa da ordem jurídica, do regime democrático, dos interesses sociais e individuais indisponíveis e a promoção da justiça. A visão é atualizada para “ser reconhecido como instituição independente com atuação proativa e resolutiva na defesa do interesse público, no combate à corrupção e à criminalidade e na garantia dos direitos fundamentais e do desenvolvimento econômico e sustentável” (Brasil, 2022). Quanto aos valores, foram mantidos os previstos no primeiro ciclo, com o acréscimo do valor relacionado a cooperação.

Essa estrutura de Missão, Visão e Valores não apenas pautou o Mapa Estratégico, mas também serviu como bússola para a maturação administrativa e a modernização do MPF durante a vigência do PEI.

O PEI alinhou os critérios de atuação da Secretaria de Tecnologia da Informação e Comunicação (STIC) no MPF, que foram formalizados e operacionalizados por meio do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) juntamente com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).

A sinergia entre a Tecnologia da Informação e Comunicação (TIC) e a estratégia institucional do MPF é concretizada por meio de mecanismos-chave que atuam em diferentes dimensões da gestão.

Na dimensão do alinhamento de iniciativas e objetivos, o PETIC garante que as iniciativas de TIC estejam diretamente alinhadas aos

objetivos estratégicos do MPF. O PETIC detalha esse direcionamento em dezesseis Objetivos Estratégicos de Tecnologia da Informação (OETIs), distribuídos nas perspectivas de Aprendizado e Crescimento, Processos Internos e Clientes, assegurando que o desenvolvimento tecnológico seja um vetor da estratégia (Brasil, 2017).

Na unificação e padronização nacional, o PETIC busca a visão de uma atuação nacional unificada, o modelo da TIC prioriza a integração nacional e a padronização de sistemas. O indicador “Índice de adoção de soluções nacionais de TI do MPF” (OETI 6.1) serve como um mecanismo explícito para incentivar a adesão a sistemas unificados, eliminando esforços redundantes e fomentando a uniformidade operacional (Brasil, 2017).

Na governança e atuação integrada, o PETIC prevê o critério de Percentual de aderência à atuação nacional da TIC (OETI 12) promovendo a atuação colaborativa e integrada entre as Coordenadorias de TIC (CTIC's) e a TIC Nacional. Esse mecanismo visa a uma gestão da TI coesa e integrada em âmbito nacional (Brasil, 2017).

Com foco na satisfação e qualidade do cliente, o PETIC sinaliza para a monitoria de performance por meio de indicadores de serviço e satisfação. O Percentual de atendimentos na área de Serviços de TIC, dentro do Acordo de Nível de Serviço (ANS) definido (OETI 2.1), e o Percentual de satisfação dos clientes de TIC com os serviços prestados (OETI 2.3) garantem que a TI cumpra o objetivo estratégico de atender às expectativas de tempo e qualidade acordadas com os clientes internos (OETI 2), solidificando seu papel de suporte eficiente à atividade-fim (Brasil, 2017).

3 Metodologia

O presente estudo adota como método a revisão sistemática da literatura (RSL), cujo objetivo é mapear e analisar o conhecimento consolidado sobre a adoção da tecnologia *blockchain* na Administração Pública.

Como forma de garantir o rigor metodológico, a presente pesquisa utilizou-se das orientações do modelo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Page *et al.*, 2022) na fase de revisão e coleta de dados e do Framework TOE (Tecnologia, Organização, Ambiente) na fase de análise.

3.1 Estratégia de revisão e coleta de dados

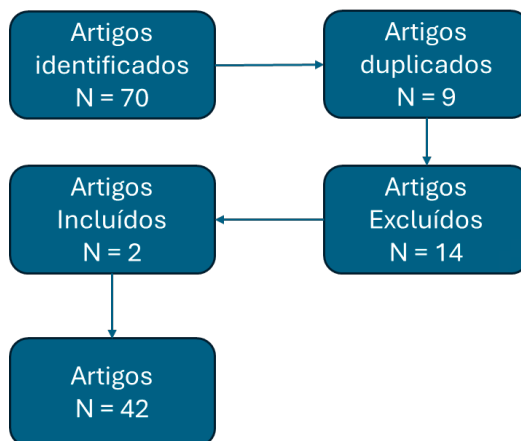
A busca por artigos foi realizada nas bases de dados Web of Science (WoS), Scielo e Google Scholar. A WoS foi utilizada para capturar artigos de alto impacto e rigor internacional, enquanto o Scielo e o Google Scholar foram empregados para incluir a literatura cinzenta relevante.

O parâmetro de pesquisa abrangeu, quando disponíveis, os campos de título, resumo e palavras-chave (Topic), por meio da seguinte *string* booleana: (“Blockchain” OR “DLT”) AND (“Adoption” OR “Implementação” OR “Fatores”) AND (“Public Sector” OR “Serviço Público”).

Buscas secundárias e complementares, focadas na literatura cinzenta, foram realizadas no Google Scholar. Nesses casos, termos específicos como “MPF”, “TCU”, “CGU”, “Cadeia de Custódia”, “Contratos Inteligentes” foram utilizados em combinação com o termo “*blockchain*” para garantir a captação de relatórios e documentos específicos do contexto da Administração Pública federal.

Como *Critérios de elegibilidade*, foram incluídos na triagem apenas artigos científicos e relatórios técnicos publicados a partir de janeiro de 2020 que abordassem os fatores de adoção, desafios de implementação e/ou casos de uso da *blockchain* no setor público, bem como textos de relevância conceitual sobre *blockchain*. A Figura 1 representa o processo de seleção.

Figura 1 – PRISMA 2020



Fonte: elaborada pelos próprios autores.

3.2 Análise dos dados

Os dados referentes aos fatores de sucesso na adoção da tecnologia *blockchain*, bem como os riscos e as oportunidades identificadas, foram agrupados, de acordo com sua natureza, em uma das seguintes dimensões: da tecnologia, da organização ou do ambiente externo, conforme previsto no Framework TOE (Tornatzky; Fleischer, 1990), o qual é utilizado para avaliar adoção de uma nova tecnologia.

3.3 Roteiro analítico da revisão

A pesquisa está metodologicamente organizada em etapas sequenciais, projetadas para oferecer uma análise da aplicabilidade da tecnologia *blockchain* no MPF.

O cerne analítico aqui proposto inicia com a apresentação dos conceitos básicos da *blockchain* e do planejamento estratégico. O objetivo primordial desta revisão teórica não é apenas definir a tecnologia, mas sim avaliar as suas características intrínsecas, como imutabilidade, descentralização e transparência, para determinar quais delas se mostraram aderentes às necessidades estratégicas do MPF.

Em seguida, o foco migra para o comparativo entre as características da *blockchain*, identificadas na revisão conceitual, e os valores organizacionais que moldam a atuação ministerial, previstos no Plano Estratégico Institucional (PEI), para depois elencar possíveis casos de uso.

Por fim, o passo mais crítico da pesquisa envolve a correlação dos dados tabulados no framework com as demandas específicas do MPF. Esse comparativo permite identificar e mapear as oportunidades mais promissoras para a adoção estratégica. O produto dessa correlação será a matriz de implementação que servirá como caminho para adoção da *blockchain*.

3.4 Limitações metodológicas da revisão

A pesquisa enfrentou limitações metodológicas e contextuais, que foram categorizadas de acordo com sua natureza, conforme especificado a seguir.

3.4.1 Limitações relacionadas à natureza da pesquisa e escopo

Predomínio de estudos teóricos e exploratórios: há uma prevalência de estudos de natureza predominantemente teórica e exploratória, baseados majoritariamente em revisões bibliográficas e análises conceituais. Isso limita a capacidade de avaliar o impacto real e concreto da aplicação das tecnologias em processos práticos.

Ausência de dados empíricos/estudos de caso em operação: em pesquisas bibliográficas e documentais, há a ausência de coleta de dados de campo ou levantamento estatístico original, sendo os resultados derivados do estado da arte do conhecimento disponível. Em alguns casos, a pesquisa se concentrou em um projeto que ainda estava em estágio de design (e não de operação), o que pode limitar as conclusões.

Delimitação estrita de fontes/idioma: algumas revisões sistemáticas limitaram a busca a artigos publicados em língua portuguesa, enquanto outras, devido à escassez de dados nacionais, recorreram exclusivamente a fontes em inglês. Outras pesquisas enfrentaram barreiras para acessar fontes pagas ou proprietárias (como dados internos de projetos-piloto governamentais).

3.4.2 Limitações de amostra e coleta de dados

Amostra reduzida e por conveniência: em um estudo sobre a adoção de *blockchain* no setor público do Espírito Santo, o número de respondentes válidos ficou aquém do esperado, o que representa uma limitação da amostra e do escopo. Similarmente, um estudo de caso múltiplo sobre a adoção no governo federal utilizou poucas entrevistas para cada caso, embora isso tenha sido mitigado por triangulação.

Falta de entrevistas/opiniões chave: em uma pesquisa sobre contratações públicas sustentáveis, uma limitação metodológica foi o fato de não se levar em consideração a opinião dos envolvidos nos processos de licitação. Em outro estudo, não foi possível realizar entrevistas com uma amostra considerável de empresas que já tivessem adotado a tecnologia, limitando a compreensão dos efeitos pós-adoção.

3.4.3 Limitações técnicas e de modelagem

Foco na aplicação gerencial em detrimento da técnica: alguns trabalhos se limitaram a discutir o uso de *blockchain* do ponto de vista da aplicação gerencial, não se aprofundando em aspectos técnicos relacionados à ciência da computação, programação, capacidade computacional, prontidão tecnológica ou infraestrutura de TI. O detalhamento de técnicas criptográficas estava fora do escopo de um relatório do TCU.

3.4.4 Limitações em áreas regulatórias e contextuais

Conflito regulatório não analisado: a pesquisa sobre a adoção de *blockchain* no setor público não teve como objeto a análise da conformidade com a Lei Geral de Proteção de Dados (LGPD), destacando que essa intersecção ainda é pouco explorada academicamente.

Falta de padronização metodológica: para a cadeia de custódia da prova digital, é notada a lacuna na adoção de mecanismos padronizados para garantir a integridade e confiabilidade, dependendo amplamente de procedimentos e metodologias adotadas pelo perito.

3.4.5 Limitações referentes ao MPF

No que tange ao MPF, as análises de compatibilidade da *blockchain* com os valores institucionais, embora embasadas no Framework TOE, dependem da interpretação dos dados contidos em relatórios de gestão do MPF, cujos indicadores podem não ter sido concebidos para avaliar especificamente o impacto de tecnologias de registro distribuído. Tais restrições delimitam o escopo conclusivo do estudo, direcionando-o para a proposição de um modelo de compatibilidade e casos de uso, em vez da validação empírica de implementação já existente.

4 Resultados e discussão

Apresenta-se a fase analítica da pesquisa, cujo propósito central é transpor a base conceitual para o escopo prático do MPF. Para tanto, será utilizado o Framework TOE (Technology-Organization-Environment) para avaliar a adoção e a difusão das inovações tecnológicas no contexto

organizacional. Esse modelo permitirá a análise da introdução da tecnologia *blockchain* sob três lentes distintas: o ambiente tecnológico existente (infraestrutura de TI e PETI); as características organizacionais (Missão, Visão e Valores do PEI, bem como a cultura de governança); e o ambiente externo (pressões regulatórias e demandas da sociedade).

Em seguida, será empreendida uma análise crítica para avaliar a compatibilidade intrínseca da *blockchain*, especialmente em relação à sua imutabilidade e transparência com os valores e a missão finalística do MPF, notadamente no que tange ao combate à corrupção, à transparência do gasto e à segurança processual, áreas que se destacaram no planejamento da instituição. Por fim, esta análise culminará na proposição de casos de uso para a aplicação da *blockchain* em processos judiciais, extrajudiciais ou administrativos do órgão, fornecendo subsídios concretos para o avanço da governança digital no MPF.

4.1 Ambiente tecnológico do MPF

A análise do vetor Tecnológico, conforme proposto pelo Framework TOE, exige a avaliação da infraestrutura e dos sistemas de informação existentes na organização, bem como a maturidade do seu planejamento tecnológico. No MPF, esse ambiente é formalmente orientado pelo PETIC, que buscou, entre 2012 e 2020, o alinhamento total da tecnologia com o PEI 2011-2021. O sucesso do PETIC em promover a modernização administrativa e finalística é um indicativo da capacidade instalada do MPF para adotar inovações, como a tecnologia *blockchain*.

Um fator que facilita a eventual adoção de uma infraestrutura distribuída, como a *blockchain*, é o histórico do MPF na promoção da unificação e padronização de sistemas em escala nacional. O modelo de atuação da TIC, que busca a visão de ter atuação nacional unificada até 2020, prioriza a integração nacional e a padronização de sistemas. O indicador percentual de adoção de soluções nacionais de TIC incentiva a adesão a sistemas unificados, eliminando esforços redundantes e fomentando a uniformidade operacional.

Os projetos como o Sisconta Eleitoral e o sistema Aptus 4.0 (gestão do conhecimento finalístico), embora centralizados, demonstram a capacidade de desenvolver plataformas complexas para o uso unificado por todas as unidades do MPF.

A transição de sistemas internos já padronizados e unificados para uma arquitetura descentralizada, mas também unificada, como uma *blockchain* de consórcio entre unidades, é facilitada pela experiência e pela cultura de adesão a soluções nacionais já estabelecidas pelo PETI. A *blockchain*, ao oferecer um registro único e distribuído, pode atuar como a próxima camada de infraestrutura para a consolidação da atuação nacional e transparente do MPF, alinhando-se diretamente ao Objetivo Estratégico de TI de promover a unificação.

4.2 Ambiente organizacional

O segundo componente do Framework TOE, o vetor organizacional, concentra-se na avaliação das características internas da instituição, como sua estrutura, cultura e, fundamentalmente, sua estratégia e valores. Para o MPF, a adoção da tecnologia *blockchain* deve ser analisada sob o prisma da sua Visão, Missão e Valores definidos no PEI 2011-2021 e no PEI 2022-2027, a fim de determinar a compatibilidade ideológica e funcional da inovação.

4.2.1 Missão

A missão do MPF é “[p]romover a realização da justiça, a bem da sociedade e em defesa do Estado Democrático de Direito” (Brasil, 2011). A *blockchain*, com sua capacidade de garantir a imutabilidade e a rastreabilidade de registros, alinha-se diretamente a essa missão ao assegurar a fidedignidade da prova, visto que a natureza criptográfica e distribuída da tecnologia pode conferir um nível de segurança e auditabilidade aos documentos jurídicos e investigatórios superior aos sistemas centralizados existentes, fortalecendo a realização da justiça e a defesa do Estado Democrático de Direito.

4.2.2 Visão

A visão do MPF, centrada em “ser reconhecido [...] pela excelência [...] no combate ao crime e à corrupção” (Brasil, 2011), é diretamente apoiada pela *blockchain*. Projetos como o Sisconta Eleitoral já demonstravam a busca por ferramentas de rastreabilidade, e a *blockchain* pode

atuar como um registro incorruptível de ativos, licitações ou transferências, dificultando o desvio e facilitando a fiscalização de forma proativa.

4.2.3 Valor

A matriz de valores do MPF atua como um forte indutor para a adoção de tecnologias de registro distribuído.

O valor da transparência traduz-se no acesso facilitado às informações, elemento que possibilita o controle social dos serviços e investimentos públicos. A essência da *blockchain*, seja em arquiteturas públicas ou permissionadas, repousa na transparência, pois a existência e a veracidade das transações são plenamente verificáveis de forma pública. Essa característica harmoniza-se com o propósito institucional de divulgar resultados transparentes, oferecendo a visibilidade auditável intrínseca de um registro distribuído (*ledger*). Consequentemente, em uma *blockchain* pública, qualquer indivíduo detém a prerrogativa de acessar e analisar os dados, podendo inclusive desenvolver sistemas para o seu monitoramento contínuo.

No MPF, o Portal da Transparência e Prestação de Contas que concentra dados detalhados sobre execução orçamentária e financeira, licitações, contratos e remuneração de membros e servidores, e o MPF Serviços (<https://tinyurl.com/yc23rw4d>), serviço destinado ao cidadão para o envio de representações, pedidos de informação, acompanhamento de processos, emissão de certidões, solicitação de dados pessoais, entre outras funcionalidades, fazem o papel de apresentar os resultados da atuação institucional para a sociedade.

O valor da unidade, já buscado através da unificação de soluções de TI, seria materializado pela *blockchain* ao criar uma base de dados única e distribuída para o uso de todas as procuradorias, fortalecendo a coesão da atuação em âmbito nacional. O valor da iniciativa é reforçado pela possibilidade de o MPF ser pioneiro na criação e gestão dessa infraestrutura de confiança.

A natureza imutável da *blockchain* reforça os valores de compromisso e ética, pois a tecnologia, ao impedir a alteração retroativa de registros, estabelece um ambiente de confiança algorítmica que coíbe falhas humanas e manipulações.

A partir desta análise, conclui-se que os atributos essenciais da *blockchain* – descentralização, imutabilidade e transparência – representam uma extensão lógica e tecnológica dos pilares estratégicos e valores fundamentais que regem o MPF em seu ciclo de modernização.

4.3 Ambiente externo

O terceiro componente do Framework TOE, ambiental, analisa as forças externas que influenciam a decisão da organização de adotar ou não uma inovação, incluindo o ambiente regulatório, a concorrência e as exigências da sociedade.

Nesse contexto, o primeiro desafio é a pressão regulatória e normativa. Embora a sociedade e os órgãos de controle, como o TCU, exijam mais segurança de dados, o próprio ordenamento jurídico impõe cautela. A LGPD, por exemplo, levanta uma questão crítica: como compatibilizar o princípio da imutabilidade da *blockchain* com o direito ao esquecimento ou à retificação de dados? Essa dicotomia legal representa um risco que exige decisões jurídicas e arquitetônicas cuidadosas por parte do MPF.

O controle social, por sua vez, impõe uma pressão contínua por um serviço público mais eficiente e auditável. O MPF já demonstrou estar sensível a essa demanda, visto que o PEI incluiu objetivos estratégicos de “Aproximação com o cidadão” e monitorou a “Percepção de imagem do MPF” (Brasil, 2011), indicando a importância de gerar resultados perceptíveis para a sociedade. A *blockchain*, ao oferecer mecanismos de transparência radical, como a consulta pública e imutável de registros, similar ao que já é feito no Portal da Transparência, responde diretamente a essa demanda social por visibilidade e confiança.

Por outro lado, o ambiente externo oferece oportunidade para a adoção da tecnologia *blockchain*, notadamente no que se refere à colaboração interinstitucional. O próprio Planejamento Estratégico Institucional (PEI) do MPF já previa o “Trabalho em grupo e parcerias” (Brasil, 2011) e o relatório estratégico institucional de 2011 a 2021 evidencia “Fomento à cooperação internacional para o aperfeiçoamento da atuação institucional” (Brasil, 2023). Nesse sentido, a *blockchain* de consórcio (*permissioned*), como o caso da RBB, se apresenta como a

infraestrutura neutra e altamente confiável capaz de suportar a troca segura de dados e provas entre o MPF, o Poder Judiciário, órgãos de controle (como TCU e CGU) e outras agências de *enforcement* nos âmbitos nacional e internacional, reforçando, assim, o valor da cooperação.

Essa tecnologia fortalece a colaboração ao oferecer uma estrutura robusta para a transação de informações entre órgãos públicos, baseada na interoperabilidade, na integração de dados confiáveis, na resiliência a fraudes, e munida de recursos de automação e execução de acordos via *Smart Contracts*.

4.4 Mapeamento de oportunidades: casos de uso estratégicos no MPF

Os casos de uso propostos a seguir visam alavancar a tecnologia de registro distribuído (DLT) para a consecução dos objetivos estratégicos de eficiência, segurança jurídica e combate à criminalidade que pautaram os PEIs 2011-2021 e 2022-2027.

4.4.1 Cadeia de custódia

Entre as funções institucionais do Ministério Público, o art. 129 da Constituição Federal de 1988 estabelece a titularidade privativa da ação penal pública. Para o exercício dessa competência, o Ministério Público Federal (MPF) detém a prerrogativa de instaurar e conduzir diretamente procedimentos investigatórios criminais, para apurar infrações de natureza pública que afetem a Justiça Federal, a exemplo de crimes contra o sistema financeiro, corrupção, tráfico internacional de drogas e crimes ambientais.

Para que esses crimes possam ser apurados, o MPF precisa garantir a cadeia de custódia das evidências digitais de forma íntegra. Com esse propósito, a Secretaria de Perícia, Pesquisa e Análise (SPPEA) elaborou a Instrução de Serviço n. 9, de 16 de maio de 2024 (IS 09/2024) que busca padronizar o manuseio de vestígios digitais no Ministério Público Federal.

A IS 09/2024 mostra de maneira detalhada como deve ser a coleta de vestígios digitais no MPF, os tipos (vestígios digitais com suporte físico visível e sem suporte físico visível), os fornecedores (Departamento de

Polícia Federal, Controladoria-Geral da União, Receita Federal do Brasil ou algum colaborador externo à entidade). Além disso, a instrução detalha os procedimentos obrigatórios para todas as etapas, como coleta, aquisição forense, descarte etc., exigindo o registro de cada ação por meio de Certidões no Sistema Único do MPF.

Para Silva (2024), o uso das tecnologias de *blockchain* e de contratos inteligentes pode ser uma solução promissora para a cadeia de custódia devido às suas características de imutabilidade, transparência e rastreabilidade.

Conforme diretrizes como a IS 09/2024 e a pesquisa de Silva, a tecnologia *blockchain* apresenta um potencial de aprimoramento substancial para a cadeia de custódia. Sua aplicação materializa-se em um livro-razão distribuído no qual cada etapa do manuseio da evidência – incluindo metadados, certidões e *hashes* criptográficos – é registrada de forma transparente para os participantes autorizados da rede. Essa estrutura permite a auditoria em tempo real de toda a trajetória da prova digital.

A garantia de integridade desse histórico provém da própria arquitetura da tecnologia. Cada bloco de informações é associado a um carimbo de tempo (*timestamp*) preciso e encadeado criptograficamente ao bloco anterior, um processo que assegura a imutabilidade e a ordem cronológica dos registros.

Consequentemente, essa capacidade de verificação da autenticidade eleva de forma significativa a confiança e o valor probatório das evidências, desde sua coleta até a eventual apresentação em juízo. Ademais, ao ser implementada sob um modelo de consórcio, a solução fomenta a eficiência e a colaboração entre diferentes órgãos governamentais. Tais entidades podem atuar como nós validadores da rede, participando conjuntamente do consenso e da governança, o que fortalece não apenas a prova, mas a própria cooperação institucional.

Para assegurar a conformidade jurídica com a Lei Geral de Proteção de Dados (LGPD), Silva ainda propõe em sua pesquisa a possibilidade de armazenar os dados pessoais fora da rede (*offchain*) para atender aos critérios de retificação e esquecimento dos dados (Silva, 2024).

Para aumentar a segurança e a transparência da cadeia de custódia, as regras de controle de acesso podem ser definidas e automatizadas

via contratos inteligentes. Esses programas, por serem imutáveis e autoexecutáveis, estipulam precisamente quais partes (ou entidades autorizadas) têm permissão para acessar ou manipular a evidência digital, garantindo que o acesso ocorra somente dentro de um período determinado, com o uso de carimbos de data e hora (*timestamps*) para registro cronológico inquestionável.

4.4.2 Contratos inteligentes

Um outro caso de uso de *blockchain* no MPF estaria relacionado à utilização de contratos inteligentes (*Smart Contracts*). Este mecanismo utiliza-se de protocolos de computador autoexecutáveis (*scripts*) que implementam os termos de um acordo em código de programação, com o objetivo de executar regras específicas e automatizar processos.

Na área fim, o MPF poderia utilizar essa ferramenta para gerenciar os termos de ajustamento de conduta (TAC); neste sentido, o funcionamento se daria pela codificação das obrigações, prazos e penalidades do TAC na *blockchain*, permitindo um monitoramento e execução automatizados.

A utilização desse mecanismo oferece vantagens em eficiência e segurança. A característica de autoexecução da tecnologia elimina a necessidade de o Ministério Público Federal (MPF) recorrer a ações de execução judicial para cobrar multas ou forçar o cumprimento das obrigações, tornando a aplicação das penalidades automática e imediata em caso de violação. Além disso, há uma significativa redução de custos e tempo para o MPF, que minimiza o monitoramento manual e a gestão burocrática dos termos, permitindo que os recursos sejam direcionados para outras atividades-fim da instituição.

No que tange à confiança e à fiscalização, o uso dos contratos inteligentes garante transparência e auditabilidade. O histórico completo do TAC – incluindo cláusulas, status de cumprimento e aplicação de multas – é registrado de forma imutável e acessível na *blockchain*, o que intensifica a fiscalização pública e a prestação de contas. Essa imutabilidade também estabelece uma garantia mútua de que o acordo será cumprido exatamente conforme codificado, oferecendo segurança tanto ao MPF quanto ao particular, desde que as condições lógicas sejam claras e precisas.

O acordo de não persecução penal (ANPP), instituído pela Lei n. 13.964/2019, representa um instrumento de política criminal que visa à desjudicialização de infrações penais de menor potencial ofensivo, mediante a celebração de um acordo entre o Ministério Público e o investigado, com a consequente extinção da punibilidade após o cumprimento das condições estipuladas. Considera-se a viabilidade de programar as obrigações desse contrato em *blockchain*, definindo as condições e os prazos em um contrato inteligente, o qual garantiria a execução autônoma e imutável do pacto mediante a verificação do cumprimento das cláusulas.

5 Considerações finais

A pesquisa demonstrou que o estudo cumpriu de forma parcial o seu objetivo central, ao investigar os fatores que influenciam o processo de adoção da tecnologia *blockchain* no Ministério Público Federal (MPF) e ao avaliar o alinhamento de suas características intrínsecas com as necessidades operacionais e estratégicas da instituição. A revisão sistemática da literatura, conduzida sob o protocolo PRISMA 2020 e analisada pelo Framework TOE, evidenciou a necessidade de mais estudos para compatibilizar o funcionamento teórico da *blockchain* com a realidade prática do MPF.

A pesquisa demonstrou uma clara aderência teórica entre a tecnologia e os valores do MPF: a imutabilidade do registro distribuído fortalece a integridade na gestão de evidências criminais; a visibilidade inerente à rede promove a transparência institucional; e a arquitetura consorciada facilita a cooperação interinstitucional, especialmente no contexto da Rede Blockchain Brasil (RBB). Foram identificadas oportunidades estratégicas de utilização da *blockchain* nas atividades relacionadas à cadeia de custódia de evidências digitais e na gestão dos termos de ajustamento de conduta (TACs) e acordos de não persecução penal (ANPPs).

Contudo, apesar do potencial e da identificação de casos de uso aderentes, não foi possível, ao final desta pesquisa, elaborar a matriz de implementação da *blockchain* aplicável ao MPF. Essa limitação decorre da carência de dados empíricos específicos e de elementos de medição que extrapolam a fase conceitual. O predomínio de estudos teóricos ou exploratórios na literatura atual, somado à ausência de dados internos

de projetos-piloto públicos, impediu a obtenção de parâmetros quantificáveis de custo-benefício, impacto real e fatores críticos de sucesso na realidade do MPF, inviabilizando a proposta de uma matriz de implementação validada por métricas.

Portanto, o estudo conclui que a *blockchain* possui um forte alinhamento teórico com algumas atividades do MPF, mas a transição da fase potencial para a fase de implementação requer um esforço contínuo de pesquisa empírica, com foco na coleta de dados práticos. Recomenda-se que pesquisas futuras explorem a escalabilidade e a interoperabilidade das redes de *blockchain*, bem como as controvérsias jurídicas atreladas à tecnologia, como a Lei Geral de Proteção de Dados (LGPD).

Referências

BRASIL. Ministério Público Federal. Procuradoria Geral da República. **Portaria PGR n. 687, de 20 de dezembro de 2011**. Institui o Planejamento Estratégico do Ministério Público Federal para o decênio 2011-2020. Brasília, DF: Procuradoria-Geral da República, [2011]. Disponível em: <https://tinyurl.com/bde4rmhp>. Acesso em: 27 mar. 2026.

BRASIL. Ministério Público Federal. Procuradoria Geral da República. **Relatório de Resultados do Procurador-Geral da República**: diálogo, unidade, transparência, profissionalismo, efetividade: 2015-2017. Brasília, DF: MPF, 2017. Disponível em: <https://tinyurl.com/w6sf4ewh>. Acesso em: 27 mar. 2026.

BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Portaria PGR/MPF n. 3, de 11 de fevereiro de 2022**. Institui o Planejamento Estratégico do Ministério Público Federal para o período 2022-2027. Diário do Ministério Público Federal Eletrônico: Caderno Administrativo, Brasília, DF, fev. 2022. Disponível em: <https://tinyurl.com/9hutkwb9>. Acesso em: 27 mar. 2026.

BRASIL. Ministério Público Federal. **Relatório de estratégia**: planejamento estratégico institucional 2011-2021. Brasília: MPF, 2023.

BRASIL. Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise. **Instrução de serviço n. 9, de 16 de maio de 2024**. Aprova orientações sobre o manuseio de vestígios digitais nos serviços prestados pela Secretaria de Perícia, Pesquisa e Análise do Ministério Público Federal e revoga a Instrução de Serviço n. 41, de 17 de dezembro 2021.

Brasília: MPF, 2024. Disponível em: <https://tinyurl.com/mrxw4kff>. Acesso em: 10 set. 2025.

BUTERIN, Vitalik. Ethereum Whitepaper: a next-generation smart contract and decentralized application platform. [S. l.]: **Ethereum.org**, 2014. Disponível em: <https://tinyurl.com/2jhpdmne>. Acesso em: 6 maio 2026.

CLIFTON, Judith; FERNÁNDEZ-GUTIÉRREZ, Marcos; CAGIGAS, Diego. Beyond the hype: the actual use of blockchain in government. **Policy Design and Practice**, Abingdon, v. 6, n. 4, p. 389-396, 2023. Disponível em: <https://doi.org/10.1080/25741292.2023.2272377>. Acesso em: 10 set. 2025.

GIAMBERARDINO, G. G.; GADDA, T. M. C.; NAGALLI, A. Uso da tecnologia blockchain nas contratações públicas sustentáveis de obras rodoviárias. **Revista de Administração Pública**, Rio de Janeiro, v. 58, n. 3, p. e2023-0073, 2024. DOI: <https://doi.org/10.1590/0034-761220230073>. Acesso em: 16 out. 2025.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system. [S. l.]: Bitcoin.org, 2008. Disponível em: <https://tinyurl.com/3ejsbuku>. Acesso em: 6 maio 2026.

PAGE, Matthew J. *et al.* A declaração PRISMA 2020: diretriz atualizada para relatar revisões sistemáticas. **Rev. Panam Salud Publica**, [s. l.], v. 46, 2022. DOI: <https://doi.org/10.26633/RPSP.2022.112>.

SCHOTTEN, P. C.; MOREIRA, D. G.; SOARES, H. V. C.; GRASIEL, J. R.; GONÇALVES, N. J. Conceitos teóricos e a aplicação prática do planejamento estratégico: um estudo em uma empresa pública do setor de saneamento básico. **Encontro Internacional de Gestão, Desenvolvimento e Inovação** (Eigedin), v. 4, n. 1, out. 2020. Disponível em: <https://tinyurl.com/2wwj3r3u>. Acesso em: 15 out. 2025.

SILVA, Fabian Andrade. **Modelo computacional para cadeia de custódia digital**: identificação e coleta com base em tecnologia blockchain. 2024. Dissertação (Mestrado em Computação Aplicada) – Universidade Tecnológica Federal do Paraná, Curitiba, 2024. Disponível em: <https://tinyurl.com/2vu4dcpz>. Acesso em: 10 set. 2025.

SZABO, Nick. **Smart contracts**. [S. l.], 1994. Disponível em: <https://tinyurl.com/msdjruvf>. Acesso em: 15 out. 2025.

TAN, E.; DAN, S.; SHAHZAD, K. Editorial convidado: preenchendo o abismo entre “o que poderia ser” e “o que é”: o impacto das tecnologias

blockchain na gestão de serviços públicos. **Revista Internacional de Gestão do Setor Público**, v. 38, n. 1, p. 1-11, jan. 2025. DOI: <https://doi.org/10.1108/IJPSM-01-2025-384>. Acesso em: 15 out. 2025.

TORNATZKY, Louis G.; FLEISCHER, Mitchell. **The processes of technological innovation**. Lexington, MA: Lexington Books, 1990.

TREVISAN, Karina. Quebra do banco Lehman Brothers completa 10 anos, relembra a crise de 2008. **G1**, Brasília, 15 set. 2018. Disponível em: <https://tinyurl.com/yc43pdsf>. Acesso em: 6 maio 2026.

VILELA, Matheus Dantas; ASSIS, Daniel Araújo de; EDUARDO, Pablo. Blockchain e processo penal: os reflexos dos avanços tecnológicos na confiabilidade da prova penal. **VirtuaJUS**, Belo Horizonte, v. 10, n. 18, p. 295-308, 2025. DOI: <https://doi.org/10.5752/P.1678-3425.2025v10n18p295-308>. Acesso em: 15 out. 2025.

Cibercriminalidade e capacidade técnica e operacional dos órgãos de apoio em tecnologia da informação e comunicação do Ministério Público Federal

Cybercrime and the technical and operational capacity of the Federal Prosecution Service's information and communication technology support bodies

DOI: https://doi.org/10.63601/978-65-88299-52-4_13

Rogério Postai

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Bacharel em Direito pelo Centro Universitário Sociesc (Unisociesc – Ânima). Servidor do Ministério Público Federal (MPF).

Waldir Peixoto da Silva Júnior dos Santos

Especialista em Governança da Tecnologia da Informação pela Escola Superior do Ministério Público da União (ESMPU). Especialista em Direito Administrativo pela Universidade Anhanguera/LFG. Graduado em Direito pela Universidade Federal de Alagoas (UFA) e em Engenharia de Software pelo Centro Universitário de Maringá/Unicesumar. Servidor do Ministério Público Federal (MPF).

Resumo: A presente pesquisa analisa a capacidade técnica e operacional dos órgãos de apoio em tecnologia da informação e comunicação (TIC) do Ministério Público Federal (MPF) no enfrentamento aos crimes cibernéticos no Brasil. Utilizando uma abordagem mista (quantitativa e qualitativa), o estudo incluiu a aplicação de questionários a servidores de TIC do MPF e análise documental de relatórios e legislações pertinentes. Os resultados obtidos evidenciam a existência de limitações na infraestrutura tecnológica, recursos humanos e falta de comunicação eficaz, destacando a importância de investimentos em capacitação, tecnologia e a sugestão de criação de núcleos periciais de TI regionalizados e especializados.

Palavras-chave: crimes cibernéticos; MPF; capacidade técnica; recursos humanos; comunicação.

Abstract: *This research analyzes the technical and operational capacity of the support units for Information and Communication Technology (ICT) within the Federal Prosecution Service (MPF) in combating cybercrimes in Brazil. Using a mixed-methods approach (quantitative and qualitative), the study includes the application of questionnaires to MPF ICT personnel and documentary analysis of relevant reports and legislation. The findings reveal limitations in technological infrastructure, human resources, and effective communication, highlighting the importance of investments in training and technology, as well as suggesting the creation of specialized and regionalized IT forensic units.*

Keywords: *cybercrimes; MPF; technical capacity; human resources; communication.*

1 Introdução

No Brasil, a investigação criminal no âmbito local é conduzida, em regra, pelas Polícias Cíveis e pelos Ministérios Públicos estaduais. Já no caso de determinadas espécies de delitos de natureza federal, essa função é atribuída à Polícia Federal e ao Ministério Público Federal (MPF).

Entre as diversas atribuições conferidas pelo texto constitucional ao Ministério Público Federal, assume grande importância a investigação e o processamento dos crimes que envolvem os interesses da União, interesses fundamentais, bem como questões de relevância nacional, conforme arts. 109 e 127 da Constituição Federal de 1988.

Assim como a sociedade se transforma ao longo do tempo, os crimes também se adaptam, alterando suas formas de execução e exigindo respostas institucionais cada vez mais complexas.

Atualmente, a impossibilidade de se separar a realidade social da virtual é facilmente perceptível, não havendo necessidade de grandes estudos ou mesmo pesquisas para tanto. Nesse viés, a investigação de crimes depende cada vez mais da análise de evidências digitais:

Documentos virtuais passam a fazer parte das relações sociais, tanto com referência às transações reais quanto às transações plenamente virtuais. Acompanhando essa tendência, a investigação dos ilícitos do mundo atual depende de evidências digitais, independentemente de terem ocorrido, total ou parcialmente, no mundo real ou no mundo virtual (Domingos; Röder, 2018).

Em uma sociedade na qual até o dinheiro passa a ser virtual, os criminosos se adaptam aos novos tempos e fazem uso crescente

da tecnologia para cometimento dos mais diversos crimes. A empresa NordVPN divulgou que o Brasil registrou cerca de 700 milhões de ataques cibernéticos no país em um período de doze meses, ou seja, 1.379 ataques por minuto (Nakamura, 2025).

O cenário de expansão da criminalidade cibernética impõe uma reflexão urgente sobre o grau de preparo das instituições nacionais de segurança pública no enfrentamento a esse tipo específico de delito. Uma das definições que precisam ser abordadas no presente artigo é, portanto, a do que configura um cibercrime ou crime cibernético.

A maior parte da doutrina nacional classifica os crimes cibernéticos em próprios e impróprios. Enquanto os crimes cibernéticos próprios somente podem ser cometidos por meio de dispositivos computacionais, os impróprios podem ser cometidos sem tais dispositivos (Sydow, 2021).

Em busca de artigos nacionais e internacionais acerca da temática, aplicou-se a seguinte *string* de pesquisa no Google Scholar (*“cybercrime investigation” OR “cybercrime law enforcement” OR “cybercrime prosecution” OR “cybercrime combat”*) AND (*“government capacity” OR “institutional capacity” OR “public sector capacity” OR “state capacity”*) AND (*“public agencies” OR “law enforcement agencies” OR “prosecutors” OR “justice system”*). Foram encontrados 94 resultados.

De modo semelhante, empregou-se a seguinte *string* em português: (*“crimes cibernéticos” OR “cibercrime” OR “criminalidade digital”*) AND (*“capacidade governamental” OR “capacidade institucional” OR “capacidade estatal”*) AND (*“órgãos públicos” OR “agências estatais” OR “Ministério Público” OR “forças de segurança”*). Nesse caso, foram obtidos 76 resultados.

A comparação entre os achados evidenciou que, no contexto da produção científica nacional, não havia estudos voltados especificamente à análise da *capacidade institucional dos órgãos de persecução penal* na investigação e responsabilização da criminalidade cibernética.

Em contrapartida, a literatura internacional apresenta um conjunto bem mais expressivo de publicações que abordam a temática, enfatizando, sobretudo, a *necessidade de especialização dos órgãos de segurança pública* para o enfrentamento eficaz dos crimes cibernéticos.

Tal lacuna é especialmente preocupante quando se considera que, em diversos países, investigações dessa natureza já vêm sendo

conduzidas com regularidade há algum tempo, contribuindo para a formulação de estratégias mais eficazes de prevenção e repressão.

Nos Estados Unidos, no ano de 2021, o pesquisador Christopher J. Moloney conduziu um estudo quantitativo com 929 agências locais de segurança pública, com o objetivo de avaliar a capacidade institucional de resposta aos crimes cibernéticos. A pesquisa teve como foco cinco dimensões fundamentais da estrutura organizacional dessas agências: (1) pessoal; (2) recursos financeiros e tecnológicos; (3) liderança e cultura organizacional; (4) processos e procedimentos de comunicação; e (5) relacionamentos, parcerias e formas de colaboração (Moloney, 2021).

Os resultados do estudo evidenciaram os impactos negativos significativos de fatores tanto internos quanto externos sobre a capacidade das agências de lidarem com incidentes relacionados a crimes cibernéticos e de responderem adequadamente às demandas da população. A partir dessa análise, tornou-se possível identificar os principais obstáculos estruturais e operacionais enfrentados pelos entes locais de segurança no enfrentamento a esse tipo de delito.

Considerando a escassez de estudos dessa natureza no contexto brasileiro, conforme a pesquisa realizada nos bancos de dados já mencionados, é imperativo que os órgãos e agências nacionais de segurança pública implementem rotinas regulares de autoavaliação institucional. Essa prática contribuiria para o aprimoramento de suas capacidades operacionais e estratégicas, promovendo uma resposta mais eficaz e coordenada diante da crescente incidência dos crimes cibernéticos.

Recentemente, o Conselho Nacional do Ministério Público (CNMP) editou a Resolução n. 294/2024, instituindo a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP). A norma tem por objetivo o estabelecimento de princípios, diretrizes e estruturas mínimas de governança voltadas à proteção dos ativos de informação das unidades e ramos ministeriais. Ela também prevê a criação de uma rede nacional de cooperação técnica entre os diversos Ministérios Públicos, além do estímulo à capacitação, ao intercâmbio e à resposta coordenada a incidentes de segurança digital (CNMP, 2024).

A norma mencionada demonstra uma preocupação institucional crescente com a integridade e disponibilidade dos sistemas

informatizados, bem como com a privacidade dos dados processados. Ainda que seja voltada à defesa interna da instituição – com foco em prevenção e resposta a ataques cibernéticos contra a infraestrutura do próprio Ministério Público –, a resolução evidencia a necessidade de amadurecimento institucional em outros temas de tecnologia da informação e segurança digital (CNMP, 2024).

Ressalte-se, no entanto, que há diferenças entre a cibersegurança institucional – voltada à proteção dos sistemas do próprio Ministério Público – e a capacidade investigativa relacionada aos crimes cibernéticos praticados contra terceiros, que é o foco do presente estudo. Embora interligadas, essas esferas não se confundem: proteger a rede interna da instituição é distinto de possuir equipes treinadas, ferramentas adequadas e estrutura organizacional apta a conduzir investigações criminais complexas em ambiente digital.

Ambas as frentes demandam investimento, planejamento e especialização, e medidas como a PNCiber-MP deveriam ser acompanhadas por iniciativas semelhantes voltadas à persecução penal, sob pena de manter-se vulnerável exatamente onde o MPF mais é chamado a atuar: na defesa da sociedade (CNMP, 2024).

Retomando a definição inicial de crimes cibernéticos e a classificação destes em crimes cibernéticos próprios e impróprios, o Ministério Público Federal atua na investigação de ambas as modalidades de cibercrime. Dentre os crimes mais frequentemente investigados pela instituição, destacam-se: 1) produção, venda e armazenamento de material pornográfico infantil; 2) crimes de racismo; 3) fraudes bancárias contra entidades autárquicas ou empresas públicas; 4) peculato eletrônico; 5) invasão de dispositivo informático; 6) lavagem de dinheiro e evasão de divisas por meio de criptomoedas.

A relação acima não esgota os crimes investigados pelo MPF, uma vez que presente a característica de transnacionalidade; da mesma forma, o crime terá sua competência atribuída à Justiça Federal quando houver quaisquer interesses federais ou matéria de relevância nacional, conforme previsto no art. 109 da Constituição Federal de 1988.

Aliás, o rol só tende a aumentar, visto que, desde a criação da Advanced Research Projects Agency Network (Arpanet) na década

de 1960, a internet evoluiu e se expandiu, fazendo com que as mais diversas atividades humanas fossem transferidas para o ambiente virtual, migração esta que abarca desde os relacionamentos humanos até a própria economia mundial.

Um dos grandes desafios do Direito e do Ministério Público Federal é o fato de que os criminosos não aguardam a tipificação legal de suas condutas antes de agir. Diante do avanço acelerado de novas tecnologias, o legislador se vê em uma corrida contra o tempo para criminalizar condutas ilícitas emergentes.

O MPF enfrenta obstáculos semelhantes, pois, como órgão estatal, só pode atuar com base em normas jurídicas – as quais, em sua maioria, têm um processo lento de aprovação e não acompanham a velocidade com que as organizações criminosas adotam inovações tecnológicas.

Do mesmo modo, os investimentos necessários para capacitar o órgão no combate a esse tipo de criminalidade também dependem da aprovação de leis orçamentárias, as quais demandam tempo.

Um exemplo dessa disparidade é a demora na adoção, pelo Brasil, da Convenção de Budapeste sobre Cibercrime, principal tratado internacional sobre o tema. A convenção foi firmada pela República Federativa do Brasil em 23 de novembro de 2001, aprovada pelo Congresso Nacional em 16 de dezembro de 2021, pelo Decreto Legislativo n. 37, e somente foi promulgada em 12 de abril de 2023 pelo Decreto n. 11.491/2023 (Brasil, 2023).

A implementação efetiva dos mecanismos de cooperação internacional ainda enfrenta desafios operacionais, evidenciando a dificuldade de harmonização entre o direito e a evolução tecnológica.

Diante desse cenário, impõe-se ao Ministério Público Federal uma necessária reflexão institucional quanto à sua real capacidade de enfrentar os desafios trazidos pelos crimes cibernéticos.

A questão central que orienta esta pesquisa é a seguinte: Qual é a estrutura organizacional e a capacidade técnica operacional do Ministério Público Federal no enfrentamento aos crimes cibernéticos no Brasil, e como se dá sua articulação com outras instituições nacionais e internacionais na área?

Diante da questão apresentada, esta pesquisa tem como objetivo geral a análise do cenário atual de atuação do MPF no combate aos

crimes cibernéticos, identificando a estrutura e a capacidade técnica da equipe de Tecnologia da Informação e Comunicação.

Deste modo, são perseguidos os seguintes objetivos específicos:

1. identificação das características especiais que cercam a investigação dos crimes cibernéticos e que demandam conhecimento e apoio técnico especializado de profissionais de Tecnologia da Informação;
2. mapeamento da estrutura organizacional do MPF dirigida ao enfrentamento dos crimes cibernéticos;
3. avaliação da capacidade técnica e operacional dos profissionais de Tecnologia da Informação do MPF, com foco nos recursos humanos e tecnológicos que possuem à sua disposição.
4. exame da cooperação do MPF com outras instituições nacionais e internacionais;
5. identificação de obstáculos/desafios enfrentados pelo MPF neste campo, a partir de percepções dos servidores que atuam no combate aos crimes cibernéticos.

A estrutura da pesquisa contempla cinco seções. A seção 1 é destinada a uma introdução do objeto e delimitação da pesquisa. A seção 2 é dedicada à exposição dos crimes cibernéticos, das atribuições do MPF, dos conceitos de prova digital e cadeia de custódia, bem como à Convenção de Budapeste. A seção 3 é dedicada à descrição da metodologia utilizada. A seção 4 traz a discussão e os resultados da pesquisa, englobando a análise da estrutura atual de recursos humanos, bem como percepções dos profissionais de TI sobre o combate à criminalidade cibernética. Por fim, a seção 5 trará as conclusões e impressões acerca da capacidade do MPF no combate aos crimes cibernéticos.

2 Revisão de literatura

Neste capítulo, são apresentados e descritos o conceito de crimes cibernéticos, bem como os critérios de definição da atribuição do MPF. Além disso, são abordados conceitos acerca da cooperação internacional e da prova eletrônica e sua cadeia de custódia, e também dos termos técnicos de tecnologia da informação necessários ao entendimento do tema.

2.1 Crimes cibernéticos

Inicialmente, cabe justificar a adoção da expressão *crimes cibernéticos* neste artigo. Na literatura nacional e internacional, são comumente utilizados termos como crimes digitais, crimes eletrônicos e crimes informáticos, cada um com sua fundamentação específica.

O termo “crimes eletrônicos” traz à tona o fato de os dispositivos computacionais serem constituídos por circuitos eletrônicos, os quais servem como meio para a prática delitiva. Por sua vez, a expressão “crimes digitais” remete à linguagem binária e digital inerente aos computadores. Já a denominação “crimes informáticos” deriva do vocábulo informática, originário do francês *informatique* – uma composição dos termos *information* (informação) e *automatique* (automático) (Informática, [20--?]).

Autores como Jesus e Milagre (2016, p. 49) utilizam a denominação de “crimes informáticos”, porém não é incomum encontrar outras denominações espalhadas na literatura, tais como “crimes de computador”, “*cybercrimes*”, “*computer crimes*”, “*computing crimes*”, “delito informático”, “crimes virtuais”, “crimes eletrônicos” ou ainda “crimes digitais”, “crimes cibernéticos”, “infocrimes”, “crimes perpetrados pela internet”, denominações distintas, mas que, no fundo, acabam por significar basicamente a mesma coisa.

Embora todas essas terminologias sejam teoricamente válidas, os termos cibercrime e cibercriminalidade foram os adotados pela Convenção de Budapeste (Brasil, 2001), razão pela qual são empregados neste estudo.

O crime cibernético é aquele cometido no ciberespaço (Levy, 1999), entendido como o espaço de comunicação aberto pela interconexão global de computadores e suas memórias, viabilizada pela internet e redes digitais. Em termos mais simples, trata-se de delitos praticados em sistemas informáticos ou por meio da internet, os quais, devido à natureza transnacional da rede, frequentemente assumem caráter transfronteiriço. Conforme mencionado na introdução, a doutrina nacional classifica os crimes cibernéticos em duas categorias, reforçando o conceito:

Há que se dizer que são algumas das condutas que ora classificam-se como delitos informáticos próprios (puros ou impuros) que terminam por lesar a coletividade com as características que se apresentam acima.

Contudo, não são somente os crimes próprios que trazem características especiais. Certamente que há peculiaridades nos crimes informáticos impróprios – crimes comuns cometidos pela eleição do computador como meio – que por serem cometidos com o uso da informática levam a sociedade a inseguranças e fragilidades também (Sydow, 2009, p. 73).

Embora a internet seja um fenômeno relativamente recente, a rápida adoção de tecnologias digitais tem tornado os crimes cibernéticos – próprios ou impróprios – cada vez mais frequentes. Em um contexto global marcado pelo trabalho remoto, guerras conduzidas por drones e ataques hackers transnacionais, o cibercrime emerge como um dos principais desafios para o Ministério Público Federal, demandando adaptação institucional às novas dinâmicas criminais.

2.2 Crimes federais

Os crimes de competência da Justiça Federal foram estabelecidos pelo legislador constituinte no art. 109 da Constituição Federal de 1988, nos seguintes termos:

Art. 109. Aos juízes federais compete processar e julgar:

[...]

IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;

V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;

VI - os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira;

[...]

IX - os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar;

X - os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o “exequatur”, e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização; [...].

Não há competência definida exclusivamente para os crimes cibernéticos, sendo a competência para julgá-los definida pelas mesmas regras estabelecidas para os demais crimes. Em outras palavras, caso o crime cibernético próprio ou impróprio se enquadre em uma das hipóteses definidas nos incisos do art. 109 do texto constitucional, ele será julgado pela Justiça Federal e, por conseguinte, sua investigação e o ajuizamento da respectiva ação penal será de atribuição do Ministério Público Federal.

2.3 Prova eletrônica e cadeia de custódia

Para o ajuizamento da ação penal, é imprescindível que o membro do Ministério Público disponha de provas concretas do delito cometido. No âmbito dos crimes cibernéticos, a prova digital destaca-se como elemento probatório por excelência, fundamentada na lógica binária e caracterizada por peculiaridades que demandam técnicas especializadas de manuseio e análise.

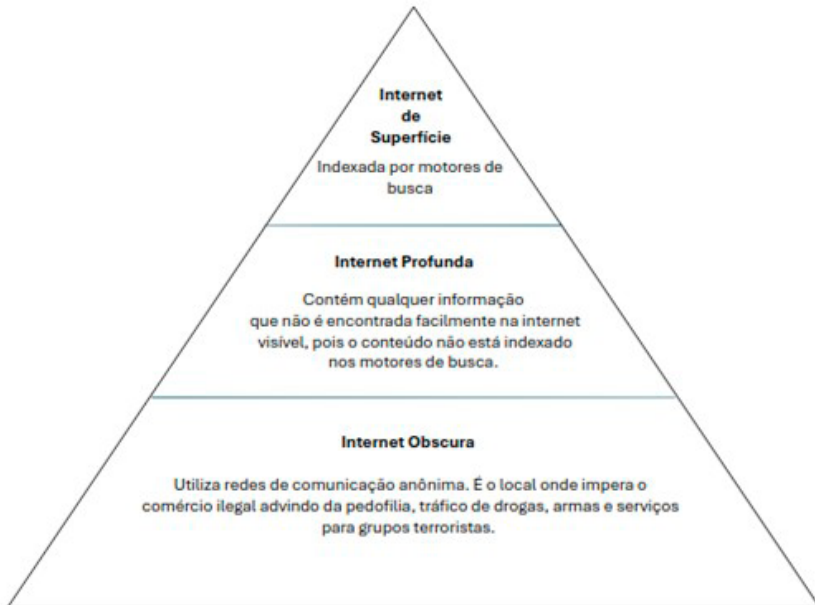
Ocorre que as provas digitais são cercadas de complexidades. A obtenção de provas digitais, em grande parte dos casos, depende do acesso a informações armazenadas por empresas privadas, notadamente os provedores de conexão e de aplicações de internet. Tais informações não são conservadas indefinidamente, pois seu armazenamento implica custos operacionais elevados e exige significativo espaço em servidores, o que confere à prova digital um caráter altamente volátil. Essa limitação impõe às autoridades investigativas a necessidade de atuação célere e tecnicamente qualificada, a fim de evitar a perda irreversível de dados relevantes à persecução penal.

Nesse contexto, o Marco Civil da Internet (Lei n. 12.965/2014) estabelece prazos máximos de guarda de registros de conexão e de acesso a aplicações, os quais, conforme seus arts. 13 e 15, são de um ano e seis meses, respectivamente. Embora seja possível ao Ministério Público requerer judicialmente a extensão desses prazos, é notório que a morosidade característica de grande parte dos inquéritos policiais no Brasil frequentemente compromete a efetividade dessa prerrogativa. Raros são os procedimentos investigatórios que se concluem dentro dos prazos estabelecidos para a guarda ordinária dos dados.

Em outras palavras, no âmbito dos crimes cibernéticos, a lentidão na investigação frequentemente se traduz em impunidade, pois os vestígios digitais – por sua própria natureza efêmera – tendem a desaparecer com o tempo. Situações típicas de processos que se estendem por anos ou mesmo décadas, comuns em outros tipos de delitos, tornam-se incompatíveis com a lógica probatória da era digital, na qual o tempo é fator decisivo para a preservação da verdade material.

Além das dificuldades relacionadas à volatilidade desse tipo de prova, conforme representado na Figura 1, baseada em outra imagem extraída da obra de Alex Alexandrou (2022, p. 77), a porção da internet acessível ao usuário comum – também conhecida como *surface web* – corresponde a uma fração bastante reduzida do total de dados disponíveis online. A maior parte das informações encontra-se em camadas menos acessíveis, como a *deep web* e a *dark web*, que exigem ferramentas ou permissões específicas para serem exploradas.

Figura 1 – Internet de superfície, internet profunda e internet obscura



Fonte: adaptada com base em imagem contida em Alexandrou (2022, p. 77).

Essa representação piramidal destaca a complexidade e a profundidade da estrutura informacional da internet, evidenciando os desafios enfrentados pelas autoridades no monitoramento e combate à cibercriminalidade e à colheita das provas digitais.

Embora o Código de Processo Penal brasileiro (CPP) enumere as espécies de provas admitidas em juízo (art. 155), não há previsão expressa do termo prova digital (Brasil, 1941). Na prática, contudo, a prova digital atua como fonte probatória para a produção da prova documental (quando registrada em arquivos) e da prova pericial (quando submetida a exame técnico). Ambas são expressamente regulamentadas pelo CPP, o que legitima sua utilização no processo penal.

Como restou mencionado, a extração, a preservação e a análise de provas digitais exigem conhecimentos especializados em tecnologia da informação (TI), tornando indispensável a atuação de profissionais da área para garantir a validade jurídica das evidências. Além disso, a prova digital não se limita a comprovar a materialidade do crime: seu objetivo é convencer o órgão julgador tanto da ocorrência delitiva quanto da autoria.

A prova digital possui características intrínsecas que a tornam especialmente vulnerável a alterações (acidentais ou intencionais). Por isso, exige-se rigoroso cumprimento da cadeia de custódia, definida no art. 158-A do Código de Processo Penal como “o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado [...] para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (Brasil, 1941).

No âmbito do MPF, a Secretaria de Perícia, Pesquisa e Análise (SPPEA) elaborou o *Manual Prático da Cadeia de Custódia*, que estabelece diretrizes para identificação, isolamento e coleta de vestígios digitais, bem como preservação da integridade por meio de técnicas como *hash* criptográfico (Brasil, 2021b).

Além disso, a SPPEA foi responsável pela criação de um portal eletrônico, destinado ao armazenamento seguro das provas digitais.

Um dos serviços disponibilizados pela SPPEA, inclusive, é a geração de *hashes*, armazenamento e manutenção de cadeia de custódia de provas digitais. O estabelecimento de padrões e protocolos a serem seguidos é imprescindível para assegurar a admissibilidade processual das provas digitais, evitando sua impugnação por vícios na coleta ou manipulação.

A eficácia da persecução penal em crimes cibernéticos depende não apenas da existência de provas digitais, mas também de sua correta interpretação pelos órgãos judiciais.

O presente artigo não tem como escopo a análise exaustiva das especificidades técnicas que envolvem a coleta, a preservação e o manuseio das provas digitais. No entanto, é possível ilustrar a variedade de metodologias e recursos tecnológicos disponíveis aos membros e servidores do MPF por meio da análise do documento *Roteiro de atuação: crimes cibernéticos e provas eletrônicas*, elaborado de forma colaborativa por integrantes da Secretaria de Cooperação Internacional, da 2ª Câmara de Coordenação e Revisão (CCR) do MPF, do Grupo de Apoio sobre Crimes Cibernéticos da referida câmara e do Núcleo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo (Brasil, MPF, 2021a).

O roteiro citado, apesar do seu acesso restrito, reúne orientações práticas e atualizadas que auxiliam na condução de investigações envolvendo delitos cibernéticos, oferecendo suporte técnico-jurídico essencial à atuação institucional.

Cabe destacar que a dinâmica da tecnologia é marcada por constante transformação, ocorrendo em ritmo acelerado. Por esse motivo, impõe-se aos servidores públicos envolvidos na persecução penal, especialmente no âmbito do MPF, a necessidade de atualização e capacitação contínuas.

Apenas por meio do conhecimento especializado é possível compreender e acompanhar as inovações tecnológicas que impactam a produção, obtenção e análise da prova digital, elemento central na elucidação de crimes praticados em ambiente virtual.

2.4 Cooperação internacional e Convenção de Budapeste

A Convenção de Budapeste é um marco importante para a cooperação internacional no combate ao crime cibernético, pois estabelece um conjunto de regras e procedimentos para que os países colaborem na investigação e julgamento desses crimes.

O Comitê da Convenção sobre Crimes Cibernéticos (T-CY), composto por representantes das partes da Convenção de Budapeste, é responsável por avaliar a implementação adequada da Convenção,

preparar notas de orientação e instrumentos legais adicionais e facilitar a cooperação entre as partes (Conselho da Europa, [2025?]).

Há ainda os projetos de capacitação pelo Escritório do Programa de Crimes Cibernéticos do Conselho da Europa (C-PROC) para ajudar países em todo o mundo a fortalecer suas capacidades de justiça criminal para a investigação, acusação e julgamento de crimes cibernéticos e outros casos envolvendo evidências eletrônicas, em conformidade com a convenção e as recomendações do T-CY (Conselho da Europa, 2022).

Por ser uma espécie de crime sem fronteiras facilmente definidas, a cooperação internacional é imprescindível para o combate efetivo dos crimes cibernéticos. Desse modo, ao facilitar o intercâmbio de informações entre as autoridades policiais e judiciais dos países signatários, a convenção possibilita a troca de dados relevantes para as investigações criminais.

Os países signatários da Convenção de Budapeste se comprometem a prestar assistência mútua na coleta de provas eletrônicas, como dados de sistemas, registros de comunicação e informações de usuários. Além de facilitar a investigação dos crimes, o instrumento normativo vai além ao estabelecer, inclusive, procedimentos para extradição de pessoas acusadas de crimes cibernéticos, facilitando o processo de envio de suspeitos para julgamento no país onde o crime foi cometido.

A necessidade de cooperação entre os países no combate aos crimes cibernéticos também tornou possível a previsão, na referida norma, de pontos de contato entre os países, facilitando a comunicação e o envio de pedidos de assistência (Conselho da Europa, 2022).

A adesão do Brasil à Convenção de Budapeste proporciona o fortalecimento da legislação nacional, visto que impulsiona o país a aprimorar sua legislação sobre crimes cibernéticos, adaptando-a aos padrões internacionais.

Em relação à cooperação com outros países, o Brasil poderá cooperar de forma mais eficaz na investigação e julgamento de crimes cibernéticos, compartilhando informações e provas.

Considerando a rápida emergência dos crimes cibernéticos, não se ignora a existência prévia de instrumentos normativos bilaterais que permitiam a persecução de crimes transnacionais. O diferencial da Convenção de Budapeste é que ela teve como seu objeto principal o

combate a essa espécie de crime, dedicando-se a ferramentas céleres e mais adequadas ao combate dos crimes cibernéticos que ultrapassam as fronteiras nacionais, envolvendo redes e sistemas de diferentes países.

A convenção também prevê a proteção de direitos como a privacidade e a liberdade de expressão, garantindo que o combate ao crime cibernético seja feito protegendo os direitos humanos e não de forma a violar esses direitos (Corrêa; Monteiro Neto, 2023).

Diante da importância de instrumentos de cooperação eficazes na investigação e persecução dos crimes cibernéticos, a adesão do Brasil à Convenção de Budapeste permite a ampliação do leque de instrumentos à sua disposição para a cooperação internacional no combate ao crime cibernético, e demonstra o compromisso do país em fortalecer sua legislação e mecanismos de combate a esses crimes.

3 Metodologia

A pesquisa adota uma abordagem mista (quantitativa e qualitativa), combinando os métodos de modo a avaliar a capacidade técnica e operacional dos órgãos de apoio em TI do MPF no combate aos crimes cibernéticos.

A natureza da pesquisa empreendida foi tanto exploratória, por investigar um tema ainda pouco mapeado no contexto do MPF, qual seja, a estrutura de TI em apoio à persecução penal aos crimes cibernéticos, quanto descritiva, ao mapear as estruturas, recursos e processos existentes no âmbito do MPF. Ela também tem um viés explicativo, ao realizar testes para hipóteses sobre as causas de eventuais limitações identificadas.

A principal pretensão é a realização do diagnóstico de eventuais problemas e apresentação de possíveis propostas de mudanças e melhorias que aumentem a eficiência do MPF no combate à criminalidade cibernética.

Uma das abordagens do estudo se deu pela aplicação de *survey* transversal, utilizando questionários online (via Google Forms) com perguntas abertas, fechadas e em escalas *Likert*.

Considerando a facilidade de envio do questionário e a limitação do envio aos profissionais atuantes na área de tecnologia da informação

da instituição, quais sejam, os 454 técnicos em tecnologia da informação e os 120 analistas em desenvolvimento de sistemas do MPF (ativos em agosto de 2025), tentou-se obter informações daqueles que tivessem atuado na persecução penal de crimes cibernéticos.

De maneira secundária, foram coletados dados públicos obtidos do Portal de Transparência do MPF (orçamentos e relatórios internos).

Além da análise da própria legislação (Convenção de Budapeste) e dos relatórios internos, foram analisadas as respostas abertas dos questionários aplicados quanto à percepção dos servidores em relação à eficácia da atuação ministerial.

O questionário foi encaminhado em três momentos distintos, por meio dos e-mails funcionais dos servidores, fazendo uso da plataforma Google Forms, de maneira anonimizada.

Quanto à estrutura do questionário, as perguntas formuladas destinaram-se a obter informações sobre cinco assuntos distintos:

1. Perfil dos profissionais: foram coletados dados sobre o cargo ou a função atual do respondente e o tempo de experiência com suporte técnico ou perícia em crimes cibernéticos.
2. Recursos e infraestrutura tecnológica: a adequação da infraestrutura tecnológica para a realização de análises e investigações em ambiente digital foi avaliada. Questões específicas abordaram as principais limitações técnicas, como a falta de softwares, licenças e equipamentos.
3. Comunicação e interação com a área jurídica: o questionário buscou avaliar a comunicação entre as equipes de TI e os procuradores da República. Foi solicitado que os participantes descrevessem as maiores dificuldades de compreensão e os tipos de informações mais difíceis de explicar.
4. Capacitação e desafios: foi investigada a participação em capacitações específicas e a percepção sobre a essencialidade da formação contínua. Os profissionais também citaram temas e certificações prioritárias e os maiores desafios técnicos nas investigações.
5. Limitações legais e cooperação: as perguntas abordaram a frequência das limitações legais, exemplos dessas limitações e a

percepção sobre a necessidade de formação jurídica. A questão da cooperação com provedores/plataformas estrangeiras e o impacto dela na perícia também foi investigada.

Em alguns assuntos, priorizaram-se perguntas abertas devido à grande quantidade de respostas possíveis, difíceis de serem limitadas a campos fechados, tais como a relativa a ferramentas tecnológicas utilizadas.

Além dos questionários online direcionados aos servidores de TIC, realizou-se a análise documental da legislação aplicável e dos documentos internos publicados pelo próprio MPF, como relatórios, orçamentos e documentos de governança.

Os dados quantitativos foram analisados para verificar a evolução de investimentos, a contratação de servidores ou mesmo para fins de confirmação de parte das informações obtidas nos questionários.

Entre as limitações da pesquisa, houve o risco de baixa adesão aos questionários pela população pretendida, bem como a possibilidade de viés das respostas, uma vez que talvez somente os servidores com posicionamento mais crítico se dispusessem a respondê-los.

Outra limitação envolveu a dificuldade de acesso a determinadas informações ou documentos que não são de acesso público, ou falta de monitoramento do órgão em relação à atuação específica na temática.

Apesar das limitações mencionadas, ao combinar métodos diferentes, tais como o *survey* e a análise documental, pretendeu-se garantir que as informações coletadas fossem tão próximas quanto possível da realidade.

Acerca da utilização de ferramentas de inteligência artificial, foram utilizados alguns dos modelos disponíveis no mercado, tais como Gemini e ChatGPT, para fins de formatação de referências obtidas, verificações e aprimoramento gramatical, bem como definição inicial de *prompts* em busca de artigos científicos nos bancos de dados indexados.

Considerando o tema complexo dos cibercrimes e os diversos fatores que influenciam um enfrentamento bem-sucedido, somente uma junção entre aspectos objetivos e percepções subjetivas daqueles envolvidos no seu enfrentamento pode fornecer *insights* relevantes quanto a uma estrutura de apoio técnico mais próxima da ideal.

4 Apresentação e discussão dos resultados

4.1 Estrutura atual de apoio

Pesquisas exploratórias realizadas no site da instituição (MPF) possibilitaram verificar a existência de poucas unidades especializadas no combate aos crimes cibernéticos, tais como o Grupo de Apoio sobre Criminalidade Cibernética (GACC/2ª CCR/MPF).

O GACC, vinculado à 2ª CCR do MPF, é um grupo técnico criado em 2011 para auxiliar no combate a crimes cibernéticos, especialmente, pornografia infantojuvenil e racismo digital.

No ano de 2024, foi criado o Grupo de Atuação Especial no Combate aos Crimes Cibernéticos e aos Crimes praticados mediante o Uso de Tecnologias de Informação (GACCTI), conforme Resolução CSMPF n. 229, de 2 de abril de 2024 (Brasil, 2024b).

Outra unidade específica, desta vez no âmbito da PRR da 3ª Região, é o Núcleo Técnico de Combate aos Crimes Cibernéticos da Procuradoria Regional da República do Estado de São Paulo (NTCCC-PR/SP).

Recentemente, a Procuradoria da República no Estado do Rio de Janeiro instituiu, no âmbito da Assessoria de Pesquisa e Análise Descentralizada da PR/RJ, o Núcleo Técnico de Combate aos Crimes Cibernéticos – NTCCC/PR-RJ, por meio da Portaria PRRJ n. 443, de 20 de maio de 2025 (Brasil, 2025e).

O Portal de Transparência não traz informações claras acerca dos núcleos especializados criados, sendo as informações acerca dos Núcleos Técnicos de Combate aos Crimes Cibernéticos obtidas a partir de informações esparsas contidas nos Relatórios de Atividades da 2ª Câmara de Coordenação e Revisão do MPF, nos quais são descritas as metas e propostas definidas e as atividades realizadas no decorrer dos anos. A leitura desses relatórios permite verificar que a instituição, paulatinamente, desenvolve atividades visando a criação de uma estrutura que permita o combate eficiente aos crimes cibernéticos.

Uma das metas (Meta 3) do Grupo de Apoio sobre Criminalidade Cibernética (GACC) contidas no Relatório de Atividades de 2024 é a implantação do Núcleo Técnico de Combate a Crimes Cibernéticos Nacional (Ncyber), do Sistema de Recepção e Análise de Vestígios Digitais

e o estabelecimento de um fluxo padronizado de recebimento de notícias referentes a crimes cibernéticos em âmbito nacional (Brasil, 2025a).

A existência de núcleos de apoio regionalizados do tipo não é a regra. A maioria dos profissionais de TIC atuam em uma variedade de funções, envolvendo desde o suporte até o atendimento de demandas específicas dos membros, carecendo o MPF de estruturas suficientes para o combate desse tipo de crime.

A preocupação com a criação de núcleos especializados, apesar de não se estender a todos os estados da Federação, permite concluir que a instituição não ignora a necessidade de especialização dos membros no combate a esses crimes, inclusive com capacitação e dedicação exclusiva de servidores.

Ao analisar o organograma do MPF disponível no site da instituição, verifica-se que os servidores em TIC estão distribuídos entre as Assessorias de Pesquisa e Análise Descentralizada (ASSPAD), as Coordenadorias de Tecnologia da Informação e Comunicação (CTIC) e na própria Secretaria de Tecnologia da Informação e Comunicação (STIC), não tendo sido encontrados dados exatos de lotação proporcional de servidores em cada um dos departamentos do órgão.

Parte das atividades solicitadas aos servidores de TIC e destinadas à instrução das investigações é realizada a pedido dos membros a partir de um catálogo de serviços, e são realizadas pelos profissionais de TIC vinculados à SPPEA.

Apesar das tentativas de se obterem dados acerca da lotação dos servidores de TIC em cada um dos departamentos, a pesquisa não logrou definir com exatidão quantos servidores estão alocados especificamente no combate aos crimes cibernéticos, não havendo campos específicos no Portal de Transparência da instituição que permitissem verificar tal informação.

4.2 Evolução orçamentária e de recursos humanos

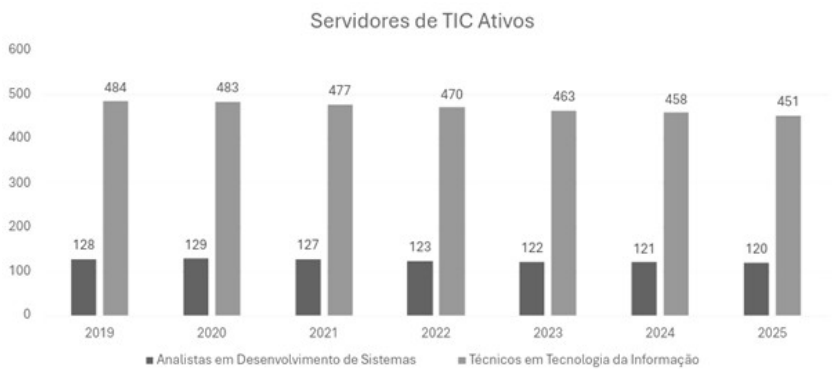
Um dos parâmetros a serem observados objetivamente quando tratamos do combate à criminalidade cibernética é a existência de investimentos, uma vez que a análise de dados e monitoramento requer, inevitavelmente, a utilização de ferramentas tecnológicas de

hardware e software próprias para a atividade, o que demanda recursos públicos consideráveis.

Com o advento da pandemia global da covid-19, a maioria dos setores públicos precisou migrar para o ambiente virtual, o que implicou na necessidade de investimentos urgentes na área de Tecnologia e Informação.

Apesar dos impactos pandêmicos, verifica-se que a quantidade de profissionais de TIC e a evolução na contratação permaneceu estável e, inclusive, com uma diminuição desses profissionais, como pode ser observado na Figura 2, criada a partir dos dados públicos disponíveis no Portal MPF em Números (Brasil, 2025c):

Figura 2 – Servidores de tecnologia da informação ativos



Fonte: extraído da plataforma MPF em Números (Brasil, 2025c).

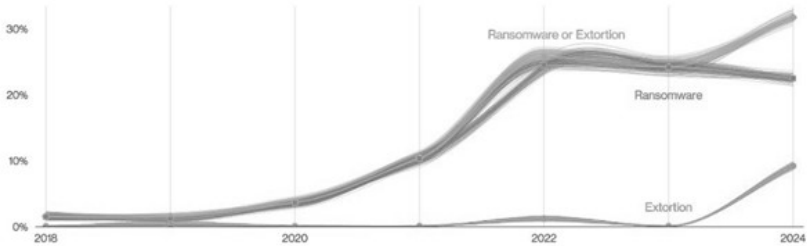
Ressalte-se que nem todos os servidores acima mencionados se dedicam ao combate de crimes cibernéticos, bem como poucos deles integram algum núcleo especializado de combate a essa espécie de crime.

Diante da alteração na nomenclatura de vários cargos no decorrer dos anos, decidiu-se por focar nos dois cargos mais prevalentes no âmbito da instituição, quais sejam o dos analistas em desenvolvimento de sistemas e o dos técnicos em tecnologia da informação.

O cenário de cibersegurança verificou uma escalada de ataques nos últimos anos, especialmente no período pós-pandêmico. Conforme ilustrado na Figura 3, com base em dados compilados pelo

relatório *Data Breach Investigations Report (DBIR)* da Verizon, somente a partir da análise dos ataques de *ransomware* e extorsão praticados pela internet já é possível ter uma ideia da trajetória ascendente no volume de incidentes cibernéticos:

Figura 3 – Tendências de incidentes (2018-2024)



Fonte: adaptado de Verizon (2024, p. 7).

A quantidade de servidores de TIC contratados no decorrer dos anos certamente não acompanhou a tendência de aumento de incidentes cibernéticos.

Quanto à evolução orçamentária, apesar de a análise não ter adentrado nas especificidades das contratações realizadas, o que pode não refletir com exatidão os gastos destinados estritamente ao combate de crimes cibernéticos, foram analisadas duas rubricas dos relatórios de detalhamento de despesas orçamentárias do MPF, disponíveis no Portal de Transparência da instituição, entre os anos de 2019 (início da pandemia) e 2025, quais sejam:

- Outras Despesas Correntes/40 Serviços de tecnologia da informação e comunicação
- Investimentos/40 Serviços de tecnologia da informação e comunicação – PJ

Há outras rubricas que podem esconder investimentos específicos em TIC, tais como “Equipamentos e material permanente”, porém a análise se limitou às rubricas acima especificadas para fins de referência da evolução orçamentária destinada à área de tecnologia da informação em geral.

Os recursos previstos para utilização nas referidas rubricas foram então comparados com os recursos totais previstos para orçamento do órgão naquele ano, para fins de definição de um percentual.

Por se tratar de uma análise breve para servir como referência, esta não se dedicou à avaliação dos valores efetivamente gastos, mas, sim, àqueles previstos pela Administração Superior do órgão como necessários para tal finalidade. A Tabela 1 consolidou os dados orçamentários disponibilizados no Portal de Transparência do MPF.

Tabela 1 – Relação entre orçamento total e custeio/investimentos em TI – MPF

	ORÇAMENTO TOTAL	CUSTEIO	P/ORÇ.	INV./PROJETOS	P/ORÇ.
2019	R\$ 4.154.402.851,00	R\$ 37.760.473,00	0,91%	R\$ 891.266,00	0,021%
2020	R\$ 4.265.241.532,00	R\$ 30.124.485,00	0,71%	R\$ 233.143,00	0,006%
2021	R\$ 4.279.195.925,00	R\$ 34.655.853,00	0,81%	R\$ 698.034,00	0,016%
2022	R\$ 4.659.339.564,00	R\$ 44.717.130,00	0,96%	R\$ 6.056.201,00	0,130%
2023	R\$ 5.116.203.226,00	R\$ 47.086.236,00	0,92%	R\$ 595.232,00	0,012%
2024	R\$ 5.388.344.859,00	R\$ 56.681.851,00	1,05%	R\$ 1.771.496,00	0,035%
2025	R\$ 5.702.534.598,00	R\$ 86.994.823,00	1,5%	R\$ 2.331.438,00	0,04%

Fonte: extraído do Portal de Transparência (Brasil, 2025b).

Legenda:

Orçamento Total: Valor Total previsto para o respectivo ano.

Custeio: Valor previsto para Despesas Correntes/TIC.

P/ORç.: Relação Percentual quanto ao Orçamento Total.

Inv./Projetos: Valor previsto para Investimentos/TIC-PJ.

P/ORç.: Relação Percentual quanto ao Orçamento Total.

Para fins de comparação, buscou-se analisar um órgão público interno com atribuições e orçamentos semelhantes, qual seja, o Ministério Público do Estado de São Paulo (MPSP).

No MPSP, não há especificação de investimentos em tecnologia da informação nos relatórios de despesas detalhadas; essa especificação somente vem colocada nos relatórios de Despesas por Ação Orçamentária no item de projetos, na rubrica 1233 – Avanço da tecnologia da informação (despesas de investimentos).

Ao analisar os dois relatórios (Despesas detalhadas e Despesas por ação orçamentária), foi possível chegar à seguinte configuração orçamentária do MPSP, conforme Tabela 2, elaborada a partir dos dados obtidos no Portal de Transparência do MPSP:

Tabela 2 – Relação entre orçamento total e custeio/investimentos em TI – MPSP

	ORÇAMENTO TOTAL	CUSTEIO	P/ORÇ.	INV./PROJETOS	P/ORÇ.
2019	R\$ 2.749.760.029,00	R\$ 49.688.181,00	1,81%	R\$ 10,00	0,00%
2020	R\$ 2.781.008.164,00	R\$ 45.544.492,00	1,64%	R\$ 10,00	0,00%
2021	R\$ 2.850.817.308,00	R\$ 49.187.717,00	1,73%	R\$ 10,00	0,00%
2022	R\$ 3.134.860.495,00	R\$ 61.110.451,00	1,95%	R\$ 24.036.821,00	0,77%
2023	R\$ 3.302.740.700,00	R\$ 60.355.906,00	1,83%	R\$ 8.000.000,00	0,24%
2024	R\$ 3.916.548.828,00	R\$ 88.935.439,00	2,27%	R\$ 9.099.661,00	0,23%
2025	R\$ 4.022.678.955,00	R\$ 79.914.069,00	1,98%	R\$ 8.074.290,00	0,20%

Fonte: extraído do Portal da Transparência (MPSP, 2025).

Legenda:

Orçamento Total: Valor Total previsto para o respectivo ano.

Custeio: Valor previsto para Despesas Correntes/TIC.

P/ORç.: Relação Percentual quanto ao Orçamento Total.

Inv./Projetos: Valor previsto para Investimentos/TIC-PJ.

P/ORç.: Relação Percentual quanto ao Orçamento Total.

Apesar de a forma de elaboração do orçamento dos dois órgãos provavelmente diferir entre si, bem como a análise não verificar as

especificidades dos recursos previstos, a comparação entre as duas tabelas permite verificar que, embora os recursos do órgão estadual sejam menores do que os previstos para o MPF, o qual atua em âmbito nacional, o percentual orçamentário destinado aos investimentos na área pelo MP/SP é superior na maioria das vezes.

Quanto à análise orçamentária, a pesquisa encontrou dificuldades em avaliar dados específicos referentes a investimentos realizados especificamente na área de combate aos crimes cibernéticos, razão pela qual foram analisados os dados gerais de previsões na área para fins de referência quanto à evolução de provisão de créditos orçamentários no decorrer dos anos.

Apesar das limitações decorrentes das informações disponíveis no Portal de Transparência, é possível verificar de maneira intuitiva que não há a esperada correspondência entre as previsões orçamentárias e a ampliação do quadro funcional de servidores com conhecimento especializado na área em função do aumento vertiginoso dos crimes cibernéticos.

4.3 Plano estratégico institucional do MPF e metas e indicadores nele existentes

O MPF possui um documento no qual foram estabelecidos os direcionamentos estratégicos da instituição. O seu primeiro ciclo estratégico englobou o período de 2011 a 2021, e atualmente está em vigor o ciclo estratégico com vigência de 2024 a 2027.

A íntegra do Planejamento Estratégico Institucional pode ser consultada na Portaria PGR/MPF n. 843, de 18 de outubro de 2024. O documento de governança estabelece diretrizes que devem nortear as ações, projetos, indicadores e metas de gestão da instituição até o final do exercício de 2027. Ele também traz uma classificação dos Objetivos Estratégicos (OE) em três perspectivas: sociedade, processos internos, e pessoas e recursos (Brasil, MPF, 2024a).

O “Objetivo Estratégico 5 – viabilizar a transformação digital” pode ser utilizado como fundamento para justificar a avaliação da capacidade em recursos humanos e tecnológicos dos servidores, bem como a identificação dos desafios tecnológicos no combate à criminalidade cibernética.

A existência desse objetivo indica que o MPF possui como estratégia institucional a necessidade de evolução tecnológica no exercício de suas atribuições constitucionais.

A leitura do Planejamento Estratégico Institucional permitiu identificar que ele não traz indicadores ou metas específicos que permitam quantificar a capacidade de atuação do MPF especificamente no combate à cibercriminalidade, nem há um detalhamento do montante de recursos ou de pessoal a ser alocado nos anos seguintes para a persecução penal de crimes cometidos no ambiente digital, dificultando uma análise sobre a efetividade e eficácia da estratégia institucional no atingimento desse objetivo.

Apesar das limitações verificadas, a introdução de temas como transformação digital e uso da inteligência artificial como objetivos estratégicos pode indicar que a instituição tem interesse na modernização tecnológica de suas atividades, o que pode levar à melhoria do enfrentamento dos crimes cibernéticos.

4.4 Respostas obtidas dos servidores de apoio em TIC

Especificamente quanto à aplicação dos questionários e sua população-alvo, cumpre apontar que os servidores da área de TIC se ocupam de demandas variadas, como manutenção e desenvolvimento de sistemas de uso interno, ou seja, nem todos se dedicam ao auxílio de investigações.

A expectativa, portanto, ao encaminhar o questionário, sempre foi de que um número menor de servidores o respondesse, o que realmente ocorreu – foi respondido por dezenove servidores.

A análise das respostas do questionário, intitulado “Dificuldades na Investigação de Crimes Cibernéticos – Percepções de Profissionais de TI que Auxiliam o Ministério Público Federal”, revela uma série de desafios enfrentados pelos profissionais de TI em sua atuação no auxílio ao combate da criminalidade cibernética.

A análise das respostas se concentrou em identificar as limitações técnicas, as dificuldades de comunicação com a área jurídica e os desafios de cooperação, endereçando diretamente os objetivos específicos 3, 4 e 5 mencionados na introdução.

A maioria dos respondentes afirmou atuar há mais de cinco anos em suporte técnico ou perícia em crimes cibernéticos. O restante deles variava entre menos de um ano a cinco anos de experiência. Todos os respondentes, exceto três, já atuaram diretamente em suporte a procuradores da área criminal ou de investigações cibernéticas.

Quanto à existência de limitações técnicas que dificultam o trabalho pericial, as respostas foram praticamente unânimes, conforme Figura 4, elaborada a partir das respostas aos questionários:

Figura 4 – Respostas ao questionário: Questão 6



Fonte: extraído do Google Forms a partir das respostas ao questionário.

- As principais limitações técnicas apontadas pelos respondentes foram:
- *Infraestrutura e equipamentos:* falta de infraestrutura tecnológica adequada, tais como estações de trabalho de alta capacidade e equipamentos mais robustos. A centralização de recursos na STIC (Secretaria de Tecnologia da Informação e Comunicação), inclusive, foi mencionada como um possível obstáculo por um dos respondentes.
 - *Recursos humanos e treinamento:* a escassez de pessoal especializado, a falta de capacitação contínua e a necessidade de mais treinamento no uso de ferramentas periciais são recorrentes nas respostas. A atualização profissional, muitas vezes, é feita por conta própria.

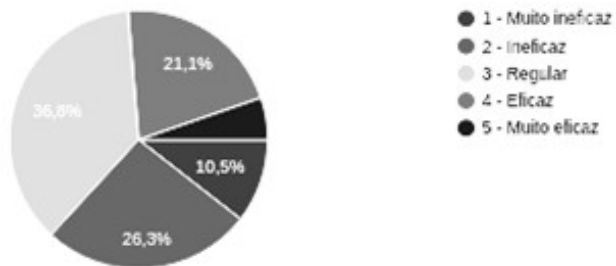
→ *Ferramentas e licenças*: os profissionais respondentes relataram a falta de opções de software, alto custo e escassez de licenças, além da restrição de uso de softwares não autorizados pela STIC.

Ao serem questionados sobre a qualidade de comunicação entre as equipes de TI e os procuradores, a maioria dos respondentes informou que ela seria “ineficaz” ou “regular”, conforme Figura 5, elaborada a partir dos dados obtidos dos questionários:

Figura 5 – Respostas ao questionário: Questão 8

Como você avalia a comunicação entre a equipe de TI e os Procuradores durante investigações?

19 respostas



Fonte: extraído do Google Forms a partir das respostas ao questionário.

Nas demais respostas, os respondentes apontaram que, embora muitos procuradores compreendam parcialmente os limites da perícia, a falta de conhecimento tecnológico e a dificuldade em entender o esforço, o tempo e a qualidade dos dados recuperados são desafios significativos. Alguns respondentes mencionaram a dificuldade em explicar conceitos como cadeia de custódia e *timestamps* de publicações.

Quanto à capacitação, os respondentes apontaram diversas certificações e cursos que seriam prioritários para formação na área, a exemplo das certificações do SANS Institute. Numa das respostas, apontou-se que poucas capacitações fornecidas institucionalmente alcançam os peritos eventuais de TI, e que a atualização seria por conta própria.

Em relação aos desafios legais, as limitações na obtenção de evidências digitais são consideradas “ocasionalmente” ou “frequentemente”

um problema. A obtenção de informações de provedores estrangeiros é um desafio apontado por diversos profissionais, assim como a falta de adaptação da legislação sobre o tema.

Ao serem questionados sobre eventuais problemas advindos da cooperação com provedores e plataformas estrangeiras, a maioria dos participantes afirmou ter sofrido atraso na perícia em decorrência de deficiências na cooperação, enquanto para outra parte não houve esse problema.

Ao serem questionados quanto a sugestões de melhoria no combate aos crimes cibernéticos, vários servidores apontaram a necessidade de uma atuação conjunta e mais próxima entre os servidores de TIC e os órgãos criminais.

Como exemplo de boa prática, apontou-se, dentre outras, a existência do núcleo técnico especializado em crimes cibernéticos existente no MPSP, mencionando-se a necessidade de uma maior cooperação entre as equipes.

4.5 Conexões entre as respostas do questionário e as pesquisas exploratórias

As respostas aos questionários, embora representem as percepções subjetivas dos profissionais em TIC, corroboram e aprofundam algumas das conclusões obtidas a partir das pesquisas exploratórias.

A percepção de que a infraestrutura tecnológica é “pouco adequada” ou “totalmente inadequada” e de que há uma “falta de recursos” e “limitações técnicas” se alinha precisamente com o fato de que os gastos e investimentos em tecnologia da informação, em comparação ao orçamento total da instituição, permanecem estagnados desde 2019. Essa falta de investimento se reflete de modo direto na escassez de softwares, licenças e equipamentos de alta capacidade.

Além disso, a carência de pessoal especializado e a necessidade de mais treinamento se conectam com a diminuição ou constância do número de servidores desde 2019. A falta de recursos humanos e de capacitação institucional leva os profissionais a buscarem atualização por conta própria, o que pode gerar inconsistências e falta de padronização nas técnicas e ferramentas utilizadas, um desafio explicitamente mencionado.

A percepção de que a comunicação entre procuradores e equipes técnicas é ineficaz, e a dificuldade dos membros em compreender os limites da perícia, reforçam a observação exploratória de que existem poucos núcleos especializados regionalizados. A ausência desses núcleos impede a criação de um “trabalho conjunto” e de uma “atuação próxima” que, segundo um dos respondentes, é crucial para alinhar as expectativas e eliminar as dificuldades de comunicação.

A sugestão de criar núcleos periciais de TI regionalizados e a referência a um setor especializado já existente em São Paulo e recém-criado no Rio de Janeiro, que integra profissionais de direito e TI, evidenciam que a solução para as dificuldades de comunicação, falta de recursos e carência de pessoal especializado pode estar na criação de estruturas dedicadas que contemplem profissionais do direito e de TI.

5 Conclusão

Diante do crescimento exponencial da criminalidade digital e da complexidade técnica envolvida em sua investigação, o presente artigo buscou analisar a capacidade técnica e operacional do MPF no enfrentamento aos crimes cibernéticos, com ênfase na atuação de suas unidades de apoio em TIC. A pesquisa parte do reconhecimento de que o avanço tecnológico exige das instituições estatais respostas cada vez mais especializadas, rápidas e coordenadas, principalmente quando se trata da persecução penal em ambiente virtual.

A problemática central que norteia esta investigação – relativa à suficiência da estrutura e capacitação técnica do MPF para enfrentar os desafios impostos pelos cibercrimes – revelou-se relevante e atual. Ao estabelecer como objetivo principal o mapeamento da estrutura organizacional e dos recursos humanos e tecnológicos disponíveis, além da análise da integração com órgãos nacionais e internacionais, o estudo forneceu um diagnóstico institucional parcial que vai além das percepções subjetivas. Por meio de uma abordagem mista, foram produzidos dados empíricos que podem fundamentar propostas de aprimoramento da atuação ministerial.

Como contribuição principal, o estudo pode subsidiar a formulação de políticas públicas internas voltadas à modernização tecnológica do

MPF, à capacitação contínua de seus servidores e ao fortalecimento da cooperação interinstitucional. Em razão de limitações decorrentes da falta de fontes de pesquisa confiáveis, não foi possível atingir com perfeição todos os objetivos pretendidos, tais como o exame da cooperação técnica e o mapeamento estrutural. Apesar disso, espera-se que os resultados obtidos sirvam não apenas como insumo para decisões administrativas, mas também como ponto de partida para futuros estudos acadêmicos e institucionais, contribuindo para uma atuação ministerial mais eficaz diante da crescente sofisticação dos delitos praticados no ciberespaço.

Este artigo não é suficiente para responder várias questões fundamentais sobre o tema, tais como: Está a instituição devidamente estruturada, do ponto de vista tecnológico e de recursos humanos, para atuar nesse campo? Qual a atual estrutura e a capacidade da equipe em tecnologia da informação e comunicação responsável pelo enfrentamento dos crimes cibernéticos no Ministério Público Federal? Quantas unidades especializadas foram criadas no âmbito do MPF? Qual o volume de recursos destinados ao combate à cibercriminalidade? Quantas denúncias foram apresentadas e quantas resultaram em condenações no âmbito da Justiça Federal?

Outra possível lacuna que poderia ser objeto de estudos futuros é a análise de decisões judiciais recentes para avaliar o grau de compreensão dos magistrados sobre provas digitais e possíveis padrões de rejeição ou aceitação com base em falhas técnicas, subsidiando a capacitação contínua de operadores do Direito e profissionais em TIC, reduzindo riscos de impunidade por deficiência probatória.

São muitas as questões a serem respondidas, não servindo o presente artigo à obtenção de resposta a todas elas, tendo, porém, a virtude de destacar a importância de estudos para respondê-las e lograr, a partir daí, planejar uma ação ordenada e mais efetiva no combate à nova criminalidade.

Referências

ALEXANDROU, Alex. **Cybercrime and information technology**: theory and practice – the computer network infrastructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices. Boca Raton: CRC Press, 2022.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**: seção 1, Brasília, DF, 13 abr. 2023. Disponível em: <https://tinyurl.com/2s4fr79e>. Acesso em: 11 maio 2025.

BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941. Institui o Código de Processo Penal. **Diário Oficial da União**, Rio de Janeiro, 3 out. 1941. Disponível em: <https://tinyurl.com/4nyywa3t>. Acesso em: 22 jun. 2025.

BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão; Secretaria de Cooperação Internacional. **Roteiro de atuação**: crimes cibernéticos e provas eletrônicas. 4. ed. atual. e ampl. Brasília: MPF, 2021a.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Relatório de atividades 2024**. Brasília: MPF, 2025a. Disponível em: <https://tinyurl.com/4t4p5w8k>. Acesso em: 10 ago. 2025.

BRASIL. Ministério Público Federal. Detalhamento de despesas. **Portal da Transparência do MPF**, Brasília, 2025b. Disponível em: <https://tinyurl.com/3crrxfm4>. Acesso em: 2 out. 2025.

BRASIL. Ministério Público Federal. MPF em Números. **Portal da Transparência do MPF**, Brasília, 2025c. Disponível em: <https://tinyurl.com/44ybx57e>. Acesso em: 2 out. 2025.

BRASIL. Ministério Público Federal. Portaria PGR/MPF n. 843, de 18 de outubro de 2024. Atualiza o Planejamento Estratégico do Ministério Público Federal para o período de 2024 a 2027. **Diário do Ministério Público Federal Eletrônico**, Brasília, Caderno Administrativo, n. 208, p. 1, 30 out. 2024a. Disponível em: <https://tinyurl.com/wf5az9hf>. Acesso em: 15 out. 2025.

BRASIL. Ministério Público Federal. Portaria PRRJ n. 443, de 20 de maio de 2025. Dispõe sobre a criação do Núcleo Técnico de Combate aos Crimes Cibernéticos da Procuradoria da República no Estado do Rio de Janeiro. **Diário do Ministério Público Federal Eletrônico**, Brasília, Caderno Administrativo, p. 40, 25 maio 2025e. Disponível em: <https://tinyurl.com/eyxc2t59>. Acesso em: 22 jun. 2025.

BRASIL. Ministério Público Federal. Resolução CSMPPF n. 229, de 2 de abril de 2024. Cria o Grupo de Atuação Especial no Combate aos Crimes Cibernéticos e aos Crimes praticados mediante o Uso de Tecnologias da Informação no âmbito do Ministério Público Federal e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, 19 abr. 2024b. Disponível em: <https://tinyurl.com/ybhyejeh>. Acesso em: 18 mar. 2026.

BRASIL. Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise. **Catálogo nacional de serviços**: perícia, pesquisa e análise. Brasília: MPF, 2021b. Disponível em: <https://tinyurl.com/bdhk6y3u>. Acesso em: 22 jun. 2025.

CNMP – CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Resolução n. 294, de 28 de maio de 2024. Institui a Política Nacional de Cibersegurança do Ministério Público (PNCiber-MP) e dá outras providências. **Diário Eletrônico do CNMP**, Brasília, Caderno Processual, 3 jul. 2024. Disponível em: <https://tinyurl.com/4dkbtzze>. Acesso em: 20 jun. 2025.

CONSELHO DA EUROPA. Action against cybercrime. **Portal do Conselho da Europa**, Estrasburgo, [2025?]. Disponível em: <https://tinyurl.com/yjn8t98x>. Acesso em: 23 jun. 2025.

CONSELHO DA EUROPA. Relatório explicativo: Cibercrime (Segundo Protocolo Adicional). (STCE n. 224). **Portal do Conselho da Europa**, Estrasburgo, 2022. Disponível em: <https://tinyurl.com/zvh3t8tw>. Acesso em: 23 jun. 2025.

CORRÊA, Isadora Donza; MONTEIRO NETO, João Araújo. A adesão à Convenção de Budapeste e o enfrentamento do cibercrime: entre a cooperação internacional e a expansão do direito penal. **Revista Eletrônica Direito & TI**, Fortaleza, v. 1, n. 16, p. 32-60, 2023. DOI: <https://doi.org/10.63451/ti.v1i16.155>. Acesso em: 20 jun. 2025.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na internet. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018. v. 3. (Coletânea de artigos). p. 26-50.

INFORMÁTICA. In: **Etimologia**: origem do conceito. [S. l.], [20--?]. Disponível em: <https://tinyurl.com/2757a854>. Acesso em: 18 jun. 2025.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

MOLONEY, Christopher J. **Exploring the cybercrime capacity and capability of local law enforcement agencies in the United States**. 2021. Dissertation (Ph.D.) – Colorado State University, Colorado, 2021. Disponível em: <https://tinyurl.com/3nx9a7up>. Acesso em: 22 jun. 2025.

MPSP – MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. **Detalhamento das despesas**. São Paulo: MPSP, 2025. Disponível em: <https://tinyurl.com/7rba4shx>. Acesso em: 2 out. 2025.

NAKAMURA, João. País tem 700 milhões de ataques virtuais em um ano, diz relatório. **CNN Brasil**, São Paulo, 18 nov. 2025. Disponível em: <https://tinyurl.com/ytn2d76e>. Acesso em: 7 dez. 2025.

SYDOW, Spencer Toth. **Curso de direito penal informático**: partes geral e especial. 2. ed. rev. e atual. Salvador: Juspodivm, 2021.

SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado) – Universidade de São Paulo, São Paulo, 2009. DOI: <https://doi.org/10.11606/D.2.2009.tde-15062011-161113>. Acesso em: 18 set. 2025.

VERIZON. **2024 Data Breach Investigations Report (DBIR)**. [S. l.]: Verizon, 2024. Disponível em: <https://tinyurl.com/4bx3rar4>. Acesso em: 10 ago. 2025.

Produção

Escola Superior do Ministério Público da União

Tipografia

Meridien LT Std e Myriad Pro

Recursos gráficos

Adobe Stock™

