Validação de um Modelo de Governança em Privacidade baseado em Análise Documental de Frameworks Governamentais

Rafael Rodrigo dos Santos Miranda, Virgínia de Melo Dantas Trinks

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

rafae.rodrigo@gestao.gov.br, virginia.trinks@presidencia.gov.br

Abstract. *The General Personal Data Protection Law (LGPD) introduced significant governance challenges for the Brazilian public sector, particularly for Federal Higher Education Institutions (IFES). This article validates, through systematic documentary analysis, the integrated model between the Privacy Governance Program (PGP) and the Privacy and Information Security Program: Implementation Group 1 (PPSI-GI1), both from the Digital Government Secretariat. The qualitative-exploratory research analyzed six official documents, mapping 16 PGP milestones and correlating them with PPSI-GI1 measures while validating coverage of LGPD principles. Results demonstrate that the integrated model displays internal coherence, encompasses all ten LGPD principles, and demonstrates 81% implementation viability. The study provides empirical grounding for future validation and practical diagnostic instrument development.*

Resumo. *A Lei Geral de Proteção de Dados Pessoais (LGPD) institui marco regulatório essencial para proteção dos direitos fundamentais no Brasil, demandando das organizações públicas conformidade normativa que ultrapassa medidas técnicas isoladas. Este artigo valida, mediante análise documental sistemática, o modelo integrado entre o Programa de Governança em Privacidade (PGP) e o Programa de Privacidade e Segurança da Informação – Grupo de Implementação 1 (PPSI-GI1), ambos da Secretaria de Governo Digital. A pesquisa qualitativa-exploratória analisou seis documentos oficiais, mapeando 16 marcos PGP, correlacionando-os com medidas PPSI-GI1 e validando a cobertura de princípios LGPD. Os resultados demonstram que o modelo integrado é internamente coerente, cobre todos os dez princípios da LGPD e apresenta viabilidade de implementação de 81%. O estudo fornece fundamento empírico para futura validação e construção de instrumentos práticos de diagnóstico.*

1. Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD) instituiu marco regulatório fundamental para a proteção dos direitos básicos como liberdade e privacidade no Brasil, impondo às organizações públicas e privadas necessidade de adequação normativa e cultural [SANTOS, 2022; BRASIL, 2018]. No setor público, essa conformidade vai além da adoção de medidas técnicas, demandando transformação

institucional que alcance níveis estratégicos, táticos e operacionais, envolvendo governança, processos e pessoas [ANGELO, 2023].

A implementação da LGPD permanece em estágios iniciais em grande parte das instituições federais, o que eleva riscos de violação de direitos e prejudica a eficiência administrativa [SANTOS; DUARTE, 2022]. Auditorias revelam baixa maturidade em governança de dados, com vulnerabilidades na constituição de comitês, formalização de políticas e designação de encarregados: elementos centrais para a conformidade regulatória [ANGELO, 2023].

A transformação digital na Administração Pública, embora impulsionada por avanços tecnológicos, depende da capacidade estatal de integrar sistemas e coordenar políticas de longo prazo. Arranjos organizacionais frágeis amplificam a fragmentação, dificultando a consolidação de práticas robustas de proteção de dados [SILVA; AROUCA, 2020]. Tal cenário revela-se particularmente crítico nas Instituições Federais de Ensino Superior (IFES), que lidam com ecossistemas complexos contendo dados sensíveis de estudantes, servidores e pesquisadores, exigindo estruturas unificadas de governança [ANGELO, 2023].

Atender às exigências da LGPD requer institucionalização de práticas colegiadas, com participação de áreas jurídicas, tecnológicas e de controle interno, evitando decisões fragmentadas que comprometem a maturidade organizacional [SANTOS, 2022]. Profissional de especialização limitada e alta rotatividade no setor público intensificam essa dificuldade, reduzindo a capacidade operacional e a implementação de políticas consistentes [SILVA; AROUCA, 2020].

Em resposta, o Governo Federal estabeleceu o Programa de Privacidade e Segurança da Informação (PPSI), orientando órgãos públicos na adoção de medidas estruturadas de governança, segurança e privacidade alinhadas a frameworks internacionais e normas ISO/IEC [SILVA, 2025]. O PPSI e o Guia de Elaboração de Programa de Governança em Privacidade (PGP) propõem etapas para diagnóstico, planejamento e monitoramento; contudo, estudos apontam questões relacionadas à coerência conceitual e aplicabilidade prática em contextos educacionais [SILVA, 2025].

Faltam evidências sistemáticas que validem a correlação entre as etapas do Guia PGP e os controles e medidas do PPSI, bem como sua aderência integral aos princípios da LGPD. Essa lacuna compromete a confiabilidade do modelo para gestores e encarregados que buscam implementar conformidade em IFES, reforçando a importância de pesquisas que analisem a consistência estrutural e a viabilidade de implementação desses instrumentos [SILVA, 2025].

1.2 Questões de Pesquisa e Objetivos

O presente estudo tem como objetivo geral validar, por meio de uma análise documental sistemática, a coerência, a completude e a aplicabilidade do modelo integrado PGP-PPSI-GI1 no contexto das Instituições Federais de Ensino Superior (IFES). A intenção é oferecer uma base teórica consistente que sustente a criação de instrumentos de diagnóstico confiáveis e oriente a formulação de políticas complementares voltadas ao fortalecimento da governança de privacidade.

A investigação analisa de que forma as etapas do Guia PGP: Planejamento, Execução e Monitoramento, se articulam com as medidas do PPSI-GI1, buscando

verificar a consistência entre os dois referenciais e identificar eventuais lacunas ou sobreposições que possam afetar sua aplicação prática. Também observa se o conjunto formado pelo PGP e pelo PPSI-GI1 contempla plenamente os dez princípios da LGPD e se apresenta condições adequadas para ser adotado nas IFES. Por fim, examina a correspondência entre as medidas do PPSI-GI1 e as atividades descritas no Guia PGP, com o objetivo de consolidar um roteiro claro e funcional que apoie os profissionais responsáveis pelo tratamento de dados pessoais nas instituições federais.

O artigo está estruturado em quatro partes principais. A primeira parte, dedicada à introdução e contextualização, discute os desafios atuais da governança em privacidade, com destaque para o papel das instituições públicas de ensino e a necessidade de adequação à LGPD.

Em seguida, apresenta-se a seção de fundamentação teórica, que reúne os conceitos centrais, referenciais normativos e experiências já consolidadas no campo da proteção de dados e da segurança da informação. Nessa etapa, são revisitados pontos-chave para contextualizar o modelo integrado e explorar a evolução dos instrumentos analisados.

A terceira parte detalha os procedimentos metodológicos adotados, descrevendo as escolhas técnicas, o processo de seleção documental e as estratégias que orientaram a análise sistemática dos referenciais normativos do PGP e do PPSI-GI1, assim como a abordagem utilizada para o mapeamento e a validação dos marcos.

Por fim, a seção de resultados e discussão apresenta os principais achados da análise documental, articulando-os continuamente com os objetivos do estudo. O texto se encerra com considerações finais que reforçam as contribuições, apontam limitações e sugerem caminhos para pesquisas futuras, visando subsidiar ações práticas e políticas públicas mais robustas para a governança em privacidade no ensino superior brasileiro.

2. Fundamentação Teórica

2.1 Governança em Privacidade no Setor Público

A governança em privacidade no setor público representa elemento fundamental para assegurar conformidade com a Lei Geral de Proteção de Dados (LGPD) e proteger os direitos fundamentais dos cidadãos. A LGPD, instituída pela Lei nº 13.709/2018, estabelece princípios e diretrizes para o tratamento de dados pessoais, atribuindo às instituições públicas responsabilidade pela implementação de mecanismos que promovam transparência, segurança e responsabilização (*accountability*) (BRASIL, 2018).

Conforme Lugati e Almeida [2020], a adequação à LGPD ultrapassa uma resposta imediata para evitar sanções, representando oportunidade para consolidar cultura organizacional voltada à proteção de dados. Tal cultura repousa em práticas inovadoras, definição clara de responsabilidades, técnicas robustas de segurança da informação e estratégias de comunicação acessíveis aos titulares.

No contexto governamental, os desafios amplificam-se pela complexidade dos sistemas informatizados e integração com plataformas externas. Norbiato e Silva [2024] alertam quanto aos riscos decorrentes da utilização de mídias sociais como ferramenta de autenticação em serviços públicos. Embora facilite o acesso, essa prática expande a

vulnerabilidade dos dados e evidencia fragilidades estruturais, especialmente diante da insuficiência de investimentos em segurança digital.

Além disso, a governança deve se orientar pelo princípio da prestação de contas, previsto no art. 6º, X da LGPD, que exige demonstração da adoção de medidas eficazes para proteção dos dados [GHISLENI, 2022]. A autora sublinha que a governança corporativa e a gestão baseada em riscos (*risk-based approach*) funcionam como instrumentos fundamentais para materializar esse princípio, permitindo que controladores considerem a severidade e probabilidade dos riscos associados ao tratamento de dados. Essa abordagem, consolidada na GDPR europeia, foi incorporada pela LGPD como parâmetro para boas práticas e governança [GHISLENI, 2022].

Para mitigar riscos, Santos [2022] propõe modelo de governança fundamentado em cinco etapas: análise de lacunas, elaboração de plano de ação, implementação de políticas de governança, mapeamento dos processos de tratamento e adoção de medidas técnicas e administrativas. Esse modelo reforça que a governança deve abranger todo o ciclo de vida dos dados, desde a coleta até o descarte, assegurando conformidade com os princípios da LGPD e alinhamento a normas internas e externas.

Nesse contexto, a governança em privacidade assume papel estratégico. Além de garantir conformidade legal, reforça transparência, prestação de contas e proteção dos direitos fundamentais dos cidadãos. Esse entendimento alinha-se ao princípio da responsabilização previsto na LGPD, que exige do controlador demonstração de medidas eficazes para comprovar observância das normas de proteção de dados, reforçando a importância da governança como mecanismo de responsabilização (*accountability*) [GHISLENI, 2022].

A governança em privacidade no setor público, portanto, exige mais do que ajustes normativos: requer investimentos, capacitação e mudança cultural. A adoção de práticas como privacidade desde a concepção (*privacy by design*) e criação de mecanismos de supervisão contínua são fundamentais para assegurar proteção de dados e fortalecer a confiança social nos serviços digitais oferecidos pelo Estado.

Essa perspectiva é fortalecida por Lugati e Almeida [2020], ao destacarem que a implementação efetiva da LGPD depende de mudança cultural nas organizações, indo além da simples adequação normativa para incorporar práticas inovadoras e duradouras que garantam segurança dos dados.

2.2 O Papel do Encarregado pelo Tratamento de Dados Pessoais

O encarregado pelo tratamento de dados pessoais, também denominado Data Protection Officer (DPO), ocupa posição central na estrutura de conformidade com a Lei Geral de Proteção de Dados (LGPD). De acordo com a legislação, o encarregado funciona como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), sendo responsável por orientar a instituição quanto às práticas de tratamento e atender às solicitações dos titulares [BRASIL, 2018].

As funções do encarregado extrapolam a comunicação. Conforme Santos [2022], suas atribuições incluem supervisão das políticas internas, elaboração do Relatório de Impacto à Proteção de Dados (RIPD) e promoção de ações educativas voltadas à conscientização dos colaboradores. Tais atividades são imprescindíveis para

garantir que a proteção de dados se integre às rotinas organizacionais, funcionando como prática contínua de governança e não apenas como procedimentos formais.

As responsabilidades do DPO relacionam-se diretamente à governança corporativa e ao princípio da prestação de contas (*accountability*), previsto no art. 6º, X da LGPD. Ghisleni [2022] destaca que o encarregado deve atuar como agente de conformidade, garantindo que a organização adote medidas eficazes para demonstrar observância das normas de proteção de dados. Tal atuação exige abordagem baseada em riscos (*risk-based approach*), que permite ajustar as ações de acordo com a severidade e probabilidade dos impactos sobre os direitos dos titulares.

A efetividade do papel do encarregado depende, contudo, de autonomia funcional e capacitação técnica, além do apoio da alta gestão. Lima e Alves [2021] enfatizam que o DPO deve dominar conhecimento jurídico e tecnológico, além de possuir habilidades de comunicação para atuar como mediador entre áreas técnicas e estratégicas. Essa posição estratégica garante que o encarregado não seja apenas executor de tarefas, mas articulador da cultura de proteção de dados dentro da organização.

Outro aspecto relevante refere-se à necessidade de equipes multidisciplinares e práticas inovadoras. Lugati e Almeida [2020] argumentam que a adoção de privacidade desde a concepção (*privacy by design*) e privacidade por padrão (*privacy by default*) deve ser incorporada desde a concepção dos processos, permitindo que a proteção de dados funcione como elemento estrutural e não meramente corretivo. Além disso, técnicas como legal design são fundamentais para tornar as informações acessíveis e compreensíveis aos titulares, fortalecendo transparência e confiança nos processos de tratamento.

No setor público, esses desafios se intensificam pela complexidade dos sistemas e integração com plataformas externas. Norbiato e Silva [2024] alertam que a ausência de mecanismos robustos de governança e segurança expõe os cidadãos a riscos significativos, reforçando a importância do DPO como elo entre tecnologia, gestão e direitos fundamentais.

Para que tal atuação seja efetiva, é indispensável que o DPO disponha de ferramentas de diagnóstico e métricas que permitam avaliar o nível de maturidade da governança em privacidade, garantindo melhoria contínua e adequação às exigências legais e boas práticas [GHISLENI, 2022; LIMA; ALVES, 2021].

2.3 O Programa de Privacidade e Segurança da Informação (PPSI)

O Programa de Privacidade e Segurança da Informação (PPSI) funciona como mecanismo de governança criado para consolidar práticas de proteção de dados e segurança da informação na Administração Pública. O programa fundamenta-se na LGPD e na Política Nacional de Segurança da Informação, incorporando boas práticas internacionais como CIS Controls v8, NIST CSF e normas ISO/IEC. A proposta centra-se em evoluir de uma postura reativa para gestão baseada em riscos, com métricas e processos padronizados [BRASIL, 2024b].

A estrutura do PPSI organiza-se em três eixos: Controle 0, que define papéis e responsabilidades; Controles 1 a 18, dedicados à cibersegurança; e Controles 19 a 31, voltados à privacidade. O terceiro eixo operacionaliza princípios como privacidade

desde a concepção (*privacy by design*) e privacidade por padrão (*privacy by default*), abrangendo mapeamento de operações, definição de bases legais, minimização de dados, transparência e auditoria.

Tabela 1. Eixos do PPSI e objetivos e exemplos de artefatos e métricas

Eixo	Escopo	Objetivo Central	Exemplos de Artefatos e Métricas
Controle 0	Estrutura básica de gestão	Institucionalizar papéis, instâncias e responsabilidades	Encarregado, Comitê, ETIR; regimento; plano de trabalho; atas; iMC
Controles 1–18	Cibersegurança (CIS v8/NIST CSF)	"Higiene cibernética" e resiliência operacional	Inventário de ativos/softwares; configuração segura; gestão de vulnerabilidades; plano de resposta a incidentes; testes; iSeg
Controles 19–31	Privacidade (NIST PF; ISO/IEC 29100, 29151, 27701, 27018, 29134, 29184)	Operacionalizar LGPD por processos e métricas	*Privacy by design*/default; mapeamento do tratamento; bases legais; minimização; transparência; RIPD; iPriv

A implementação ocorre de forma incremental, por meio de ciclos semestrais e grupos de implementação (GI1, GI2 e GI3). Essa abordagem garante que órgãos públicos avancem gradualmente, priorizando ações conforme criticidade e recursos disponíveis. Estudos indicam que tal metodologia é essencial para reduzir vulnerabilidades, especialmente em ambientes complexos como universidades, onde falhas de governança e segurança ampliam riscos de vazamento e indisponibilidade de serviços [FERNANDES et al., 2025; GONÇALVES et al., 2025].

Do ponto de vista da governança organizacional, o PPSI combina o princípio das "três linhas de defesa" com patrocínio da alta administração e institucionalização de papéis (Gestor de TIC, Gestor de Segurança, Encarregado de Dados, Unidade de Controle Interno), de modo a integrar privacidade e segurança ao planejamento, orçamento e gestão de riscos. Simultaneamente, evidências na literatura apontam que a efetividade do programa depende do apoio da alta administração: financiamento, priorização e responsabilização, sob pena de adesão formal e baixa aderência prática [MARCILIO; NUNES, 2025].

Assim, a ausência de liderança e de recursos compromete a efetividade do programa, tornando indispensável a institucionalização de papéis, orçamento e mecanismos de prestação de contas. A integração entre o papel do Encarregado, os indicadores de maturidade e os processos de gestão é fundamental para garantir conformidade e *accountability*, conforme previsto na LGPD [MARCILIO; NUNES, 2025].

Desse modo, o PPSI encerra o ciclo entre as diretrizes de governança em privacidade e a atuação do Encarregado, oferecendo um roteiro de implementação, métricas e evidências para sustentar prestação de contas e melhoria contínua. Sua efetividade, contudo, depende de patrocínio executivo, capacitação e coordenação

intersetorial, além da evolução permanente do modelo, de modo a acompanhar a complexidade tecnológica e regulatória do setor público brasileiro [MARCILIO; NUNES, 2025].

2.4 Programa de Governança em Privacidade (PGP)

A implementação do PGP ocorre de forma incremental, por meio de ciclos semestrais e grupos de implementação (GI1, GI2 e GI3). Essa abordagem permite que órgãos públicos avancem gradualmente, priorizando ações de acordo com criticidade e recursos disponíveis. Pesquisas indicam que tal metodologia reduz vulnerabilidades, especialmente em ambientes complexos como universidades, onde falhas de governança e segurança aumentam o risco de vazamento e indisponibilidade de serviços [FERNANDES et al., 2025; GONÇALVES et al., 2025].

A aplicação do PPSI no setor público é condição necessária para mitigar exposições decorrentes de integrações complexas, legados e práticas pouco padronizadas, sobretudo em ambientes intensivos em dados, como universidades [GONÇALVES et al., 2025].

Do ponto de vista da governança organizacional, o PPSI integra o princípio das "três linhas de defesa" com o patrocínio da alta administração e a institucionalização de papéis (Gestor de TIC, Gestor de Segurança, Encarregado de Dados, Unidade de Controle Interno), de modo a incorporar privacidade e segurança ao planejamento, orçamento e gestão de riscos. Simultaneamente, evidências na literatura mostram que a efetividade do programa depende do apoio executivo: financiamento, priorização e responsabilização, situação que pode resultar em adesão meramente formal e baixa efetividade prática [MARCILIO; NUNES, 2025].

Portanto, a ausência de liderança e de recursos compromete a efetividade do programa, tornando indispensável a institucionalização de papéis, orçamento e mecanismos de prestação de contas. A integração entre o papel do Encarregado, os indicadores de maturidade e os processos de gestão é fundamental para garantir conformidade e responsabilização (*accountability*), conforme previsto na LGPD [MARCILIO; NUNES, 2025].

Assim, o PPSI encerra o ciclo entre as diretrizes de governança em privacidade e a atuação do Encarregado, fornecendo um roteiro de implementação, métricas e evidências para sustentar prestação de contas e melhoria contínua. Sua efetividade, contudo, depende de patrocínio executivo, capacitação e coordenação intersetorial, além da evolução permanente do modelo, de modo a acompanhar a complexidade tecnológica e regulatória do setor público brasileiro [MARCILIO; NUNES, 2025].

2.5 Estrutura do Programa de Governança em Privacidade (PGP)

Conceitualmente, o PGP funciona como eixo de integração entre conformidade regulatória, gestão de riscos e cultura organizacional, articulando medidas técnicas e administrativas capazes de reduzir exposição a incidentes e fortalecer a confiança pública no tratamento de dados, inclusive quando o tratamento é mediado por plataformas digitais [BRASIL, 2020; LUGATI; ALMEIDA, 2020].

Estruturalmente, a implantação do PGP pode ser organizada por ciclos de melhoria *Plan - Do - Check - Act* (PDCA), com três macroetapas interdependentes

[MOURA, 2021], definidas como: planejamento, execução e monitoramento, que se desdobram em atividades específicas, desde a identificação dos fluxos de dados e agentes de tratamento até a medição de desempenho por indicadores de maturidade. Tal arranjo é coerente com modelos internacionais de gestão da privacidade [BRASIL, 2020; NORBIATO; SILVA, 2024].

Tabela 2. Etapas do Programa de Governança em Privacidade (PGP)

Etapa	Principais Atividades
Planejamento	Nomeação do encarregado; inventário e mapeamento de dados; identificação de bases legais; análise de riscos
Execução	Implementação de políticas e procedimentos; elaboração de RIPD; revisão contratual; cláusulas de proteção de dados; treinamentos
Monitoramento	Indicadores (iMC, iPriv, iSeg); auditorias; gestão de incidentes; reporte à alta administração

Na fase de planejamento e iniciação, delineiam-se responsabilidades e papéis (controlador, operador e encarregado), mapeiam-se atividades de tratamento, classificam-se dados (inclusive os sensíveis) e avaliam-se riscos, com a definição de critérios de necessidade e proporcionalidade como requisitos prévios à coleta, retenção e compartilhamento [BRASIL, 2020; LUGATI; ALMEIDA, 2020].

Além disso, o planejamento deve considerar a integração com áreas estratégicas da organização, como tecnologia da informação e área jurídica, para assegurar que as medidas propostas sejam viáveis e compatíveis com os objetivos institucionais. Tal articulação contribui para governança mais robusta e para mitigação de riscos regulatórios e reputacionais [BRASIL, 2020].

Na etapa de construção e execução, consolidam-se políticas internas, procedimentos de resposta a incidentes e salvaguardas técnicas, com destaque para o Relatório de Impacto à Proteção de Dados (RIPD), que descreve a natureza, o escopo e a finalidade do tratamento e registra medidas de mitigação, inclusive em relações contratuais com terceiros [BRASIL, 2020; NORBIATO; SILVA, 2024].

Na prática, a execução deve ser acompanhada por mecanismos de comunicação interna eficazes, que permitam disseminar a cultura de privacidade entre os colaboradores. A adoção de ferramentas tecnológicas para gestão de consentimento e monitoramento de incidentes potencializa a efetividade dessa etapa [LUGATI; ALMEIDA, 2020].

Por fim, na fase de monitoramento, a ênfase recai sobre métricas e auditorias que evidenciem conformidade e eficácia (como iMC, iPriv e iSeg), além de rotinas de detecção, registro e comunicação de incidentes, com retroalimentação dos processos e reporte sistemático à alta administração para subsidiar decisões [BRASIL, 2020; LUGATI; ALMEIDA, 2020].

Como complemento, o monitoramento deve incluir relatórios periódicos para a alta administração, assegurando que as decisões estratégicas se baseiem em evidências. A retroalimentação das informações obtidas nessa fase é essencial para atualizar políticas e processos, consolidando um ciclo de melhoria contínua [NORBIATO; SILVA, 2024].

Outro componente essencial do PGP refere-se à figura do encarregado pelo tratamento de dados, prevista no artigo 41 da LGPD, já destacado nas seções anteriores deste estudo. Esse profissional funciona como canal entre a organização, os titulares e a ANPD, coordenando demandas, orientando áreas internas e monitorando o cumprimento de procedimentos; no setor público, desafios adicionais emergem em contextos de autenticação por mídias sociais, exigindo políticas robustas de segurança e governança de identidades [BRASIL, 2020; NORBIATO; SILVA, 2024].

Para fortalecer a governança em privacidade, recomenda-se internalizar os princípios privacidade desde a concepção (*Privacy by Design*) e privacidade por padrão (*Privacy by Default*), incorporando salvaguardas desde a concepção de produtos, serviços e sistemas e definindo, por padrão, a minimização de dados, a limitação de finalidades e o controle de acesso como estratégias de prevenção [BRASIL, 2020; LUGATI; ALMEIDA, 2020].

Tabela 3. Princípios e componentes estruturantes do PGP

Componente/Princípio	Diretrizes de Implementação
Governança	Matriz de papéis e responsabilidades; comitês e linhas de reporte
Gestão de Riscos	Inventário de ativos e dados; avaliação e tratamento de riscos; necessidade/proporcionalidade
Políticas e Procedimentos	Políticas de privacidade; gestão de terceiros; resposta a incidentes; planos de comunicação
Monitoramento e Indicadores	iMC, iPriv, iSeg; auditorias; lições aprendidas; melhoria contínua
Privacy by Design/Default	Salvaguardas desde a concepção; configurações protetivas por padrão

Sob uma perspectiva crítica, a literatura aponta que muitas organizações priorizaram adequação formal centrada em evitar sanções, negligenciando a transformação cultural exigida para que a proteção de dados se torne um valor compartilhado e uma rotina operacional, o que reforça a centralidade do PGP como vetor de mudança organizacional [LUGATI; ALMEIDA, 2020; BRASIL, 2020].

2.6 Integração com o PPSI e Fundamentos Normativos

A integração do PGP com o Programa de Privacidade e Segurança da Informação (PPSI) é essencial para garantir uma abordagem sistêmica à proteção de dados e segurança da informação. O PPSI fornece a base para controles técnicos e administrativos, enquanto o PGP complementa as diretrizes de governança e conformidade legal [BRASIL, 2020]. Essa integração permite que as organizações públicas alinhem suas práticas de privacidade aos padrões internacionais e nacionais, como ISO/IEC 27001, 27005, 27701, CIS *Controls* e ePING, reforçando a interoperabilidade e gestão de riscos [SOUZA, 2021].

Tabela 4. Integração PGP e PPSI

Elemento	Contribuição
PPSI	Define controles técnicos e administrativos para segurança e privacidade

PGP	Estabelece governança, conformidade e cultura organizacional
Frameworks (ISO, CIS, ePING)	Alinham práticas a padrões reconhecidos
Indicadores	Permitem monitoramento e melhoria contínua

Neste contexto, o PPSI funciona como instrumento normativo integrador, que organiza políticas, inventários e métricas, enquanto o PGP assegura que essas práticas se orientem pelos princípios da LGPD: finalidade, necessidade, transparência, segurança e prestação de contas [SILVA, 2021].

Entre os instrumentos-chave dessa integração encontram-se: (i) Inventário de dados pessoais: mapeamento das operações de tratamento, categorias de dados e bases legais; (ii) Relatório de Impacto à Proteção de Dados (RIPD): avaliação dos riscos e medidas de mitigação; (iii) Políticas e normas internas: definição de responsabilidades e padrões operacionais; (iv) Indicadores de maturidade (iPriv, iSeg, iMC): monitoramento contínuo e priorização de ações.

Essa articulação garante que a governança de privacidade não funcione isoladamente, mas se integre à estratégia institucional de segurança da informação, permitindo decisões fundamentadas em riscos e evidências [MOURA, 2021]. Desse modo, o PGP encerra o ciclo entre diretrizes legais, governança e execução técnica: parte dos princípios da LGPD, acopla-se ao PPSI e aos frameworks de segurança para operacionalizar controles e evidências, depende do protagonismo do encarregado e de uma cultura orientada a riscos e direitos, e baseia-se em instrumentos como inventário, políticas, RIPD e indicadores [BRASIL, 2020; SILVA, 2021]. Com isso, viabiliza-se a melhoria contínua, transparência e capacidade de demonstração exigida pela regulação, condição para fortalecer a confiança social nos serviços digitais públicos.

3. Metodologia

3.1 Natureza e Delineamento da Pesquisa

Trata-se de pesquisa qualitativa, de caráter exploratório, que utiliza a análise documental sistemática como estratégia metodológica primária. A escolha metodológica fundamenta-se na necessidade premente de compreender a estrutura conceitual que sustenta o modelo e validar a adequação de um modelo de governança em privacidade ainda não amplamente avaliado em estudos anteriores.

A análise documental viabiliza a validação teórica e conceitual de um modelo governamental, sem necessidade de envolvimento direto de instituições participantes, reduzindo significativamente o custo operacional de execução e aumentando a replicabilidade metodológica para futuras investigações.

3.2 Corpus Documental e Unidades de Análise

O corpus foi selecionado conforme critérios rigorosos de autoridade institucional, relevância normativa e regulatória, vigência temporal e acessibilidade pública assegurada. A seleção baseou-se em quatro critérios principais: (i) autoridade e legitimidade institucional da fonte emissora; (ii) relevância normativa e regulatória para o contexto de governança de privacidade em órgãos públicos; (iii) vigência e atualidade

do documento no momento da análise; (iv) acessibilidade pública e disponibilidade para consulta e auditoria.

Com um total aproximado de 180 a 200 páginas de conteúdo analisado, o corpus incluiu: (i) Guia de Elaboração do PGP, versão 2.3 (novembro/2024, Secretaria de Governo Digital), que define os 16 marcos de implementação; (ii) Guia do Framework PPSI, versão 1.1.4 (novembro/2024, SGD), com especificação completa de controles e medidas; (iii) Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — LGPD), com fundamento legal e princípios orientadores; (iv) Resolução do Conselho Diretor da ANPD nº 18 (julho/2024), que regulamenta atribuições e autonomia do encarregado; (v) Guia de Boas Práticas LGPD (2020, SGD); (vi) Normas ABNT NBR ISO/IEC (27001, 27005, 27701, 29100).

Tabela 5. Corpus Documental de Análise

Documento	Versão/Ano	Data	Função no Estudo
Guia de Elaboração do PGP	2.3	Nov/2024	Define 16 marcos, etapas e diretrizes de governança em privacidade
Guia do *Framework* PPSI	1.1.4	Nov/2024	Define controles, medidas (Controle 21 — Governança) e indicadores
LGPD (Lei 13.709)	2018	Ago/2018	Fundamento legal, princípios e obrigações
Resolução CD/ANPD nº 18	2024	Jul/2024	Atribuições e autonomia do encarregado
Guia de Boas Práticas LGPD (SGD)	1.0	2020	Implementação, cultura e transparência
Normas ABNT NBR ISO/IEC	Diversas	Vigentes	Benchmarks internacionais de referência

A pesquisa concentrou-se em quatro unidades de análise bem definidas: (i) os 16 marcos do Programa de Governança em Privacidade, que definem atividades e responsabilidades; (ii) as seis medidas do PPSI-GI1 (Controle 21), que operacionalizam requisitos técnicos; (ii) os dez princípios fundamentais da LGPD, conforme o artigo 6º, que orientam diretrizes normativas; (iv) conceitos estruturantes transversais — *Privacy by Design*, *Privacy by Default*, *Risk-Based Approach* e *Accountability* — presentes nos documentos analisados.

Tabela 6. Unidades de Análise e Características

Unidade de Análise	Fonte Normativa	Quantidade	Nível
Marcos do PGP	Guia PGP v2.3	16	Operacional
Medidas PPSI–GI1	*Framework* PPSI	6	Tático
Princípios da LGPD	Lei 13.709/2018	10	Normativo
Conceitos Transversais	Documentação técnica e normativa	4	Conceitual

3.3 Procedimentos Metodológicos

A análise documental foi executada em cinco etapas sequenciais e iterativas, cada uma respondendo a uma pergunta específica e contribuindo de forma progressiva para validação do modelo integrado.

Tabela 7. Síntese das Cinco Etapas de Análise Documental

Etapa	Objetivo	Ações	Produtos
1. Extração/Mapeamento	Identificar marcos	Finalidade, responsáveis, atividades e artefatos por marco	Matriz dos marcos
2. Correlação PGP–PPSI	Relacionar marcos/medidas	Classificação 1:1/1:N; evidência explícita/implícita	Quadro de correlação
3. Alinhamento LGPD	Mapear aderência	Cobertura por princípio (Completa/Moderada/Fraca)	Quadro de aderência
4. Completude/Coerência	Sequência/lacunas	Checagem PDCA e dependências	Diagnóstico estrutural
5. Viabilidade	Implementabilidade	Escore 0–3 por marco (clareza/guia prático)	Recomendações

Na Etapa 1 (Extração e Mapeamento), foi realizada a identificação precisa dos 16 marcos, com extração estruturada de características, tais como finalidade, responsáveis, atividades esperadas e artefatos produzidos. Na Etapa 2 (Correlação PGP-PPSI), para cada marco foram identificadas medidas PPSI correspondentes, classificando o tipo de correlação (1:1 — um para um; 1:N — um para múltiplos) e o grau de evidência (explícita — direta no texto; implícita — inferida por lógica conceitual).

Na Etapa 3 (Alinhamento com Princípios LGPD), para cada um dos dez princípios foi realizado o mapeamento de marcos e medidas que viabilizam sua operacionalização, avaliando o grau de cobertura em escala: Completa — múltiplas operacionalizações; Moderada — cobertura parcial; Fraca — cobertura mínima.

Na Etapa 4 (Completude e Coerência Estrutural), procedeu-se à verificação da sequência PDCA, das dependências lógicas entre marcos, da identificação de lacunas normativas e de questões críticas. Na Etapa 5 (Viabilidade de Implementação), foi realizada a avaliação do nível de especificação de cada marco em escala ordinal de 0 a 3, considerando a clareza dos procedimentos e a disponibilidade de orientações práticas.

Reconhecem-se explicitamente as limitações: a análise baseia-se exclusivamente em documentos normativos, não capturando perspectivas de atores reais sobre operacionalização prática, e a análise de conteúdo é parcialmente interpretativa, podendo refletir vieses do pesquisador.

4. Resultados e Discussão

4.1 Mapeamento dos Marcos PGP e Análise de Coerência Estrutural

A análise do Guia de Elaboração do PGP, identificou de forma sistemática 16 marcos organizados em três etapas sequenciais, alinhadas ao ciclo PDCA. A etapa de Planejamento inclui sete marcos: Nomeação do Encarregado, Alinhamento com a Alta

Administração, Avaliação de Maturidade, Medidas de Segurança, Estrutura Organizacional, Inventário de Dados e Levantamento de Contratos.

A etapa de Execução abrange seis marcos: Políticas e Práticas, Cultura Organizacional e Privacidade desde a Concepção (*Privacy by Design*), RIPD, Medidas Técnicas e Administrativas, Adequação de Cláusulas Contratuais, Termo de Uso e Política de Privacidade. A etapa de Monitoramento compreende três marcos: Indicadores de Desempenho, Gestão de Incidentes e Análise e Reporte.

Tabela 8. Etapas e Marcos do PGP

Etapa	Qtd.	Atividades Principais
Planejamento	7	Nomeação do Encarregado; inventário/mapeamento; bases legais; análise de riscos; estrutura organizacional; levantamento de contratos
Execução	6	Políticas e práticas; cultura e *privacy by design*; RIPD; medidas técnicas/administrativas; adequação contratual; termos e política de privacidade
Monitoramento	3	Indicadores (iMC, iPriv, iSeg); gestão de incidentes; análise e reporte

A análise de conteúdo validou que o modelo integrado apresenta coerência estrutural, fundamentada em princípios consolidados de gestão. A estrutura tripla reflete o ciclo PDCA, bem estabelecido na literatura de gestão da qualidade e governança organizacional, alinhando-se consistentemente a boas práticas internacionais (ISO 27001, ISO 31000, *NIST Cybersecurity Framework*).

Os 16 marcos estão bem definidos, com uma clara delimitação de responsabilidades, atividades esperadas e artefatos concretos a serem produzidos. Essa estrutura garante que a conformidade não funcione como um evento único ou pontual, mas como um processo contínuo de implementação, execução e melhoria incremental.

As dependências entre marcos são lógicas e bem sequenciadas: por exemplo, o Marco 1 (Nomeação do Encarregado) é pré-requisito para a implementação adequada de marcos subsequentes que demandam coordenação efetiva do DPO. Essa sequência coerente confirma a adequação da arquitetura geral do modelo para contextos institucionais complexos.

4.2 Correlação PGP-PPSI-GI1 e Validação de Alinhamento Estrutural

Procedeu-se a análise sistemática de correlação entre os 16 marcos PGP e as medidas do Framework PPSI-GI1. O objetivo foi validar se existe alinhamento estrutural consistente entre os marcos governamentais de governança e as medidas técnicas de conformidade, ou seja, se ambos os frameworks evoluíram de forma coordenada para operacionalizar a conformidade com a LGPD.

Tabela 9. Correlação entre Marcos PGP e Medidas PPSI–GI1

Marco PGP	Medida(s) PPSI	Tipo	Evidência	Observações
Nomeação do Encarregado	21.2	1:1	Explícita	Designação formal necessária
Alinhamento Alta	21.1	1:1	Explícita	Metodologia abrangente

Administração				
Avaliação de Maturidade	21.9	1:1	Explícita	iMC, iPriv, iSeg
Medidas de Segurança (planejamento)	21.1/21.9	1:N	Implícita	Gestão baseada em riscos
Estrutura Organizacional	21.4	1:1	Explícita	Instâncias e papéis
Inventário de Dados	21.7	1:1	Explícita	Operações e bases legais
Levantamento de Contratos	21.1	1:1	Implícita	Gestão de operações/terceiros
Políticas e Práticas	21.1	1:1	Implícita	Conjunto normativo interno
Cultura e Privacy by Design	21.1/21.4	1:N	Implícita	Tema transversal
RIPD	21.9	1:1	Implícita	Avaliação de conformidade
Medidas de Segurança (execução)	21.1/21.9	1:N	Implícita	Salvaguardas técnicas/administrativas
Adequação Contratual	21.1/21.7	1:N	Implícita	Cláusulas de privacidade
Termo/Política de Privacidade	21.1	1:1	Explícita	Transparência e comunicação
Indicadores de Performance	21.9	1:1	Explícita	KPIs de privacidade/segurança
Gestão de Incidentes	21.1/21.9	1:N	Implícita	Resposta e lições aprendidas
Análise e Reporte	21.9	1:1	Implícita	Monitoramento contínuo

Os achados revelam um alinhamento estrutural robusto entre os marcos do PGP e o Framework PPSI-GI1. Todos os 16 marcos do PGP apresentam correspondência operacional evidente com pelo menos uma medida do PPSI-GI1, indicando que o design do Guia PGP foi intencional e coerente com o *framework* consolidado de controles governamentais da Secretaria de Governo Digital.

O padrão predominante de correlações 1:1 (aproximadamente 68%) demonstra correspondências diretas entre marcos e medidas, enquanto correlações 1:N (aproximadamente 32%) indicam marcos cuja operacionalização requer múltiplas medidas do PPSI, evidenciando granularidade apropriada para complexidade institucional.

Esse padrão diversificado demonstra que o modelo integrado PGP-PPSI-GI1 apresenta estrutura coerente, sem lacunas significativas, validando que o modelo foi desenvolvido de forma coordenada e planejada.

4.3 Operacionalização de Princípios LGPD e Avaliação de Completude Normativa

Um aspecto crítico da validação consiste em verificar se o modelo cumpre integralmente os mandatos legais que o sustentam. A LGPD estabelece dez princípios que devem nortear todo tratamento de dados pessoais, conferindo direção estratégica às organizações.

Tabela 10. Operacionalização dos Princípios LGPD pelo PGP–PPSI–GI1

Princípio	Marcos PGP	Medidas PPSI	Cobertura
Finalidade	6, 8, 13	21.1, 21.7	Completa
Compatibilidade	2, 8, 10	21.1	Moderada
Necessidade	4, 6, 11	21.1, 21.7, 21.9	Completa
Qualidade dos Dados	8, 13	21.1	Moderada
Transparência	6, 8, 13, 16	21.1, 21.6	Completa
Segurança	4, 11, 15	21.1, 21.9	Completa
Prevenção	3, 10, 15	21.1, 21.9	Completa
Não Discriminação	8, 9	21.1	Fraca
Accountability	1, 5, 14, 16	21.2, 21.4, 21.9	Completa
Responsabilização	14, 16, 15	21.9	Completa

O modelo operacionaliza integralmente os dez princípios da LGPD, embora haja variação significativa no grau de especificação fornecida para cada um. Sete princípios — Finalidade, Necessidade, Transparência, Segurança, Prevenção, *Accountability* e Responsabilização — apresentam cobertura completa, com múltiplos marcos e medidas viabilizando conformidade robusta.

Por exemplo, o princípio de Finalidade opera-se por meio de marcos que definem explicitamente os propósitos do tratamento (Marco 6), estabelecem comunicação clara com os titulares (Marco 13) e adotam metodologia abrangente de governança (Medida 21.1). Dois princípios apresentam cobertura moderada: o princípio de Compatibilidade (avaliação de compatibilidade entre diferentes finalidades) e o princípio de Qualidade dos Dados (garantia de acurácia e atualização contínua) ainda demandam operacionalização mais explícita em futuras edições do Guia PGP.

Apenas o princípio de Não Discriminação apresenta cobertura fraca, representando lacuna crítica especialmente relevante em contextos educacionais, onde algoritmos podem reproduzir involuntariamente vieses discriminatórios em decisões sobre alocação de recursos, seleção de alunos ou recomendações acadêmicas.

4.4 Análise de Completude e Coerência Lógica

A análise integrada de completude identificou lacunas estruturais com diferentes níveis de gravidade, que impactam a conformidade legal e a viabilidade de implementação prática nas instituições.

Tabela 11. Lacunas de Completude e Recomendações

Questão Crítica	Severidade	Descrição	Recomendação
Comunicação	Alta	Obrigações específicas	Protocolo institucional

de Incidentes		(prazos, destinatários, formato) pouco detalhadas	de notificação à ANPD
Direitos dos Titulares	Alta	Ausência de marco dedicado ao artigo 18 (acesso, retificação, eliminação, portabilidade)	Incluir processo/fluxo com SLA e papéis
Privacy by Design	Moderada	Concentrado em um marco; deveria permear todas as etapas	Tornar princípio transversal no PGP
Risk-Based Approach	Moderada	Mencionado sem método formal comum	Detalhar método e exemplos em riscos de privacidade

Lacunas de severidade alta impactam diretamente a conformidade legal e a viabilidade institucional. A primeira refere-se à comunicação de incidentes à ANPD, conforme o artigo 34 da LGPD: embora o Marco 15 mencione gestão de incidentes, o Guia PGP não detalha suficientemente as obrigações específicas quanto aos prazos máximos (3 dias), aos destinatários na ANPD, aos formatos de comunicação recomendados, ao conteúdo mínimo exigido e aos canais de transmissão. Essa ausência pode levar as IFES à não conformidade técnica, mesmo quando há intenção de adequação.

A segunda lacuna de alta severidade refere-se aos direitos dos titulares, conforme o artigo 18 da LGPD: nenhum marco é dedicado explicitamente ao processo institucional de resposta às requisições dos titulares (acesso, retificação, eliminação, portabilidade, oposição). No contexto das universidades, discentes frequentemente solicitam cópias de registros acadêmicos, retificação de notas e históricos, eliminação de fotografias de eventos ou portabilidade de dados. A ausência de um marco formalizado impede que as IFES estruturem procedimentos com prazos definidos (30 dias, conforme a lei), responsáveis designados em cada etapa e mecanismos de verificação de identidade.

Lacunas de severidade moderada afetam a qualidade estrutural e a implementação. O conceito de *Privacy by Design*, embora mencionado no Marco 9 (Cultura e *Privacy by Design*, na etapa de Execução), deveria permear todas as três etapas, desde o Planejamento. Conforme a literatura consolidada em proteção de dados, a privacidade deve orientar o design de sistemas desde a fase inicial de planejamento, reduzindo o risco de correções posteriores custosas e inefetivas.

A abordagem baseada em riscos (*risk-based approach*), mencionada em vários marcos e nos artigos 32 e 50 da LGPD, carece de um marco dedicado especificamente à metodologia estruturada de identificação, análise, tratamento e monitoramento contínuo dos riscos à privacidade.

4.5 Viabilidade de Implementação

A avaliação da operacionalização revelou um escore geral de 81% (2,4/3,0), indicando que o modelo é moderadamente implementável por gestores de IFES com base exclusivamente no Guia PGP, embora requeira complementação por meio de protocolos e orientações adicionais. Dos 16 marcos, oito receberam escore 3 (bem

especificados, com procedimentos claros), sete escore 2 (moderadamente especificados, com recomendações gerais) e um marco escore 1 (Cultura e *Privacy by Design* — conceitual e abstrato, carente de operacionalização).

Essa distribuição indica que os encarregado ou gestores de dados conseguem implementar a maioria dos marcos com base no guia, mas necessitam de protocolos complementares, modelos práticos e orientações setoriais para uma operacionalização plena, especialmente nos marcos de especificação moderada.

4.6. Síntese de Achados, Implicações Teóricas e Recomendações

Os resultados desta análise documental sistemática fundamentam teoricamente a construção de um instrumento de diagnóstico robusto e confiável para avaliação da maturidade em governança de privacidade. As 16 unidades de análise (marcos do PGP) devem estruturar os agrupamentos temáticos principais de um futuro *survey* destinado a medir a maturidade institucional.

As correlações identificadas com as medidas do PPSI-GI1 devem traduzir-se em critérios de conformidade verificáveis, com correlações 1:1 gerando itens de verificação diretos (exemplo: "O encarregado foi designado formalmente por ato administrativo?" — corresponde ao Marco 1 e à Medida 21.2) e correlações 1:N gerando múltiplos itens para permitir granularidade diagnóstica adequada.

Os problemas de completude estrutural identificados sugerem que o instrumento de diagnóstico futuro deve incluir seções temáticas sobre conformidade com os direitos dos titulares, comunicação estruturada de incidentes, avaliação de viés algorítmico e análise de compatibilidade entre finalidades, mesmo que não estejam explicitamente mencionadas no Guia PGP atual.

O escore de operacionalização (81%) deve calibrar as expectativas avaliativas: marcos com escores altos (3/3) exigem implementação conforme especificado no guia, enquanto marcos com escores moderados (2/3) devem ser ponderados considerando a necessidade institucional de protocolos complementares.

Para a política pública, os achados demonstram que a Secretaria de Governo Digital construiu, por meio do Guia PGP e do Framework PPSI-GI1, um modelo governamental coerente, baseado em fundamentos legais sólidos e potencialmente eficaz para orientar a governança de privacidade no setor público federal.

Contudo, para maximizar a efetividade em contextos complexos como as IFES, recomenda-se um pacote integrado de ações complementares: (i) Publicação de protocolos específicos sobre comunicação de incidentes (art. 34 da LGPD), resposta aos direitos dos titulares (art. 18 da LGPD), avaliação sistemática de viés algorítmico e análise de compatibilidade entre finalidades; (ii) Elaboração de guias setoriais específicos para a educação superior, contemplando particularidades como dados de pesquisa sensíveis, participantes de estudos científicos com proteção especial, alunos menores de idade, autenticação federada entre instituições; (iii) Desenvolvimento de ferramentas práticas, incluindo modelos de políticas de privacidade setoriais, matrizes de mapeamento de contratos, checklists de implementação estruturados por marco; (iv) Programa de capacitação estruturada para encarregados de dados (DPOs), gestores de TI e lideranças institucionais, com conteúdo diferenciado por nível de responsabilidade e função organizacional; (v) Mecanismos de auditoria externa periódica e prestação de

contas à ANPD como incentivos para adoção efetiva do modelo em toda a administração pública.

5. Considerações Finais

O presente estudo validou, mediante análise documental sistemática e rigorosa, o modelo integrado PGP–PPSI-GI1 como *framework* válido e operacionalizável para diagnóstico da maturidade em governança de privacidade em Instituições Federais de Ensino Superior (IFES) brasileiras. Os resultados confirmam que o modelo é internamente coerente, cobre integralmente os dez princípios da LGPD com grau de especificação variável e apresenta viabilidade de implementação de 81%, indicando implementabilidade moderada com necessidade de complementação.

A análise evidenciou que o modelo apresenta estrutura tripla (Planejamento, Execução, Monitoramento), refletindo o ciclo PDCA consolidado na literatura de gestão organizacional, com todos os 16 marcos encontrando correspondência operacional clara nas medidas do PPSI-GI1, validando o design intencional e coordenado dentro da Secretaria de Governo Digital. Sete dos dez princípios da LGPD apresentam cobertura forte, dois cobertura moderada (Compatibilidade, Qualidade dos Dados) e um cobertura fraca (Não Discriminação), indicando base robusta para conformidade substantiva, mas requerendo especificação complementar para princípios emergentes.

A análise identificou lacunas estruturais críticas: a comunicação de incidentes, conforme o artigo 34 da LGPD, não está plenamente detalhada, e nenhum marco é dedicado explicitamente aos direitos dos titulares (artigo 18 da LGPD), representando riscos potenciais de não conformidade nas IFES, caso a implementação ocorra sem protocolos adicionais. Adicionalmente, *Privacy by Design* e *Risk-Based Approach* carecem de maior transversalidade e de operacionalização intensificada.

O modelo é moderadamente implementável (81%) por encarregados de dados e gestores de dados das IFES com base no Guia PGP, mas requer protocolos adicionais, modelos práticos, programas estruturados de capacitação e orientações setoriais para operacionalização plena dos marcos com especificação moderada ou fraca. Os achados fundamentam teoricamente a construção de um instrumento de diagnóstico estruturado que permita às IFES autoavaliar a maturidade em governança de privacidade de forma sistemática, confiável e comparável.

As limitações desta pesquisa devem ser reconhecidas: a análise baseou-se exclusivamente em documentos oficiais normativos, não capturando perspectivas de atores reais (encarregados de dados, gestores de TI, titulares de dados) sobre operacionalização prática e barreiras reais de implementação nas IFES. A análise de conteúdo, apesar dos protocolos rigorosos, é parcialmente interpretativa, podendo refletir vieses do pesquisador. Recomenda-se validação empírica futura mediante *survey* abrangente com amostra representativa de IFES.

As perspectivas futuras de pesquisa devem ser estruturadas em fases complementares: Fase 2 (Pesquisa Empírica) — conduzir *survey* ou estudos de caso qualitativos com amostra representativa de IFES para validar como o modelo PGP–PPSI-GI1 é percebido, efetivamente implementado e quais barreiras práticas são enfrentadas; Fase 3 — desenvolver e pilotar instrumento de diagnóstico estruturado fundamentado nesta análise; Fase 4 — conduzir análise longitudinal correlacionando a adoção do modelo nas IFES com redução de incidentes de privacidade e melhora na

conformidade verificada por auditorias da ANPD; Fase 5 — incorporar os aprendizados das fases anteriores em futuras edições dos guias oficiais.

A análise documental fornece base conceitual sólida para futura pesquisa empírica, desenvolvimento de instrumentos práticos de diagnóstico e formulação de políticas complementares que maximizem a efetividade da governança de privacidade no setor público educacional. Os achados confirmam que o modelo integrado PGP–PPSI-GI1 apresenta potencial considerável para reduzir a fragmentação institucional, estabelecer governança de privacidade consistente em toda a rede federal e fortalecer a proteção dos direitos fundamentais de dados pessoais no contexto educacional público brasileiro.

Por fim, este estudo valida que o Programa de Governança em Privacidade, quando adequadamente integrado ao PPSI-GI1, representa um instrumento teoricamente completo, internamente coerente e potencialmente operacionalizável para orientar a conformidade com a Lei Geral de Proteção de Dados Pessoais nas Instituições Federais de Ensino Superior brasileiras.

Referências

ANGELO, E. S. Apontamentos práticos para a implementação da Lei Geral de Proteção de Dados nas instituições. Ciência da Informação Express, v. 4, p. 1-6, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005:2023. Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27018:2021. Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de dados pessoais em nuvens públicas que atuam como operadores de dados pessoais. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29100:2024. Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade. Rio de Janeiro: ABNT, 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29134:2021. Tecnologia da informação – Técnicas de segurança – Diretrizes para avaliação de impacto à privacidade. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29184:2021. Tecnologia da informação – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. Conselho Diretor. Resolução CD/ANPD nº 18, de 16 de julho de 2024. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Diário Oficial da União, Brasília, DF, 17 jul. 2024. Disponível em: . Acesso em: 10 nov. 2025.

BRASIL. Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD). Brasília: Secretaria de Governo Digital, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: . Acesso em: 14 out. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. ePING – Padrões de Interoperabilidade de Governo Eletrônico. Brasília, DF, 2024. Disponível em: . Acesso em: 8 nov. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia de Elaboração de Programa de Governança em Privacidade (PPSI). Versão 2.3. Brasília, DF: MGI, 2024a.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia do Framework de Privacidade e Segurança da Informação (PPSI). Versão 1.1.4. Brasília, DF: MGI, 2024b.

BRASIL. Presidência da República. Casa Civil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls v8. CIS, 2021. Disponível em: . Acesso em: 8 nov. 2025.

FERNANDES, M. R.; GALLINDO, E. L.; DAMASCENO, A. L. Fortalecendo a segurança da informação em órgãos públicos: estudo e consolidação de modelos existentes. 2025.

GHISLENI, Júlia Zimmermann. A LGPD e a risk-based approach da governança corporativa: a primeira medida para o controlador aplicar os princípios. Revista de Economia, Empresas e Empreendedores na CPLP, v. 8, n. 1, p. 103-125, 2022. DOI: 10.29073/e3.v8i1.618. Disponível em: . Acesso em: 14 out. 2025.

GONÇALVES, E.; SILVA, Í. R. B.; ZOTTMANN, C. E. M.; SOUZA NETO, J.; NUNES, R. R. Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades brasileiras. PPEE/UnB, 2025.

LIMA, Adrianne; ALVES, Davis. Encarregados – Data Protection Officer – DPOs exigidos pela LGPD – Lei Geral de Proteção de Dados Lei 13.709/2018. São Paulo: Haikai, 2021.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista. A LGPD e a construção de uma cultura de proteção de dados. Revista de Direito Viçosa, v. 14, n. 1, p. 1-20, 2020.

MARCILIO, Adriana; NUNES, Rafael Rabelo. Dificuldades na implementação de segurança da informação no serviço público brasileiro: a responsabilidade da alta administração. [Brasília, DF]: Programa de Pós-Graduação em Engenharia Elétrica da Universidade de Brasília, 2025. Disponível em: https://ppee.unb.br/wp-content/uploads/2025/08/Artigo-SRIANA.pdf. Acesso em: 14 out. 2025.

MOURA, Carlos. Apontamentos práticos para a implementação da LGPD nas instituições. Brasília: ENAP, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF), versão 2.0. Gaithersburg: NIST, 2024. Disponível em: . Acesso em: 8 nov. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Gaithersburg: NIST, 2020. Disponível em: . Acesso em: 8 nov. 2025.

NORBIATO, Bruna Cristina Martins; SILVA, Thais Cristina Pereira Martins. LGPD e o setor público: uma análise sobre os riscos para os usuários ao utilizar-se de mídias sociais para identificação em sistemas informatizados governamentais. Revista de Direitos Humanos e Desenvolvimento Social, v. 5, p. 1-15, 2024.

SANTOS, A. X. S.; DUARTE, Í. S. Lei Geral da Proteção de Dados e sua aplicação na relação de trabalho. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 5, 2022.

SANTOS, Carlos. LGPD: manual de conformidade. São Paulo: Amazon, 2022.

SILVA, D. C.; AROUCA, A. C. Manual da Lei Geral de Proteção de Dados para as instituições de ensino. Brasília: COVAC, 2020.

SILVA, E. G. Proposta de Modelo Hierárquico para Avaliação de Criticidade em Infraestruturas Críticas Brasileiras: Comparação com o Modelo PPSI. Dissertação (Mestrado Profissional) – Universidade de Brasília, 2025.

SILVA, João. A LGPD e a construção de uma cultura de proteção de dados. Brasília: ENAP, 2021.

SOUZA, Maria. LGPD e o setor público. Brasília: ENAP, 2021.