SEGURANÇA DA INFORMAÇÃO NO TRABALHO REMOTO PÚBLICO FEDERAL: VULNERABILIDADES E A APLICAÇÃO DO GUIA DO FRAMEWORK PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Rosemeire Soares de Sousa, Virginia de Melo Dantas Trinks

rosemeiresoares.sousa@gmail.com, virginia.trinks@presidencia.gov.br

Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - CEP 70910-900.

Abstract

The advancement of digital transformation and the consolidation of remote work in the Brazilian Federal Public Administration have introduced new vulnerabilities related to information security and the protection of government data. This article aims to analyze the effectiveness of the Privacy and Information Security Program (PPSI) as a strategic framework to ensure the integrity, confidentiality, and availability of informational assets in the context of remote work within the federal public sector. The study was conducted through bibliographic research with a qualitative approach, grounded in current legislation, official reports, normative guides, and specialized academic literature on information security, LGPD, and telework. The results demonstrate that the adoption of PPSI guidelines significantly strengthens institutional maturity, mitigates vulnerabilities, and ensures compliance with LGPD legal requirements. As the main contribution, the work highlights the PPSI as an essential tool for governance and digital protection, capable of supporting public policies and enhancing information security management in remote public service.

Keywords*: remote work, vulnerabilities, information security, PPSI*.

Resumo

O avanço da transformação digital e a consolidação do trabalho remoto na Administração Pública Federal introduziram novas vulnerabilidades relacionadas à segurança da informação e à proteção de dados governamentais. Este artigo tem como objetivo analisar a efetividade do Programa de Privacidade e Segurança da Informação (PPSI), enquanto framework estratégico para assegurar a integridade, confidencialidade e disponibilidade das informações no contexto do trabalho remoto público federal. O estudo foi conduzido por meio de pesquisa bibliográfica com abordagem qualitativa, fundamentada em legislações vigentes, relatórios oficiais, guias normativos e literatura acadêmica especializada sobre segurança da informação, LGPD e teletrabalho. Os resultados demonstram que a adoção das diretrizes do PPSI contribui significativamente para o fortalecimento da maturidade institucional, mitigação de vulnerabilidades e conformidade com as exigências legais da LGPD. Como principal contribuição, o trabalho evidencia o PPSI como instrumento essencial de governança e proteção digital, capaz de subsidiar políticas públicas e aprimorar a gestão da segurança da informação no serviço público remoto.

Palavras-chave: trabalho remoto, vulnerabilidades, segurança da informação, PPSI.

1 Introdução

A popularização do trabalho remoto, inicialmente adotado como medida emergencial durante a pandemia da COVID-19 e, atualmente, consolidado como modalidade permanente no setor público federal, promoveu transformações significativas na dinâmica organizacional, assim como trouxe desafios relacionados à segurança da informação (Lucas; Santos, 2021). Embora o teletrabalho tenha possibilitado ganhos em eficiência e maior flexibilidade na prestação dos serviços públicos, também expôs fragilidades históricas referentes à proteção dos dados governamentais e à gestão de riscos cibernéticos (Brasil, 2020).

Sob essa perspectiva, o uso crescente da internet evidenciou novas ameaças cibernéticas emergentes, deslocando o foco das políticas de segurança para a proteção dos dados, especialmente no âmbito do setor público, onde a salvaguarda das informações governamentais assume papel central. As medidas de proteção e segurança da informação que inicialmente se preocupavam com equipamentos físicos e prevenção de acessos não autorizados, passaram a abranger de forma mais acirrada o ambiente digital (Aslan *et al.,*2023).

Na ausência de ferramentas ou softwares específicos projetados para proteger a informação durante a transferência de dados pela internet, criminosos cibernéticos podem facilmente acessar, modificar ou até mesmo substituir conteúdos sensíveis, resultando em comprometimentos graves à integridade, confidencialidade e disponibilidade das informações. Essa vulnerabilidade é ainda mais acentuada pelo emprego de protocolos de rede e dispositivos originalmente desenvolvidos sem considerações robustas de segurança, o que amplia a superfície de ataque e expõe os sistemas a ameaças persistentes (Aslan *et al.,* 2023).

Diante da crescente adoção do trabalho remoto no setor público federal, intensificada por transformações digitais e demandas por maior flexibilidade laboral, torna-se imperativo o fortalecimento das práticas de segurança da informação. Nesse cenário, o Programa de Privacidade e Segurança da Informação (PPSI), regulamentado em 2023, por meio da Portaria SGD/MGI n. 852/2023, é uma iniciativa estratégica do governo brasileiro para fortalecer a proteção de dados e a segurança da informação nos órgãos públicos, tendo como foco principal, elevar a maturidade e a resiliência dos órgãos federais em relação à segurança e privacidade de dados, instituindo políticas, controles e processos formalizados (Brasil, 2023).

Com as transformações impostas pela adoção do trabalho remoto, justifica-se avaliar a eficácia do PPSI frente aos novos desafios que emergem nesse contexto. A modalidade remota introduziu vulnerabilidades adicionais à segurança da informação, tais como a exposição a ataques cibernéticos, o uso de dispositivos pessoais não homologados, a dependência de redes domésticas potencialmente inseguras e a ocorrência de falhas humanas (Coro, 2024).

Esses fatores representam riscos significativos à integridade de dados confidenciais e à continuidade da prestação de serviços públicos essenciais. Nesse cenário, é fundamental que o PPSI contemple mecanismos eficazes de controle de acesso, gestão de ativos e resposta a incidentes, alinhados às especificidades operacionais do setor público**.**

O presente trabalho propõe como objetivo geral, demonstrar a relevância e a efetividade do PPSI, enquanto framework com padrões reconhecidos de segurança da informação, essencial para assegurar a integridade, confidencialidade e disponibilidade dos ativos informacionais no contexto do trabalho remoto, especialmente no âmbito do setor público federal.

Para tanto os objetivos específicos se concentraram em: a) identificar as principais vulnerabilidades da segurança da informação associadas ao trabalho remoto no setor público federal; b) avaliar a aderência do PPSI às melhores práticas de segurança da informação, e sua aplicação em órgãos públicos federais como framework estratégico de mitigação de vulnerabilidade e, c) propor recomendações para o aprimoramento da implementação do PPSI no contexto do trabalho remoto, considerando aspectos técnicos, humanos e organizacionais.

Este artigo está organizado em cinco seções, além das referências. A primeira introduz o tema do trabalho remoto no serviço público federal e as vulnerabilidades associadas ao acesso remoto a sistemas institucionais. A segunda apresenta o referencial teórico, com os principais fundamentos legais e conceituais sobre proteção de dados e segurança da informação. A terceira descreve a metodologia adotada, enquanto a quarta aborda os resultados e discussões. Por fim, a quinta seção expõe as considerações finais, sintetizando as conclusões e contribuições do estudo.

2 Referencial Teórico

Nesta seção, apresentam-se os principais fundamentos para a análise da segurança da informação no trabalho remoto no setor público federal. Inicialmente, discute-se os aspectos operacionais e tecnológicos dessa modalidade e suas implicações para a gestão da

informação. Em seguida, abordam-se os princípios da LGPD, com foco na proteção de dados sensíveis em ambientes descentralizados. Também são consideradas as vulnerabilidades específicas do trabalho remoto e, por fim, destaca-se a importância do Framework de PPSI como ferramenta estratégica para mitigar riscos e garantir a continuidade dos serviços públicos essenciais em regime remoto.

2.1 Panorama do Trabalho Remoto no Setor Público Federal

O panorama do trabalho remoto e segurança da informação no setor público federal apresenta um cenário de expansão e consolidação dessa modalidade, impulsionado principalmente pela pandemia da COVID-19 e atualmente regulamentado por normativas como o Decreto nº 11.072/2022, que estabelece diretrizes para sua implementação, monitoramento e avaliação de desempenho (Brasil, 2022).

As principais políticas, normativas e diretrizes que fundamentam a implementação do trabalho remoto na Administração Pública Federal (APF) no Brasil são:

Quadro 1 – Principais Políticas de implementação do Trabalho Remoto na APF

Políticas, Normativas e Diretrizes	**Descrição**
Programa de Gestão e Desempenho – PGD: Decreto nº 11.072, de 17 de maio de 2022	- Regulamenta o Programa de Gestão e Desempenho (PGD) e estabelece diretrizes para teletrabalho no Executivo Federal, incluindo regras sobre autorização, controle de produtividade e manutenção da capacidade de atendimento ao público (Brasil, 2022). - Substitui o controle de frequência pelo controle de produtividade baseado em resultados, e define critérios para participação e monitoramento do teletrabalho, com atenção especial à situação dos servidores, como pessoas com deficiência e responsáveis por dependentes (Brasil, 2022).
Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.	Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.
Instrução Normativa nº 98/2024 do Conselho Nacional de Justiça de 12 de abril de 2024	- Detalha os procedimentos para adesão, pactuação de metas, suporte tecnológico e a necessidade de capacitação de servidores e gestores para o trabalho remoto (CNJ, 2024).
Portaria GM/MGI Nº 8.213, de 29 de outubro de 2024	Institui, no âmbito do Gabinete da Ministra, o Programa de Gestão e Desempenho (PGD) para o exercício de atividades que serão avaliadas em função da efetividade e da qualidade das entregas.

Fonte: Elaborado pelo autor

Além disso, o Tribunal de Contas da União (TCU), destaca a necessidade de transparência ativa e monitoramento para garantir a eficiência e o controle social nessa

modalidade de trabalho na Administração Pública Federal, estabelecendo normas para a obrigação de compatibilidade do perfil do servidor para o trabalho remoto, a faculdade da modalidade, a ausência de controle de jornada presencial, e a especificação ao teletrabalho em atividades que exijam presença física obrigatória (Oliveira, 2024).

De acordo com o Sindicato Interestadual dos Servidores Públicos do Inmetro (ASMETRO-SI), em 2025, a tendência de ampliação do teletrabalho, com projeções para que até 50% dos servidores possam atuar remotamente, indicou ganhos em eficiência, redução de custos administrativos e maior flexibilidade. Sob essa ótica, o governo federal demonstrou maior empenho por ampliação do teletrabalho permitindo novas regras para o PGD, "permitindo que servidores públicos participem do teletrabalho integral ou parcial, desde que cumpram requisitos específicos, como a disponibilização de um número de telefone atualizado" (ASMETRO-SI, 2025, p. 1).

Entretanto, o trabalho remoto no setor público enfrenta desafios importantes, principalmente culturais e tecnológicos, incluindo a resistência gerencial a modelos baseados em resultados ao invés de controle presencial. Sobretudo, a segurança da informação torna-se um ponto crítico, visto que o setor público lida com dados sensíveis e que a proteção desses ativos exige o uso obrigatório de redes seguras, boas práticas de segurança digital e políticas robustas como o PPSI (Lucas; Santos, 2021).

A implementação progressiva de estratégias tecnológicas que visam garantir a continuidade e a eficiência dos serviços, mesmo diante da descentralização dos ambientes de trabalho inclui uso de sistemas digitais avançados para protocolo eletrônico, gerenciamento de materiais e serviços, além de ferramentas de comunicação e colaboração online, que permitem a atuação remota segura e eficiente dos servidores públicos (Oliveira, 2021).

Embora essas estratégias sejam benéficas, a descentralização dos ambientes digitais impõe desafios à segurança da informação. A dispersão dos recursos tecnológicos e dos dados aumenta a superfície de ataque, exigindo a implantação rigorosa de controles de acesso, autenticação multifatorial, criptografia e monitoramento contínuo para proteção contra ameaças cibernéticas. Ainda há uma necessidade de superar barreiras culturais e estruturais internas, como a resistência à adoção de novas tecnologias e à capacitação técnica dos servidores (Oliveria, 2021).

Vale destacar que o atendimento ao público vem sendo amplamente realizado por meio de plataformas virtuais. Neste contexto, é necessário garantir que, caso o serviço seja prestado por servidores em regime de teletrabalho, além dos recursos automáticos

disponibilizados, estes observem rigorosamente os horários previamente estabelecidos para o atendimento ao público. Nessa possibilidade, a flexibilidade da jornada no teletrabalho é reduzida, exigindo cumprimento estrito dos períodos específicos ao atendimento (Oliveira, 2024).

Por outro lado, a infraestrutura tecnológica deve ser robusta e atualizada para evitar vulnerabilidades decorrentes de sistemas obsoletos ou mal configurados. O desafio reside em garantir que a integração entre tecnologias, processos e pessoas ocorra de forma harmoniosa, preservando a integridade, confidencialidade e disponibilidade das informações enquanto se maximiza a produtividade no regime remoto (Oliveira, 2021).

Assim, equilibrar a inovação tecnológica com práticas rigorosas de segurança tornou-se essencial para o sucesso do trabalho remoto no setor público, promovendo benefícios como maior flexibilidade, economia de recursos e aprimoramento dos serviços públicos, sem comprometer a proteção dos dados governamentais.

2.2 Lei Geral de Proteção de Dados (LGPD)

A Lei n. 13.853, de 8 de julho de 2019, promoveu algumas alterações na Lei n. 13.709/2018. Para garantir o cumprimento das normas sobre proteção de dados, criou a Autoridade Nacional de Proteção de Dados (ANPD) e criou a composição do Conselho Nacional de Proteção de Dados Pessoais e Privacidade (CNPDPP). À ANPD, cabe elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados que descumpra a legislação; promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; e promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional (Brasil, 2019).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018, normatiza sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais. No âmbito dessa Lei, o tratamento de dados pode ser exercido por dois agentes: o Controlador e o Operador. Além desses, destaca-se a figura do Encarregado (Brasil, 2018).

O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado. A ele compete as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento. No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei (Brasil, 2020).

São considerados Controladores os órgãos públicos que contratam empresas privadas para gerir o registro de visitantes, uma vez que tais empresas atuam sob as determinações do órgão contratante. Nessa relação, o órgão público define a finalidade do tratamento dos dados pessoais e deve exigir da empresa contratada, na qualidade de Operadora, a adoção dos meios técnicos necessários para assegurar a observância dos princípios previstos no art. 6º da Lei Geral de Proteção de Dados – LGPD (BRASIL, 2020, p. 11).

O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O Encarregado, indivíduo nomeado pelo Controlador para desempenhar a função de canal de comunicação entre o Controlador, o Operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (Brasil, 2020). A ANPD tem a missão precípua de zelar pela proteção de dados pessoais e por regulamentar e fiscalizar o cumprimento da LGPD. Suas principais competências estão listadas no artigo 55-j da LGPD (Brasil, 2024).

A distinção entre Controlador e Operador no contexto do tratamento de dados, considera fundamentalmente que o Controlador detenha autonomia decisória sobre os fins e os meios de tratamento, assumindo a responsabilidade pelas decisões estratégicas e especificamente pelo uso dos dados pessoais. Em contrapartida, o Operador exerce um papel de contribuição executório, atuando conforme as instruções do Controlador, sem independência na definição das específicas ou dos procedimentos, estando subordinado aos desígnios estabelecidos para este último (Brasil, 2020).

Além desses agentes, um conceito essencial da LGPD é o tratamento de dados seguindo as normas colocadas pela Lei, que garantem aos cidadãos acesso, correção, exclusão, portabilidade e outras ações relacionadas aos seus dados pessoais. O tratamento de dados diz respeito a qualquer atividade que utiliza um dado pessoal na execução da sua operação. Deve-se observar rigorosamente determinados requisitos, como finalidade e necessidade, previamente comunicadas ao titular, a fim de garantir a legalidade, legitimidade e a proteção dos direitos do indivíduo frente ao uso de suas informações pessoais. O consentimento do titular dos dados é considerado elemento essencial para o tratamento, regra prevista no art. 11, II, da Lei (Brasil, 2018).

Tais condições, previstas e comunicadas de forma clara e transparente ao titular dos dados evita o tratamento arbitrário e promove a conformidade com os princípios norteadores da proteção de dados pessoais. Para fins dessa Lei, considera-se tratamento de dados pessoais qualquer operação realizada com esses dados, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essa definição abrangente reflete a intenção do legislador de cobrir todas as possíveis formas de manipulação de dados pessoais, conforme estabelecido no art. 5º, inciso X, da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018).

Antes do início de qualquer tratamento de dados pessoais, é imperativo que o agente responsável assegure que a finalidade da operação seja marca registrada de maneira clara e inequívoca. Além disso, os propósitos devem ser especificados e comunicados ao titular dos dados de forma transparente. No âmbito do setor público, a principal finalidade do tratamento de dados pessoais está intrinsecamente ligada à execução de políticas públicas, as quais devem estar claramente estabelecidas em legislações, regulamentos ou ser respaldadas por contratos, convênios ou instrumentos similares, conforme estipulado pela LGPD (BRASIL, 2018, art. 7o, III).

As atribuições do CNPDPP envolvem a proposição de diretrizes estratégicas para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, a confecção de relatórios anuais de avaliação da política nacional e a realização de debates e audiências públicas sobre a proteção de dados pessoais. O compartilhamento dentro da administração pública, no âmbito da execução de políticas públicas, é previsto na lei e dispensa o consentimento específico. Contudo, o órgão que coleta deve informar com transparência (Brasil, 2019).

No que diz respeito à adequação dos órgãos e entidades públicas à LGPD, inicialmente exige-se uma transformação cultural abrangente, que se estende aos níveis estratégico, tático e operacional da instituição. Essa mudança cultural implica a incorporação sistemática do respeito à privacidade dos dados pessoais em todas as etapas do tratamento, bem como a promoção contínua de ações de conscientização entre os servidores, com a finalidade de estabelecer uma cultura organizacional que valoriza a proteção de dados de forma integrada e permanente (Brasil, 2020).

A LGPD garante autonomia aos titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos perante os controladores de dados. Esses direitos, estabelecidos no art. 6º e respectivos incisos, da Lei n.13.709/2018, decorrem dos princípios da finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção e princípio da não discriminação, os quais garantem ao titular direito ao tratamento restrito aos propósitos legítimos, tratamento compatível com as finalidades informadas, limitação do tratamento ao mínimo necessário, consulta facilitada e gratuita,

exatidão e clareza, disponibilização de informações, adoção de medidas técnicas e administrativas para proteger dados, entre outros (Brasil, 2018).

Nesse cenário, a LGPD exerce influência decisiva sobre o trabalho remoto na APF, ao exigir que a flexibilidade dessa modalidade seja acompanhada de políticas e práticas robustas de proteção de dados. No contexto de acesso remoto e uso intensivo de tecnologias digitais, a lei reforça a responsabilidade institucional e promove uma cultura de segurança e privacidade que sustenta a eficiência e a conformidade no serviço público.

2.3 Vulnerabilidades em Segurança da Informação no Trabalho Remoto do Setor Público Federal

À medida que sistemas de informação e bancos de dados se tornaram predominantes na internet, a segurança de sistemas operacionais passou a enfrentar desafios ainda mais complexos, muitos deles associados às diversas vulnerabilidades exploradas no ciberespaço. Esse cenário é amplificado pelo crescimento do trabalho remoto, que expande a superfície de ataque e intensifica a necessidade de proteger dados, conexões e dispositivos fora do perímetro tradicional das organizações (Stallings; Brown, 2014).

A vulnerabilidade em um sistema pode ser conceituada como uma fragilidade, falha ou deficiência presente em software, hardware, procedimentos ou controles de segurança, capaz de ser explorada – intencionalmente ou acidentalmente – para comprometer a confidencialidade, integridade e disponibilidade das informações (ISO/IEC 27005:2018).

De acordo com Pfleeger e Pfleeger (2023), vulnerabilidades incluem desde erros de codificação, configurações inadequadas, falta de atualizações, até processos organizacionais frágeis, abrindo portas para ameaças ativamente explorarem recursos computacionais. A identificação, classificação e correção dessas vulnerabilidades constituem etapas fundamentais no ciclo de gestão de riscos de segurança da informação, sendo essenciais para a construção de ambientes computacionais mais resilientes.

Quando não são devidamente tratadas, essas vulnerabilidades podem comprometer todo o funcionamento de sistemas críticos dos sites do governo federal, tornando-os suscetíveis a ataques de diferentes naturezas, como invasões, roubo de dados, indisponibilidade de serviços (DoS/DDoS) e manipulação indevida de informações sensíveis (Anderson, 2020; Stallings, 2017).

Considerando o contexto governamental, no qual são processados dados pessoais e institucionais estratégicos, a exploração de falhas pode causar graves impactos, tais como danos à reputação do Estado, prejuízos financeiros e descumprimento de arcabouços legais

como a LGPD. Segundo a ISO/IEC 27002:2022, a mitigação contínua de vulnerabilidades é indispensável para assegurar a confiança, disponibilidade e integridade dos portais governamentais, protegendo efetivamente a sociedade e a administração pública frente às constantes ameaças do ciberespaço.

Os requisitos de segurança de computadores não são tão simples quanto possam parecer. Em sua maioria, os mecanismos ou algoritmos de segurança desenvolvidos, consideram ataques potenciais bem-sucedidos aos requisitos de confidencialidade, autenticação, irretratabilidade e integridade. Além de exigir informações secretas, pode haver dependência de protocolos de comunicação, que dificultam o desenvolvimento de mecanismos de segurança (Stallings; Brown, 2014).

De acordo com os autores, a segurança de computadores pode ser compreendida como uma disputa constante de capacidades entre o atacante, que busca explorar brechas existentes, e o projetista ou administrador, que procura identificá-las e corrigi-las. Nessa relação, o agressor possui a vantagem de precisar encontrar apenas uma única vulnerabilidade para obter êxito, enquanto o responsável pela segurança precisa localizar e mitigar todas as fragilidades para se aproximar de um estado ideal de proteção (Stallings; Brown, 2014, p. 12).

A análise dos autores evidencia que a segurança da informação é um processo dinâmico e desafiador, marcado por uma constante disputa entre vulnerabilidades e mecanismos de proteção. No contexto do trabalho remoto na APF, esse cenário torna-se ainda mais complexo, uma vez que a descentralização dos acessos amplia o campo de exposição a ameaças, exigindo políticas preventivas, vigilância contínua e o fortalecimento dos controles definidos pelo PPSI.

2.4 Implementação do Framework do PPSI

O Programa de Privacidade e Segurança da Informação (PPSI), regulamentado pela Portaria SGD/MGI nº 852/2023, orienta a identificação e mitigação de vulnerabilidades, promovendo a conformidade regulatória com a LGPD e demais normativas correlatas, oferecendo uma estrutura de referência para proteger os ativos informacionais e garantir a conformidade com as melhores práticas de segurança. O PPSI é um framework especialmente relevante para enfrentar as principais vulnerabilidades de segurança da informação no contexto do trabalho remoto no setor público federal (Brasil, 2023).

Conforme disposto no art. 8º, da Portaria SGD/MGI n. 852/2023, órgãos da administração pública federal estão sujeitos a adotarem PPSI. Embora sua implementação

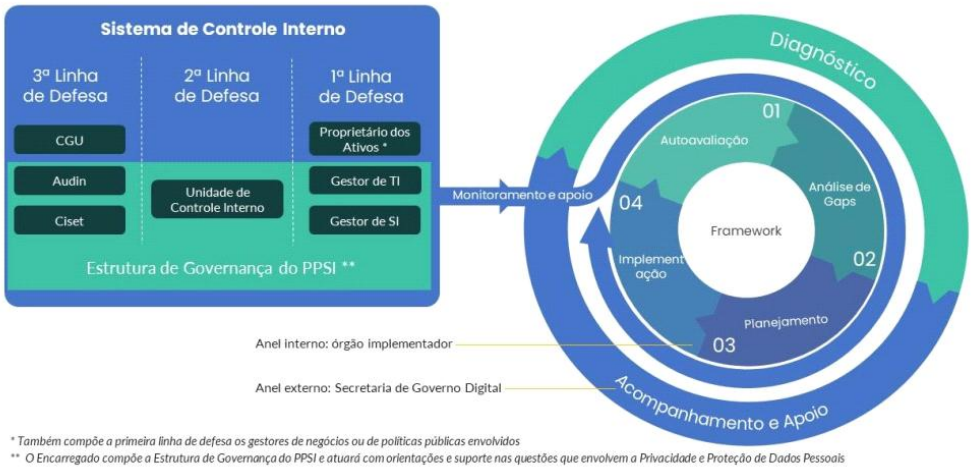
seja obrigatória para essas instituições, o PPSI também é recomendado para os governos estaduais e municipais, bem como para organizações do setor privado. Tal preceito evidencia o caráter abrangente e estratégico do framework, visando aprimorar a governança da segurança da informação e proteção de dados pessoais em diferentes esferas administrativas (Brasil, 2023).

A responsabilidade pela implementação das diretrizes e medidas previstas em um quadro de governança recai sobre a estrutura de governança de cada órgão ou entidade. As decisões devem ser fundamentadas por meio de uma análise criteriosa de riscos, a fim de garantir transparência, responsabilidade e conformidade com as normativas vigentes. Essa estrutura consiste em um conjunto integrado de controles, metodologias e ferramentas de apoio que visam garantir a eficiência, a eficácia e a responsabilidade na gestão organizacional, promovendo o alinhamento estratégico e a mitigação de riscos (Brasil, 2023).

De acordo com o Guia do Framework do PPSI, a justificativa da não implementação das medidas, deverá ser fundamentada na análise de riscos associada ao tratamento dos dados pessoais, demonstrando conformidade com os princípios e bases legais previstos na LGPD, tais como a finalidade, necessidade, adequação, segurança e prevenção. Assim, a justificativa deve refletir uma avaliação técnica e legal que integra o respeito à legislação de proteção de dados e às políticas institucionais de segurança, conforme exigido pela Portaria SGD/MGI nº 852/2023 e pelas normas da LGPD e do Gabinete de Segurança Institucional – GSI (Brasil, 2023).

A implementação do PPSI segue o ciclo baseado no modelo PDCA (*Plan, Do, Check, Act* – Planejar, Fazer, Verificar e Agir), permitindo avaliações e melhorias contínuas. São previstas etapas de autoavaliação, análise de lacunas, planejamento e implementação das medidas, com prazos definidos para a execução inicial e possibilidade de prorrogação justificada. O framework enfatiza a atuação coordenada entre as linhas de defesa do controle interno, gestores de TI, segurança da informação, e auditoria, garantindo supervisão e conformidade (Brasil, 2024).

Figura 1 – Metodologia de Implementação do Framework do PPSI



Fonte: Guia do Framework do PPSI (Brasil, 2024)

Além disso, disponibiliza ferramentas para autodiagnóstico, acompanhamento e indicadores, como o Indicador de Segurança (iSeg) e Indicador de Privacidade (iPriv), que medem a maturidade em segurança da informação e privacidade. O objetivo central é elevar o nível de maturidade dos órgãos, fortalecendo suas defesas contra ameaças cibernéticas e assegurando a proteção eficaz dos dados pessoais. Desse modo, o Guia sustenta a adoção do Framework como um instrumento essencial para a governança da segurança e privacidade na administração pública federal (Brasil, 2024).

2.5 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD está fundamentado na LGPD (Brasil, 2018), em seus artigos 5º, inciso XVII, e 38. O inciso XVII do artigo 5º, define o RIPD como um documento elaborado pelo controlador dos dados, que deve conter descrição dos processos de tratamento de dados pessoais; identificação dos riscos potenciais à privacidade e aos direitos dos titulares e apresentar as medidas de segurança e mitigação adotadas para reduzir esses riscos.

O artigo 38 da LGPD (Brasil, 2018), reforça a responsabilidade do controlador em documentar e justificar o tratamento de dados pessoais, especialmente quando há risco elevado à privacidade dos titulares. Prevê que a Agência Nacional de Proteção de Dados (ANPD) pode determinar que o controlador elabore este relatório para operações de alto risco, como tratamento de dados sensíveis ou em larga escala. O relatório deve conter: a) Descrição dos tipos de dados coletados; b) Justificativa para sua coleta e tratamento; c) Medidas de segurança adotadas e, Análise de riscos e medidas de mitigação.

Na prática, o RIPD formaliza o balanço de riscos e benefícios de uma operação de tratamento e serve como base para a fiscalização da ANPD, que pode exigir sua elaboração para garantir que a proteção dos direitos fundamentais dos titulares seja prioritária. Portanto, o RIPD é um documento técnico que descreve os processos de tratamento de dados pessoais que podem representar alto risco para os direitos e liberdades dos titulares desses dados.

2.6 Aplicação do PPSI no Trabalho Remoto do Setor Público Federal

O Framework PPSI aplicado ao trabalho remoto no setor público federal brasileiro representa um avanço crucial para a proteção dos dados e para a continuidade segura dos serviços públicos em ambientes digitais. Ao estabelecer medidas de proteção e de controles específicos para garantir a privacidade e a segurança da informação no contexto do serviço público federal, visa elevar a maturidade e a resiliência dos órgãos no que concerne à privacidade e segurança da informação, especialmente frente ao incremento das atividades remotas impulsionadas pela pandemia da COVID-19 (Tomazetti; Costa; Silva, 2022).

No contexto do trabalho remoto, o PPSI propõe diretrizes que contemplam a governança, a metodologia, a capacitação de pessoas e a utilização de tecnologias específicas para garantir o controle dos acessos, a proteção contra vulnerabilidades e a mitigação de riscos cibernéticos. A coordenação do Programa por centros especializados como o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br) é fundamental para identificar ameaças, disseminar informações e promover respostas rápidas a incidentes (Tomazetti; Costa; Silva, 2022).

Além disso, o PPSI exige que os órgãos adaptem seus planos de trabalho para o ambiente remoto, assegurando monitoramento do desempenho dos servidores e a integridade das operações. A adoção dessas medidas promove um ambiente de trabalho remoto seguro, confiável e eficiente, alinhado aos princípios de governança pública e à legislação vigente, garantindo a proteção dos dados sensíveis, a privacidade dos usuários e a continuidade dos serviços públicos essenciais (Brasil, 2024).

Ao compreender a distinção das medidas de proteção e medidas de controle, torna-se mais claro o papel de cada ação na segurança da informação dentro da Administração Pública Federal. Assim, a implementação do PPSI no trabalho remoto fortalece a segurança da informação pública, permitindo que o setor público federal responda adequadamente aos desafios tecnológicos contemporâneos e às demandas por transparência e responsabilidade digital (Brasil, 2023).

Conforme descrito nos Quadros 2 e 3, os exemplos práticos de medidas de proteção e de controles de segurança, que podem ser incorporados ao trabalho remoto em instituições públicas federais, evidenciam padrões de segurança capazes de manterem a integridade, a confidencialidade e a disponibilidade das informações públicas, protegendo a instituição de incidentes e passivos legais.

Quadro 2 - Exemplos práticos de Medidas de Proteção de segurança adotados pelo PPSI aplicáveis ao trabalho remoto

Medidas	**Finalidade**
Uso obrigatório de VPN (Rede Privada Virtual)	- Exigir que todo acesso remoto aos sistemas e dados institucionais seja realizado por meio de VPNs, garantindo a criptografia do tráfego de informações entre o usuário e a rede da instituição, mesmo quando este utiliza redes domésticas ou públicas.
Atualização de sistemas e dispositivos utilizados remotamente	- Redução de vulnerabilidades técnicas. Controle sobre *endpoints* utilizados remotamente
Autenticação Multifator (MFA)	- Implementar a autenticação em duas etapas para qualquer acesso remoto, combinando senha forte e um segundo fator (token, app autenticador, biometria etc.), a fim de impedir acessos não autorizados, mesmo em caso de vazamento de credenciais. Para quem usa MFA, recomenda-se no mínimo senhas de 8 caracteres e uma senha de 14 caracteres para contas que não usam o MFA.
Políticas de atualização e *Patch Management*	- Estabelecer a obrigatoriedade de uso de dispositivos (corporativos ou pessoais autorizados) com sistemas operacionais e aplicativos sempre atualizados, reduzindo vulnerabilidades exploradas por criminosos.
Permissões e controles de acessos baseados em perfil e necessidade de uso	- Aplicar o princípio do mínimo privilégio, concedendo apenas os acessos estritamente necessários aos servidores para execução de suas atividades, com revisões periódicas dessas permissões, especialmente em cenários de trabalho remoto.
Política clara de uso de recursos	- Orientar e regulamentar o uso de recursos institucionais, como e-mail, sistemas e armazenamento em nuvem, proibindo o armazenamento e a transmissão de informações sensíveis por canais não autorizados ou pessoais.
Criptografia de dados em trânsito e em repouso	- Exigir a criptografia de dados em trânsito (na comunicação remota) e em repouso (no dispositivo), inclusive nos backups de arquivos sensíveis.
Treinamento em segurança da Informação	- Realizar campanhas e treinamentos regulares sobre boas práticas de segurança, abordando temas como identificação de fraudes, prevenção de golpes comuns em trabalho remoto, cuidados com dados sensíveis e manipulação segura de informações
Procedimentos de resposta a incidentes	- Manter um fluxo claro de comunicação, com orientações sobre como agir e a quem reportar em caso de incidentes (como suspeita de invasão, vazamento de dados, perda de dispositivo), inclusive fora do horário de expediente.

Segmentação de rede	- Limitação do alcance de ataques internos ou externos. Segmentação de rede favorece níveis básicos de disponibilidade e maior grau de privacidade para usuários da rede corporativa.
Proteção antivírus e malware	- Prevenção de ameaças digitais
Backup periódico	- Garantia de recuperação de dados em caso de falhas
Acordo de responsabilidade	- Exigir que todos os servidores e colaboradores assinem termo de ciência e responsabilidade pelo uso dos recursos da instituição durante o trabalho remoto, reforçando consequências administrativas e legais em caso de mau uso.
Gestão segura de credenciais	- Proibir o compartilhamento de senhas e implementar sistemas de gestão segura de credenciais, recomendando o uso de cofres digitais ou gerenciadores de senha aprovados pela instituição.

Fonte: Adaptado do Guia do Framework PPSI (Brasil, 2024)

Quadro 3 - Exemplos de Medidas de controle de segurança adotados pelo PPSI aplicáveis ao trabalho remoto

Medidas	**Finalidade**
Restrições de dispositivos e inventário	- Controlar quais dispositivos podem acessar os sistemas institucionais, preferencialmente limitando o acesso a equipamentos cedidos pela Administração, devidamente inventariados, com antivírus e soluções de *endpoint* de segurança instaladas e monitoradas.
Inventário de ativos de informação e tecnologia	- Mapeamento e rastreabilidade dos recursos. Sem o mapeamento não há possibilidade de rastrear e realizar o monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas.
Monitoramento e auditoria de acessos e *logs* de usuários	- Controlar quais dispositivos podem acessar os sistemas institucionais, preferencialmente limitando o acesso a equipamentos cedidos pela Administração, devidamente inventariados, com antivírus e soluções de *endpoint* de segurança instaladas e monitoradas.
Gestão de incidentes de respostas rápidas	- Mitigação de impactos e recuperação eficiente. Proteger as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo: planos, definição de papéis, treinamento, comunicações, gerenciamento de supervisão).
Indicadores de maturidade (iSeg e iPriv) para avaliação institucional	- Avaliação do nível de segurança e privacidade institucional. Detecção de comportamentos suspeitos ou não autorizados.
Documentação e padronização de processos e políticas	- Uniformização e transparência nas práticas institucionais.
Acompanhamento por estruturas de governança e comitês de segurança	- Supervisão estratégica e tomada de decisão baseada em evidências.

Fonte: Adaptado do Guia do Framework PPSI (Brasil, 2024)

A adesão ao PPSI é uma demonstração de conformidade ativa com a LGPD, pois, ao documentar as medidas de proteção e controle (conforme exemplificado nos Quadros 2 e 3), os órgãos federais, além de minimizarem incidentes, também mitigam passivos legais exigidos pela ANPD.

Nesse contexto, as medidas de proteção e controle estabelecidas pelo PPSI revelam-se complementares e essenciais para a gestão de riscos no teletrabalho. Enquanto as medidas de proteção implementam barreiras técnicas e operacionais contra ameaças cibernéticas, as medidas de controle garantem a eficácia contínua dessas barreiras por meio de monitoramento, auditoria e aprimoramento sistemático, conforme preconizado pelo Guia do Framework de Privacidade e Segurança da Informação (BRASIL, 2023). A padronização de exigências de segurança para dispositivos e conexões remotas, nesse sentido, constitui uma estratégia fundamental para mitigar os riscos inerentes ao uso de redes domésticas menos seguras e à convergência entre sistemas pessoais e institucionais, promovendo assim uma postura proativa de segurança da informação no setor público federal.

Vale destacar que o uso de VPNs garante a criação de túneis seguros para a transmissão de dados, mitigando riscos de interceptação em redes públicas ou não confiáveis. A criptografia, por sua vez, assegura que as informações trafeguem de forma ilegível para agentes não autorizados, mesmo em caso de acesso indevido (Brasil, 2024).

A autenticação multifator adiciona uma camada adicional de verificação, dificultando ataques baseados em credenciais comprometidas. Já as políticas de senhas robustas reduzem significativamente a vulnerabilidade a ataques de força bruta e engenharia social (Tomazetti; Costa; Silva, 2022).

O Framework PPSI orienta que o uso de ferramentas de colaboração remota no serviço público federal deve garantir a confidencialidade, integridade e disponibilidade dos dados, por meio de controles de acesso rigorosos, autenticação segura dos usuários e monitoramento contínuo das atividades. Além disso, enfatiza a importância da capacitação dos servidores para o uso consciente e seguro das tecnologias colaborativa (Brasil, 2024).

O framework também recomenda a adoção de tecnologias confiáveis e a aplicação de boas práticas de segurança, como o uso de redes privadas virtuais (VPNs), criptografia e atualizações constantes dos sistemas, visando mitigar riscos associados ao trabalho remoto e assegurar a continuidade dos serviços públicos com qualidade e segurança, tudo isso alinhado ao cumprimento das disposições da LGPD e outras normas correlatas (Brasil, 2024).

A atualização e o gerenciamento contínuo dos dispositivos utilizados remotamente são cruciais para evitar brechas de segurança decorrentes de softwares obsoletos ou configurações inadequadas. Ao exigir esses mecanismos, o framework não apenas promove uma cultura institucional de segurança, mas também estabelece um padrão mínimo de proteção compatível com os desafios contemporâneos da transformação digital.

3 Metodologia da Pesquisa

O trabalho foi conduzido por meio de pesquisa bibliográfica, de natureza qualitativa, voltada à compreensão aprofundada dos fenômenos, das percepções e dos contextos normativos que envolvem a segurança da informação no trabalho remoto no setor público federal. Conforme Gil (2003), a pesquisa bibliográfica possibilita ao pesquisador o contato direto com a produção já publicada sobre determinado tema, permitindo a construção de uma base teórica sólida e sistematizada para a investigação. Ainda segundo o autor, a abordagem qualitativa privilegia a compreensão dos significados e das interpretações atribuídas pelos sujeitos e pelas instituições, adotando métodos flexíveis e uma análise que valoriza a descrição detalhada, o aprofundamento e a articulação entre o pesquisador e o objeto de estudo (GIL, 2003).

Inicialmente, procedeu-se ao levantamento de legislações vigentes relacionadas à proteção de dados pessoais, à segurança da informação e ao teletrabalho na APF, com destaque para leis, decretos, portarias e normas infralegais. Em paralelo, foram realizadas buscas em bases de dados científicas e repositórios institucionais a fim de identificar artigos e estudos que abordassem o trabalho remoto durante a pandemia de COVID-19, com ênfase em publicações que tratassem explicitamente de seus impactos, desafios e riscos para a segurança da informação. Nessa etapa, foram adotados critérios de filtragem por palavras-chave, tais como “teletrabalho”, “trabalho remoto”, “pandemia”, “segurança da informação” e “administração pública”, priorizando materiais produzidos ou atualizados a partir de 2020.

Em um segundo momento, o foco da pesquisa voltou-se à análise do Guia do Framework de Privacidade e Segurança da Informação e dos documentos correlatos ao Programa de Privacidade e Segurança da Informação (PPSI) no âmbito da APF. A partir dessa documentação, foram identificados e selecionados os controles, princípios e diretrizes com potencial de aplicação direta ao contexto do trabalho remoto, especialmente no que se refere a acessos remotos, uso de dispositivos, proteção de dados, gestão de riscos e governança de segurança da informação.

Os materiais utilizados compreenderam, assim, artigos científicos, legislações vigentes (leis, decretos e portarias), guias de boas práticas, manuais operacionais e relatórios oficiais atualizados, todos diretamente relacionados aos temas de Segurança da Informação (SI), Gestão do Trabalho Remoto/Teletrabalho e Programa de Privacidade e Segurança da Informação (PPSI).

Essa metodologia permitiu analisar criticamente os documentos selecionados, com foco nas vulnerabilidades de segurança da informação associadas ao trabalho remoto, tomando como parâmetro central as diretrizes e controles estabelecidos pelo PPSI. A partir dessa análise, buscou-se discutir cenários atuais, identificar lacunas e propor melhorias na gestão da segurança da informação no teletrabalho, fundamentando-se principalmente no Framework de Privacidade e Segurança da Informação e em sua aplicação ao contexto da APF.

4 Resultados e Discussão

O posicionamento do TCU sobre o teletrabalho na Administração Pública Federal (APF), transforma o teletrabalho de uma simples medida operacional em um processo que exige gestão ativa e controle social. (Oliveira, 2024). As normas emitidas pelo Tribunal visam garantir a eficiência da APF ao mesmo tempo em que preservam a legalidade e a equidade. O TCU exige transparência ativa e monitoramento das atividades, assegurando que a ausência do controle de jornada presencial seja compensada pela entrega de resultados e pela possibilidade de fiscalização social.

Nesse sentido, o TCU consolida o entendimento de que o teletrabalho na APF deve ser implementado de forma criteriosa, orientada à produtividade e estritamente vinculada às necessidades da função, assegurando que os benefícios da flexibilidade não comprometam o desempenho do serviço público.

A LGPD (Lei nº 13.709/2018), estabelece um regime normativo abrangente para o tratamento de dados pessoais, aplicável a qualquer pessoa, física ou jurídica, de direito público ou privado, e a todas as formas de dados (físicos ou digitais, manuais ou automatizados). O cerne dessa estrutura legal é definido pelos agentes de tratamento, sendo o mais crucial o Controlador.

O Controlador, que na administração pública é o próprio órgão ou entidade, é a figura que detém o poder de decisão sobre o tratamento de dados pessoais. Compete a ele definir as finalidades (o "porquê") e os meios (o "como") do tratamento. Nesse cenário, a LGPD impõe que a pessoa jurídica, seja ela do setor público ou privado, que determina a lógica e o

objetivo do uso dos dados, assume a responsabilidade máxima pelas decisões e pelas consequências do tratamento realizado.

O alinhamento entre as diretrizes do TCU para o teletrabalho e as exigências da LGPD reforça a necessidade de uma governança sólida sobre dados e processos na Administração Pública Federal. Nesse contexto, o Programa de Privacidade e Segurança da Informação (PPSI) assume papel estratégico ao estabelecer políticas, controles e mecanismos que garantem a proteção dos dados pessoais, a integridade das informações institucionais e a conformidade das práticas remotas. Ao disciplinar condutas e assegurar o cumprimento dos princípios de segurança, confidencialidade e transparência, o PPSI fortalece a confiança no trabalho remoto, assegurando que a flexibilidade operacional conviva harmoniosamente com a responsabilidade legal e com a cultura de proteção da informação no serviço público.

O PPSI não é apenas um conjunto de diretrizes técnicas, esse programa representa uma estratégia indispensável para a viabilização segura do trabalho remoto na Administração Pública Federal (Brasil, 2023). Em um cenário cada vez mais digitalizado, onde o acesso remoto a sistemas e dados se tornou rotina, o PPSI atua como uma salvaguarda essencial, impondo padrões rigorosos que asseguram a integridade, a confidencialidade e a disponibilidade das informações públicas.

A responsabilidade pela implementação das diretrizes previstas na Portaria SGD/MGI nº 852/2023 é atribuída à estrutura de governança de cada órgão ou entidade, sendo de responsabilidade de cada governança ou entidade, a eventual decisão de não implementar alguma medida considerada obrigatória pelo *framework,* justificada mediante análise de riscos (Brasil, 2023).

Essa exigência visa assegurar que a articulação deve evidenciar que, mesmo diante da dispensa de alguma medida, a proteção dos direitos dos titulares e a mitigação de riscos à privacidade permanecem asseguradas, em consonância com as diretrizes do GSI para a segurança nacional e da informação.

Dessa forma, o art. 8º assegura que a adoção do PPSI seja uma prioridade institucional. Ao estabelecer as atribuições de forma clara, o PPSI fortalece o caráter mandatário e a importância da conformidade alinhada às políticas de segurança da informação. Isso demonstra que a adoção do *Framework* PPSI pelos órgãos e entidades da administração pública federal é uma obrigatoriedade.

Ao estabelecer controles e protocolos de proteção, o PPSI protege os órgãos públicos contra incidentes cibernéticos, vazamentos de dados sensíveis e potenciais passivos

jurídicos, garantindo que a transformação digital do setor público ocorra de forma responsável, ética e resiliente. Sem essa estrutura normativa, a exposição a vulnerabilidades tecnológicas e a riscos legais seria significativamente ampliada.

O *Framework* PPSI no serviço público federal brasileiro, pode ser indicado como uma ferramenta estratégica para mitigar riscos e elevar o grau de maturidade e resiliência dos órgãos públicos em termos de proteção de dados pessoais e segurança da informação. Sua implementação ocorre por meio de etapas como autoavaliação, análise de lacunas, planejamento e execução de medidas que abarcam cinco pilares fundamentais: governança, pessoas, metodologia, tecnologia e gestão da maturidade (Brasil, 2023).

Isso pode ser facilmente verificado pela imposição de requisitos obrigatórios como o uso de VPNs, criptografia, autenticação multifator, políticas de senhas robustas e o gerenciamento adequado de dispositivos remotos, os quais, representam medidas para a preservação da segurança da informação em ambientes digitais cada vez mais distribuídos. Em um contexto marcado pela intensificação do trabalho remoto, tais exigências não apenas reforçam a proteção dos ativos informacionais, como também asseguram a continuidade operacional das instituições.

O RIPD constitui um instrumento de governança essencial no contexto da LGPD. Sua estrutura formalmente prevista nos artigos 5º, inciso XVII, e 38 da LGPD, torna esse relatório um documento de autodeclaração do controlador, exigindo a descrição detalhada dos processos de tratamento de dados pessoais, a identificação dos riscos potenciais aos direitos e à privacidade dos titulares e, a explicitação das medidas de segurança e mitigação adotadas para neutralizar ou reduzir esses riscos.

O artigo 38 da LGPD, reforça que o RIPD, é a materialização do princípio da prevenção e demonstração de conformidade, destaca a responsabilidade probatório do controlador, especialmente por justificar a necessidade do tratamento em operações consideradas de alto risco (como tratamento de dados sensíveis ou em larga escala).

No contexto do trabalho remoto na Administração Pública Federal, o RIPD assume relevância ainda maior como ferramenta de governança e responsabilidade prevista na LGPD. A análise sistemática das operações de tratamento, das vulnerabilidades associadas ao acesso remoto de sistemas institucionais e das medidas de mitigação adotadas permite identificar riscos específicos decorrentes da descentralização dos ambientes de trabalho, como o uso de redes domésticas, dispositivos pessoais e plataformas de colaboração virtual.

Assim, o RIPD torna-se instrumento essencial para assegurar que a flexibilização trazida pelo teletrabalho não comprometa a segurança da informação nem a conformidade

legal, viabilizando uma gestão preventiva e transparente dos dados públicos e pessoais tratados pelos órgãos da APF.

Na aplicação do Framework do Programa de Privacidade e Segurança da Informação (PPSI) ao contexto do trabalho remoto no setor público federal, os resultados observados demonstram que a adoção de suas diretrizes contribui diretamente para o fortalecimento da maturidade institucional em segurança da informação.

Esse avanço não apenas eleva a capacidade de mitigação de riscos cibernéticos e de proteção de dados pessoais, mas também alinha as práticas remotas ao cumprimento integral da LGPD, garantindo que o tratamento de informações sensíveis ocorra com transparência e responsabilidade, independentemente da localização dos agentes. Ademais, essa maturidade reforça as recomendações do TCU quanto ao teletrabalho na APF, promovendo a eficiência operacional e o monitoramento de resultados sem comprometer a legalidade e a equidade no serviço público.

A estrutura do PPSI em quatro eixos fundamentais: governança, metodologia, capacitação de pessoas e tecnologias específicas, (Tomazetti; Costa; Silva, 2022), sustentam um conjunto de medidas de proteção e de controle que, quando implementadas de forma integrada, promovem o controle de acessos, a mitigação de vulnerabilidades e a resposta ágil a incidentes cibernéticos.

Concentrando-se nos quatro pilares é possível especificar a aplicação do PPSI como o estabelecimento de uma abordagem de segurança da informação e privacidade, pois ao interconectar esses pilares evidencia-se:

Figura 2 – Aplicação do PPSI

Fonte: Elaborado pela autora

O *framework* não se restringe à segurança, mas se conecta à eficiência operacional. Ao exigir a adaptação dos planos de trabalho e o monitoramento de desempenho, o PPSI promove um ambiente de trabalho remoto que é simultaneamente seguro, confiável e alinhado aos princípios de governança pública.

Outro aspecto relevante refere-se à exigência de adaptação dos planos de trabalho dos órgãos públicos ao contexto remoto. Essa adaptação inclui o monitoramento do desempenho dos servidores, a preservação da integridade das operações e a conformidade com os princípios da governança pública. A implementação dessas medidas tem se mostrado eficaz na construção de um ambiente remoto mais seguro, confiável e alinhado à legislação vigente, especialmente no que tange à proteção de dados sensíveis e à privacidade dos usuários.

A distinção entre medidas de proteção (preventivas) e medidas de controle (detectivas e corretivas) revelou-se essencial para a compreensão do papel estratégico de cada ação no fortalecimento da segurança da informação. Conforme ilustrado nos Quadros 2 e 3, os exemplos práticos dessas medidas demonstram padrões de segurança capazes de assegurar a integridade, a confidencialidade e a disponibilidade das informações públicas, reduzindo a exposição institucional a riscos legais e operacionais.

Os resultados apontam que o PPSI, ao ser incorporado às rotinas de trabalho remoto, não apenas responde aos desafios tecnológicos contemporâneos, como também reforça o compromisso da Administração Pública Federal com a transparência, a responsabilidade digital e a proteção dos ativos informacionais do Estado.

5 Considerações Finais

No contexto das transformações digitais, o trabalho remoto deixou de ser uma alternativa e passou a integrar a rotina da Administração Pública Federal. No entanto, essa mudança exige mais do que conectividade: requer segurança, responsabilidade e governança. É nesse cenário que o PPSI se consolida como um alicerce indispensável, estabelecendo diretrizes que visam garantir a confiabilidade, a integridade e a disponibilidade das informações públicas.

Isso significa proteger dados sensíveis contra vazamentos, acessos indevidos e ataques cibernéticos e outros riscos que se intensificam com o trabalho remoto. Além da segurança técnica, o PPSI atua como uma barreira contra passivos legais. Ao definir protocolos claros de acesso, armazenamento e compartilhamento de informações, o Programa reduz a exposição da instituição a sanções, processos e danos reputacionais.

A adoção do PPSI demonstra o compromisso da APF em assegurar à sociedade que o serviço público está preparado para operar com responsabilidade no ambiente digital. O PPSI viabiliza a inovação ao oferecer uma base segura, permitindo que novas tecnologias e formas de trabalho sejam adotadas com confiança, impulsionando a eficiência sem comprometer a proteção institucional.

Considerando que existe risco migratório do trabalho remoto, visto que essa modalidade de trabalho transfere o perímetro de segurança da infraestrutura física da instituição para os ambientes domiciliares e as redes domésticas dos servidores, a implementação do PPSI no contexto do teletrabalho da APF é uma resposta formal para mitigação desses riscos, especialmente porque exige que as medidas de proteção (preventivas) e os controles de segurança (detectivos/corretivos) sejam adaptados para manter a integridade, confidencialidade e disponibilidade dos dados, independentemente da localização física.

Dessa forma, a adoção dessas medidas contribui significativamente para a redução da superfície de ataque da organização, limitando as possibilidades de exploração de vulnerabilidades e dificultando tentativas de acesso não autorizado aos sistemas e informações institucionais. Além disso, estabelece-se que todos os colaboradores e profissionais terceirizados sejam devidamente orientados e capacitados quanto às práticas seguras no contexto do trabalho remoto, promovendo a conscientização contínua sobre ameaças cibernéticas, como golpes de engenharia social e *phishing*, e reforçando a importância do comportamento responsável e da cultura de segurança no ambiente digital.

Em síntese, este trabalho cumpriu seu objetivo principal de analisar as vulnerabilidades de segurança da informação associadas ao trabalho remoto na APF, à luz das diretrizes do PPSI e da LGPD, identificando desafios emergentes e medidas complementares de proteção e controle que podem mitigar riscos cibernéticos no contexto pós-pandemia. Os resultados obtidos, fundamentados em pesquisa bibliográfica qualitativa e análise de normativas e guias institucionais, revelam que, embora o teletrabalho tenha promovido ganhos em eficiência e flexibilidade, sua implementação demanda uma abordagem integrada de governança, capacitação e padronização tecnológica para assegurar a integridade, confidencialidade e disponibilidade dos dados governamentais.

Reconhece-se, contudo, como limitações desta investigação a ausência de análise empírica direta em órgãos específicos e a dependência de fontes secundárias, o que sugere a necessidade de estudos complementares para validação prática das recomendações propostas. Nesse sentido, as linhas de pesquisa futura delineadas – com ênfase na integração

de tecnologias emergentes, no fortalecimento da cultura de segurança e na avaliação comparativa de práticas institucionais – não apenas superam essas limitações, mas também pavimentam o caminho para uma APF mais resiliente e preparada para os desafios da transformação digital contínua, contribuindo, assim, para a evolução sustentável da segurança da informação no serviço público remoto e híbrido.

6 Trabalhos Futuros

Considerando o avanço contínuo da transformação digital e o caráter dinâmico do trabalho remoto na Administração Pública Federal, estudos futuros poderão aprofundar a investigação sobre a integração entre o PPSI e a LGPD e, o uso de tecnologias emergentes, tais como inteligência artificial, computação em nuvem, identidade digital e mecanismos avançados de autenticação.

Pesquisas poderão, por exemplo, avaliar como modelos de inteligência artificial podem ser empregados para detecção de anomalias, prevenção de incidentes e resposta automatizada a ameaças em ambientes de teletrabalho, bem como analisar os desafios de conformidade e de governança de dados decorrentes da adoção massiva de soluções em nuvem no setor público. Outra vertente promissora consiste em examinar o papel das infraestruturas de identidade digital e dos mecanismos de autenticação forte na redução de riscos de acesso indevido a sistemas institucionais a partir de redes domésticas ou dispositivos pessoais.

Tais estudos tendem a contribuir para o desenvolvimento de soluções mais adaptativas e inteligentes, capazes de responder a ameaças em tempo quase real, apoiar a tomada de decisão baseada em dados e fortalecer a resiliência digital em um cenário de crescente mobilidade tecnológica e interconectividade entre sistemas públicos e privados.

Nesse sentido, pesquisas que investiguem o impacto do ambiente institucional, incluindo políticas internas, estruturas de governança e grau de maturidade em segurança da informação, e das práticas de capacitação contínua dos servidores no aprimoramento da governança de dados e na consolidação de uma cultura organizacional voltada à segurança mostram-se fundamentais. A análise de programas de treinamento, campanhas de conscientização e mecanismos de responsabilização, bem como de indicadores de comportamento seguro no uso de recursos tecnológicos, constitui etapa importante para compreender em que medida o fator humano pode deixar de ser apenas um ponto de vulnerabilidade e passar a atuar como elemento central de proteção no contexto do serviço público remoto.

REFERÊNCIAS

ASLAN, Omer; ATOG, Semih Serkant, OZKAN-OKAY, Merve; YIMAZ, Abdullah Asim; APARENTADO, Erdal. ***A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions***. Eletrônica, v.12, n. 13333, 2023. https://doi.org/10.3390/electronics12061333. Disponível em: https://x.gd/bwSz8 Acesso em: 11 jul. 2025.

ASMETRO-SI. Secretaria Geral. **Ascensão do teletrabalho no governo federal.** Rio de Janeiro, 13 jan. 2025. Disponível em: https://x.gd/zHOn4 Acesso em: 23 jul. 2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispões sobre a Lei Geral de Proteção de Dados Pessoais [última atualização em 2019). **Diário Oficial da União**, Seção 1,n. 157, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 20 ago. 2025.

BRASIL. Lei n. 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da União**, seção 1, ano CLVII, n. 130 Brasília, DF, p. 01, 09 jul. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm Acesso em: 20 ago. 2025.

BRASIL, Comitê Central de Governança de Dados. **Guia de Boas Práticas Lei Geral De Proteção de Dados (LGPD):** Guia de Boas Práticas para implementação na Administração Pública Federal**.** Governo Federal, agosto, 2020, 69p.

BRASIL. Ministério da Economia. Portaria nº 9.573, de 26 de outubro de 2020. **Estabelece orientações para a implementação de programa de gestão no âmbito do Ministério da Economia**. Diário Oficial da República Federativa do Brasil, Brasília, DF, 27 out. 2020.

BRASIL, Presidência da República. Decreto nº 11.072, de 17 de maio de 2022. Dispõe sobre o Programa de Gestão e Desempenho - PGD da administração pública federal direta, autárquica e fundacional. **Diário Oficial da União**, seção 1, ano 201º da Independência e 134º da República, Brasília, DF, p. 112, 18 maio 2022. Disponível em: https://x.gd/3DTyB Acesso em: 17 jul. 2025.

BRASIL, Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital. Portaria SGD/MGI n. 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI. **Diário Oficial da União,** seção 1, ed.62, Brasília, DF, p. 92, 30 mar. 2023. Disponível em: https://x.gd/90UbZ Acesso em: 04 jul. 2025.

BRASIL, Ministério da Gestão e da Inovação em Serviços Público. **Guia do Framework de Privacidade e Segurança da Informação**: Programa de Privacidade e Segurança da Informação (PPSI)- Versão 1.1.4. Brasília: MGISP, dez., 2024.

CNJ – Conselho Nacional de Justiça. Instrução Normativa N. 98, De 12 De abril de 2024. **Regulamenta as modalidades de trabalho no âmbito do Conselho Nacional de Justiça**

e dá outras providências. SEI/CNJ - 1820987 - Instrução Normativa Presidência. Disponível em: https://x.gd/rjZrC Acesso em: 08 ago. 2025.

CORO, Marcello Bortolin. **Segurança da informação no trabalho remoto**: estratégias e desafios em um mundo pós-pandemia. Revista Científica Sistemática, v. 14, n. 4, jun., 2024.

GIL, Antônio Carlos. **Como elaborar Projetos de Pesquisas**. 4ª ed. São Paulo: Editora Atlas S/A, 2002.

LUCAS, André do Carmo; SANTOS, Rayane Leite dos. Trabalho remoto na administração pública brasileira: desafios e perspectiva. **Rev. Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v.7.n.4. abr. 2021. Disponível em: https://x.gd/Vxb50 Acesso em: 06 ago. 2025.

OLIVEIRA, Kelly Vanessa. ***Tecnologias Digitais e a prática de home office na pandemia da severe acute respiratory syndrome – coronavirus2*** (Sars-Cov-2) Dissertação [Pós-graduação em Gestão em Organizações Mestrado Profissional em Gestão em Organizações Aprendentes], João Pessoa, 115f., 2021. Disponível em: https://x.gd/V3Zgt Acesso em: 12 ago. 2025.

OLIVEIRA, Josir Alves. **Trabalho remoto para o serviço público desnecessariamente presencial**. Consultor Jurídico, 18 fev. 2024. Disponível em: https://x.gd/mdeXms Acesso em: 06 ago. 2025

PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence; KEMP, Lizzie Coles. ***Security in Computing***. Boston: Addison-Wesley, 2023. 6th. ed.

STALLINGS, William; BROWN, Lavrie.[1945]. **Segurança de computadores**: princípios e práticas. [tradução Arlete Simille Marques]. 2. ed. Rio de Janeiro: Elsevier, 2014. Tradução de: Computer security, 2nd. ed. ISBN 978-85-352-6449-4. Disponível em: https://x.gd/IukHG
Acesso em: 05 jul. 2025.

TOMAZETTI, André Luiz Dias; COSTA, Eliete Cristina Rezende; SILVA, Ismael Deyber Oliveira. **Trabalho remoto no serviço público municipal**: proposta de estratégia para implementação. Repositório da Fundação Getúlio Vargas, Rio de Janeiro, 2022. Disponível em: https://x.gd/vJFIG Acesso em: 05 set. 2025.