DESAFIOS PERCEBIDOS NA IMPLEMENTAÇÃO DAS MEDIDAS DO PPSI

Marília Tolentino da Silva
E-mail: 242200163@aluno.unb.br

RESUMO

Este artigo investiga os desafios enfrentados pelos órgãos da Administração Pública Federal (APF) na implementação das medidas de cibersegurança do Grupo de Implementação 1 do Programa de Privacidade e Segurança da Informação (PPSI). A pesquisa, de natureza qualitativa e delineamento exploratório-descritivo, utilizou questionários e entrevistas para captar percepções de profissionais sobre recursos humanos, no tempo necessário para execução e complexidade das ações propostas. Os resultados revelam que há deficiências de pessoal qualificado, o tempo elevado para execução e a falta de padronização institucional, obstáculos específicos para a efetividade do programa. Conclui-se que o fortalecimento da maturidade institucional e o alinhamento de recursos humanos, tecnológicos e processuais são essenciais para o sucesso das iniciativas de segurança da informação na administração pública.

Palavras-chave: Programa de Privacidade e Segurança da Informação; Segurança da Informação; Implementação PPSI.

ABSTRACT

This article investigates the challenges faced by agencies of the Federal Public Administration (FPA) in implementing the cybersecurity measures of Implementation Group 1 of the Privacy and Information Security Program (PISP). The research, qualitative in nature with an exploratory-descriptive design, used questionnaires and interviews to capture professionals' perceptions regarding human resources, the time required for execution, and the complexity of the proposed actions. The results reveal deficiencies in qualified personnel, lengthy execution times, and a lack of institutional standardization as specific obstacles to the program’s effectiveness. It is concluded that strengthening institutional maturity and aligning human, technological, and process resources are essential for the success of information security initiatives in public administration.
Keywords: Privacy and Information Security Program; Information Security; PISP Implementation.

1. INTRODUÇÃO

A transformação digital e o avanço das ameaças cibernéticas impõem à Administração Pública Federal (APF) desafios crescentes que não dizem respeito à proteção de dados e à segurança da informação. No Brasil, esse cenário motivou a criação de instrumentos normativos como a Estratégia Nacional de Segurança Cibernética (E-Ciber) e a Política Nacional de Segurança da Informação (PNSI), que estabelecem diretrizes fundamentais para garantir a continuidade dos serviços públicos e proteger de dados.

Apesar dos avanços regulatórios, a atualização na segurança da informação ainda permanece limitada em diversos órgãos da APF. O Relatório de 2022 do Tribunal de Contas da União (TCU) evidenciou que a maioria desses órgãos apresenta vulnerabilidades em cibersegurança (TCU, 2022 apud CERQUEIRA; BRUNO, 2024).

Nesse contexto de fragilidades identificadas, destaca-se o papel do Framework do Programa de Privacidade e Segurança da Informação (PPSI), que enfatiza a importância de diagnosticar o grau de implementação dos controles, sensibilizar continuamente as estruturas de governança e monitorar o cumprimento dos planos de trabalho pactuados (BRASIL, MGI, 2023). Embora o PPSI proponha diretrizes e mecanismos orientadores ao fortalecimento institucional, a efetividade dessas medidas ainda encontra diversos entraves práticos que precisam ser compreendidos à luz da realidade dos órgãos públicos.

Além disso, percebe-se uma escassez de estudos empíricos que exploram, na prática, como esses desafios se apresentam no cotidiano dos órgãos públicos, especialmente no contexto das medidas iniciais previstas para o Grupo de Implementação 1 (GI1) do PPSI. Esse grupo abrange controles essenciais e obrigatórios, voltados principalmente para órgãos com menor atualização tecnológica e estrutura reduzida, formando a base comum de requisitos para toda a Administração Pública Federal.

Diante desse panorama, torna-se fundamental estabelecer propósitos claros que orientam a análise dos desafios vivenciados pela Administração Pública Federal, permitindo compreender os fatores que influenciam o sucesso das iniciativas de segurança da informação. Partindo desse entendimento, este estudo identifica e análisa as percepções dos profissionais envolvidos na implementação das medidas do PPSI, contribuindo, assim, para o aprimoramento das políticas públicas de segurança da informação.

2. REFERENCIAL TEÓRICO

2.1. Segurança da Informação no Setor Público

O conceito de segurança da informação (SI) abrange o conjunto de medidas destinadas à proteção dos ativos informacionais contra acesso, uso, divulgação, alteração, destruição, perda ou dano não autorizados, sejam estes de natureza acidental ou maliciosa. O objetivo central reside na garantia dos princípios fundamentais de confidencialidade, integridade e disponibilidade da informação, elementos essenciais para a preservação de dados sensíveis e para assegurar a continuidade dos serviços oferecidos no âmbito da administração pública (BRASIL, GSI, 2023).

No contexto brasileiro, a segurança da informação, com foco especial na segurança cibernética, está respaldada por um conjunto robusto de normativos, entre eles: Decreto nº 10.222/2020, que institui a Estratégia Nacional de Segurança Cibernética (E-Ciber); Decreto nº 10.748/2021, que estabelece a Rede Federal de Gestão de Incidentes Cibernéticos; Portaria GSI/PR nº 93/2021, que aprova o Glossário de segurança da informação e Decreto nº 9.637/2018, que define a Política Nacional de Segurança da Informação (PNSI).

Adicionalmente, existem as diretrizes do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), tais como a Instrução Normativa GSI/PR no 1, de 27 de maio de 2020, que estabelece a Estrutura de Gestão da segurança da informação e a Instrução Normativa GSI/PR no 5, de 31 de agosto de 2021, que estabelece os padrões mínimos de segurança da informação para o uso de soluções de computação em nuvem nos órgãos e entidades da APF.

Além disso, estudos recentes enfatizam a complexidade da segurança cibernética no setor público, destacando desafios como infraestrutura tecnológica defasada, ausência de coordenação centralizada e lacunas de governança (Georg et al., 2022). A literatura também salienta a importância da cultura organizacional, capacitação adequada dos servidores e a necessidade de adaptação das políticas diante das rápidas transformações digitais e das crescentes ameaças cibernéticas (Veiga et al., 2020; Costa et al., 2019; Shapira et al., 2021).

Importante como referência adicional, ressalta-se que a adoção efetiva da segurança da informação no setor público requer a superação de entraves institucionais relacionados a recursos humanos, tecnológicos e burocráticos, tal como apontado em recentes análises de caso

no âmbito da Administração Pública Federal (Cerqueira & Bruno, 2024). Essa visão reforça a necessidade de ações integradas e consolidadas para fortalecer a segurança institucional.

Diante dessa realidade e da necessidade de auxiliar as entidades públicas na implementação de práticas adequadas, foi criado no âmbito do governo federal um programa que fornece orientações para a aplicação de controles de segurança da informação e privacidade, em conformidade tanto com as normas legais quanto com os padrões internacionais, buscando aprimorar a governança e a proteção dos dados públicos.

2.2. O Programa de Privacidade e Segurança da Informação (PPSI)

O Programa de Privacidade e Segurança da Informação (PPSI) constitui uma estratégia governamental voltada ao fortalecimento da governança e da proteção informacional no setor público. Sua finalidade primordial consiste em orientar os órgãos públicos na adoção de práticas que assegurem não apenas a segurança das informações, mas também a observância das legislações pertinentes à privacidade e à proteção de dados pessoais (BRASIL, MGI, 2023).

Além disso, essa iniciativa representa uma resposta estruturada às necessidades das organizações públicas frente às crescentes ameaças à segurança cibernética, perdas de dados e incidentes de segurança. Simultaneamente, busca garantir a conformidade com marcos legais fundamentais, tais como a Lei Geral de Proteção de Dados (LGPD) e a própria Política Nacional de Segurança da Informação (PNSI) (BRASIL, 2018b).

Nesse contexto, o PPSI foi concebido como um instrumento central para orientar a atuação dos órgãos públicos. Desenvolvido pela Secretaria de Governo Digital (SGD) do MGI, tem por objetivo fornecer diretrizes para ajudar a identificar, abordar e mitigar lacunas relacionadas à privacidade e à segurança da informação. Seu desenvolvimento é baseado nos requisitos estabelecidos pela PNSI e pela LGPD, além da implementação de controles internacionais reconhecidos, como os do Center for Internet Security (CIS Controls v8), do National Institute of Standards and Technology (NIST), das normas da ISO/IEC e da Associação Brasileira de Normas Técnicas (ABNT) (BRASIL, MGI, 2023).

Adicionalmente, a estrutura do programa é dividida em três grandes grupos de medidas: Controle 0: estabelece os fundamentos da gestão, incluindo governança, papéis e responsabilidades, planejamento e recursos; Controles de Cibersegurança (1 a 18): alinhados às funções do NIST Cybersecurity Framework: Identificar, Proteger, Detectar, Responder e

Recuperar (NIST, 2018); e Controles de Privacidade (19 a 31): voltados à proteção dos dados pessoais no ambiente organizacional (BRASIL, MGI, 2023).

Logo, para tornar sua implementação mais acessível, levando em consideração as diversas realidades das organizações públicas, o PPSI adota uma abordagem escalonada, composta por três grupos de implementação: GI1, GI2 e GI3. O GI1 reúne as medidas essenciais e prioritárias, sendo voltado para instituições com estrutura tecnológica mais simples ou menor capacidade técnica, além de ser a base obrigatória para todos os órgãos, independentemente de porte ou complexidade (BRASIL, MGI, 2023).

Além dessa estrutura gradativa, o PPSI incorpora uma metodologia de monitoramento que, para além dos controles propostos, inclui a atuação do Sistema de Controle Interno (SCI) e a realização de dois ciclos de atividades complementares, um interno e outro externo. Contempla ainda processos contínuos para avaliar a maturidade organizacional e manter o nível adequado de proteção dos sistemas em relação à segurança da informação e privacidade (BRASIL, MGI, 2023).

Nesse contexto, torna-se ainda mais evidente a necessidade premente de identificar e analisar, de forma aprofundada, os principais obstáculos enfrentados na implementação das medidas do GI1, especialmente considerando a elevada complexidade técnica de certas ações, a escassez de recursos humanos especializados e as distintas etapas de maturidade institucional presentes entre os órgãos públicos.

2.3. Implementação das Medidas do PPSI

A implementação das medidas do PPSI representa um esforço institucional que vai além da execução técnica de tarefas, mesmo em sua fase inicial, o processo demanda tempo, coordenação e alocação de pessoal especializado (BRASIL, MGI, 2023). Assim, diversas medidas exigem não apenas o domínio de ferramentas e processos, mas também a mobilização de equipes interdisciplinares, envolvimento da alta gestão e articulação entre diferentes áreas.

Além da atuação técnica, a implementação envolve ações como elaboração de normativos internos, capacitação de servidores, definição de papéis e responsabilidades, entre outras iniciativas que requerem clareza institucional e estabilidade organizacional. Dessa forma, adotar o PPSI não se resume à aplicação de controles, mas sim à incorporação de uma cultura institucional voltada à segurança e à privacidade da informação.

Conforme destaca Ximenes (2018), a implementação de políticas públicas é um processo que exige articulação entre diferentes níveis decisórios, adaptação aos contextos locais e constante diálogo entre formulação, execução e avaliação, sendo a capacidade institucional um fator determinante para o sucesso das políticas. No caso do PPSI, isso significa que sua adoção não se resume à aplicação mecânica de controles, mas à incorporação de uma cultura organizacional voltada à segurança e à privacidade da informação.

Portanto, essa multiplicidade de fatores torna a implementação das medidas um desafio que vai além da capacidade operacional do campo de tecnologia da informação. Trata-se de um processo que depende fortemente do comprometimento institucional, da cooperação de vários setores e da superação de barreiras estruturais, culturais e de recursos.

3. METODOLOGIA

Este estudo caracteriza-se como uma pesquisa de natureza aplicada, com abordagem qualitativa, de caráter exploratório e descritivo, cujo objetivo é compreender os desafios enfrentados por profissionais da APF na implementação das medidas de cibersegurança do Grupo de Implementação 01 (GI1) do Framework do PPSI.

A pesquisa aplicada busca gerar conhecimento para a solução de problemas práticos em contextos institucionais, fornecendo subsídios à administração pública (GIL, 2017). Uma abordagem qualitativa foi escolhida para permitir uma análise mais aprofundada das percepções, experiências e interpretações dos interessados envolvidos, proporcionando compreensão das complexidades e nuances das reflexões estudadas (MINAYO, 2001; YIN, 2016).

O percurso metodológico incluiu inicialmente o levantamento documental, com revisão de literatura técnica, análise de documentos oficiais e estudos acadêmicos sobre avaliação e implementação de políticas de segurança da informação. Essa etapa serviu de base para a elaboração dos instrumentos de coleta de dados. Em seguida, foram aplicados questionários semiestruturados a profissionais diretamente envolvidos na implementação do GI1 nos órgãos federais, focando tempo de execução, demanda de recursos humanos e complexidade das ações. Além disso, realizou-se uma entrevista em profundidade com um profissional da área, ampliando e validando as informações coletadas nos questionários, e permitindo uma análise qualitativa ainda mais detalhada sobre os desafios e estratégias vivenciadas na prática.

A análise dos dados foi conduzida segundo a técnica de análise de conteúdo, conforme Bardin (2016), permitindo identificar categorias temáticas, padrões de resposta e diferenças de percepção entre os participantes. A seleção dos entrevistados foi intencional, incluindo apenas aqueles diretamente envolvidos nas ações propostas, seguindo recomendações para pesquisas qualitativas (GIL, 2017). O estudo respeitou os princípios éticos científicos, garantindo anonimato e confidencialidade, em conformidade com a Resolução CNS nº 510/2016.

No contexto delineado, a análise dos dados permitiu identificar não apenas os principais obstáculos enfrentados pelos órgãos da APF, mas também nuances relativas às percepções de esforço, maturidade institucional e práticas impostas na implementação das medidas de cibersegurança do GI1.

3.1. Delimitação e Registro da Pesquisa

A pesquisa tem como foco exclusivamente nas medidas de cibersegurança do GI1, que, segundo o Framework do PPSI (BRASIL, MGI, 2023), são aquelas voltadas a organizações com estrutura de TI reduzida ou com menor maturidade em segurança, mas fundamentais para qualquer instituição pública.

Inicialmente, foram mapeadas 55 medidas de cibersegurança atribuídas ao GI1. Entretanto, foi adotado como critério metodológico a exclusão de medidas com alto potencial de automação tecnológica. Assim foram priorizadas aquelas demandas que exigem participação humana direta, particularmente aquelas relacionadas a: Elaboração de políticas e processos; Definição de papéis e responsabilidades; Capacitação de pessoas; e Governança, compliance e aspectos éticos ou legais.

Após esse filtro, selecionaram-se dez medidas com maior dependência de esforço humano e articulação institucional:

1. Medida 3.1: O órgão estabelece e mantém um processo de gestão de dados?
2. Medida 3.2: O órgão estabelece e mantém um inventário de dados?
3. Medida 4.1: O órgão estabelece e mantém um processo de configuração segura?
4. Medida 6.2: O órgão estabelece um Processo de Revogação de Acesso?
5. Medida 14.1: O órgão implanta e mantém um programa de conscientização de segurança?
6. Medida 14.2: O órgão treina colaboradores para reconhecer ataques de engenharia social?

7. Medida 14.4: O órgão treina os colaboradores nas Melhores Práticas de Tratamento de Dados?

8. Medida 14.5: O órgão treina os colaboradores sobre as causas da exposição não intencional de dados?

9. Medida 14.6: O órgão treina os colaboradores sobre como Reconhecer e Relatar incidentes de Segurança?

10. Medida 17.3: O órgão estabelece e mantém um processo institucional para relatar incidentes?

Cabe destacar que as medidas do controle de privacidade do PPSI não foram objeto deste estudo porque sua análise exigiria uma metodologia diferente, mais apropriada aos procedimentos específicos de proteção de dados pessoais e privacidade, que extrapolam os objetivos deste trabalho.

3.2. Estratégia e Procedimentos de Coleta de Dados

A pesquisa foi conduzida em duas principais ferramentas metodológicas: pesquisa de campo com perguntas estruturadas e entrevistas com perguntas abertas aplicadas a profissionais diretamente envolvidos na implementação das medidas do PPSI.

3.2.1. Pesquisa de Campo

Foram aplicados questionários eletrônicos, via Google Forms, compostos por perguntas fechadas e uma questão aberta ao final, para dois grupos diferentes. O primeiro foi direcionado a servidores do Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (MDS), atuantes nas áreas de segurança da informação.

O segundo, de abrangência externa, foi aplicado a servidores de diferentes órgãos da Administração Pública Federal, incluindo profissionais do serviço pública e alunos do curso de Pós-Graduação Lato Sensu em Privacidade e Segurança da Informação da Universidade de Brasília (UnB).

Ambos os formulários abordaram três dimensões principais:

- Pessoas: quantitativo de profissionais necessário para implementar cada medida;
- Tempo: esforço estimado, em dias, para a execução de cada medida; e

- Complexidade: percepção do grau de dificuldade, classificado em três níveis: baixo (realizável com recursos disponíveis), médio (exige adaptações) e alto (demanda investimentos significativos, reestruturação ou contratação de pessoal).

Adicionalmente, incluiu-se uma pergunta aberta ao final dos questionários, visando captar sugestões e comentários dos participantes sobre o instrumento aplicado e as percepções gerais sobre o tema.

3.2.2. Entrevista

Complementando a pesquisa quantitativa, realizou-se uma entrevista estruturada com perguntas abertas, aplicada à Coordenadora de Planejamento e responsável pela segurança da informação no MDS, profissional diretamente envolvida na implementação do PPSI no âmbito ministerial.

A entrevista abordou quatro eixos temáticos principais: as percepções sobre a não padronização das respostas obtidas na pesquisa de campo; os desafios enfrentados na implementação das medidas de cibersegurança; as sugestões de melhorias nos processos de comunicação, capacitação e acompanhamento; e, por fim, as reflexões sobre possíveis aprimoramentos no próprio framework do PPSI.

Cabe destacar que não foi possível realizar a entrevista externa com representantes da Secretaria de Governo Digital (SGD) do MGI, responsável pela elaboração e coordenação do PPSI, devido à indisponibilidade institucional no período de coleta dos dados.

3.3. Técnica de Análise dos Dados

A análise dos dados foi realizada por meio da técnica de análise de conteúdo, conforme sistematizado por Farago e Fofonca (2025), que discutem as etapas de organização do material, codificação, categorização das informações e interpretação dos resultados, bem como as potencialidades e limitações desse método para pesquisas qualitativas em educação, aspectos que se aplicam também ao campo da administração pública.

Essa abordagem possibilita identificar padrões, regularidades e nuances presentes nas respostas dos participantes, ao mesmo tempo em que exige atenção às limitações e desafios inerentes ao método (FARAGO; FOFONCA, 2025).

Para fortalecer a validade e abrangência da análise, adotou-se a triangulação metodológica, entendida como a combinação de diferentes métodos, fontes de dados e perspectivas teóricas

para ampliar a compreensão do fenômeno estudado e conferir maior rigor científico à pesquisa qualitativa (ZAPPELLINI; FEUERSCHÜTTE, 2015). A triangulação, conforme discutido por Flick (2013) e Denzin (1989), contribui para a ampliação da qualidade, da confiabilidade e da profundidade dos resultados, ao permitir a análise do objeto sob múltiplos enfoques (ZAPPELLINI; FEUERSCHÜTTE, 2015).

No presente estudo, essa abordagem contribuiu para ampliar a consistência dos resultados e oferecer uma leitura mais integrada dos desafios enfrentados na implementação das medidas do PPSI, considerando diferentes perspectivas institucionais.

4. RESULTADOS

A pesquisa de campo foi conduzida para mensurar a percepção de servidores públicos sobre o esforço e a complexidade na implementação de controles de segurança. Ao todo, participaram do estudo 23 respondentes, sendo 7 servidores do MDS e 16 servidores de diferentes órgãos da APF. A análise dos dados quantitativos e qualitativos revela uma notável heterogeneidade nas respostas, indicando que a implementação de uma política uniforme enfrenta desafios que vão além da técnica, esbarrando em diferentes realidades institucionais.

4.1. Análise Técnica dos Resultados – MDS

A pesquisa realizada com servidores do MDS permitiu identificar padrões consistentes entre o esforço estimado para implementação das medidas do GI1 do PPSI e a percepção de sua complexidade.

As três medidas com maior tempo médio de execução foram gestão de dados, configuração segura e inventário de dados, com médias acima de 55 dias e necessidade superior a seis analistas, conforme mostrado na Tabela 1. Concomitantemente, essas ações também foram classificadas por uma parcela significativa dos respondentes como de alta complexidade, indicando uma forte relação entre esforço exigido e grau de dificuldade percebido.

TABELA 1 – Recursos humanos, tempo e complexidade percebida na implementação das medidas de cibersegurança do PPSI no MDS.

Medida	Analistas (média)	Tempo (dias)	Baixa (%)	Média (%)	Alta (%)
Gestão de Dados	6,2	67,8	15%	45%	40%
Inventário de Dados	6,5	55,4	20%	35%	45%
Configuração Segura	7,1	58,9	10%	50%	40%
Revogação de Acesso	2,8	8,6	40%	50%	10%
Programa de Conscientização	4,6	45,2	25%	55%	20%
Treinamento em Engenharia Social	4,3	27,4	30%	50%	20%
Melhores Práticas de Dados	4,1	32,7	35%	45%	20%
Exposições Não Intencionais	3,7	29,5	30%	50%	20%
Reconhecimento de Incidentes	4,5	36,2	25%	55%	20%
Relato de Incidentes	4,9	52,1	15%	50%	35%

Fonte: Elaborado pelo autor com base na pesquisa de campo (2025).

Por outro lado, a medida revogação de acesso apresentou os menores valores em todos os indicadores: tempo médio inferior a 10 dias, menos de três profissionais envolvidos e apenas 10% de percepção de alta complexidade. Essa diferença reforça a ideia de que tarefas operacionais e rotineiras, com processos já institucionalizados, tendem a ser percebidas como mais simples e menos exigentes.

Medidas intermediárias como melhores práticas de dados, reconhecimento de incidentes e treinamentos apresentam tempos médios entre 27 e 45 dias, com envolvimento de cerca de quatro analistas. A complexidade dessas ações foi predominantemente avaliada como média, revelando que o grau de padronização e a articulação necessária entre setores influenciam diretamente a percepção de dificuldade.

Os resultados indicam que, mesmo entre medidas consideradas prioritárias pelo framework, há grande variação no esforço estimado, reforçando a necessidade de um planejamento institucional sensível às especificidades de cada ação.

4.2. Análise Técnica dos Resultados – Administração Pública Federal

Em seguida, foi realizada a pesquisa com servidores de diversos órgãos da Administração Pública Federal (excluindo o MDS) que revelou uma tendência clara de percepção elevada quanto ao tempo necessário para implementar as medidas do GI1 do PPSI. Em praticamente todas as medidas avaliadas, o tempo médio estimado foi superior ao registrado na pesquisa do MDS, sugerindo maior complexidade operacional ou menor maturidade institucional dos respondentes.

Na Tabela 2, observa-se que as medidas “Gestão de Dados” e “Configuração Segura” concentram os maiores indicadores de esforço e complexidade, exigindo, em média, mais de 6,5 analistas e sendo classificadas como de alta complexidade por 71% dos participantes. O tempo estimado para implementação dessas medidas supera 60 dias, com destaque para “Gestão de Dados”, cuja média foi de 99,6 dias. Esses números reforçam que ações estruturantes exigem maior articulação institucional, planejamento e capacidade técnica especializada.

TABELA 2 – Esforço e complexidade percebida na implementação de medidas de cibersegurança (outros órgãos da APF)

Medida	Analistas (média)	Tempo (dias)	Baixa (%)	Média (%)	Alta (%)
Gestão de Dados	7,0	99,6	14%	14%	71%
Inventário de Dados	5,9	76,6	14%	42%	42%
Configuração Segura	6,7	62,7	14%	14%	71%
Revogação de Acesso	2,8	6,6	28%	71%	0%
Programa de Conscientização	4,7	55,1	14%	28%	57%
Treinamento em Engenharia Social	4,4	42,6	14%	42%	42%
Melhores Práticas de Dados	4,3	40,0	14%	57%	28%
Exposições Não Intencionais	4,1	44,5	14%	42%	42%

Reconhecimento de Incidentes	4,7	50,1	14%	42%	42%
Relato de Incidentes	4,6	65,7	28%	42%	28%

Fonte: Elaborado pelo autor com base na pesquisa de campo (2025).

Por outro lado, “Revogação de Acesso” foi novamente a medida com menor percepção de esforço, com tempo médio de apenas 6,6 dias e cerca de 2,8 analistas envolvidos, classificada como de baixa ou média complexidade por 100% dos respondentes. Esse resultado evidencia que rotinas operacionais bem consolidadas tendem a ser percebidas como mais simples, mesmo quando envolvem certa sensibilidade em termos de segurança.

As demais medidas apresentam padrão intermediário. “Programa de Conscientização”, “Reconhecimento de Incidentes” e “Treinamento em Engenharia Social”, por exemplo, registraram tempo médio entre 42 e 55 dias, com envolvimento de menos de cinco analistas. A complexidade percebida dessas ações foi majoritariamente média ou alta, indicando a necessidade de planejamento institucional, capacitação contínua e integração entre as áreas técnicas e de gestão para que possam ser implementadas de forma eficaz.

Esses dados indicam que, mesmo medidas com escopo aparentemente simples exigem preparação técnica e maturidade institucional para que possam ser implementadas com sucesso. O padrão observado na Tabela 2 ressalta a importância de estratégias personalizadas, apoio da alta gestão e investimentos consistentes em pessoal e tecnologia como pré-requisitos para viabilizar a adoção plena do PPSI nos órgãos da administração pública federal.

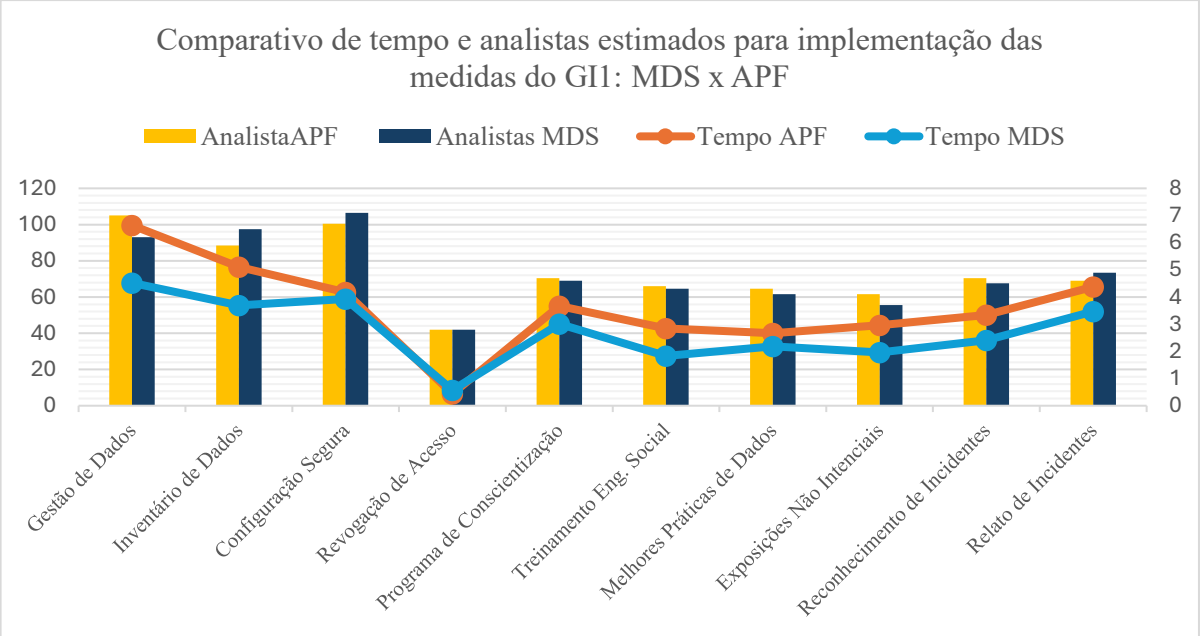
4.3. Comparativo entre os resultados do MDS e da Administração Pública Federal

A análise comparativa dos resultados entre o MDS e outros órgãos da Administração Pública Federal (APF) revela não apenas diferenças de médias, mas também padrões de dispersão e contraste na percepção de esforço, tempo e complexidade que aprofundam a compreensão dos desafios institucionais do PPSI.

Os dados do Gráfico 1 evidenciam que, para todas as medidas estratégicas, o tempo estimado para implementação é sistematicamente maior na APF do que no MDS, com destaque para “Gestão de Dados” e “Inventário de Dados”, onde a diferença ultrapassa 30 dias. No entanto, chama atenção o fato de que a diferença no número médio de analistas envolvidos é muito menor, variando entre 0,5 e 1 analista para a maioria das medidas. Isso sugere que,

embora o tamanho das equipes seja semelhante, a eficiência percebida ou a capacidade de execução é significativamente diferente entre os contextos.

GRÁFICO 1 – Comparativo de tempo e analistas estimados para implementação das medidas do GI1: MDS x APF



Fonte: Elaborado pelo autor com base na pesquisa de campo (2025).

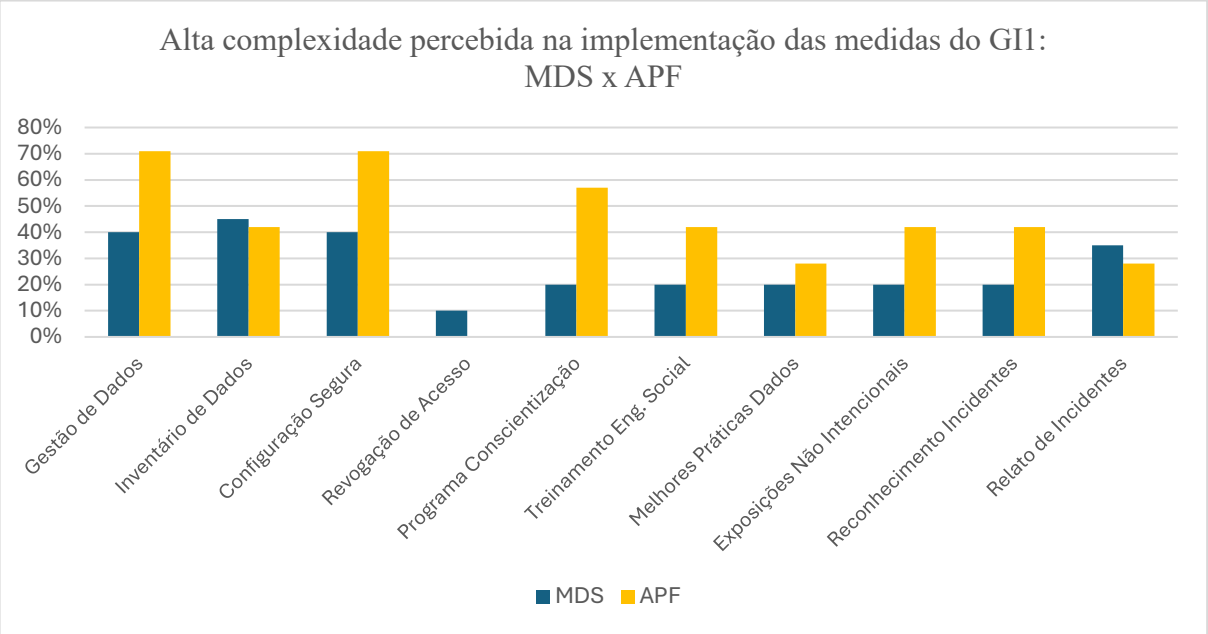
Outro ponto não abordado anteriormente é a estabilidade dos indicadores nas medidas operacionais. “Revogação de Acesso”, por exemplo, mantém valores baixos de tempo e analistas em ambos os grupos, mas na APF há uma predominância de avaliação como complexidade média (71%), enquanto no MDS predomina a avaliação de baixa complexidade (40%). Isso pode indicar que, mesmo em tarefas rotineiras, a percepção de dificuldade é impactada por fatores institucionais menos tangíveis, como burocracia, cultura organizacional ou falta de padronização de processos.

No grupo das medidas intermediárias, como “Programa de Conscientização”, “Treinamento em Engenharia Social” e “Reconhecimento de Incidentes”, observa-se que o tempo de implementação na APF é, em média, 20% a 30% maior do que no MDS, mesmo quando o número de analistas é praticamente idêntico. Esse padrão pode refletir gargalos de comunicação, menor experiência prévia ou dificuldades de coordenação intersetorial nos órgãos federais.

O Gráfico 2 traz um elemento novo à análise: a dispersão da percepção de alta complexidade. Enquanto no MDS a classificação de alta complexidade está concentrada nas

medidas mais estruturantes (até 45%), na APF há um espalhamento maior, com várias medidas intermediárias e até operacionais sendo consideradas altamente complexas por mais de 40% dos respondentes. Esse fenômeno sugere que, na APF, a sensação de desafio é mais difusa, atingindo até mesmo tarefas que, teoricamente, deveriam ser mais simples de implementar.

GRÁFICO 2 – Alta complexidade percebida na implementação das medidas do GI1: MDS x APF



Fonte: Elaborado pelo autor com base na pesquisa de campo (2025).

Além disso, a diferença entre os contextos é ainda mais acentuada em medidas como "Programa de Conscientização" e "Treinamento em Engenharia Social", que na APF são percebidas como altamente complexas por mais da metade dos servidores, enquanto no MDS essa percepção não ultrapassa 20%. Isso pode indicar que a cultura de segurança da informação e a maturidade dos processos de treinamento estão mais avançadas no MDS, refletindo em maior confiança dos servidores para executar tais atividades.

Outro aspecto inédito é a constatação de que, mesmo para medidas de menor escopo técnico, como "Exposições Não Intencionais" e "Reconhecimento de Incidentes", a APF apresenta índices elevados de alta complexidade (acima de 40%), enquanto no MDS esses índices permanecem abaixo de 20%. Isso reforça a hipótese de que fatores estruturais, como ausência de normatização, rotatividade de pessoal e falta de clareza nas atribuições, impactam diretamente a percepção dos desafios.

Por fim, a análise dos gráficos evidencia que a diferença mais marcante entre os contextos não está apenas nas médias, mas na amplitude da percepção de complexidade e no tempo de execução, que na APF são mais elevados e dispersos. Esses achados sugerem que políticas de cibersegurança precisam ser sensíveis não só à capacidade técnica, mas também à cultura organizacional e à maturidade institucional de cada órgão, sob pena de subestimar os desafios reais enfrentados na implementação do PPSI.

4.4. Entrevista com a responsável pela segurança da informação no MDS

Para complementar a análise dos dados, foi realizada uma entrevista com a responsável pela segurança da informação no MDS. O conteúdo da entrevista permitiu aprofundar a compreensão dos desafios institucionais enfrentados na implementação das medidas do PPSI.

Logo no início da conversa, a entrevistada destacou que a diversidade de percepções entre os servidores reflete o desnível tecnológico existente na APF. Segundo ela, órgãos como o Banco Central e a Receita Federal possuem maior estabilidade institucional, orçamentos contínuos e processos bem definidos, o que favorece a padronização e a execução de medidas estruturantes. Já os órgãos mais frágeis ou sujeitos a constantes mudanças políticas enfrentam maiores dificuldades para evoluir tecnicamente e manter ações permanentes.

Na sequência, ao ser questionada sobre a clareza das diretrizes do PPSI, a gestora apontou que o problema não está propriamente na comunicação do programa, mas sim na capacidade dos órgãos de manter ações estruturadas e contínuas. Em sua avaliação, há uma lacuna organizacional que compromete a consolidação de políticas como o PPSI. Por esse motivo, defende que o MGI deveria promover uma iniciativa nacional de reestruturação da governança de TI, com financiamento garantido no Orçamento Geral da União (OGU), por meio de uma dotação específica e não contingenciável.

Ao tratar dos principais desafios enfrentados, a entrevistada mencionou: escassez de recursos financeiros, carência de pessoal técnico qualificado, entraves burocráticos em processos de aquisição, resistência institucional a mudanças e falta de autonomia decisória das áreas técnicas. Como proposta, sugeriu a criação de um grupo técnico interministerial com autonomia para propor ações estratégicas, além da adoção de soluções baseadas em hiperautomação e da implementação de uma infraestrutura compartilhada em Nuvem de Governo, com acesso subsidiado para os órgãos menos estruturados.

Por fim, sobre possíveis melhorias no PPSI, a entrevistada propôs a definição de metas obrigatórias, com horizonte de dois anos, especialmente voltadas à reestruturação dos órgãos que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), ressaltando a importância de o programa reconhecer explicitamente as assimetrias institucionais entre os órgãos públicos e de estabelecer estratégias proporcionais à realidade de cada contexto.

5. CONCLUSÃO

O estudo cumpriu seus objetivos ao analisar os principais desafios percebidos pelos órgãos da APF na implementação das medidas do GI1 do PPSI. A pesquisa respondeu à questão central da proposta, mostrando claramente que obstáculos como deficiência de qualificação pessoal, elevado tempo de execução e alta complexidade das medidas estratégicas prejudicam significativamente o avanço do programa no setor público federal.

Além disso, ao comparar diferentes organizações, ficou evidente que a existência de instituições mais modernas e com processos bem padronizados facilita a implementação das medidas do GI1. Os dados demonstraram que ambientes organizacionais mais estruturados, conseguem alcançar melhores resultados na adoção dos controles. As sugestões dos participantes, especialmente em relação à capacitação contínua, adoção de políticas flexíveis e fortalecimento da governança, reforçam a importância do alinhamento entre pessoas, tecnologia e processos para a efetividade do PPSI.

Em relação aos limites do estudo, destaca-se a ausência de entrevistas com representantes da Secretaria de Governo Digital do MGI, o que restringe o entendimento da perspectiva do órgão responsável pela formulação do PPSI. Além disso, o foco em dados qualitativos, obtidos por meio de questionários e entrevistas, embora tenha permitido captar a experiência prática dos profissionais, dificulta a generalização total dos resultados para toda a APF.

De modo geral, o estudo contribui para mapear obstáculos e oportunidades para o aprimoramento da segurança da informação na administração pública federal. Recomenda-se, para pesquisas futuras, o aprofundamento dos controles de privacidade do PPSI e a análise dos impactos das políticas orçamentárias e dos modelos de governança na maturidade e efetividade das ações de segurança da informação nos órgãos públicos.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABDALLA, Maria de Fátima; OLIVEIRA, Maria Aparecida; AZEVEDO, Célia; GONÇALVES, Regina. Estratégia da triangulação. Atos de Pesquisa em Educação, Blumenau, v. 15, n. 4, p. 1150-1166, out./dez. 2020. Disponível em: https://dx.doi.org/10.7867/1809-0354.2020v15n4p1150-1166. Acesso em: 25 jun. 2025.

BARDIN, Laurence. Análise de conteúdo. São Paulo: Edições 70, 2016. Disponível em: https://portalseer.ufba.br/index.php/educacao/article/download/19171/12427 . Acesso em: 28 jul. 2025.

BRASIL. Conselho Nacional de Saúde. Resolução nº 510, de 7 de abril de 2016. Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais. Diário Oficial da União: seção 1, p. 44, 24 maio 2016. Disponível em: https://atticodigital.files.wordpress.com/2016/05/resolucao-cns-no-510-2016.pdf . Acesso em: 28 jul. 2025.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber). Diário Oficial da União: seção 1, Brasília, DF, 6 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm . Acesso em: 2 jun. 2025.

BRASIL. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Diário Oficial da União: seção 1, Brasília, DF, 19 jul. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm. Acesso em: 4 jun. 2025.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 2 jun. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Glossário de segurança da informação. Brasília, DF, 2023. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1. Acesso em: 5 jun. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 93, de 18 de outubro de 2021. Aprova o Glossário de Segurança da Informação. Diário Oficial da União: seção 1, Brasília, DF, 19 out. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370 . Acesso em: 1 jun. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação no âmbito da Administração Pública Federal. Brasília, DF. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN01_consolidada.pdf . Acesso em: 5 jun. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa nº 5, de 31 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem. Brasília, DF. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684 . Acesso em: 4 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 3 jun. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia do Framework de Privacidade e Segurança da Informação – PPSI. Brasília, DF, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados. Acesso em: 5 jun. 2025.

CERQUEIRA, Carlos Frederico Queiroz; BRUNO, Rafael do Nascimento. Política nacional de segurança da informação: análise e desafios para o setor público federal. Revista do Serviço Público, v. 1-24, 2024. Disponível em: https://revista.enap.gov.br/index.php/RSP . Acesso em: 28 jul. 2025.

COSTA, Francisco de Assis; CASTANHAR, José Cândido. Avaliação de políticas públicas: conceitos e experiências. Planejamento e Políticas Públicas, Brasília, n. 21, pág. 9-24, jul./dez.

2003. Disponível em: https://www.ipea.gov.br/ppp/index.php/PPP/article/view/345/276 . Acesso em: 28 jul. 2025.

COSTA, P.; MONTENEGRO, R.; PEREIRA, T.; PINTO, P. The Security Challenges Emerging from the Technological Developments: A Practical Case Study of Organizational Awareness to the Security Risks. Mobile Networks and Applications, v. 24, n. 6, p. 2032–2037, 2019. Disponível em: https://doi.org/10.1007/s11036-018-01208-0 . Acesso em: 29 ago. 2025.

FARAGO, Cátia Cilene; FOFONCA, Eduardo. Análise de conteúdo na perspectiva de Bardin: contribuições e limitações para a pesquisa qualitativa em educação. Educação em Revista, Belo Horizonte, v. 41, e49377, 2025. Disponível em: https://doi.org/10.35699/edur.v41i41.49377. Acesso em: 23 jun. 2025.

Georg, M. A. C.; Rodrigues, W. M. S.; Alves, C. A. M.; Silveira Júnior, A.; Nunes, R. R. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. Revista Ibérica de Sistemas e Tecnologias de Informação, n. E54, p. 602-616, 2022. Disponível em: https://www.risti.xyz/issues/ristie54.pdf . Acesso em: 29 ago. 2025.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2017. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4809681/mod_resource/content/1/Gil_Ant%C3%B4nio_Carlos_Metodos_Tecnicas_Pesquisa_Social.pdf . Acesso em: 28 jul. 2025.

HOEPMAN, Jaap-Henk. Privacy design strategies. IFIP International Information Security and Privacy Conference. Springer, 2014. p. 446–459. Disponível em: https://arxiv.org/abs/1210.6621. Acesso em: 23 jun. 2025.

MINAYO, Maria Cecília de Souza. O desafio do conhecimento: pesquisa qualitativa em saúde. 11. ed. São Paulo: Hucitec, 2001. Disponível em: https://www.arca.fiocruz.br/bitstream/icict/46500/2/Minayo_O_desafio_do_conhecimento.pdf . Acesso em: 30 jul. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for improving critical infrastructure cybersecurity. Version 1.1. Gaithersburg, MD, 2018. Disponível em: https://csrc.nist.gov/News/2016/Framework-for-Improving-Critical-Infrastructure-Cy . Acesso em: 2 jun. 2025.

SHAPIRA, N. et al. Cybersecurity in Water Sector: Stakeholders Perspective. Journal of Water Resources Planning and Management, 2021. Disponível em: https://doi.org/10.1061/(ASCE)WR.1943-5452.0001400 . Acesso em: 29 ago. 2025.

SILVA, João Marco; RIBEIRO, Diogo; RAMOS, Luis Felipe; et al. A worldwide overview on the information security posture of online public services. arXiv, 2 out. 2023. Disponível em: https://arxiv.org/abs/2310.01200. Acesso em: 25 jun. 2025.

VEIGA, A. da et al. Defining organisational information security culture-Perspectives from academia and industry. Computers & Security, v. 92, p. 101713, 2020. Disponível em: https://doi.org/10.1016/j.cose.2020.101713 . Acesso em: 29 ago. 2025.

XIMENES, Daniel de Aquino (org.). Implementação de políticas públicas: questões sistêmicas, federativas e intersetoriais. Brasília: Escola Nacional de Administração Pública (ENAP), 2018. Disponível em: https://repositorio.enap.gov.br/handle/1/3364. Acesso em: 4 jun. 2025.

YIN, Robert K. Pesquisa qualitativa do início ao fim. 2. ed. Porto Alegre: Penso, 2016. Disponível em: https://repositorio.bc.ufg.br/bitstream/ri/23304/2/Robert%20K.%20Yin%20-%20Pesquisa%20qualitativa%20do%20inicio%20ao%20fim.pdf . Acesso em: 30 jul. 2025.

ZAPPELLINI, Marcello Beckert; FEUERSCHÜTTE, Simone Ghisi. O uso da triangulação na pesquisa científica brasileira em Administração. Administração: Ensino e Pesquisa, Rio de Janeiro, v. 16, n. 2, p. 241–273, abr./jun. 2015. Disponível em: https://www.redalyc.org/pdf/5335/533556754005.pdf. Acesso em: 25 jun. 2025.