Controle 0 do PPSI na Rede Federal: Desafios e Estratégias de Implementação

Autora: Pâmela Hélia de Oliveira / **Orientadora:** Virgínia de Melo Dantas Trinks

RESUMO:

Este artigo analisa a implementação do Controle 0 do Programa de Privacidade e Segurança da Informação (PPSI) no âmbito da Rede Federal de Educação Profissional, Científica e Tecnológica. Criada pela Lei nº 11.892/2008, a Rede ampliou a oferta educacional, mas trouxe também desafios de governança, marcados pela fragmentação de sistemas e pela ausência de padronização. A instituição do PPSI, por meio da Portaria SGD/MGI nº 852/2023, reforçou a urgência de estruturas básicas de governança, sintetizadas no Controle 0, que constitui a base mínima em privacidade e segurança da informação. A pesquisa, de caráter qualitativo e exploratório, foi conduzida a partir de entrevistas com gestores de 16 Institutos Federais, realizadas entre julho e agosto de 2025. Os resultados revelam que, embora o Controle 0 tenha induzido avanços como a atualização de políticas e a criação de Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIRs), sua implementação permanece concentrada em áreas técnicas, assumida como cumprimento formal, e marcada pela ausência de diretrizes claras da alta administração, déficit de pessoal qualificado, acúmulo de funções e limitações orçamentárias. Apesar das fragilidades, práticas inovadoras de baixo custo, como a criação de comitês multidisciplinares, GTs integrados e capacitações EaD, demonstraram potencial para fortalecer a governança. Conclui-se que a efetividade do Controle 0 depende de articulação intersetorial, capacitação contínua, investimentos adequados e valorização dos recursos humanos. O estudo contribui para levantar a pauta da privacidade e da segurança da informação na Rede Federal, fortalecendo o debate coletivo e o papel do FORTI como agente estratégico para a consolidação da governança em segurança da informação e privacidade.

Palavras-chave: Controle 0, PPSI, Rede Federal.

1. INTRODUÇÃO

A criação dos Institutos Federais, consolidada pela Lei nº 11.892/2008, promoveu uma transformação significativa na educação profissional e tecnológica do Brasil. A legislação integrou antigas escolas técnicas, escolas agrotécnicas, Centros Federais de Educação Tecnológica (Cefets) e escolas vinculadas a universidades federais, dando origem a instituições multicampi e pluricurriculares, com autonomia administrativa, patrimonial e pedagógica (BRASIL, 2008).

Essa transformação resultou na formação da Rede Federal de Educação Profissional, Científica e Tecnológica, composta por 38 Institutos Federais, 2 Cefets, a Universidade Tecnológica Federal do Paraná (UTFPR), 22 escolas técnicas vinculadas a universidades federais e o Colégio Pedro II. Atualmente, a Rede Federal conta com mais de 680 unidades, atendendo a mais de 1,6 milhão de estudantes em cursos presenciais e a distância (MEC, 2025). Sua configuração territorial e socialmente capilarizada permite à Rede atuar como agente estratégico na interiorização do ensino, no enfrentamento das desigualdades educacionais e na consolidação de uma educação voltada à cidadania, à inovação e ao desenvolvimento regional (BRASIL, 2025a).

Desde sua constituição, a Rede Federal carrega modos de atuação e culturas organizacionais distintas, herdadas das instituições que a originaram. As escolas técnicas, agrotécnicas e Cefets possuem formas próprias de gerenciar informações acadêmicas, administrativas e de pessoal, muitas vezes baseadas em soluções locais ou sistemas isolados. Com a criação da Rede, não se estabeleceu, de imediato, um sistema unificado de governança da informação capaz de contemplar a diversidade e a escala dessa nova estrutura institucional.

Foi nesse contexto que surgiu o Sistema Unificado de Administração Pública (SUAP), desenvolvido inicialmente pelo Instituto Federal do Rio Grande do Norte (IFRN), como uma tentativa de integrar os sistemas de gestão acadêmica, administrativa e de pessoal. No entanto, sua adoção não ocorreu de forma integral e homogênea entre os institutos. Algumas instituições utilizam a versão referencial do SUAP, alinhada aos desenvolvimentos conduzidos pelo IFRN; outras, embora baseadas no mesmo sistema, realizam manutenções e personalizações autônomas; e há ainda aquelas que adotam soluções próprias ou terceirizadas (RODRIGUES; LIMA, 2024).

Esse cenário da Rede Federal apresenta uma pluralidade de ambientes tecnológicos, com diferentes níveis de integração, maturidade e segurança na gestão de dados. Embora essa diversidade reflita a autonomia administrativa prevista em lei, evidencia também a ausência de um modelo comum de governança da informação — uma problemática amplamente identificada na literatura sobre gestão pública digital. A fragmentação institucional e a falta de padronização dificultam a criação de estruturas de governança, comprometendo a eficácia regulatória e a accountability no setor público (FILGUEIRAS; LUI, 2023).

A falta de padronização compromete a capacidade institucional de manter a eficiência administrativa e a resiliência organizacional, uma vez que estruturas fragmentadas de sistemas geram retrabalho, duplicidade de dados e dificultam a integração (RODRIGUES; LIMA, 2024). Além disso, a ausência de um modelo unificado impõe desafios significativos à segurança da informação: a fragmentação de sistemas e a falta de governança integrada elevam os riscos de vazamento de dados, comprometem a integridade da informação e dificultam a implementação de controles consistentes e efetivos (CARVALHO, 2019).

Paralelamente, a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) trouxe novos desafios à conformidade regulatória. A proteção dos dados pessoais tornou-se uma exigência legal, demandando a formalização de políticas, a nomeação de responsáveis e o estabelecimento de processos contínuos de adequação. A ausência de um modelo nacional integrado de governança da informação, somada à diversidade de sistemas administrativos nas instituições federais, impõe obstáculos adicionais à implementação plena da LGPD (CARVALHO, 2019; FACHIN, 2022).

Com o intuito de enfrentar esses desafios e elevar a maturidade institucional no tratamento da informação, o Governo Federal instituiu, por meio da Portaria SGD/MGI nº 852/2023, o Programa de Privacidade e Segurança da Informação (PPSI), coordenado pela Secretaria de Governo Digital (SGD). O programa orienta os órgãos e entidades da administração pública federal direta, autárquica e fundacional, integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), na adoção de medidas estruturadas de segurança da informação e privacidade (BRASIL, 2023).

O PPSI é composto por um conjunto de projetos, metodologias e controles organizados em cinco áreas temáticas — governança, maturidade, metodologia, pessoas e tecnologia — e estruturado em eixos como o Framework de Privacidade e Segurança da Informação, o Centro Integrado de Segurança Cibernética (CISC Gov.br) e o Centro de Excelência em Privacidade e Segurança (BRASIL, 2023b).

Nesse contexto, o Controle 0 constitui o alicerce do programa, estabelecendo os elementos fundamentais da governança, como a designação de responsáveis institucionais, a criação de comitês e equipes técnicas especializadas, além da formalização de políticas e diretrizes organizacionais. Sua implementação é essencial para garantir a conformidade com a LGPD e promover avanços nos níveis de maturidade em privacidade e segurança da informação no setor público (BRASIL, 2022a).

Em 2024, o Tribunal de Contas da União (TCU), por meio do Acórdão nº 2387/2024 – Plenário, reforçou a importância da implementação do PPSI ao constatar, por meio de auditoria operacional, que a maioria dos órgãos e entidades auditadas ainda apresentava níveis iniciais de maturidade em segurança da informação. Apenas 6% das instituições demonstraram maturidade intermediária, e nenhuma havia implementado integralmente os 18 controles essenciais do CIS v8[1]. O relatório destacou a adoção do Controle 0 como medida mínima necessária para estruturar a governança da informação, recomendando ações coordenadas pela Secretaria de Governo Digital (BRASIL, 2024).

[1] O Center for Internet Security Controls (2021) v8 (CIS v8) , publicado em 2021 pelo Center for Internet Security, é um framework internacionalmente reconhecido de boas práticas em segurança da informação, composto por 18 controles essenciais.

A elaboração deste artigo surgiu da necessidade de compreender como a estrutura de governança proposta pelo PPSI, especialmente por meio do Controle 0, tem sido implementada nas instituições que compõem a Rede Federal. Importa ressaltar que, embora os indicadores de maturidade institucional como o iPriv e o iSeg — previstos no modelo de avaliação do PPSI — forneçam uma visão estatística da adesão aos controles, esta pesquisa busca compreender as dimensões práticas e contextuais que essas métricas não capturam.

Assim, o caráter qualitativo da investigação permite aprofundar a análise dos fatores que condicionam ou favorecem a implementação do Controle 0 no cotidiano institucional das Instituições que compõem a Rede Federal. A pesquisa teve por objetivo identificar o estágio atual de implementação da governança, mapear boas práticas, reconhecer obstáculos enfrentados e reunir recomendações que possam ser compartilhadas e reaproveitadas pelas instituições da Rede Federal. O estudo pretende contribuir para o fortalecimento da cultura de proteção de dados e segurança da informação, considerando os desafios que emergem da descentralização de sistemas, da diversidade institucional e da ausência de padronização normativa.

2. REFERENCIAL TEÓRICO

Transformação Digital e Governança na Administração Pública Brasileira

A transformação digital no setor público brasileiro tem sido impulsionada pela aceleração global das tecnologias da informação e comunicação (TICs), como computação em nuvem, inteligência artificial, big data, internet das coisas, entre outros. Mais do que avanços técnicos, essas tecnologias demandam a revisão de processos de gestão, de tomada de decisão e da relação entre Estado e cidadão. Nesse contexto, a abertura de dados governamentais, conforme destacam Janssen et al. (2012), impõe novos desafios à administração pública, exigindo não apenas infraestrutura tecnológica, mas também capacidade institucional de adaptação, governança e mecanismos de participação social.

Assim, a transformação digital não se limita à adoção de novas tecnologias, mas está intrinsecamente condicionada à capacidade institucional do Estado de promover integração e coordenação entre diferentes órgãos. Como destacam Filgueiras e Palotti (2020), as escolhas organizacionais e arranjos institucionais podem tanto impulsionar avanços quanto reforçar bloqueios, resultando em processos marcados pela fragmentação, pela descontinuidade administrativa e pela dificuldade de consolidar políticas digitais de longo prazo. Essa perspectiva evidencia que a transformação digital, mais do que uma questão tecnológica, constitui um desafio de governança.

A pesquisa das autoras Macedo e Dufloth (2025) demonstra que as barreiras à interoperabilidade no setor público não se restringem à esfera técnica, mas envolvem normas, estruturas e comportamentos enraizados. Esses elementos revelam limitações

institucionais e organizacionais que comprometem a formação de capacidades adequadas para sustentar projetos estratégicos de digitalização. Nesse sentido, a ausência de inovação na gestão e na valorização dos recursos humanos em tecnologia da informação pode ser interpretada como parte desse cenário, fragilizando a governança e a implementação e consolidação de iniciativas digitais.

As autoras também ressaltam que a falta de padronização e a desarticulação tecnológica resultam em barreiras significativas à interoperabilidade. A coexistência de diferentes soluções e a ausência de compatibilidade entre sistemas produzem ilhas de informação que fragilizam a gestão integrada e a coordenação interinstitucional. Para as autoras, esse quadro afeta não apenas a formulação de políticas públicas consistentes, mas também expõe o governo a riscos de redundância, inconsistência e perda de confiabilidade dos dados.

Para a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) a maturidade institucional em governo digital não se resume à digitalização de processos, mas envolve a construção de um ambiente organizacional orientado por dados, com capacidade de coordenar ações multissetoriais, garantir a proteção de direitos e responder a demandas sociais complexas. Nesse contexto, a ausência de uma governança digital estruturada e consolidada limita a efetividade das políticas públicas e amplia as desigualdades no acesso aos serviços estatais (OCDE, 2022).

O Tribunal de Contas da União (TCU) aponta que a governança de tecnologia da informação e comunicação - TIC ainda é incipiente na maioria dos órgãos públicos. Os achados indicam baixa maturidade em planejamento estratégico de TI, insuficiência de comitês de governança e carência de políticas consolidadas de gestão da informação (TCU, 2018). Isso compromete diretamente a implementação de serviços digitais eficientes, seguros e orientados ao cidadão.

Entre os marcos normativos e estratégicos mais relevantes para a consolidação da governança digital no setor público brasileiro, destacam-se a Estratégia de Governo Digital 2020–2022, o Plano Nacional de Internet das Coisas (IoT), a criação da Autoridade Nacional de Proteção de Dados (ANPD), o Programa de Gestão Estratégica de TIC do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação) e a Lei nº 14.129/2021, conhecida como Lei do Governo Digital. Esses instrumentos visam estruturar um ecossistema de transformação digital centrado no usuário, orientado por dados e sustentado por princípios de interoperabilidade, segurança, privacidade e inovação (BRASIL, 2020; BRASIL, 2021). No entanto, a efetividade dessas iniciativas depende de fatores como liderança institucional, cultura organizacional, capacitação técnica e disponibilidade orçamentária, além da articulação entre os diversos entes federativos e setores da administração pública.

Ainda nesse cenário, a transparência pública, a proteção de dados e a segurança da informação tornam-se dimensões mais desafiadoras. A promulgação da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — impôs

obrigações adicionais às instituições públicas, como o dever de nomear encarregados, mapear fluxos de dados e implementar políticas de privacidade e segurança (DONEDA, 2019). O cumprimento dessas exigências, no entanto, depende de um grau de governança e maturidade institucional que ainda está em construção, conforme analisado por Bergamini e Cristóvam (2021), especialmente no que tange à adaptação dos órgãos públicos às exigências legais e à gestão estratégica da informação.

Segundo o Acórdão nº 1.384/2022 – Plenário do TCU, apenas uma pequena parcela dos órgãos auditados demonstrou ações concretas para atender às diretrizes da LGPD, sobretudo no que se refere à estruturação de comitês, políticas formais e designação de encarregados. O TCU alerta que a maioria das instituições ainda está em estágio inicial de conformidade com a legislação, o que representa um risco significativo de violação de direitos e ineficiência administrativa (TCU, 2022).

Além disso, a transparência — considerada pilar da democracia e da integridade pública — depende fortemente da qualidade da gestão informacional (SOUZA; PRODEL JUNIOR, 2023).. A ausência de dados abertos, atualizados, acessíveis e confiáveis compromete tanto o controle social quanto o monitoramento de políticas públicas (PIMENTEL; MOURA, 2021). A publicação de informações sem critérios padronizados pode, paradoxalmente, gerar desinformação, opacidade e perda de credibilidade institucional.

O Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023, surgiu como resposta do governo federal às recomendações da LGPD, do TCU e da OCDE. Com uma abordagem integrada e baseada em cinco dimensões — governança, maturidade, metodologia, pessoas e tecnologia — o PPSI orienta a administração pública na institucionalização de políticas e estruturas voltadas à segurança da informação e a proteção de dados pessoais (BRASIL, 2025).

O desafio da implementação do PPSI, entretanto, não está apenas na definição de diretrizes, mas na superação de barreiras organizacionais históricas: baixa cultura de conformidade, falta de coordenação entre setores, resistência à mudança, escassez de pessoal técnico e ausência de incentivos institucionais. A efetivação do Controle 0 — que trata da estrutura básica de governança — é vista como ponto de partida para o avanço da maturidade institucional nesse campo (TCU, 2024).

Fragmentação Sistêmica na Rede Federal de Educação Profissional, Científica e Tecnológica

Nesse panorama desafiador, a Rede Federal de Educação Profissional, Científica e Tecnológica representa um recorte emblemático das possibilidades da transformação digital no setor público. Constituída por instituições com culturas e sistemas herdados de diferentes origens — como escolas agrotécnicas, Cefets e escolas técnicas — a Rede

enfrenta dificuldades específicas na unificação de sistemas, na adoção de políticas comuns de governança da informação.

Tal contexto representa um microcosmo dos desafios enfrentados pela administração pública federal, mas com maior complexidade, dada a amplitude e diversidade das instituições envolvidas. Como destacam Rodrigues e Lima (2024), os Institutos Federais operam com uma sobreposição de plataformas e bancos de dados — muitos deles herdados ou adaptados regionalmente, sem integração efetiva com os sistemas de outras unidades — o que acarreta baixa interoperabilidade, retrabalho e inconsistência de dados. A próxima seção está dedicada à análise da fragmentação sistêmica na Rede Federal, onde tais limites se manifestam de forma ainda mais evidente.

A Rede Federal é formada por um conjunto diversificado de instituições federais com variadas naturezas jurídicas e perfis históricos. Ela inclui 38 Institutos Federais de Educação, Ciência e Tecnologia, que atuam de forma pluricurricular e multicampi, oferecendo desde formação inicial e continuada até ensino técnico de nível médio, cursos superiores de graduação (tecnológica, bacharelados e licenciaturas) e pós-graduação — tudo isso articulado com ensino, pesquisa e extensão, sob autonomia administrativa, patrimonial, financeira e didático-pedagógica (BRASIL, 2025).

Fazem parte também a Universidade Tecnológica Federal do Paraná (UTFPR), dois Centros Federais de Educação Tecnológica (o Cefet-RJ e o Cefet-MG), além de escolas técnicas vinculadas a universidades federais e o Colégio Pedro II — instituições estas que, ainda que mantenham vínculos históricos distintos, integram organicamente a REPCT. Essa composição heterogênea, que inclui Autarquias federais com diferentes trajetórias administrativas como escolas agrotécnicas, Cefets históricos, institutos multicampi, centros técnicos e colégio tradicional, reflete a expansão e interiorização da educação profissional e tecnológica, garantindo presença em múltiplos níveis de ensino e em praticamente todos os estados brasileiros, fortalecendo a capilaridade da oferta e, ao mesmo tempo, apresentando desafios para a gestão integrada e a consolidação de políticas institucionais únicas.

A criação dos Institutos Federais, embora tenha fortalecido a interiorização e a capilaridade da oferta educacional, também resultou em uma estrutura organizacional heterogênea, caracterizada por fragmentação sistêmica que ainda impõe desafios à gestão integrada e à consolidação de políticas institucionais unificadas (OLIVEIRA; SOUZA, 2020).

Nessa perspectiva, os Institutos Federais se configuram como autarquias multicampi e pluricurriculares, dotadas de autonomia administrativa, financeira e didático-pedagógica, articulando-se em torno de uma reitoria e conselhos superiores, e lidando, em seu cotidiano, com as distintas trajetórias históricas de suas unidades de origem, o que revela singularidades na governança.

De acordo com Oliveira e Souza (2020), os Institutos Federais foram constituídos a partir de instituições com perfis administrativos e técnicos distintos. Essa diversidade institucional resultou na manutenção de sistemas próprios de gestão por campus. Como demonstram Rodrigues e Lima (2024), essa autonomia tecnológica levou à adoção de diferentes plataformas de gestão, como o SUAP, o SIG-UFRN e sistemas desenvolvidos internamente.

Além disso, Souza (2017) evidencia que a governança de TI nas Instituições Federais de Ensino Superior apresenta níveis de eficiência variados, resultantes das estruturas organizacionais divergentes. Essa heterogeneidade institucional torna impraticável a padronização de sistemas e reforça a falta de integração tecnológica entre instituições federais — ampliando os desafios da interoperabilidade. A fragmentação institucional das IFES impacta diretamente a segurança da informação, os mecanismos de controle e a capacidade de rastreabilidade de dados — elementos essenciais para a conformidade com a LGPD, transparência pública e governança integrada.

Assim, a fragmentação compromete a consolidação de dados institucionais, gera retrabalho e limita a interoperabilidade, exigindo esforços adicionais por parte das equipes técnicas locais. A pesquisa realizada pelos autores Rodrigues e Lima (2024), baseada na percepção de usuários do IFAM e do IFRO, evidencia que, além das dificuldades operacionais, a diversidade de sistemas impacta negativamente a eficiência administrativa e a formulação de políticas públicas integradas na Rede Federal.

É possível observar a verossimilhança quando Carneiro (2023), ao analisar a implementação da LGPD no âmbito do Comando do Exército, destaca que a efetividade das políticas de proteção de dados depende diretamente do engajamento da alta administração e da criação de modelos de governança que articulem equipes multidisciplinares. Embora trate de um contexto distinto, suas conclusões revelam que a ausência de liderança institucional e de mecanismos claros de coordenação tende a aprofundar a fragmentação e comprometer a maturidade em segurança da informação. A experiência analisada aponta que mesmo em instituições altamente hierarquizadas, a conformidade com a LGPD requer não apenas recursos técnicos, mas sobretudo uma estratégia de governança capaz de integrar setores, superar resistências culturais e consolidar práticas de proteção de dados.

O relatório de auditoria operacional realizado pelo TCU (2024) identificou que a maioria das instituições da Rede Federal possui baixos níveis de maturidade em segurança da informação. As principais deficiências apontadas dizem respeito à inexistência de políticas formalizadas, ausência de responsáveis nomeados e desarticulação entre os setores de TI e as instâncias de gestão superior.

No mesmo sentido, a fiscalização do TCU (2025) sobre a adequação à Lei Geral de Proteção de Dados revelou que grande parte das organizações federais ainda se

encontra nos níveis iniciais de conformidade, carecendo de políticas de privacidade publicadas, de nomeação de encarregados e de mecanismos para atender aos direitos dos titulares. Essa situação evidencia que a governança em privacidade e proteção de dados ainda não está institucionalizada, permanecendo como um desafio estratégico a ser conduzido pela alta gestão, em articulação com as unidades de controle interno, para garantir a integração entre segurança da informação, transparência e proteção da privacidade.

No âmbito dos Institutos Federais, um dos espaços que tem buscado preencher esse vazio da governança da informação é o Fórum de Gestores de Tecnologia da Informação (FORTI), instância colegiada do Conselho Nacional das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (CONIF). O FORTI articula gestores de TI dos diversos institutos, promovendo o intercâmbio de experiências e a proposição de estratégias conjuntas para desafios comuns (CONIF, 2025).

Apesar de seu potencial articulador, o FORTI ainda não dispõe de estrutura normativa ou executiva que lhe permita coordenar de forma vinculante às ações de governança digital em âmbito nacional. Conforme descrito no portal oficial, a capacidade de promover transformações estruturais depende da adesão voluntária das instituições e do apoio político das reitorias, o que limita sua efetividade enquanto órgão indutor de políticas unificadas de tecnologia da informação (FORTI, 2025).

Em grande parte das instituições públicas, os profissionais de Tecnologia da Informação acumulam múltiplas funções, enquanto a defasagem salarial e a falta de perspectivas de carreira dificultam a retenção desses especialistas, que frequentemente migram para a iniciativa privada. O Tribunal de Contas da União (TCU, 2023) identificou que a desproporção no quantitativo de servidores de TI, o envelhecimento do quadro e a evasão de analistas têm limitado a capacidade operacional dos órgãos e comprometido a agenda de modernização digital. Esse cenário revela que a baixa capacidade de retenção de profissionais e a insuficiência na estruturação da governança de TI caminham juntas, fragilizando a consolidação de mecanismos para a proteção de dados e a segurança da informação no setor público.

À luz dessas constatações, observa-se que a governança de TI na Administração Pública ainda enfrenta entraves estruturais que impactam diretamente a implementação de iniciativas de transformação digital e de proteção de dados. É nesse contexto que programas institucionais, como o Programa de Privacidade e Segurança da Informação (PPSI), ganham relevância, ao oferecer um referencial de práticas e controles capazes de induzir maior padronização, fortalecer a cultura de segurança e alinhar a gestão de dados às exigências legais. Frente a esse cenário, torna-se imprescindível compreender em que medida o Programa de Privacidade e Segurança da Informação (PPSI), e em particular o Controle 0, pode contribuir para superar tais desafios, constituindo o foco do capítulo seguinte.

Controle 0 do Programa de Privacidade e Segurança da Informação (PPSI) no âmbito da Rede Federal

A crescente preocupação com a proteção de dados pessoais e a segurança da informação na administração pública motivou a formulação do Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023. Trata-se de uma resposta do governo às fragilidades identificadas em auditorias do TCU e em estudos sobre a baixa maturidade institucional, buscando orientar os órgãos federais na adoção de medidas estruturadas e promover uma cultura organizacional voltada à conformidade, à integridade e à proteção de dados sensíveis. Vinculado à Secretaria de Governo Digital (SGD), o programa se organiza em cinco áreas temáticas: governança, maturidade, metodologia, pessoas e tecnologia, tendo como eixos o Framework de Privacidade e Segurança da Informação, o Centro Integrado de Segurança Cibernética (CISC Gov.br) e o Centro de Excelência em Privacidade e Segurança. Seu desenho é progressivo, baseado em níveis de maturidade e controles escalonados (BRASIL, 2023).

O Controle 0, denominado “Estrutura Básica de Governança em Privacidade e Segurança da Informação”, constitui o ponto de partida do PPSI. Ele reúne sete medidas mínimas obrigatórias: nomeação do encarregado de dados (DPO); instituição de Comitê de Privacidade e Segurança da Informação; elaboração de políticas de privacidade e segurança; criação de planos específicos; definição de procedimentos de resposta a incidentes; integração com a gestão de riscos e controles internos; e comunicação transparente com a sociedade por meio de canais oficiais. Sem essa base, qualquer tentativa de avançar em controles técnicos ou processos mais sofisticados tende a se fragilizar (BRASIL, 2023).

O Tribunal de Contas da União, por meio do Acórdão nº 2387/2024 – Plenário, reforçou a centralidade do Controle 0, ao demonstrar que apenas 6% dos órgãos federais apresentavam maturidade intermediária em privacidade e segurança e nenhuma instituição havia implementado integralmente os controles essenciais do CIS v8. Como resposta, recomendou-se a adoção prioritária do Controle 0 como alicerce para o avanço das demais medidas (TCU, 2024).

Mais do que um checklist operacional, o Controle 0 representa a institucionalização da governança, obrigando a alta administração a assumir responsabilidades formais e integrando a proteção de dados às rotinas organizacionais. A própria Secretaria de Governo Digital assinala que a efetividade do PPSI depende do cumprimento dessa estrutura mínima, que garante sustentabilidade aos demais níveis de maturidade (BRASIL, 2022; BRASIL, 2023).

Entretanto, sua implementação na Rede Federal de Educação Profissional, Científica e Tecnológica encontra desafios expressivos. Em muitos institutos, a responsabilidade permanece concentrada nas áreas de TI, o que desconsidera o caráter transversal da governança em privacidade e segurança. A institucionalização de

práticas deliberativas e colegiadas, com participação plural de reitoria, pró-reitorias, áreas finalísticas, jurídicas e de controle interno, é fundamental para decisões integradas. O Comitê de Governança de Dados do MCTI, criado pela Portaria nº 6.533/2022, ilustra como instâncias colegiadas podem fortalecer políticas de dados e segurança de forma transversal (BRASIL, 2022a).

Além disso, auditorias recentes do TCU com 382 organizações federais revelaram que 76,7% das entidades avaliadas estavam nos graus inexpressivo ou inicial de adequação à LGPD; apenas 45% haviam concluído as etapas de preparação e 77% não tinham mapeado todas as categorias de titulares com os quais se relacionam (TCU, 2020). Esses achados confirmam lacunas de governança, processos e capacidade organizacional que comprometem a implementação do Controle 0.

No âmbito da Rede Federal, o quadro se agrava pela escassez de profissionais especializados, pelo acúmulo de funções e pela dificuldade de retenção de servidores qualificados devido à concorrência com o setor privado. Muitos institutos carecem de planos de capacitação específicos sobre privacidade e segurança, o que restringe a difusão da cultura de proteção de dados a um círculo reduzido de técnicos de TI (CONIF,2025). Como reforça Pilói (2025), a conformidade com a LGPD no setor público depende diretamente do engajamento da alta gestão e da formação contínua dos servidores, elementos decisivos para fortalecer a confiança da sociedade nas instituições.

Outro desafio recorrente é a indefinição institucional sobre a posição do PPSI: em diversas instituições, ainda não está claro se os comitês e unidades técnicas devem se vincular à TI, à gestão estratégica ou à controladoria, o que fragiliza a legitimidade e efetividade das ações. Sem liderança institucional clara e metas factíveis, o risco é de que o Controle 0 permaneça apenas no plano documental, sem se traduzir em práticas de governança sustentáveis.

Por fim, a implementação precisa conciliar privacidade e transparência na Administração Pública. A literatura especializada alerta que não há contradição automática entre LGPD e LAI; ao contrário, recomenda-se sua aplicação conjunta, com medidas como anonimização de dados e justificativas proporcionais de sigilo quando estritamente necessárias (BATAGLIA; LEMOS; FARRANHA, 2020). A jurisprudência recente do STJ tem reforçado esse equilíbrio, afastando usos abusivos da LGPD como obstáculo genérico à publicidade e ao controle social (STJ, 2024).

Assim, o Controle 0 faz sentido no conjunto deste artigo porque materializa, no plano institucional, a tentativa de superar os problemas recorrentes já identificados nos capítulos anteriores: fragmentação de sistemas, baixa padronização de processos, insuficiência de políticas unificadas e lacunas de governança na Rede Federal. Ao exigir a designação de responsáveis, a criação de comitês, a publicação de políticas e a integração com a gestão de riscos, o Controle 0 oferece a base mínima para transformar recomendações normativas em práticas de governança concretas. Sua

adoção, embora desafiadora, representa um ponto de inflexão: é o elo entre a trajetória histórica de heterogeneidade institucional da Rede Federal e a possibilidade de construção de um modelo de governança mais integrado, maduro e orientado à proteção de dados e à segurança da informação.

3. METODOLOGIA

Este estudo adota uma abordagem qualitativa, de caráter exploratório, com o propósito de analisar, em profundidade, as percepções dos gestores da Rede Federal de Educação Profissional, Científica e Tecnológica acerca da implementação do Controle 0 do Programa de Privacidade e Segurança da Informação (PPSI). De acordo com Denzin e Lincoln (2006), a pesquisa qualitativa é apropriada para investigar fenômenos complexos inseridos em contextos institucionais dinâmicos, pois permite captar a multiplicidade de sentidos atribuídos pelos sujeitos, considerando suas experiências, interações e os condicionantes organizacionais que influenciam suas práticas.

A escolha pela vertente qualitativa justifica-se pela natureza do objeto de estudo: a governança da privacidade e da segurança da informação em instituições públicas. Conforme Minayo (2014), tal abordagem é especialmente indicada quando se busca compreender as estruturas simbólicas, os valores e os sentidos atribuídos pelos atores sociais às suas ações e decisões. Neste caso, o foco recai sobre os processos de implementação do Controle 0 do PPSI, em sua dimensão política, técnica e institucional.

A etapa de coleta de dados exigiu um esforço meticuloso de identificação e contato com os responsáveis pelas áreas de Tecnologia da Informação, Segurança da Informação ou governança de dados pessoais nos 38 Institutos Federais que compõem a Rede. Inicialmente, elaborou-se o mapeamento da Rede Federal por meio da consulta à lista oficial do Ministério da Educação (MEC) (BRASIL, 2025). Em seguida, os portais eletrônicos das instituições foram acessados individualmente com o objetivo de localizar os contatos institucionais de diretores e coordenadores de TI, assim como canais alternativos, como WhatsApp e redes sociais institucionais.

O convite à participação na pesquisa foi padronizado e encaminhado por e-mail institucional, contendo uma apresentação da pesquisadora, os objetivos do estudo (Anexo I), alinhado às diretrizes do Controle 0 do PPSI, o roteiro da entrevista e o Termo de Consentimento Livre e Esclarecido (TCLE) - Anexo II. Para maximizar a taxa de retorno, os convites foram também reforçados por mensagens diretas via aplicativos de comunicação. A estratégia de contato multicanal está alinhada ao que Yin (2015) chama de “triangulação operacional”, reforçando a legitimidade e o alcance da investigação em contextos institucionais.

As entrevistas foram realizadas individualmente por videoconferência, via Google Meets, com duração média de 30 minutos. Para respeitar a disponibilidade dos

gestores, os agendamentos foram flexíveis e não houve gravação em áudio ou vídeo, sendo as informações registradas por meio de anotações sistemáticas durante as falas.

A amostra foi intencional, formada por gestores com atribuições formais ligadas à implementação do PPSI. Essa escolha buscou garantir que os participantes tivessem relação direta com o objeto de estudo, o que, segundo Bogdan e Biklen (1994), aumenta a relevância dos dados em pesquisas voltadas à realidade institucional.

Como resultado desse esforço, foi possível organizar agendas com 16 Institutos Federais, cujas entrevistas ocorreram entre julho e agosto de 2025, sendo as respostas analisadas de forma agregada, sem identificação nominal das instituições participantes.

Mesmo entre os institutos que não puderam participar da entrevista, alguns retornos contribuíram para o entendimento do cenário investigado. Um dos gestores, por exemplo, respondeu informando que sua equipe de TI era composta por apenas dois técnicos e que a instituição não realizava concursos há mais de uma década, o que impossibilitava qualquer avanço na pauta de proteção de dados.

As entrevistas seguiram um roteiro semiestruturado, previamente validado pela orientadora da pesquisa e construído com base nos sete eixos do Controle 0 do Framework PPSI. A opção por entrevistas semiestruturadas é coerente com o que defendem Meuser e Nagel (2009), pois permite explorar o conhecimento tácito e especializado dos sujeitos em posições técnicas e decisórias, captando nuances institucionais que escapariam a métodos puramente quantitativos.

O instrumento de coleta contemplou dois blocos principais: (1) verificação da implementação das medidas do Controle 0 — como a nomeação de encarregado, existência de comitês, políticas e planos formais —; e (2) percepção dos gestores sobre os desafios, fragilidades institucionais, ações exitosas e sugestões de aprimoramento. Essa estrutura possibilita tanto a coleta de informações factuais quanto a apreensão de sentidos subjetivos e estratégicos (GIL, 2017).

Por fim, os dados foram organizados em uma tabela comparativa e submetidos à análise temática, conforme proposta de Braun e Clarke (2006). Essa técnica envolve a identificação, codificação e agrupamento de padrões de conteúdo, permitindo a construção de categorias analíticas que dialogam com o referencial teórico do estudo. O processo de análise foi conduzido de forma iterativa e reflexiva, com retornos frequentes ao corpus empírico, conforme orienta Bardin (2016), assegurando rigor e coerência interpretativa.

4. RESULTADOS E DISCUSSÕES

Esta seção apresenta os principais achados da pesquisa a partir da análise das entrevistas realizadas com gestores da Rede Federal de Educação Profissional, Científica e Tecnológica, responsáveis ou diretamente envolvidos com a implementação do Programa de Privacidade e Segurança da Informação (PPSI), em especial no que se

refere ao Controle 0 – Estrutura Básica de Gestão. Os resultados foram organizados em sub seções temáticas, construídas a partir das falas dos entrevistados e da análise das recorrências observadas. As categorias emergentes foram interpretadas à luz do referencial teórico adotado, buscando conectar a experiência dos gestores com os desafios estruturais de governança no campo da segurança da informação e da privacidade de dados na administração pública.

4.1 - Análise da implementação das medidas do Controle 0

A verificação da implementação das medidas do Controle 0 foi realizada a partir das entrevistas conduzidas com gestores da Rede Federal, tomando como referência o roteiro estruturado que contemplava sete dimensões essenciais: a nomeação da autoridade máxima de TI, a designação do Gestor de Segurança da Informação, a atribuição de responsabilidade à Unidade de Controle Interno, a constituição de Comitês de Segurança da Informação, a formação de Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), a elaboração de Políticas de Segurança da Informação (POSIN) e a nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO).

A análise revelou que a maioria das instituições já nomeou formalmente uma autoridade máxima de TI, todas vinculadas às Diretorias de Tecnologia da Informação (DTI). Mais do que um dado administrativo, esse resultado evidencia que a Rede Federal, em grande parte, não compreendeu o desenho do framework do PPSI, ao atribuir às DTIs a responsabilidade central de sua implementação. Tal escolha desloca para o campo técnico o que deveria ser assumido como uma pauta estratégica da alta administração, capaz de articular governança, integridade e proteção de dados em nível institucional. Essa interpretação corrobora as críticas de Doneda (2019), que adverte para os riscos de reduzir a proteção de dados a uma dimensão meramente tecnológica, em vez de consolidá-la como tema transversal de governança pública.

No que se refere ao Gestor de Segurança da Informação (GSI), verificou-se que pouco mais da metade das instituições declarou possuir essa função formalizada (62,5%), enquanto um terço afirmou não contar com qualquer designação específica (37,5%). Entre as que possuem GSI, a vinculação institucional revelou grande heterogeneidade: em alguns casos, o gestor está alocado em áreas tradicionais de TI, em outros no Gabinete, em unidades de Gestão de Dados ou até mesmo em setores de Integridade e Controle Interno. Também foram relatadas situações de improviso, como a designação de um “servidor interessado no assunto, sem função gratificada”, ou a atribuição cumulativa a coordenadores já sobrecarregados. Esse achado mostra que o peso da responsabilidade recai desproporcionalmente sobre servidores, que acumulam funções, reforçando a percepção de que o PPSI tem sido tratado como um “trabalho extra” em vez de uma pauta estratégica da alta administração.

Tal indefinição pode comprometer a consolidação de uma governança consistente em segurança da informação, pois a responsabilidade tende a recair sobre

indivíduos sem respaldo institucional, resultando em baixa capacidade de articulação e fragilidade de legitimidade. Esse quadro confirma a análise de Macedo e Dufloth (2025), segundo a qual a ausência de valorização dos recursos humanos e de inovação na gestão cria barreiras institucionais à transformação digital, especialmente no campo da proteção de dados e da segurança da informação. Mais do que uma lacuna operacional, trata-se de um desafio de governança: sem a definição clara do papel do GSI, o framework do PPSI não encontra sustentação prática, permanecendo dependente de arranjos precários e da disponibilidade individual de servidores.

Em relação à definição da Unidade de Controle Interno (UCI), as entrevistas revelaram uma dificuldade recorrente de compreensão sobre o que de fato configuraria essa unidade, com debates reincidentes acerca de sua vinculação — se deveria estar na Auditoria Interna, na área de Governança e Riscos, ou em setores administrativos como Planejamento e Gabinete. A maioria das instituições declarou possuir algum tipo de designação (68,7%), mas em arranjos bastante heterogêneos, chegando a casos atípicos como a atribuição a docentes de informática em cargo comissionado. Essa indefinição conceitual refletiu-se na falta de clareza quanto ao papel da UCI, resultando na nomeação de responsáveis que, em muitos casos, apresentaram pouca ou nenhuma atuação prática, havendo inclusive situações de recusa explícita por parte de auditores em assumir a atribuição. Tal cenário fragiliza a legitimidade da governança em privacidade e segurança, justamente porque a UCI deveria se consolidar como elo de controle e confiança no processo de implementação. O desalinhamento entre a proposta do framework do PPSI — que prevê uma atuação estruturada e integrada do controle interno — e sua operacionalização nas instituições confirma a análise de Bergamini e Cristóvam (2021), segundo a qual a administração pública enfrenta entraves recorrentes para institucionalizar mecanismos de governança de dados de forma clara e consistente.

No que se refere às ETIRs, observou-se um cenário de implementação ainda bastante incipiente. Dos 16 institutos que responderam à questão, 9 (56,2%) declararam possuir ETIR, enquanto 6 (37,5%) afirmaram não contar com qualquer estrutura e 1 (6,2%) relatou estar em fase de implantação. Entre os que responderam positivamente, entretanto, a análise qualitativa revela que a existência da ETIR não significa, necessariamente, atuação estruturada: em cerca de um terço dos casos (33,3% das respostas positivas), as equipes foram criadas ou reformuladas apenas após a implementação do PPSI, evidenciando um movimento reativo e motivado por exigências normativas.

Esse dado revela que a adesão ao Controle 0, no aspecto das ETIRs, tem sido majoritariamente passiva, derivada da indução do PPSI e não de uma decisão estratégica da alta administração. Muitos gestores relataram que, mesmo quando a ETIR existe formalmente, sua atuação é restrita, com responsabilidades delegadas a servidores da TI sem capacitação específica, o que compromete a efetividade. Essa constatação confirma a análise de Carvalho (2019), segundo a qual a ausência de

equipes estáveis e treinadas aumenta a vulnerabilidade institucional frente a incidentes cibernéticos e expõe dados sensíveis a riscos elevados.

O fato de parte das ETIRs ter sido constituída “após o PPSI” mostra o papel indutor do programa, mas também revela sua apropriação limitada, visto que a implementação ainda carece de integração a planos de resposta a incidentes, processos de gestão de risco e rotinas de monitoramento. O Tribunal de Contas da União (TCU, 2024) já havia identificado que a maioria dos órgãos federais se encontra em níveis iniciais de maturidade em segurança da informação, justamente pela ausência de instâncias consolidadas de resposta a incidentes, o que se repete no caso da Rede Federal.

Quanto à existência de Políticas de Segurança da Informação (POSIN), todas as instituições afirmaram possuir documento normativo publicado. Contudo, a análise revelou um quadro heterogêneo: algumas políticas permanecem em versões antigas, datadas de 2016; outras encontram-se em processo de atualização; e uma parcela significativa foi reformulada recentemente em decorrência da implementação do PPSI e do apoio da consultoria em rede fomentada pela RNP/SETEC. Esse movimento indica que o PPSI funcionou como catalisador para a revisão e modernização dos instrumentos, conferindo novo fôlego a uma pauta que antes avançava de forma lenta e fragmentada.

Apesar desse avanço, em muitos casos as POSIN ainda assumem caráter declaratório, sem planos operacionais vinculados, metas de monitoramento ou integração com a gestão de riscos. Essa lacuna reforça a constatação de Bergamini e Cristóvam (2021), de que a adequação documental, por si só, não assegura maturidade institucional, sendo indispensável sua efetiva integração às rotinas administrativas e à cultura organizacional. Assim, embora a atualização das políticas represente um marco positivo, ela permanece mais associada à indução normativa do PPSI do que a uma estratégia institucional transversal.

Por fim, a nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO) foi a medida mais amplamente observada, presente em 93,7% das instituições que responderam à pesquisa. No entanto, a análise revela forte heterogeneidade de vinculação institucional: em alguns casos, a designação recaiu sobre setores mais estratégicos, como Gabinete, Ouvidoria, Diretoria de Governança e Riscos, Coordenação de Integridade e Controle Interno e mesmo em áreas de Auditoria, o que fortalece a legitimidade da função e confere caráter transversal à proteção de dados. Em contrapartida, foram identificados arranjos que evidenciam fragilidade da governança, como a designação de docentes sem função específica para além do cargo comissionado, profissionais de áreas técnicas distantes da pauta (como Eletrônica) ou servidores administrativos sem respaldo organizacional direto. Também foram relatados casos de instabilidade, como DPOs que já manifestaram intenção de deixar a função, o que compromete a continuidade do processo de adequação.

Esse quadro confirma a ideia de que, embora o Controle 0 tenha induzido a formalização da função, a maturidade ainda é desigual: em muitos contextos, a nomeação cumpre mais um requisito formal do que representa uma mudança institucional robusta. Como destacam Filgueiras e Lui (2023), a superação da fragmentação institucional e a consolidação da governança de dados dependem da construção de modelos plurais e integrados, que transcendam o âmbito técnico e envolvam a alta administração. Nesse sentido, as experiências em que o DPO foi vinculado a instâncias de integridade, auditoria ou gabinete representam boas práticas a serem difundidas na Rede Federal, por aproximarem a função de espaços de decisão e fortalecerem sua capacidade de articulação transversal.

4.2 - Da percepção dos gestores sobre os desafios, fragilidades institucionais, ações exitosas e sugestões de aprimoramento.

Além da verificação objetiva da implementação das medidas do Controle 0, as entrevistas também permitiram captar as percepções dos gestores acerca dos principais obstáculos enfrentados, das fragilidades institucionais que condicionam o processo, bem como das experiências exitosas e recomendações que emergiram da prática. Essa dimensão interpretativa revela nuances que os indicadores quantitativos não captam, permitindo compreender como a realidade da Rede Federal dialoga com os desafios estruturais já apontados pela literatura sobre governança digital, segurança da informação e proteção de dados.

4.2.1 - Dos desafios enfrentados

Os desafios enfrentados pelos gestores na implementação do Controle 0 do PPSI revelam um conjunto de fragilidades estruturais, metodológicas e organizacionais. O problema mais recorrente foi a escassez de recursos humanos, apontada de forma quase unânime. Os entrevistados relataram que a governança em privacidade e segurança tem sido conduzida, em grande parte, pela boa vontade de técnicos já responsáveis por múltiplas atribuições, sem respaldo de cargos ou funções formais. Esse quadro confirma a análise de Macedo e Dufloth (2025), segundo a qual a ausência de valorização dos recursos humanos e a sobrecarga de funções comprometem a transformação digital no setor público, transformando a pauta da proteção de dados em um “trabalho extra” em vez de uma prioridade estratégica.

A capacidade de retenção e capacitação dos profissionais também se mostrou um ponto crítico. Embora haja uma oferta crescente de trilhas de formação pela RNP, ENAP e iniciativas internas, os gestores destacaram que a participação é limitada pela reduzida quantidade de servidores disponíveis e pela falta de continuidade dos programas. Muitas capacitações são pontuais, restritas a poucos indivíduos, sem efeito multiplicador para toda a instituição. A rotatividade e vacância de cargos agravam essa limitação, impondo reinícios constantes no processo de aprendizagem e resultando em perda de memória organizacional — o que corrobora os achados de Bergamini e

Cristóvam (2021) sobre a dificuldade da administração pública em consolidar competências permanentes de governança.

Outro eixo de dificuldade recai sobre a ausência de orçamento específico e investimentos adequados. Sem recursos financeiros, a criação de estruturas mínimas de governança ou a institucionalização de equipes dedicadas torna-se inviável, reforçando arranjos improvisados e frágeis. Nesse contexto, a designação de responsáveis muitas vezes ocorre de forma precária, com uso de cargos comissionados ou sobrecarga de servidores.

As entrevistas também evidenciaram críticas à metodologia do PPSI e às ferramentas disponibilizadas. Muitos gestores consideraram que os controles não estão plenamente alinhados à realidade heterogênea da Rede Federal, dificultando a padronização e a aplicabilidade. Essa percepção de descompasso gera sentimentos de desestímulo, especialmente porque os prazos para cumprimento das medidas foram avaliados como exíguos diante das condições estruturais reais.

Somam-se a isso a pressão das auditorias externas e a concorrência gerada por índices como o iPriv e o iSeg, que muitas vezes induzem comparações entre instituições sem considerar suas diferentes capacidades institucionais. Embora relevantes como mecanismos de avaliação, esses instrumentos foram percebidos mais como fator de cobrança e competição do que como apoio à melhoria, já que não vieram acompanhados de suporte técnico e orçamentário. Nesse ponto, os relatos dialogam com a avaliação do TCU (2024), que identificou baixos níveis de maturidade em segurança da informação em órgãos federais e alertou para a falta de infraestrutura necessária à implementação das medidas.

Por fim, destacou-se a necessidade de uma articulação mais consistente entre a Secretaria de Governo Digital (SGD) e a alta administração das instituições. A percepção predominante é que o PPSI permanece restrito às áreas técnicas, sem o protagonismo da gestão superior. Essa limitação compromete o caráter transversal do programa, reduzindo-o a uma pauta operacional. Esse achado corrobora Doneda (2019) e Bergamini e Cristóvam (2021), que defendem que a proteção de dados deve ser consolidada como tema estratégico de governança pública, sob risco de permanecer apenas como exigência formal.

4.2.2 Das experiências, considerações e ou sugestões

No tocante às experiências e sugestões levantadas pelos gestores, destacou-se, de forma quase unânime, o reconhecimento da relevância do PPSI como iniciativa estratégica para a consolidação da privacidade e da segurança da informação na Administração Pública. Ainda que permeado por desafios, os entrevistados ressaltaram que o programa representa um avanço normativo indispensável para induzir a formalização de práticas e a construção de uma cultura organizacional voltada à proteção de dados. Esse reconhecimento corrobora o argumento de Doneda (2019) de

que a LGPD e as políticas dela derivadas exercem papel pedagógico e indutivo sobre as instituições, mesmo em cenários de baixa maturidade inicial.

Por outro lado, as percepções revelaram fragilidades na comunicação e na condução do programa. Embora as reuniões promovidas pelo CONIF tenham sido mencionadas como espaços de articulação, os gestores consideraram que tais iniciativas ainda não foram suficientes para sensibilizar a alta administração, permanecendo a governança restrita às áreas técnicas. Além disso, a apresentação do Ciclo 3 do PPSI, em julho de 2025, foi avaliada como confusa e pouco estimulante, sinalizando que os instrumentos de indução precisam ser aprimorados para engajar mais efetivamente as instituições. Esse achado confirma a análise de Filgueiras e Palotti (2020) sobre a importância da clareza metodológica e da coordenação interinstitucional como fatores decisivos para o sucesso de políticas digitais.

As sugestões apresentadas pelos entrevistados apontam para a necessidade de instrumentos mais adaptados à realidade da Rede Federal. Entre as propostas, destacam-se: a criação de templates operacionais mais próximos da realidade da rede federal, reuniões estruturadas de sensibilização da alta administração, investimento orçamentário, investimento em funções e cargos, a oferta de instrumentos de respaldo que legitimam e consolidam a governança, e a promoção de consultorias em rede e soluções integradas capazes de induzir um avanço mais uniforme entre os institutos. Além disso, algumas falas ressaltaram que a ferramenta utilizada para monitoramento dos controles contribuiu positivamente ao abrir e organizar frentes de trabalho, funcionando como suporte para o encaminhamento das medidas de adequação.

4.2.3 Práticas inovadoras de baixo custo e alto impacto

Apesar das limitações, diversas práticas inovadoras e de baixo custo foram relatadas como experiências positivas. Entre elas estão o uso da infraestrutura EaD para capacitar servidores, o desenvolvimento de materiais acessíveis sobre LGPD, a adoção de checklists práticos para padronizar procedimentos e a realização de campanhas internas integradas com TI e comunicação interna sobre a relevância do tema. Em alguns casos, observou-se a articulação com o FORTI, favorecendo a troca de boas práticas entre os institutos.

Nesse contexto, foi evidenciado o papel do Fórum de Gestores de Tecnologia da Informação da Rede Federal (FORTI), que tem tratado de forma recorrente, nos últimos anos, a temática da privacidade e segurança da informação, justamente com o objetivo de fomentar a discussão sobre a governança e buscar soluções conjuntas. As pautas do FORTI têm contribuído para colocar o tema na agenda estratégica da Rede, reforçando a necessidade de articulação institucional e de integração entre diferentes áreas na implementação do PPSI.

Destaca-se, ainda, que a junção de Grupos de Trabalho (GTs) e comissões temáticas foi uma solução adotada em vários contextos pelo corpo de TI como forma

de atender, ainda que parcialmente, às exigências do framework do PPSI. Essa prática reflete a capacidade adaptativa das instituições diante da ausência de estruturas consolidadas e da limitação de equipes reduzidas, que frequentemente acumulam múltiplas atribuições. Nesses cenários, a utilização dos GTs com funções múltiplas tem permitido encaminhar as demandas de segurança da informação e privacidade de maneira mais ágil e colaborativa, demonstrando que a integração de instâncias já existentes pode ser um caminho viável para dar respostas mínimas às exigências do programa.

Essas iniciativas demonstram que, mesmo em cenários de restrição orçamentária, é possível avançar na consolidação da cultura de proteção de dados e segurança da informação. Esse achado dialoga com a análise de Macedo e Dufloth (2025), segundo a qual a superação das barreiras estruturais na administração pública requer não apenas tecnologia, mas também criatividade institucional, valorização dos recursos humanos e inovação na gestão.

5. CONCLUSÃO

A pesquisa demonstrou que o recorte de 16 Institutos Federais foi suficiente para aprofundar a compreensão sobre os desafios e estratégias de implementação do Controle 0 do Programa de Privacidade e Segurança da Informação (PPSI) na Rede Federal. A análise qualitativa permitiu captar não apenas o grau de cumprimento das medidas mínimas, mas também os obstáculos estruturais e culturais que condicionam o processo, como a sobrecarga de servidores, a indefinição de papéis institucionais e a escassez de recursos humanos e orçamentários.

As entrevistas apontaram que o PPSI, apesar de seus limites, tem exercido um papel indutor fundamental: provocou a atualização de políticas e fomentou a criação de estruturas como ETIRs. Os resultados revelaram também que a implementação ainda é marcada por improvisos e por uma lógica de cumprimento formal, concentrada em áreas técnicas, mas também evidenciaram práticas criativas e colaborativas — como a atuação de GTs, a criação de comitês multidisciplinares e o uso de recursos EaD para capacitação — que mostram caminhos possíveis mesmo em cenários de restrição. Nesse sentido, o PPSI tem se consolidado como um mecanismo pedagógico capaz de induzir avanços, provocando a atualização de políticas, a criação de estruturas mínimas e o debate coletivo sobre privacidade e segurança da informação.

Entretanto, a efetividade do Controle 0 exige que deixe de ser visto como tarefa isolada ou “trabalho extra” e seja incorporado como pauta estratégica da alta administração. Para tanto, sua consolidação depende de articulação intersetorial, de investimentos contínuos em capacitação e tecnologia e da valorização dos profissionais responsáveis por sustentar a governança.

Por fim, os achados desta pesquisa contribuem para levantar e fortalecer a pauta da privacidade e da segurança da informação no âmbito da Rede Federal,

oferecendo insumos para que o debate avance de forma coletiva. Ao reunir fragilidades e experiências positivas, o estudo reforça o papel do FORTI como espaço estratégico de articulação, que pode dar musculatura e legitimidade ao Controle 0, desde que consiga sensibilizar e envolver as instâncias de alta gestão.

Cabe destacar, contudo, as limitações deste trabalho: o número reduzido de instituições participantes e o período de coleta de dados — realizado em meses de férias escolares — resultaram em um recorte que, embora suficiente para levantar questões relevantes, deixa uma lacuna que permite o aprofundamento da discussão que oferece elementos que podem subsidiar novos estudos e apoiar a construção de uma governança mais madura, integrada e sustentável no campo da privacidade e da segurança da informação.

Assim, a amostra restrita não possibilitou a comparação com a totalidade da Rede, o que limita a compreensão mais abrangente sobre como diferentes arranjos institucionais têm lidado com a implementação do Controle 0. Observou-se, contudo, que a cada entrevista novas questões e escopos de análise emergiam, revelando a complexidade do tema e a necessidade de abordagens mais amplas. Nesse sentido, pesquisas futuras que expandem o universo de instituições participantes podem não apenas reforçar a compreensão das heterogeneidades existentes, mas também oferecer novas perspectivas sobre os impactos de médio e longo prazo do Controle 0 na consolidação da maturidade em segurança da informação e privacidade.

6. REFERÊNCIAS

BATAGLIA, M. B.; LEMOS, A. N. L. E.; FARRANHA, A. C. Proteção de dados pessoais e acesso à informação: interfaces do papel da sociedade civil no processo legislativo brasileiro. Anais do EnANPAD 2020. Disponível em: https://arquivo.anpad.org.br/abrir_pdf.php?e=Mjg5NDA%3D. Acesso em: 1 ago. 2025.

BARDIN, Laurence. Análise de conteúdo. Lisboa: Edições 70, [s.d.]. Disponível em: https://ia802902.us.archive.org/8/items/bardin-laurence-analise-de-conteudo/bardin-laurence-analise-de-conteudo.pdf. Acesso em: 1 ago. 2025.

BERGAMINI, José Carlos Loitey; CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. Governança de dados no setor público brasileiro: uma análise a partir da Lei Geral de Proteção de Dados (LGPD). Interesse Público – IP, Belo Horizonte, v. 23, n. 129, p. 75–101, set./out. 2021. Disponível em: https://www.researchgate.net/publication/363917428_Governanca_de_dados_no_setor_publico_brasileiro_uma_analise_a_partir_da_Lei_Geral_de_Protecao_de_Dados_LGPD. Acesso em: 1 ago. 2025.

BOGDAN, R. C.; BIKLEN, S. K. Investigação qualitativa em educação: fundamentos, métodos e técnicas. Porto: Porto Editora, 1994. Disponível em:

https://sites.ufpe.br/gepifhri/wp-content/uploads/sites/86/2023/12/PESQUISA-QUALITATIVA-EM-EDUCACAO-METODOS-E-TECNICAS-EM-EVIDENCIA-Colecao-GEPIFHRI.pdf. Acesso em: 1 ago. 2025.

BRASIL. Decreto nº 12.603, de 28 de agosto de 2025. Institui a Política Nacional de Educação Profissional e Tecnológica – PNEPT, regulamenta o art. 4º da Lei nº 14.645, de 2 de agosto de 2023, e institui o Sistema Nacional de Avaliação da Educação Profissional e Tecnológica – SINAEPT. Diário Oficial da União: seção 1, Brasília, DF, n. 164, p. 6, 29 ago. 2025a.

BRASIL. Estratégia de Governo Digital 2020–2022. Ministério da Economia. Secretaria de Governo Digital. Brasília, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional. Acesso em: 1 ago. 2025.

BRASIL. Lei nº 11.892, de 29 de dezembro de 2008. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 145, n. 252, p. 1, 30 dez. 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm. Acesso em: 1 ago. 2025.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre os princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, e altera a Lei nº 7.116, de 29 de agosto de 1983. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 1 ago. 2025.

BRASIL. Ministério da Educação. Rede Federal de Educação Profissional, Científica e Tecnológica. Brasília, DF: MEC, 2025b. Disponível em: https://www.gov.br/mec/pt-br/assuntos/ept/rede-federal. Acesso em: 1 ago. 2025.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. Cartilha de Governança de Dados – Volume III. Brasília, DF: Governo Federal, 2023a. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhaGovDadosvol3.pdf. Acesso em: 1 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Cartilha do Programa de Privacidade e Segurança da Informação (PPSI). Brasília, 2023b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/cartilha_ppsi.pdf. Acesso em: 2 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Ministério da Gestão regulamenta o Programa de Privacidade e Segurança da Informação do Governo

Federal. Brasília, DF, 30 mar. 2023c. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/marco/ministerio-da-gestao-regulamenta-o-programa-de-privacidade-e-seguranca-da-informacao-do-governo-federal. Acesso em: 1 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Programa de Privacidade e Segurança da Informação (PPSI). Brasília, 2023d. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-atual. Acesso em: 1 ago. 2025.

BRASIL. Secretaria de Governo Digital. Guia do Framework de Privacidade e Segurança da Informação. Brasília, nov. 2022a. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. . Acesso em: 5 set. 2025

BRASIL. Portaria nº 6.533, de 8 de novembro de 2022. Institui o Comitê de Governança de Dados no âmbito do Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCTI_n_6533_de_08112022.html. Acesso em: 2 ago. 2025.

BRASIL. Tribunal de Contas da União. Acórdão nº 1.372/2025 – Plenário. Relator: ministro Walton Alencar Rodrigues. Brasília, DF, 2025c. Auditoria de conformidade à LGPD em 387 organizações públicas federais. Diário Oficial da União: Seção 1. Disponível em: https://contas.tcu.gov.br/sagas/SvlVisualizarRelVotoAcRtf?codFiltro=SAGAS-SESSAO-ENCERRADA&seOcultaPagina=S&item0=884653. Acesso em: 1 ago. 2025.

BRASIL. Tribunal de Contas da União. Acórdão nº 1.384/2022 – Plenário. Relator: ministro Augusto Nardes. Brasília, DF, 2022. Auditoria de conformidade à LGPD em 382 organizações públicas federais. Diário Oficial da União: Seção 1. Disponível em: https://www.trt7.jus.br/files/acesso_informacao/transparencia/acoes_de_controle/TCU/Acordao_1384-2022-TCU-Plenario.pdf. Acesso em: 1 ago. 2025.

BRASIL. Tribunal de Contas da União. Acórdão nº 2.387/2024 – Plenário. Relator: ministro Augusto Nardes, de 6 de novembro de 2024. Auditoria operacional sobre segurança da informação e cibersegurança em órgãos integrantes do SISP, em execução do PPSI. Brasília: TCU, 2024. Disponível em: https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2686174. Acesso em: 1 ago. 2025.

BRASIL. Tribunal de Contas da União. Governança em tecnologia de informação e comunicação para o setor público [recurso eletrônico]. Brasília: Tribunal de Contas da União, 2018. 164 p. Disponível em: https://portal.tcu.gov.br/data/files/.../Governanca_e_tecnologia_informacao_comunicacao_setor_publico.pdf. Acesso em: 1 ago. 2025.

BRASIL. Tribunal de Contas da União. Ofício nº 47.268/2023 – SEPROC. Processo TC 007.205/2022-8. Relator: ministro Antonio Anastasia. Brasília, DF, 2023e. Monitoramento do Acórdão nº 2.789/2019 – Plenário. Disponível em: Oficio_047.268_2023_SEPROC.pdf. Acesso em: 1 ago. 2025.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology. Qualitative Research in Psychology, Abingdon, v. 3, n. 2, p. 77-101, 2006. DOI: 10.1191/1478088706qp063oa. Disponível em: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology. Acesso em: 2 ago. 2025.

CARNEIRO, Plínio Maria. A implementação da Lei Geral de Proteção de Dados Pessoais na governança do processo de pagamento de pessoal do Comando do Exército. 2023. Dissertação (Mestrado em Governança e Desenvolvimento) – Escola Nacional de Administração Pública, Brasília, 2023. Disponível em: https://repositorio.enap.gov.br. Acesso em: 18 jul. 2024.

CARVALHO, Laura Estela Madeira de. A governança de tecnologia da informação na administração pública sob a ótica dos princípios da governança corporativa. 2019. 87 f. Dissertação (Mestrado em administração) - Universidade do Grande Rio Prof. José de Souza Herdy, Rio de Janeiro, 2019. Disponível em: https://rigeo.sgb.gov.br/handle/doc/22780?mode=full. Acesso em: 1 ago. 2025.

CENTER FOR INTERNET SECURITY. CIS Controls v8. East Greenbush, NY: CIS, 2021. Disponível em: https://www.cisecurity.org/controls/v8 . Acesso em: 5 set. 2025.

CONIF – Conselho Nacional das Instituições da Rede Federal. Em reunião, Forti prioriza segurança da informação e governança de TI. Brasília, 30 maio 2025. Disponível em: https://portal.conif.org.br/comunicacao/gerais/forti-2025-seguranca-governanca-ti. Acesso em: 1 ago. 2025.

DENZIN, N. K.; LINCOLN, Y. S. The SAGE Handbook of Qualitative Research. Thousand Oaks, CA: Sage, 2005. Disponível em: https://us.sagepub.com/sites/default/files/upm-binaries/48453_ch_1.pdf. Acesso em: 2 ago. 2025.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3. ed., rev. e ampl. Rio de Janeiro: Forense, 2019. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2021;001203055. Acesso em: 1 ago. 2025.

FACHIN, Luiz Edson. O Direito Fundamental à proteção de dados pessoais: análise da decisão paradigmática do STF na ADI 6.387 DF. Revista Videre, Dourados, v. 14, n. 29, p.

298-313, jan./abr. 2022. Disponível em: https://ojs.ufgd.edu.br/index.php/videre/article/view/15629. Acesso em: 1 ago. 2025.

FILGUEIRAS, Fernando; LUI, Lizandro. Os desafios da governança de dados para a construção da política de governo digital no Brasil. In: CGI.br (Org.). TIC Governo Eletrônico 2023. São Paulo: Comitê Gestor da Internet, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20240826104638/tic_governo_eletronico_2023_livro_eletronico.pdf. Acesso em: 1 ago. 2025.

FILGUEIRAS, Fernando; PALOTTI, Pedro L. M. Digital Transformation and Public Service Delivery in Brazil. Latin American Policy, v. 10, n. 2, p. 195–219, 2019/2020. Disponível em: https://www.researchgate.net/publication/330145305_Digital_Transformation_and_Public_Service_Delivery_in_Brazil. Acesso em: 1 ago. 2025.

FORTI – Fórum de Gestores de Tecnologia da Informação e Comunicação. Conselho Nacional das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (CONIF). Disponível em: https://portal.conif.org.br/forti. Acesso em: 1 ago. 2025.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008. Disponível em: https://ayanrafael.com/wp-content/uploads/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf. Acesso em: 21 ago. 2025.

JANSSEN, Marijn; CHARALABIDIS, Yannis; ZUIDERWIJK, Anneke. Benefits, adoption barriers and myths of open data and open government. Information Systems Management, Philadelphia, v. 29, n. 4, p. 258–268, 2012. Disponível em: https://pad.undp.org.mx/files/g/820dcf0c1242364677545293.44594fd/banco/arquivo/107/0/benefits-adoption-barriers-and-myths-of-open-data-and-open-government.pdf. Acesso em: 1 ago. 2025.

MACEDO, Laura Dilly Generoso; DUFLOTH, Simone Cristina. Interoperabilidade no serviço público: uma revisão sistemática sob a lente do e-Ping no Brasil. Informação & Informação, Londrina, v. 30, n. 1, p. 83–108, jan./mar. 2025. DOI: 10.5433/1981-8920.2025v30n1p83. Disponível em: https://brapci.inf.br/v/351783. Acesso em: 1 ago. 2025.

MINAYO, M. C. S. Pesquisa social: teoria, método e criatividade. 18. ed. Petrópolis: Vozes, 2014. Disponível em: https://www.faed.udesc.br/arquivos/id_submenu/1428/minayo__2001.pdf. Acesso em: 1 ago. 2025.

OCDE. Digital Government Index: 2019 results. OECD Public Governance Policy Papers, No. 03. Paris: OECD Publishing, 2020. Disponível em: https://doi.org/10.1787/4de9f5bb-en. Acesso em: 1 ago. 2025.

OLIVEIRA, Adilson Ribeiro de; XAVIER, Gláucia do Carmo; SILVA, José Fernandes da; OLIVEIRA, Shirlene Bemfica de (org.). Educação profissional e tecnológica no Brasil: da história à teoria, da teoria à práxis. Curitiba: CRV, 2020. 276 p. (Coleção Educação Profissional e Tecnológica no Brasil – v. 1). DOI: 10.24824/978652510120.0. Disponível em: https://www.ifmg.edu.br/ourobranco/nossos-cursos/profept-2/LivroProfEPT2020.pdf. Acesso em: 1 ago. 2025.

PECI, A.; TEIXEIRA, M. A. C. Desafios da administração pública brasileira: a crise da covid-19 evidenciou o papel central da gestão e burocracia profissional do Estado. GV Executivo, v. 20, n. 1, jan./mar. 2021. Disponível em: https://www.researchgate.net/publication/352702118_Desafios_da_administracao_publica_brasileira. Acesso em: 2 ago. 2025.

PILÓI, Felipe Thadeu. Segurança da informação no setor público e adequação à LGPD. RevistaFT, v. 29, n. 146, p. 1–34, maio 2025. DOI: 10.69849/revistaft/dt10202505272130. Disponível em: https://revistaft.com.br/seguranca-da-informacao-no-setor-publico-e-adequacao-a-lgpd/. Acesso em: 2 ago. 2025.

PIMENTEL, Gilberto; MOURA, Ivens de Oliveira. Transparência e dados abertos na administração pública: desafios e limites da interoperabilidade. Revista Brasileira de Políticas Públicas, Brasília, v. 15, n. 2, p. 34–50, jul./dez. 2021. Disponível em: https://brapci.inf.br/v/149455. Acesso em: 1 ago. 2025.

RODRIGUES, José Carlos; LIMA, Wagner Soares de. Padronização e integração de Sistemas de Informação Gerenciais: percepção de usuários no IFAM e IFRO. Revista Acadêmica da Lusofonia, n. 12, p. 48–67, 2024. Disponível em: https://revistaacademicadalusofonia.com/index.php/lusofonia/article/view/69. Acesso em: 1 ago. 2025.

STJ – Superior Tribunal de Justiça. Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais. Brasília, 27 out. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/27102024-Os-precedentes-do-STJ-nos-primeiros-quatro-anos-de-vigencia-da-Lei-Geral-de-Protecao-de-Dados-Pessoais.aspx. Acesso em: 2 ago. 2025.

Souza, L. C. de, & Prodel Júnior, L. H. (2023). Diretrizes de gestão de riscos e de integridade na administração pública. Revista Do Direito Público, 18(1), 26–43. https://doi.org/10.5433/1980-511X.2023v18n1p26

YIN, R. K. Case Study Research and Applications: Design and Methods. 5. ed. Thousand Oaks, CA: Sage, 2018. Disponível em: https://ebooks.umu.ac.ug/librarian/books-file/Case%20Study%20Research%20and%20Applications.pdf. Acesso em: 2 ago. 2025.

ANEXO I

PERGUNTAS RELACIONADAS AO CONTROLE 0

1 - O órgão nomeou uma autoridade máxima de Tecnologia da Informação? (Sim/Não)
Se Sim, qual cargo essa autoridade ocupa?
Se Não, há previsão para essa nomeação?
O órgão nomeou um Gestor de Segurança da Informação? (Sim/Não)
Se Sim, quais são suas principais atribuições?
Se Não, qual a principal barreira para essa nomeação?
O órgão nomeou um responsável pela unidade de controle interno? (Sim/Não)
Esse responsável possui atribuições relacionadas à segurança da informação?
O órgão instituiu um Comitê de Segurança da Informação? (Sim/Não)
Se Sim, como é composto o comitê?
Se Não, qual a principal dificuldade para sua instituição?
O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR)? (Sim/Não)
Se Sim, quais tipos de incidentes essa equipe trata?
Se Não, como os incidentes de segurança são tratados atualmente?
O órgão elaborou uma Política de Segurança da Informação (POSIN)? (Sim/Não)
Se Sim, essa política está alinhada às diretrizes do PPSI?
Se Não, há previsão para sua elaboração?
O órgão nomeou um Encarregado pelo Tratamento de Dados Pessoais? (Sim/Não)
Se Sim, essa nomeação foi formalizada e divulgada publicamente?
Se Não, qual a principal dificuldade para essa nomeação?

2. Desafios Enfrentados
Quais os principais desafios enfrentados na implementação das medidas do Controle 0? (Resposta aberta)
Houve dificuldades relacionadas a orçamento, pessoal ou conhecimento técnico para implementar essas medidas? (Múltipla escolha: Orçamento / Pessoal / Conhecimento técnico / Outros)
A liderança da instituição apoia ativamente a implementação dessas diretrizes? (Sim/Parcialmente/Não)
A instituição possui políticas formais para segurança da informação e proteção de dados pessoais? (Sim/Parcialmente/Não)
O Comitê de Segurança da Informação ou a equipe de segurança recebe treinamento regular? (Sim/Não/Parcialmente)

Quais ações adotadas pela sua instituição contribuíram para a implementação bem-sucedida das diretrizes do Controle 0? (Resposta aberta)
Quais estratégias poderiam ser compartilhadas com outras instituições da Rede para facilitar a implementação dessas diretrizes? (Resposta aberta)
Quais recomendações você faria para fortalecer as políticas de segurança da informação e privacidade na Rede Federal? (Resposta aberta)

ANEXO II

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Título da Pesquisa: Implementação do Controle 0 do Programa de Privacidade e Segurança da Informação (PPSI) na Rede Federal

Pesquisadora Responsável: Pâmela Hélia de Oliveira

Orientadora: Virgínia de Melo Dantas Trinks

Instituição: Universidade de Brasília (UnB)

Contato: pamela.oliveira@ifsuldeminas.edu.br

Objetivo da Pesquisa: Esta pesquisa tem como objetivo compreender o contexto real da Rede Federal em relação à implementação do Controle 0 do PPSI. Os dados coletados serão utilizados para fins científicos e acadêmicos, podendo ser incluídos em relatórios, artigos e publicações científicas.

Procedimentos: O(a) participante será entrevistado(a) por uma reunião online, podendo com respostas na forma oral. As respostas serão registradas e analisadas de forma agregada, garantindo a privacidade dos participantes.

Uso e Compartilhamento das Informações: Os dados coletados poderão ser divulgados em publicações científicas e acadêmicas, bem como compartilhados com a Universidade de Brasília (UnB) para fins de análise e elaboração de relatórios técnicos. Em nenhuma hipótese serão divulgadas informações que permitam a identificação direta dos participantes, salvo quando autorizado expressamente pelo(a) entrevistado(a).

Confidencialidade: Os dados serão tratados de forma sigilosa e utilizados exclusivamente para os fins mencionados. Somente a pesquisadora e a equipe envolvida terão acesso às informações individuais dos participantes.

Direitos do Participante: A participação na pesquisa é voluntária e o(a) participante poderá desistir a qualquer momento sem qualquer prejuízo. O(a) participante pode solicitar a exclusão de suas informações até o momento da análise dos dados. Caso tenha dúvidas, o(a) participante poderá entrar em contato com a pesquisadora responsável para esclarecimentos adicionais.

Declaração de Consentimento: Declaro que fui informado(a) sobre os objetivos da pesquisa, a forma de utilização dos dados e que minha participação é voluntária. Autorizo a divulgação das informações fornecidas para fins científicos e acadêmicos, bem como o compartilhamento dos resultados com a Universidade de Brasília (UnB), conforme descrito neste documento.

Nome do(a) participante:

Cargo/Função:
Instituição:

E-mail (opcional): _____

Data: //_____

Assinatura: _____