

UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
CAMPUS CHAPECÓ
CURSO DE MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA EM
REDE NACIONAL

FLAVIO HUMBERTO TESTA

AVALIAÇÃO DA EFETIVIDADE DO PROGRAMA DE PRIVACIDADE E
SEGURANÇA DA INFORMAÇÃO (PPSI) NAS INSTITUIÇÕES FEDERAIS DE
ENSINO SUPERIOR

CHAPECÓ

2026

FLAVIO HUMBERTO TESTA

**AVALIAÇÃO DA EFETIVIDADE DO PROGRAMA DE PRIVACIDADE E
SEGURANÇA DA INFORMAÇÃO (PPSI) NAS INSTITUIÇÕES FEDERAIS DE
ENSINO SUPERIOR**

Dissertação apresentada ao Mestrado Profissional em
Administração Pública em Rede Nacional (PROFIAP)
da Universidade Federal da Fronteira Sul (UFFS),
como requisito para obtenção do título de Mestre em
Administração Pública.

Orientadora: Dra. Débora Regina Schneider Locatelli

CHAPECÓ

2026

FLAVIO HUMBERTO TESTA

**AVALIAÇÃO DA EFETIVIDADE DO PROGRAMA DE PRIVACIDADE E
SEGURANÇA DA INFORMAÇÃO (PPSI) NAS INSTITUIÇÕES FEDERAIS DE
ENSINO SUPERIOR**

Dissertação apresentada ao Mestrado Profissional em Administração Pública em Rede Nacional (PROFIAP) da Universidade Federal da Fronteira Sul (UFFS), como requisito para obtenção do título de Mestre em Administração Pública.

Esta Dissertação foi defendida e aprovada pela banca examinadora em 17 de Agosto de 2026.

BANCA EXAMINADORA

Documento assinado digitalmente
 **DEBORA REGINA SCHNEIDER LOCATELLI**
Data: 15/09/2026 17:20:47-0300
Verifique em <https://validar.iti.gov.br>

Prof.^a Dr.^a Débora Regina Schneider Locatelli – UFFS (Orientadora)

Documento assinado digitalmente
 **GEORGE LAURO RIBEIRO DE BRITO**
Data: 15/09/2026 17:37:26-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. George Lauro Ribeiro De Brito – UFT (Membro)

Documento assinado digitalmente
 **RAFAEL RABELO NUNES**
Data: 17/09/2026 10:23:34-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. Rafael Rabelo Nunes – UNB (Membro)

Bibliotecas da Universidade Federal da Fronteira Sul - UFFS

Testa, Flavio Humberto

AVALIAÇÃO DA EFETIVIDADE DO PROGRAMA DE PRIVACIDADE E
SEGURANÇA DA INFORMAÇÃO (PPSI) NAS INSTITUIÇÕES FEDERAIS
DE ENSINO SUPERIOR / Flavio Humberto Testa. -- 2026.
200 f.

Orientadora: Dra. Débora Regina Schneider Locatelli

Dissertação (Mestrado) - Universidade Federal da
Fronteira Sul, Programa de Pós-Graduação Profissional
em Administração Pública em Rede Nacional, Chapecó, SC,
2026.

1. segurança da informação. 2. privacidade. 3.
políticas públicas. 4. capacidade institucionais. 5.
efetividade. I. Locatelli, Débora Regina Schneider,
orient. II. Universidade Federal da Fronteira Sul. III.
Título.

RESUMO

Esta dissertação avalia a efetividade percebida do Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior (IFES) e identifica as capacidades institucionais que mais se associam a esses resultados. O estudo insere-se na linha de pesquisa Políticas Públicas do PROFIAP e contribui para a agenda de avaliação de políticas públicas digitais ao articular as literaturas de capacidades estatais, governança de segurança da informação e valor público, tratando a efetividade como resultado percebido, e não como conformidade declarada. A metodologia articulou três etapas: revisão sistemática da literatura conforme o protocolo PRISMA 2020, que consolidou 82 estudos e delimitou seis domínios de capacidade e seis de efetividade; construção e validação de conteúdo de instrumento com 18 itens, por painel de 11 especialistas (método de Lawshe); e aplicação a todo o universo de 110 IFES, com 58 respostas institucionais válidas (52,7%), analisadas por estatística descritiva, correlações de Spearman e regressões exploratórias com erros-padrão robustos. Os resultados indicam assimetria entre a governança formal, dimensão mais consolidada, e as capacidades de sustentação material: recursos orçamentários, integração da gestão de riscos ao planejamento e gestão de dados pessoais figuraram entre as mais frágeis. A maturidade autorrelatada associou-se às capacidades, mas não à efetividade percebida, cuja variação foi explicada pelas capacidades institucionais. A originalidade do trabalho reside em evidenciar, no contexto brasileiro, a distinção empírica entre maturidade e efetividade, com as capacidades como elo entre implementação e resultados. Como contribuição prática, de impacto potencial nas esferas organizacional e de políticas públicas, propõem-se recomendações à gestão das IFES e ao órgão central e o Guia de Avaliação de Capacidades e Efetividade do PPSI nas IFES (GACE-PPSI), produto técnico-tecnológico autoaplicável derivado dos achados.

Palavras-chave: segurança da informação; privacidade; efetividade; capacidades institucionais; PPSI; Instituições Federais de Ensino Superior.

ABSTRACT

This dissertation evaluates the perceived effectiveness of the Brazilian Privacy and Information Security Program (PPSI) in Federal Higher Education Institutions (IFES) and identifies the institutional capacities most strongly associated with these results. The study belongs to the Public Policy research line of PROFIAP and contributes to the digital public policy evaluation agenda by combining the literatures on state capacities, information security governance, and public value, treating effectiveness as a perceived outcome rather than declared compliance. The methodology articulated three stages: a systematic literature review following the PRISMA 2020 protocol, which consolidated 82 studies and delimited six capacity and six effectiveness domains; the construction and content validation of an 18-item instrument by a panel of 11 experts (Lawshe's method); and its application to the entire population of 110 IFES, with 58 valid institutional responses (52.7%), analyzed through descriptive statistics, Spearman correlations, and exploratory regressions with robust standard errors. Results indicate an asymmetry between formal governance, the most consolidated dimension, and material sustainability capacities: budget resources, risk management integrated into planning, and personal data management were among the most fragile. Self-reported maturity was associated with capacities, but not with perceived effectiveness, whose variation was explained by institutional capacities. The study's originality lies in providing empirical evidence, in the Brazilian context, of the distinction between maturity and effectiveness, with capacities as the linking mechanism. As a practical contribution, with potential impact in the organizational and public policy spheres, the study proposes management recommendations and the PPSI Capacity and Effectiveness Assessment Guide for IFES (GACE-PPSI), a self-applicable technical-technological product derived from the findings.

Keywords: information security; privacy; effectiveness; institutional capacities; PPSI; Brazilian federal universities.

LISTA DE ILUSTRAÇÕES

FIGURA 1 – RELAÇÃO ENTRE CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO.....	25
FIGURA 2 – MODELO CONCEITUAL DO NIST FRAMEWORK	31
FIGURA 3 – FLUXO PRISMA 2020	37
GRÁFICO 1 – TRIAGEM POR TÍTULO, <i>ABSTRACT</i> E <i>KEYWORDS</i>	39
GRÁFICO 2 – EXCLUSÃO APÓS LEITURA COMPLETA	41
FIGURA 4 – FLUXO ENTRE MATURIDADE, CAPACIDADES E EFETIVIDADE ...	50
GRÁFICO 3 – DISTRIBUIÇÃO TEMPORAL DAS PUBLICAÇÕES INCLUÍDAS (RSL)	58
GRÁFICO 4 – DISTRIBUIÇÃO POR MÉTODO UTILIZADO.....	59
GRÁFICO 5 – DISTRIBUIÇÃO POR SETOR PÚBLICO	60
GRÁFICO 6 – PAÍSES MAIS FREQUENTES.....	61
GRÁFICO 7 – EIXO TEMÁTICO DO ESTUDO (SEGURANÇA, PRIVACIDADE OU AMBOS)	62
GRÁFICO 8 – FREQUÊNCIA DAS CAPACIDADES.....	63
GRÁFICO 9 – FREQUÊNCIA DA EFETIVIDADE.....	65
GRÁFICO 10 – MATRIZ DE COCORRÊNCIA (CAPACIDADE X EFETIVIDADE)	68
FIGURA 5 – FLUXO DE COMPOSIÇÃO DA BASE ANALÍTICA	78

LISTA DE QUADROS

QUADRO 1 – DEFINIÇÃO DE CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO POR ESTUDO	27
QUADRO 2 – COMPARATIVO DE <i>STANDARDS</i> E <i>FRAMEWORKS</i>	30
QUADRO 3 – DOMÍNIOS DE CAPACIDADE E EFETIVIDADE E SEUS REFERENCIAIS.....	42
QUADRO 4 – CORPUS FINAL DA RSL.....	55
QUADRO 5 – ESTRUTURA DO INSTRUMENTO DE PESQUISA DERIVADA DOS DOMÍNIOS TEÓRICOS.....	70
QUADRO 6 – SÍNTESE DA PRIMEIRA RODADA DE VALIDAÇÃO DE CONTEÚDO POR ESPECIALISTAS	72
QUADRO 7 – ITENS REVISADOS APÓS A RODADA COMPLEMENTAR COM ESPECIALISTAS	75
QUADRO 8 – CRITÉRIOS DE COMPOSIÇÃO DA BASE ANALÍTICA.....	79
QUADRO 9 – SÍNTESE DO CONFRONTO ENTRE ACHADOS EMPÍRICOS E LITERATURA DO PORTFÓLIO	129
QUADRO 10 – RECOMENDAÇÕES, ACHADOS E RESPALDO NA LITERATURA	

LISTA DE TABELAS

TABELA 1 – COMPOSIÇÃO DA AMOSTRA POR TIPO DE IFES	81
TABELA 2 – RELAÇÃO DO RESPONDENTE COM O PPSI	82
TABELA 3 – PERFIL PREDOMINANTE DE ATUAÇÃO DO RESPONDENTE.....	82
TABELA 4 – DISTRIBUIÇÃO REGIONAL DAS IFES PARTICIPANTES.....	83
TABELA 5 – PORTE DAS IFES POR NÚMERO APROXIMADO DE SERVIDORES 83	
TABELA 6 – PORTE DAS IFES POR TAMANHO APROXIMADO DA EQUIPE DE TI/TIC.....	83
TABELA 7 – PORTE DAS IFES POR NÚMERO APROXIMADO DE ESTUDANTES 84	
TABELA 8 – CONDIÇÃO MULTICAMPI DAS IFES PARTICIPANTES.....	84
TABELA 9 – ESTATÍSTICA DESCRITIVA DOS ITENS DE CAPACIDADES INSTITUCIONAIS.....	85
TABELA 10 – DISTRIBUIÇÃO DAS RESPOSTAS DO ITEM C1	86
TABELA 11 – RECORTES EXPLORATÓRIOS DAS IFES COM C1 INFERIOR AO PONTO NEUTRO.....	87
TABELA 12 – MÉDIAS DAS CAPACIDADES SEGUNDO AVALIAÇÃO DE C1	91
TABELA 13 – ESTATÍSTICA DESCRITIVA DOS ITENS DE EFETIVIDADE PERCEBIDA	92
TABELA 14 – EFETIVIDADE PERCEBIDA SEGUNDO A AVALIAÇÃO DE RECURSOS (C8)	96
TABELA 15 – CORRELAÇÃO ENTRE CAPACIDADE TOTAL E EFETIVIDADE PERCEBIDA TOTAL	98
TABELA 16 – CORRELAÇÕES ENTRE CAPACIDADES ESPECÍFICAS E EFETIVIDADE TOTAL.....	99
TABELA 17 – CORRELAÇÕES ENTRE CAPACIDADE TOTAL E DOMÍNIOS DE EFETIVIDADE PERCEBIDA.....	100
TABELA 18 – CORRELAÇÕES ENTRE CAPACIDADES ESPECÍFICAS E DOMÍNIOS DE EFETIVIDADE.....	102
TABELA 19 – CORRELAÇÕES DA MATURIDADE COM CAPACIDADE E EFETIVIDADE PERCEBIDAS	103

TABELA 20 – MODELOS EXPLORATÓRIOS DE REGRESSÃO PARA	
CAPACIDADE E EFETIVIDADE	104

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
CAAE	Certificado de Apresentação de Apreciação Ética
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CEP	Comitê de Ética em Pesquisa
CID	Confidencialidade, Integridade e Disponibilidade
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technologies
CSF	Cybersecurity Framework (NIST)
CVR	Content Validity Ratio (Razão de Validade de Conteúdo)
DPIA	Data Protection Impact Assessment (Avaliação de Impacto à Proteção de Dados)
EDR	Endpoint Detection and Response
GACE-PPSI	Guia de Avaliação de Capacidades e Efetividade do PPSI nas IFES
GDPR	General Data Protection Regulation
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
HC3	Estimador de erros-padrão robustos à heterocedasticidade (tipo 3)
iBase / iSeg / iPriv	Índices de maturidade do PPSI (estrutura básica, segurança da informação e privacidade)
IDS / IPS	Intrusion Detection System / Intrusion Prevention System
IES	Instituições de Ensino Superior
iESGo	Índice de Governança e Sustentabilidade
IFES	Instituições Federais de Ensino Superior
iGG	Índice Integrado de Governança e Gestão Públicas
iGovTI	Índice de Governança de Tecnologia da Informação
IoT	Internet of Things (Internet das Coisas)
ITIL	Information Technology Infrastructure Library
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
MTTD	Mean Time to Detect (tempo médio de detecção)
MTTR	Mean Time to Repair (tempo médio de reparo)

NBR — Norma Brasileira (ABNT)

NIST — National Institute of Standards and Technology

OCDE — Organização para a Cooperação e Desenvolvimento Econômico

ODS — Objetivos de Desenvolvimento Sustentável

PIA — Privacy Impact Assessment (Avaliação de Impacto à Privacidade)

PIMS — Privacy Information Management System (Sistema de Gestão de Privacidade da Informação)

PPSI — Programa de Privacidade e Segurança da Informação

PRISMA — Preferred Reporting Items for Systematic Reviews and Meta-Analyses

PROFIAP — Mestrado Profissional em Administração Pública em Rede Nacional

PTT — Produto Técnico-Tecnológico

RIPD — Relatório de Impacto à Proteção de Dados Pessoais

RSL — Revisão Sistemática da Literatura

SEM — Structural Equation Modeling (Modelagem de Equações Estruturais)

SGD — Secretaria de Governo Digital

SGSI — Sistema de Gestão de Segurança da Informação

SIEM — Security Information and Event Management

SISP — Sistema de Administração dos Recursos de Tecnologia da Informação

SOC — Security Operations Center (Centro de Operações de Segurança)

TCLE — Termo de Consentimento Livre e Esclarecido

TCU — Tribunal de Contas da União

TI / TIC — Tecnologia da Informação / Tecnologia da Informação e Comunicação

UFFS — Universidade Federal da Fronteira Sul

VIF — Variance Inflation Factor (Fator de Inflação da Variância)

WoS — Web of Science

SUMÁRIO

1	INTRODUÇÃO	14
1.1	PROBLEMA DE PESQUISA	16
1.1.1	Problema central	17
1.1.2	Questões norteadoras	17
1.2	OBJETIVO GERAL E OBJETIVOS ESPECÍFICOS.....	17
1.2.1	Objetivo Geral	17
1.2.2	Objetivos Específicos	17
1.3	JUSTIFICATIVA E RELEVÂNCIA DA PESQUISA.....	18
2	REFERENCIAL TEÓRICO.....	20
2.1	POLÍTICAS PÚBLICAS DIGITAIS E VALOR PÚBLICO	20
2.2	GOVERNANÇA E GESTÃO DE TI NO SETOR PÚBLICO.....	24
2.3	CONCEITOS FUNDAMENTAIS DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA.....	25
2.4	PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.....	28
2.5	O PPSI E SEUS REFERENCIAIS NORMATIVOS E TÉCNICOS.....	30
2.6	AValiação de Efetividade em Políticas e Programas.....	33
3	METODOLOGIA	35
3.1	DESENHO E ABORDAGEM DO ESTUDO.....	35
3.2	REVISÃO SISTEMÁTICA DA LITERATURA (RSL).....	35
3.2.1	Objetivo e pergunta.....	35
3.2.2	Bases, termos e filtros	36
3.2.3	Triagem, elegibilidade e códigos de exclusão	38
3.2.4	Leitura integral e extração dos dados.....	40
3.3	DO PORTFÓLIO DA RSL À ETAPA EMPÍRICA.....	41
3.4	MATRIZ DE DOMÍNIOS E INSTRUMENTO PRIMÁRIO: CONSTRUÇÃO, CODIFICAÇÃO, VALIDAÇÃO E COLETA	42
3.4.1	Derivação dos domínios e construção do instrumento	44
3.4.2	Validação de conteúdo por especialistas	46
3.4.3	Aplicação do questionário, qualificação dos respondentes e tratamento de duplicidades.....	47
3.5	INDICADORES IBASE, ISEG E IPRIV E PLANO DE ARTICULAÇÃO ANALÍTICA.....	49
3.6	TRATAMENTO E ANÁLISE DOS DADOS.....	49

3.7	VALIDADE, ÉTICA, LIMITAÇÕES E REPRODUTIBILIDADE	51
4	ANÁLISE SITUACIONAL: RESULTADOS DA REVISÃO SISTEMÁTICA E VALIDAÇÃO DO INSTRUMENTO	55
4.1	RESULTADOS DA REVISÃO SISTEMÁTICA	58
4.2	VALIDAÇÃO DE CONTEÚDO DO INSTRUMENTO POR ESPECIALISTAS.....	71
5	RESULTADOS DA PESQUISA EMPÍRICA COM AS IFES	77
5.1	PREPARAÇÃO DA BASE E COMPOSIÇÃO DA AMOSTRA	78
5.2	PERFIL DOS RESPONDENTES E DAS INSTITUIÇÕES PARTICIPANTES	81
5.3	ESTATÍSTICA DESCRITIVA DAS CAPACIDADES INSTITUCIONAIS....	85
5.4	ESTATÍSTICA DESCRITIVA DA EFETIVIDADE PERCEBIDA	92
5.5	ASSOCIAÇÕES ENTRE CAPACIDADES E EFETIVIDADE PERCEBIDA	97
5.6	ASSOCIAÇÕES COM OS ÍNDICES DE MATURIDADE DO PPSI.....	102
5.7	MODELOS EXPLORATÓRIOS DE REGRESSÃO	104
5.8	SÍNTESE DOS ACHADOS EMPÍRICOS	106
6	DISCUSSÃO, RECOMENDAÇÕES E PRODUTO TÉCNICO	108
6.1	O DESCOMPASSO ENTRE INSTITUCIONALIZAÇÃO FORMAL E CAPACIDADE DE EXECUÇÃO	109
6.2	EFETIVIDADE OPERACIONAL SEM RECONHECIMENTO ESTRATÉGICO.....	112
6.3	MATURIDADE NÃO É EFETIVIDADE: AS CAPACIDADES COMO ELO	115
6.4	A PRIVACIDADE COMO ELO FRÁGIL: ENTRE A CONFORMIDADE EPISÓDICA E A GESTÃO OPERANTE DE DADOS.....	119
6.5	A GESTÃO DE RISCOS COMO CAPACIDADE-PONTE: O MAIOR POTENCIAL, UM DOS MENORES DESENVOLVIMENTOS	121
6.6	RECURSOS E HETEROGENEIDADE INSTITUCIONAL: A SUSTENTAÇÃO MATERIAL DA POLÍTICA	123
6.7	A DIMENSÃO HUMANA: COMPETÊNCIAS, CULTURA E OS LIMITES DA CONSCIENTIZAÇÃO	126
6.8	SÍNTESE INTERPRETATIVA: UM MODELO EM CAMADAS DA EFETIVIDADE DO PPSI	128

6.9	RECOMENDAÇÕES FUNDAMENTADAS PARA A GESTÃO	131
6.10	ANCORAGEM DO PRODUTO TÉCNICO-TECNOLÓGICO.....	134
6.11	PROPOSTA CONTEXTUALIZADA DO PRODUTO TÉCNICO- TECNOLÓGICO	135
6.11.1	Contexto de aplicação da proposta.....	136
6.11.2	Público-alvo da proposta.....	136
6.11.3	Situação-problema: diagnóstico, análise e linha de intervenção.....	137
6.11.4	Objetivo da proposta.....	139
6.11.5	A proposta de intervenção: o GACE-PPSI	139
7	CONSIDERAÇÕES FINAIS	141
	REFERÊNCIAS	145
	APÊNDICE A – INSTRUMENTO DE PESQUISA (VERSÃO APLICADA).....	160
	APÊNDICE B – DOCUMENTAÇÃO DA REVISÃO SISTEMÁTICA.....	173
	APÊNDICE C – APROVAÇÃO ÉTICA.....	174
	APÊNDICE D – PRODUTO TÉCNICO-TECNOLÓGICO (GACE-PPSI)	177

1 INTRODUÇÃO

A proteção de dados e da segurança da informação na transformação digital dos serviços públicos é apontada como uma das questões prioritárias do mundo digital (Möller, 2020, p. 4), ante o desafio de impedir ameaças cibernéticas.

O mesmo entendimento é compartilhado por Shah e Mehtre (2013, p. 47) ao destacar a cibersegurança como um dos maiores problemas dos sistemas de informação corporativos, na medida em que a conectividade através da internet ganha escala, os sistemas ficam mais complexos e o negócio passa a depender da disponibilidade, integridade e confidencialidade desses sistemas.

O Fórum Econômico Mundial (World Economic Forum, 2023), em seu relatório anual *Global Risks Report*, identifica a “insegurança cibernética” entre os 10 riscos mais significativos da próxima década, apontando a vulnerabilidade das infraestruturas digitais em governos e sociedades como um problema sistêmico.

O Tribunal de Contas da União (TCU) elaborou a Lista de Alto Risco na Administração Pública, na qual a segurança da informação tem lugar de destaque. Observa o relatório do TCU que “segundo o portal do governo digital brasileiro, em 2021, 73,1% dos serviços públicos prestados pelo governo federal já eram totalmente digitais, o que corresponde a 3.598 serviços” (Brasil, 2022, p. 114). Somados os serviços parcialmente digitalizados, o relatório aponta que o total alcança 86,7% dos serviços públicos. “Esses números por si só mostram a dimensão dos riscos e o prejuízo que falhas de segurança e indisponibilidade de serviços podem acarretar” (Brasil, 2022, p. 114).

A Estratégia Nacional de Cibersegurança, orientação manifesta do Governo Federal publicada no Decreto nº 12.573, de 4 de agosto de 2025, assevera ciberameaça como evento capaz de impactar, entre outros, a imagem ou reputação de indivíduos e organizações (art. 2º, II) e estabelece ações para prevenção, resposta e continuidade dos serviços essenciais (arts. 5º–6º), inclusive por meio de planos de contingência e mitigação de riscos (art. 6º, VII e IX). Tais diretrizes corroboram que incidentes não adequadamente tratados podem produzir impactos operacionais, financeiros, de continuidade de serviços e de conformidade (Brasil, 2025b).

No Brasil, o Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria nº 852, de 28 de março de 2023, da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), visa

estabelecer um referencial consistente para a governança de segurança da informação e a proteção de dados nas instituições públicas do Executivo Federal que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Composto por órgãos públicos de diferentes finalidades, como universidades, institutos, fundações, ministérios, agências reguladoras e órgãos de pesquisa, o SISP é um reflexo da pluralidade e da complexidade do Poder Executivo federal (Brasil, 2023a).

Dada essa diversidade, a implementação de um programa de segurança e privacidade efetivo enfrenta desafios específicos em cada tipo de instituição. Universidades e institutos federais, por exemplo, enfrentam desafios únicos na implementação de programas de segurança e privacidade da informação. Essas instituições, além de atenderem a demandas administrativas complexas, possuem necessidades acadêmicas e de pesquisa que as diferenciam de outros órgãos públicos, como ministérios e agências reguladoras.

De acordo com Araújo Neto (2016), as universidades federais têm particularidades organizacionais que tornam a implementação de controles de segurança da informação especialmente desafiadora, destacando-se a necessidade de proteger dados sensíveis de estudantes, pesquisadores e projetos científicos. Além disso, o ambiente universitário exige a garantia de disponibilidade contínua dos serviços essenciais à comunidade acadêmica, o que intensifica a complexidade dos mecanismos de proteção.

O PPSI se estrutura por meio de um *framework* proposto em dois eixos principais: segurança da informação e privacidade, que, na versão 2.0 do *framework*, reúnem os controles de estruturação básica (Controle 0), os controles de segurança da informação (1 a 18) e os controles de privacidade (19 a 25), desdobrados em 210 medidas de implementação. Esses controles foram desenvolvidos com base em diretrizes internacionais consagradas, como os CIS Controls v8 (CIS, 2021), o NIST Cybersecurity Framework (NIST, 2024) e a norma ISO/IEC 27001:2022, buscando garantir uma abordagem estruturada para proteger o ciberespaço, dados e sistemas governamentais. Além disso, o programa visa assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD), especificados nos controles de privacidade, que estabelece parâmetros específicos para o tratamento e proteção de dados pessoais no âmbito público e privado (Brasil, 2018b).

Diante desse cenário, torna-se necessário compreender em que medida a implementação do PPSI se traduz em resultados concretos para as instituições, indo além da mera mensuração da maturidade. Essa questão é particularmente relevante no contexto das Instituições Federais de Ensino Superior, cuja diversidade organizacional e desafios operacionais exigem compreender não apenas quanto foi implementado, mas o que essas implementações produzem em termos de valor público e desempenho organizacional. O estudo parte da relação entre a maturidade de implementação do PPSI e os resultados organizacionais obtidos, considerando a efetividade como a dimensão que conecta conformidade e desempenho institucional.

1.1 PROBLEMA DE PESQUISA

Embora o *framework* estabeleça diretrizes claras, as universidades e institutos federais apresentam diferenças estruturais, de governança e de capacidade de investimento que influenciam a implementação dos controles e medidas de segurança e privacidade. Ainda que compartilhem uma missão voltada à educação superior, pesquisa e extensão, essas instituições enfrentam desafios distintos relacionados ao porte, orçamento, distribuição geográfica e às demandas específicas de suas comunidades acadêmicas e administrativas.

A identificação das capacidades institucionais associadas a melhores resultados orienta universidades e institutos federais para práticas com maior potencial de gerar resultados relevantes, otimizando recursos e fortalecendo a proteção de dados, redes e sistemas. Neste estudo, a efetividade é compreendida como a capacidade do PPSI de gerar resultados mensuráveis de valor público e desempenho organizacional, incluindo a mitigação de riscos, a melhoria na detecção e resposta a incidentes, a continuidade e disponibilidade de serviços digitais, a proteção de dados pessoais, a transparência e conformidade nas notificações e o fortalecimento da confiança institucional. Trata-se, portanto, da dimensão de resultados que traduz a maturidade implementada em evidências observáveis de desempenho e resiliência organizacional. O foco desloca-se de “quanto foi implementado” para “quais resultados são produzidos para a instituição e para a sociedade”.

1.1.1 Problema central

Como a implementação do PPSI nas IFES se traduz em efetividade, em termos de desempenho organizacional e valor público?

1.1.2 Questões norteadoras

Q1. Quais capacidades institucionais associadas à implementação do PPSI se relacionam com melhores resultados de efetividade percebida nas IFES?

Q2. Como capacidades e efetividade percebida variam segundo características institucionais das IFES, como tipo, porte, equipe de TI e condição multicampi?

1.2 OBJETIVO GERAL E OBJETIVOS ESPECÍFICOS

1.2.1 Objetivo Geral

Avaliar a efetividade percebida do PPSI nas IFES e identificar as capacidades institucionais que mais se associam a esses resultados.

1.2.2 Objetivos Específicos

a) Delimitar, a partir de revisão sistemática da literatura, os domínios de capacidade institucional e de efetividade pertinentes à avaliação de programas de segurança da informação e privacidade no setor público, com ênfase nas IFES.

b) Construir e validar, por meio de painel de especialistas, um instrumento de mensuração desses domínios.

c) Mensurar capacidades institucionais e efetividade percebida nas IFES e estimar suas associações entre si e com a maturidade autorrelatada do PPSI (iBase, iSeg e iPriv), considerando variáveis de contexto institucional.

d) Priorizar, a partir dos resultados, as capacidades com maior potencial de conversão em efetividade e traduzi-las em recomendações às IFES e ao órgão central, consolidadas em produto técnico-tecnológico (Guia de Avaliação de Capacidades e Efetividade do PPSI nas IFES — GACE-PPSI).

1.3 JUSTIFICATIVA E RELEVÂNCIA DA PESQUISA

O framework do PPSI avalia a implementação do Programa a partir do nível atribuído a cada medida, que constitui sua unidade de análise de maior granularidade. As medidas são organizadas em controles temáticos, de modo que cada controle reúne um conjunto específico de medidas relacionadas ao mesmo objeto de implementação. Com base nos níveis de implementação dessas medidas, calcula-se o índice correspondente a cada controle; posteriormente, os índices dos controles são consolidados nos indicadores iBase, iSeg e iPriv, relativos, respectivamente, aos eixos de estrutura básica, segurança da informação e de privacidade. (Brasil, 2023a). No modelo atual a organização progride em maturidade à medida que implementa integralmente as medidas correspondentes de cada controle.

Contudo, maturidade não equivale a efetividade. Enquanto a maturidade captura conformidade e implementação, a efetividade diz respeito aos resultados produzidos pelo Programa para a organização e para a sociedade. Este estudo, portanto, busca evidenciar a efetividade do PPSI em termos de resultados de desempenho e de valor público nas IFES, identificando quais capacidades institucionais se associam a melhores resultados, de modo a oferecer base empírica para priorização e alocação de recursos. A definição final das dimensões e indicadores de efetividade foi derivada da revisão sistemática da literatura e validada por especialistas, assegurando coerência teórica e parcimônia na construção do instrumento.

A literatura recente reforça que frameworks de segurança são pontos de partida que requerem ajustes contextuais para promover avanços concretos nos programas (McIntosh et al., 2024). Nesses termos, a pesquisa busca evidências que possam contribuir para o aprimoramento do PPSI no contexto das IFES.

No plano de formulação e implementação de políticas públicas, a construção do PPSI apresentou traços de abordagem *top-down*, com baixa participação dos gestores responsáveis pela execução nos órgãos. A literatura de implementação de políticas públicas aponta limitações dessa abordagem (Sabatier, 1986; Stoker, 1989; Matland, 1995). Este estudo não opõe modelos, mas acrescenta uma camada *bottom-up*, valorizando contextos locais e os atores de implementação, por meio de instrumento aplicado aos responsáveis institucionais pelo PPSI e da articulação com os índices de maturidade autorrelatados do programa.

Além da contribuição avaliativa, os achados também se relacionam à literatura sobre gestão de riscos em segurança da informação, que destaca a necessidade de priorizar controles e medidas de proteção com base em critérios de risco e contexto organizacional. Nesse sentido, Moreira *et al.* (2021) mostram como abordagens multicritério podem apoiar decisões estruturadas em segurança da informação, reforçando que o planejamento deve partir de uma visão integrada de riscos, controles e capacidades institucionais. A pesquisa aqui proposta adota essa mesma lógica integradora ao buscar mensurar em que medida a maturidade declarada e as capacidades institucionais se associam a resultados organizacionais e de valor público.

Em síntese, ao identificar as capacidades institucionais mais associadas à efetividade e evidenciar os resultados do PPSI quanto ao desempenho institucional e valor público, a pesquisa contribui para o fortalecimento da governança e para o aprimoramento da segurança e da privacidade nas IFES, oferecendo subsídios práticos e analíticos para políticas e programas congêneres no setor público.

Além desta introdução, o trabalho organiza-se em mais seis seções. A seção 2 apresenta o referencial teórico, articulando políticas públicas digitais e valor público, governança e gestão de TI no setor público, conceitos de segurança da informação e cibersegurança, privacidade e proteção de dados pessoais, o PPSI e seus referenciais normativos e técnicos e a avaliação de efetividade em políticas e programas. A seção 3 detalha o percurso metodológico. A seção 4 apresenta a análise situacional, com os resultados da revisão sistemática da literatura e a validação do instrumento. A seção 5 reúne os resultados da pesquisa empírica com as IFES, e a seção 6 desenvolve a discussão, as recomendações e o produto técnico-tecnológico, seguida das considerações finais (seção 7), das referências e dos apêndices. Do ponto de vista metodológico, trata-se de pesquisa de abordagem quantitativa, com delineamento exploratório-descritivo, desenvolvida em três macro-etapas: revisão sistemática da literatura conduzida sob as diretrizes PRISMA-2020, construção e validação de conteúdo de um instrumento por painel de especialistas e aplicação censitária ao universo de 110 IFES, cujas 58 respostas válidas foram analisadas por meio de estatística descritiva, correlações de Spearman e regressões exploratórias.

2 REFERENCIAL TEÓRICO

2.1 POLÍTICAS PÚBLICAS DIGITAIS E VALOR PÚBLICO

A digitalização das atividades governamentais é um processo de longa duração, intensificado globalmente a partir do final do século XX, responsável por mudanças progressivas nas práticas administrativas e na relação entre Estado e sociedade (Carvalho; Castro; Fernandes-Sobrinho, 2024). No Brasil, as primeiras aplicações de tecnologias da informação na administração pública, voltadas à gestão interna, remontam às décadas de 1970 e 1980; o movimento consolidou-se nos anos 1990, no bojo das agendas de modernização e reforma administrativa, e institucionalizou-se como governo eletrônico a partir dos anos 2000 (Diniz *et al.*, 2009; Carvalho; Castro; Fernandes-Sobrinho, 2024).

Nas duas primeiras décadas do século XXI, a transformação digital passou a ser compreendida como processo estrutural que envolve mudanças organizacionais, reconfiguração de processos e foco na experiência do usuário, superando a mera informatização. A literatura identifica três ondas desse processo: a primeira, marcada pela superação do *New Public Management* e pela reintegração de processos; a segunda, caracterizada pela integração de serviços digitais em plataformas unificadas; e, mais recentemente, a terceira, pautada pelo uso intensivo de ciência de dados, inteligência artificial e automação (Margetts; Dunleavy, 2013; Dunleavy; Margetts, 2023). Nesse estágio, a administração pública busca combinar centralização estratégica e descentralização operacional, equilibrando inovação tecnológica com exigências de transparência e regulação.

No Brasil, a última década foi marcada por esforços de institucionalização das políticas digitais por meio de marcos legais e estratégicos. Destacam-se a Lei nº 14.129/2021 (Lei de Governo Digital) e as Estratégias de Governo Digital 2020–2022 e 2024–2027, instituídas pelos Decretos nº 10.332/2020 e nº 12.198/2024, respectivamente (Brasil, 2020; 2021; 2024a), a plataforma Gov.br como ambiente de integração de serviços e o Programa de Privacidade e Segurança da Informação (PPSI). Essas iniciativas representam não apenas a adoção de ferramentas tecnológicas, mas a reformulação de modelos organizacionais e capacidades institucionais voltadas à geração de valor público.

A implementação dessas políticas depende da atuação das diferentes camadas burocráticas do Estado, que exercem funções distintas ao longo do ciclo de políticas públicas. Em especial, burocratas de médio escalão atuam como mediadores entre diretrizes estratégicas e execução prática, desempenhando papel crítico na coordenação de políticas digitais em contextos federativos complexos (Cavalcante; Lotta, 2015; Gomide; Pires, 2014; Wu; Ramesh; Howlett, 2015).

A efetividade das políticas digitais também está condicionada às capacidades estatais mobilizadas em sua implementação. Gomide e Pires (2014) propõem três dimensões centrais: a capacidade técnico-administrativa, associada a recursos humanos, infraestrutura e processos de gestão; a capacidade analítica, relacionada à produção e uso de dados para planejamento e tomada de decisão; e a capacidade político-relacional, que envolve negociação, articulação interinstitucional e construção de consensos. No contexto brasileiro, observa-se que a capacidade técnico-administrativa é desigual entre órgãos e níveis federativos, a capacidade analítica ainda apresenta déficits estruturais em termos de governança de dados, e a capacidade político-relacional é frequentemente limitada pela fragmentação institucional e pela baixa coordenação federativa. Essas assimetrias explicam parte das dificuldades na consolidação de uma governança digital integrada e na geração de valor público de forma equitativa.

No campo das políticas públicas digitais, a mediação assume papel central como mecanismo de ativação das capacidades estatais. A efetividade dessas políticas exige não apenas domínio técnico, mas a capacidade de articular, integrar e reconfigurar recursos de tecnologia da informação em contextos institucionais marcados por fragmentação e demandas imprevisíveis. Evidências no contexto brasileiro associam a presença de mecanismos de governança de TI, como planejamento estratégico, comitês e práticas de *compliance*, a melhores resultados percebidos na gestão de TI, sugerindo que arranjos institucionais e capacidades relacionais potencializam o desempenho (Lunardi; Becker; Maçada, 2010). Nesse sentido, a atuação dos gestores de TI demanda competências de mediação, improvisação e coordenação entre múltiplas áreas e agentes, reforçando o caráter dinâmico e relacional das capacidades estatais no âmbito da transformação digital (Marchiori *et al.*, 2023).

A discussão sobre desempenho em políticas públicas parte da distinção entre *outputs* e *outcomes*, conforme proposto por Moore (1995) e detalhado por Pollitt e

Bouckaert (2011). Enquanto os *outputs* correspondem a produtos imediatos da ação governamental, como a emissão de documentos ou a implantação de sistemas, os *outcomes* dizem respeito a efeitos sociais mais amplos, como a confiança da sociedade, a continuidade de serviços críticos e a proteção de direitos. Van Dooren, Bouckaert e Halligan (2015) destacam que a efetividade das políticas públicas deve ser avaliada a partir dos *outcomes*, ainda que sua mensuração apresente desafios metodológicos significativos. Poister (2003) reforça que sistemas de mensuração devem cobrir, de forma combinada, efetividade, eficiência, produtividade, qualidade dos serviços, satisfação do usuário e custo-efetividade, vinculando-se a processos de decisão e planejamento para evitar diagnósticos pouco úteis.

A literatura também aponta que a mensuração de desempenho em políticas públicas enfrenta limitações decorrentes da prevalência de fatores intangíveis e multidimensionais. Poister (2003) ressalta que organizações públicas e sem fins lucrativos apresentam dificuldade em estabelecer métricas únicas de desempenho, dada a diversidade de objetivos e a natureza coletiva dos resultados. De forma complementar, Berenguer (2016) sistematiza métricas em três categorias principais, insumo, produto e eficiência, e argumenta que, em contextos de missão pública ou social, não existe um indicador universal, sendo necessário trabalhar com múltiplos objetivos, *trade-offs* e dimensões como equidade e cobertura.

No campo da governança de TI, os indicadores de desempenho são tradicionalmente associados à capacidade de alinhar recursos tecnológicos às estratégias organizacionais e à geração de valor. De Haes e Van Grembergen (2005) propõem que a governança de TI seja avaliada pela integração entre processos, estruturas e mecanismos relacionais, de forma a assegurar a entrega de valor ao negócio. Estudos nacionais, como os de Lunardi, Becker e Maçada (2010), reforçam que o nível de maturidade da governança de TI está correlacionado à maior capacidade de inovação, qualidade dos serviços e desempenho organizacional. Esse referencial justifica a análise de políticas digitais sob a ótica de desempenho, indo além da mera conformidade normativa.

No Brasil, o próprio Guia do Framework de Privacidade e Segurança da Informação estabelece indicadores de maturidade como forma de acompanhamento dos controles de segurança e privacidade. Ainda que relevantes, tais métricas concentram-se em estágios de implementação e não captam diretamente os efeitos das políticas sobre o desempenho institucional ou a percepção social, relação que

deve ser tratada como questão empírica, investigada com indicadores coerentes com a lógica de valor público.

Em perspectiva internacional, a OCDE tem insistido que a transformação digital deve ser avaliada pela capacidade de gerar valor público, e não apenas pela digitalização de processos. O Digital Government Policy Framework (OECD, 2020a) e o Digital Government Index (OECD, 2020b) incorporam dimensões como “setor público orientado por dados”, “centrado no usuário” e “digital por design”. De forma convergente, a Tallinn Declaration on eGovernment (EU, 2017) e a Berlin Declaration on Digital Society and Value-Based Digital Government (EU, 2020) destacam que a efetividade das políticas digitais deve ser aferida em termos de inclusão, confiança e proteção de dados pessoais. Esses referenciais permitem situar o Brasil em um quadro comparativo internacional e reforçam a importância de considerar privacidade e segurança como *outcomes* centrais da agenda de valor público digital.

A incorporação do conceito de valor público eleva o horizonte das políticas públicas digitais além de sua função instrumental, conectando diretamente o desempenho da administração ao benefício percebido pela sociedade e à legitimidade estatal. Moore (1995) define valor público como a capacidade do Estado de produzir benefícios que são reconhecidos como socialmente relevantes, em equilíbrio com legitimidade democrática e viabilidade operacional. A realização desse valor demanda não apenas a entrega de *outputs*, mas sobretudo *outcomes* com relevância social, como continuidade dos serviços, promoção da confiança pública e resposta efetiva a desafios complexos.

A produção de valor público é uma construção coletiva que exige a articulação de múltiplos atores estatais e sociais, gestores, burocratas, organizações do terceiro setor e cidadãos, em torno de um propósito compartilhado e alinhado à legitimidade institucional. Bryson, Crosby e Bloomberg (2014) e Van Dooren, Bouckaert e Halligan (2015) argumentam que a avaliação de desempenho no setor público deve distinguir claramente entre *outputs* e *outcomes*; apenas os *outcomes*, relacionados à geração de valor público, permitem avaliar efetividade. Nessa linha, Pollitt e Bouckaert (2011) lembram que *outcomes* só adquirem sentido quando situados em contextos políticos e sociais, o que reforça a necessidade de interpretar dados de desempenho à luz de legitimidade democrática e capacidade estatal.

A governança do valor público na era digital requer, portanto, capacidades estatais dinâmicas e relacionalmente construídas, envolvendo liderança integradora,

gestão estratégica, transparência e articulação interinstitucional. Para além da adesão normativa ou do *compliance* técnico, a efetividade de políticas digitais deve ser analisada em termos de sua capacidade de produzir resultados sustentáveis e equitativos, de fomentar capacidades coletivas para resolução de problemas e de distribuir de maneira justa os benefícios sociais. Nesse sentido, o Programa de Privacidade e Segurança da Informação (PPSI) pode ser situado como política pública digital cuja efetividade depende de sua capacidade de articular controles de segurança e privacidade e convertê-los em *outcomes* socialmente relevantes, como confiança institucional, continuidade de serviços críticos e proteção efetiva de dados pessoais, compreendidos como dimensões centrais do valor público.

2.2 GOVERNANÇA E GESTÃO DE TI NO SETOR PÚBLICO

A governança e a gestão de tecnologia da informação (TI) constituem dimensões centrais da modernização da administração pública, especialmente em um cenário marcado pela crescente digitalização dos serviços governamentais. A literatura distingue governança de TI como o conjunto de mecanismos estratégicos voltados à definição de diretrizes, monitoramento de investimentos e alinhamento da tecnologia aos objetivos institucionais (Weill; Ross, 2004; De Haes; Van Grembergen, 2009). Já a gestão de TI concentra-se na operacionalização dessas diretrizes, envolvendo planejamento, execução e controle de serviços tecnológicos (Cepik; Canabarro; Possamai, 2014). Essa diferenciação é fundamental, pois evita confusões conceituais e permite compreender como funções estratégicas e operacionais se articulam para gerar valor público.

No setor público, a adoção de *frameworks* internacionais de referência, como os padrões ISO/IEC 38500 e 27001, o COBIT e o ITIL, tem desempenhado papel relevante para estruturar práticas de governança e gestão de TI. Essas abordagens oferecem diretrizes para assegurar eficiência, transparência e alinhamento estratégico, ao mesmo tempo em que contribuem para a conformidade regulatória e a proteção de dados. Tonelli *et al.* (2017) ressaltam que a incorporação dessas práticas no setor público brasileiro tem buscado superar fragilidades históricas ligadas à fragmentação tecnológica e à ausência de monitoramento consistente de resultados.

No Brasil, a institucionalização de métricas de avaliação desenvolvidas pelo TCU consolidou instrumentos de mensuração da maturidade em governança e

gestão, como o antigo iGovTI, posteriormente substituído pelo Índice Integrado de Governança e Gestão Públicas (iGG) e, mais recentemente, pelo iESGo (Índice de Governança e Sustentabilidade). O iESGo 2024, por exemplo, estrutura indicadores de liderança, estratégia e controle, além de índices específicos de governança e de gestão de TI e segurança da informação (Brasil, 2024c). O uso desses instrumentos, embora sujeito a críticas por sua ênfase normativa e padronizada (Souza Neto; Carvalho, 2020), representa um avanço ao permitir comparações sistemáticas entre instituições federais e identificar lacunas de capacidades institucionais.

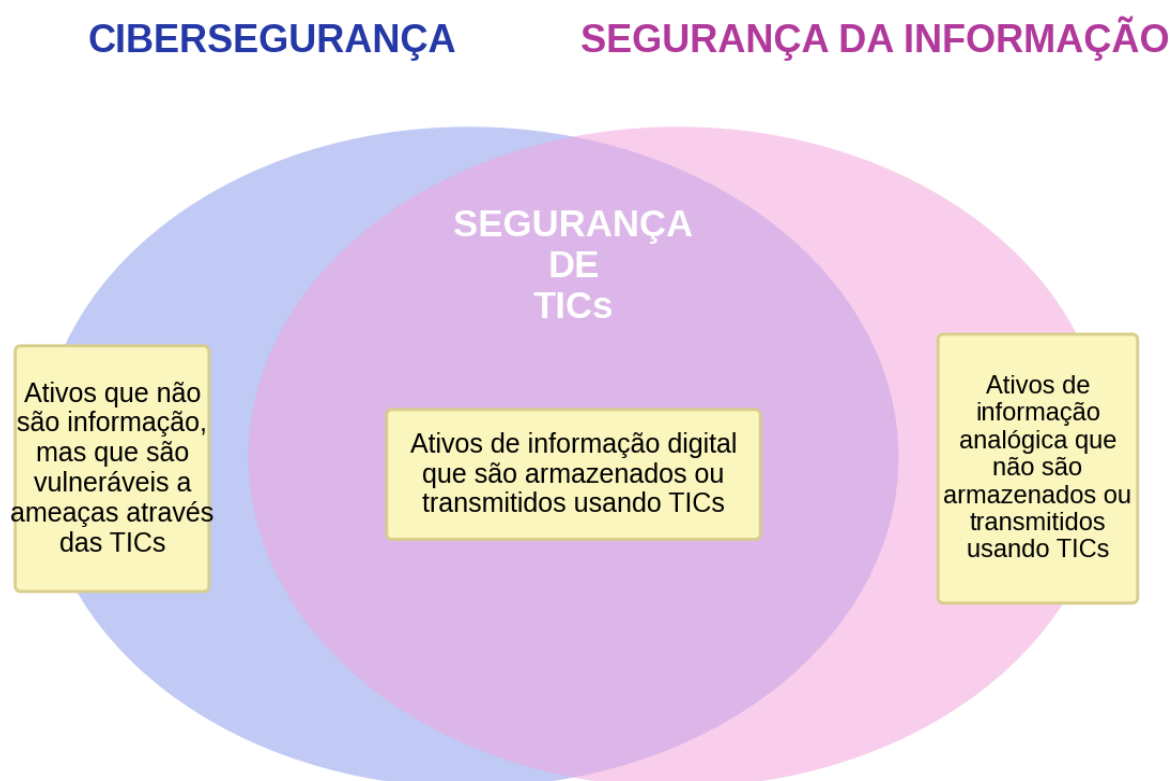
2.3 CONCEITOS FUNDAMENTAIS DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

A fim de aplicar um entendimento amplo sobre o campo da presente pesquisa, é importante definir os conceitos comumente utilizados, tendo em vista que os termos cibersegurança e segurança da informação são usados, muitas vezes, de formas intercambiáveis, principalmente no contexto aplicado. No entanto, no campo teórico, mesmo com muitos domínios em comum, as diferentes terminologias para segurança representam diferenças importantes (Von Solms; Van Niekerk, 2013; Reid; Van Niekerk, 2014; Von Solms; Von Solms, 2018; Eswaran; Vinayagamoorthi, 2019; Alexei; Alexei, 2022; Taherdoost, 2022).

Essa relação pode ser visualizada como dois conjuntos sobrepostos: a cibersegurança é um subconjunto da segurança da informação, pois depende de seus princípios, mas adiciona uma camada especializada para lidar com os riscos digitais modernos, como ciberataques, espionagem digital e vulnerabilidades em dispositivos IoT. Por outro lado, a segurança da informação inclui aspectos que a cibersegurança não cobre, como a proteção de informações em formatos analógicos ou não conectados ao ciberespaço, conforme Eswaran e Vinayagamoorthi (2019, p. 372) e Von Solms e Van Niekerk (2013, p. 101).

A Figura 1 ilustra essa interseção, destacando a sobreposição significativa entre os dois campos e as áreas exclusivas de cada um.

Figura 1 – Relação entre cibersegurança e segurança da informação



Fonte: Adaptado de Von Solms e Van Niekerk (2013).

Portanto, o domínio da segurança da informação tem a informação como eixo central de proteção e versa sobre a preservação dos atributos de confidencialidade, integridade e disponibilidade (modelo CID) das informações organizacionais seja em formato digital, físico ou processado (ISO/IEC 27000:2018, Seção 3.28). Enquanto a Cibersegurança tem o ciberespaço como eixo central e busca a preservação de pessoas, sociedades, organizações e nações dos riscos no ciberespaço (ISO/IEC 27032:2023, Seção 3.6), por meio de atributos que consistem em identificar, proteger, detectar, responder e recuperar (ISO/IEC 27002:2022, p. 8).

Segundo Von Solms e Van Niekerk (2013), alguns contextos da cibersegurança não estão necessariamente relacionados com a proteção da informação, em que o interesse de pessoas, sociedades e nações devem ser protegidos dos riscos advindos da interação com o ciberespaço. Enquanto a segurança da informação se preocupa com a informação em si, ou o sistema de guarda da informação de pessoas e organizações, a cibersegurança foca em proteger as pessoas e organizações que usam estes recursos no ambiente digital.

Os dois universos se encontram em tudo que envolve segurança em tecnologia da informação e comunicações. Enquanto a segurança da informação tem a

informação como ativo em meio eletrônico ou analógico, a cibersegurança tem também as pessoas como ativos e as consequências, riscos e vulnerabilidades que sofrem no meio eletrônico e digital ou através do meio eletrônico e digital. Entre os exemplos citados por Von Solms e Van Niekerk (2013) estão a automação de residências, o *cyber terrorism*, o *cyber bullying* e as atividades ilegais em redes sociais: riscos que partem da TIC, mas têm consequências para fora dela, e que não necessariamente exploram informações no comprometimento da segurança de indivíduos, sociedades ou nações.

O Quadro 1 demonstra com clareza analítica como os principais estudos se posicionam entre os conceitos.

Quadro 1 – Definição de cibersegurança e segurança da informação por estudo

Autores	Conceito de Segurança da Informação	Conceito de Cibersegurança	Objetivo do Artigo	Achados
Rossouw von Solms e Johan van Niekerk (2013)	Proteção da confidencialidade, integridade e disponibilidade da informação, abrangendo dados em qualquer formato e sistemas associados.	Proteção de ativos no ciberespaço, incluindo indivíduos, dispositivos conectados e infraestrutura crítica, indo além da segurança da informação tradicional.	Distinguir segurança da informação de cibersegurança e explorar as implicações éticas e sociais da cibersegurança.	A cibersegurança abrange a proteção de ativos tangíveis e intangíveis relacionados ao ciberespaço, indo além da informação em si.
Arina Alexei e Anatolie Alexei (2022)	Proteção de dados contra acessos não autorizados, alterações ou destruição, independentemente do formato.	Foco em ameaças e vulnerabilidades específicas do ambiente cibernético, com ênfase em ataques como phishing, malware e espionagem.	Analisar as diferenças e semelhanças entre cibersegurança e segurança da informação, destacando o uso apropriado dos termos.	Cibersegurança é mais ampla que segurança da informação, abrangendo ativos físicos e digitais conectados ao ciberespaço, enquanto a segurança da informação foca principalmente nos dados.
R. Eswaran e G. Vinayagamoorthi (2019)	Proteção da confidencialidade, integridade e disponibilidade de informações em qualquer formato, com foco nos dados como principal ativo.	Segurança de dispositivos, processos, infraestrutura e ativos vulneráveis no ciberespaço, abrangendo proteção contra ataques cibernéticos e roubo de dados.	Clarificar as diferenças entre segurança da informação e cibersegurança, abordando confusões e definições amplamente aceitas.	Cibersegurança é vista como uma extensão ou subconjunto da segurança da informação, mas com foco no ciberespaço e ativos digitais.

Basie von Solms e Rossouw von Solms (2018)	Proteção da confidencialidade, integridade e disponibilidade de informações em qualquer formato e local.	Subconjunto da segurança da informação focado na proteção de ativos digitais conectados à internet contra ameaças cibernéticas.	Definir claramente as diferenças entre cibersegurança e segurança da informação, destacando seu relacionamento do ponto de vista da governança.	Cibersegurança é uma parte da segurança da informação, concentrando-se em riscos associados ao uso da internet e ativos digitais.
Rayne Reid e Johan van Niekerk (2014)	A proteção de informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação, inspeção, gravação e destruição, com foco na preservação do modelo CID (confidencialidade, integridade e disponibilidade).	A proteção dos interesses de uma pessoa, sociedade ou nação, incluindo suas informações e ativos não informacionais, contra riscos relacionados à interação com o ciberespaço. Envolve a preservação do modelo CID dentro do ciberespaço.	Propor uma definição de cultura de cibersegurança (Cybersecurity Culture - CSC) e diferenciá-la de uma cultura de segurança da informação (Information Security Culture - ISC).	A cibersegurança expande o escopo da segurança da informação, tratando ameaças específicas ao ciberespaço e reconhecendo humanos como ativos que precisam de proteção digital.

Fonte: Elaboração própria (2026).

A abordagem voltada para a segurança da informação pode ser eficaz no tratamento de diversos aspectos relacionados à cibersegurança. No entanto, essa abordagem pode não ser suficiente para lidar com determinados riscos e ameaças que emergem do ciberespaço (Domínguez-Dorado *et al.*, 2023), sendo assim uma abordagem mais abrangente de cibersegurança é muitas vezes recomendada, conforme defendido por Von Solms e Van Niekerk (2013) e Reid e Van Niekerk (2014).

Portanto, o uso intercambiável dos termos se justifica em contextos aplicados, tanto pela sobreposição de medidas de proteção adotadas em ambas as áreas quanto pelo potencial de integração que amplia o universo de atuação da segurança da informação. Nesse contexto foi desenvolvido o *framework* do PPSI, que se apoia nos universos da segurança da informação e da cibersegurança para alcançar um escopo mais completo de atuação, integrando proteção tecnológica e salvaguarda de direitos, especialmente no que se refere à privacidade e à proteção de dados pessoais.

2.4 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A privacidade e a proteção de dados pessoais configuram-se como pilares fundamentais na governança digital contemporânea, não apenas como exigência regulatória, mas como condição de legitimidade e confiança no uso de serviços digitais. No cenário internacional, a referência mais influente é o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que estabelece princípios como finalidade, minimização, transparência, responsabilidade e direitos reforçados aos

titulares. Este marco regulatório tornou-se padrão de comparação global e inspirou legislações em diversas jurisdições, incluindo o Brasil (Voigt; Von dem Bussche, 2017).

Entre os principais referenciais técnicos, destacam-se as normas da família ISO/IEC, que oferecem diretrizes sobre governança da privacidade e práticas organizacionais. O ISO/IEC 29100:2024 apresenta uma estrutura conceitual para a proteção de dados pessoais; o ISO/IEC 29151:2017 detalha requisitos para controles de segurança em dados pessoais; o ISO/IEC 27701:2025 estende o Sistema de Gestão de Segurança da Informação (SGSI) para a gestão de informações de privacidade (PIMS); o ISO/IEC 27018:2025 foca na proteção de dados em serviços de nuvem; e o ISO/IEC 29134:2023 trata da avaliação de impacto à privacidade (PIA). Complementarmente, o NIST Privacy Framework (NIST, 2020) oferece uma abordagem voltada à gestão de riscos de privacidade, alinhando práticas organizacionais aos princípios de governança e *compliance*.

No Brasil, o marco regulatório foi estabelecido pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), que introduziu direitos fundamentais aos titulares, disciplinou as hipóteses de tratamento de dados, previu obrigações a agentes de tratamento e estabeleceu parâmetros para a atuação do poder público (Brasil, 2018b). A Agência Nacional de Proteção de Dados (ANPD), criada no âmbito da LGPD, tem a missão de zelar pela aplicação da lei, editar normativos complementares, fiscalizar, aplicar sanções e orientar os órgãos públicos e privados na conformidade regulatória. Entre suas competências, previstas no art. 55-J da LGPD, incluem-se a promoção da cultura de proteção de dados e a harmonização da legislação nacional com padrões internacionais (Brasil, 2018b).

Essa regulação posiciona a privacidade não apenas como obrigação legal, mas como dimensão estratégica da governança digital. Políticas públicas e programas, como o PPSI, incorporam a proteção de dados como eixo estruturante de sua atuação, reconhecendo que a legitimidade e a sustentabilidade dos serviços digitais dependem de sua capacidade de assegurar direitos dos titulares, reduzir riscos de incidentes e fortalecer a confiança da sociedade no Estado digital (Brasil, 2023a; Voigt; Von dem Bussche, 2017).

2.5 O PPSI E SEUS REFERENCIAIS NORMATIVOS E TÉCNICOS

O Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023, constitui o principal instrumento normativo da administração pública federal voltado à padronização e aprimoramento das práticas de segurança e proteção de dados. Ele traduz, em termos operacionais, a necessidade de alinhar os órgãos do SISP a padrões técnicos internacionais, à legislação nacional — em especial a de Segurança da Informação, instituída pelo Decreto nº 9.637/2018 (Brasil, 2018a) e atualmente disciplinada pelo Decreto nº 12.572/2025 (Brasil, 2025a) e a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (Brasil, 2018b) — e às diretrizes regulatórias do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e da ANPD.

A elaboração do *framework* que estrutura o PPSI não ocorreu em isolamento. Ele é resultado da convergência de *standards* e *frameworks* consolidados na literatura e na prática de segurança da informação. Conforme Dedeker e Masterson (2019) e Taherdoost (2022), os *standards* estabelecem especificações, procedimentos e requisitos de conformidade, enquanto os *frameworks* oferecem guias gerais de implementação, com flexibilidade para adaptação ao contexto organizacional. Essa distinção é sintetizada no Quadro 2, elaborado a partir de Taherdoost (2022) e Brasil (2023a), e evidencia como o PPSI articula referenciais normativos e metodológicos de diferentes naturezas.

Quadro 2 – Comparativo de *standards* e *frameworks*

Aspecto	<i>Standards</i>	<i>Frameworks</i>
Definição	“Os <i>standards</i> definem especificações, procedimentos e diretrizes para garantir consistência, confiabilidade e segurança de sistemas, produtos e serviços” (Taherdoost, 2022, p. 1).	“ <i>Frameworks</i> são guias gerais que fornecem uma estrutura para atingir objetivos sem prescrever etapas específicas.” (Taherdoost, 2022, p. 3).
Foco Principal	“ <i>Standards</i> se concentram na conformidade com requisitos técnicos e regulatórios, garantindo a adesão às políticas e leis” (Taherdoost, 2022, p. 1).	“ <i>Frameworks</i> visam reduzir os riscos identificando, protegendo e respondendo às ameaças cibernéticas através de diretrizes flexíveis” (Taherdoost, 2022, p. 3).
Exemplos	A série ISO/IEC 27000: “A série ISO/IEC 27000 fornece orientação abrangente para implementação de sistemas de gerenciamento de segurança da informação (SGSI)” (Taherdoost, 2022, p. 4).	O NIST Cybersecurity Framework (CSF): “Amplamente adotada para gerenciar riscos cibernéticos através de setores críticos” (Taherdoost, 2022, p. 10).
Uso no PPSI	O PPSI utiliza padrões como ISO/IEC 29100:2011 para estabelecer políticas gerais e proteger dados organizacionais, utilizado na construção dos	O PPSI adota o NIST CSF para tratar ameaças digitais, como ataques cibernéticos e riscos de IoT (Brasil, 2023a, p. 24) e o NIST Privacy

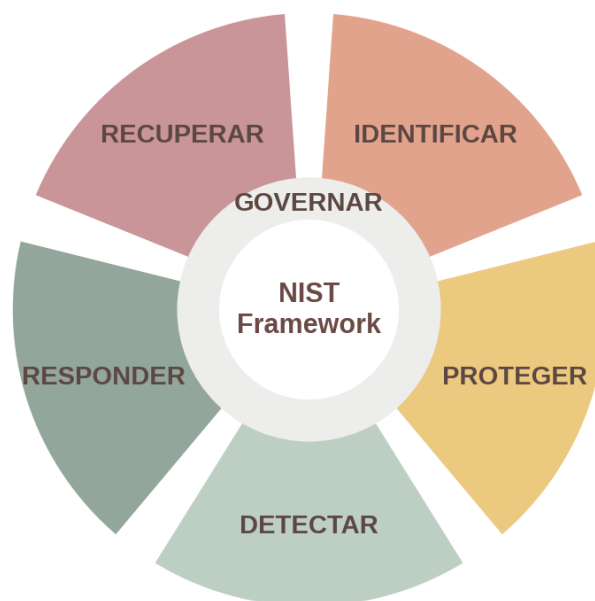
	controles de privacidade (Brasil, 2023a, p. 27).	Framework para tratar a privacidade (Brasil, 2023a, p. 30).
--	--	---

Fonte: Baseado em Taherdoost (2022) e Brasil (2023a).

No campo da cibersegurança, dois referenciais ocupam posição central: o CIS Controls v8 (CIS, 2021), que fornece um conjunto priorizado de boas práticas, e o NIST Cybersecurity Framework (CSF), amplamente adotado desde 2014. O NIST CSF foi atualizado em 2018, e em 2024 alcançou sua versão 2.0, que introduziu a função governar (Govern) como eixo adicional às cinco funções originais. Essa mudança é de relevância, pois reconhece que a segurança não é apenas responsabilidade técnica, mas um componente de governança organizacional estratégica, abrangendo contexto, papéis, responsabilidades, supervisão e gestão de riscos da cadeia de suprimentos (NIST, 2024; Brasil, 2023a).

O modelo atualizado passa a compor seis funções interdependentes: Governar, Identificar, Proteger, Detectar, Responder e Recuperar. Essa estrutura ressalta a conexão entre segurança e valor público, na medida em que insere a cibersegurança no núcleo do processo decisório organizacional. A Figura 2 ilustra a representação gráfica dessa arquitetura, conforme adaptado pelo MGI.

Figura 2 – Modelo conceitual do NIST Framework



Fonte: Adaptado de NIST (2024).

Na dimensão da privacidade, o PPSI adota normas internacionais amplamente reconhecidas. A ISO/IEC 27018:2025 estabelece diretrizes para provedores de nuvem no tratamento de dados pessoais; a ISO/IEC 29134:2023 fornece parâmetros para avaliações de impacto à privacidade e elaboração de Relatórios de Impacto à Proteção de Dados Pessoais; e a ABNT NBR ISO/IEC 29184:2021 orienta políticas de privacidade online e coleta de consentimento. Complementarmente, a ISO/IEC 27701:2025 estende o SGSI para a gestão de informações de privacidade, e o NIST Privacy Framework (2020) contribui com uma abordagem de gestão de riscos que conecta privacidade à governança organizacional. A ANPD, por sua vez, atua como órgão regulador nacional, emitindo guias interpretativos que operacionalizam os princípios da LGPD.

A incorporação simultânea de referenciais de segurança e privacidade confere ao PPSI um caráter abrangente. Estudos recentes destacam que a complexidade de uma economia baseada em dados exige abordagens integradas, em que aspectos técnicos, organizacionais e regulatórios sejam tratados de forma convergente (Culot *et al.*, 2021; Domínguez-Dorado *et al.*, 2023). Essa integração se traduz na estrutura do programa, que reúne dois eixos temáticos, segurança da informação (controles 1 a 18) e privacidade (controles 19 a 25), desdobrados em medidas cuja avaliação resulta nos índices consolidados iSeg (Índice de Segurança da Informação) e iPriv (Índice de Privacidade). A esses eixos soma-se o controle 0, dedicado à estrutura básica, índice iBase (Índice de Estrutura Básica), seus segmentos abrangem a estruturação básica, relativa às nomeações; a estruturação da governança, com a definição de papéis e de mecanismos de apoio; e os instrumentos fundamentais, introduzidos na versão 2.0 do framework para ampliar as funções de governança (Brasil, 2025c).

Mais do que mensurar conformidade normativa, esses índices buscam induzir práticas de governança, fortalecer capacidades institucionais e alinhar segurança e privacidade às políticas digitais de maior alcance, como a Estratégia Federal de Governo Digital (Brasil, 2024a) e a Estratégia Nacional de Cibersegurança (Brasil, 2025b). Ao se apoiar em referenciais internacionais e marcos regulatórios nacionais, o PPSI reafirma a centralidade da proteção da informação e dos dados pessoais como condição de legitimidade e confiança no Estado digital.

2.6 AVALIAÇÃO DE EFETIVIDADE EM POLÍTICAS E PROGRAMAS

A avaliação de políticas públicas ocupa posição central no ciclo de gestão estatal, pois permite aferir em que medida os objetivos estabelecidos se convertem em resultados socialmente relevantes. A literatura distingue três dimensões centrais: eficiência, relacionada ao uso racional dos recursos disponíveis; eficácia, ligada ao alcance dos objetivos previstos; e efetividade, que corresponde à produção de impactos sociais atribuíveis à intervenção (Rossi; Lipsey; Freeman, 2004; Van Dooren; Bouckaert; Halligan, 2015). Essa distinção é particularmente relevante para programas de governança digital e segurança da informação, nos quais a conformidade formal com normas ou controles não garante a geração de valor público. À luz dessa distinção, a pesquisa avalia a efetividade do PPSI em termos de resultados de desempenho e de valor público, mantendo a maturidade como variável explicativa de implementação.

A mensuração da efetividade no setor público enfrenta desafios inerentes à natureza multifacetada do valor público e aos *trade-offs* frequentemente presentes entre objetivos distintos. Como destacam Pollitt e Bouckaert (2011), reformas e políticas quase sempre implicam escolhas difíceis entre metas em competição, exigindo decisões sobre prioridades organizacionais e alocação de recursos. No contexto de políticas digitais como o PPSI, esses dilemas se manifestam quando medidas rigorosas de segurança podem impactar a experiência do usuário ou quando a transparência pode inadvertidamente expor vulnerabilidades institucionais.

A avaliação da efetividade em políticas de segurança da informação e privacidade demanda abordagens que captem tanto aspectos técnicos quanto organizacionais e sociais (Poister, 2003). Isso implica observar não apenas métricas de maturidade (*compliance* com controles), mas também resultados percebidos pelos gestores e usuários: continuidade de serviços críticos, capacidade de resposta a incidentes, proteção efetiva de dados pessoais e confiança no governo digital. Essa perspectiva multicritério é especialmente importante em contextos federativos complexos, em que a implementação depende de capacidades institucionais heterogêneas. Ao incorporar tais dimensões, a avaliação supera a lógica meramente procedimental e conecta *compliance* regulatório, capacidade institucional e geração de valor público.

Do ponto de vista metodológico, diferentes tradições coexistem. Estudos clássicos, como os de Sabatier (1986) e Matland (1995), enfatizam as tensões entre modelos *top-down*, nos quais a política é formulada e imposta centralmente, e abordagens *bottom-up*, que valorizam o contexto local e os atores implementadores. No caso do PPSI, a combinação dessas perspectivas é especialmente pertinente: enquanto o programa é formulado centralmente pelo MGI, sua efetividade depende de como universidades e institutos federais, com realidades diversas de recursos e capacidades, implementam e adaptam os controles previstos.

Este referencial organiza conceitos e achados centrais sobre efetividade em segurança da informação e privacidade no setor público, integrando também discussões sobre valor público e abordagens orientadas a risco. A seleção aqui apresentada constitui síntese preliminar baseada em literatura internacional e documentos técnicos de reconhecida credibilidade. A revisão sistemática formal, cujo protocolo, critérios de inclusão/exclusão e estratégia de busca serão detalhados na seção metodológica, permitirá refinar e validar as dimensões de efetividade utilizadas no questionário com gestores e na posterior contraposição com os indicadores de maturidade do PPSI.

3 METODOLOGIA

3.1 DESENHO E ABORDAGEM DO ESTUDO

Esta pesquisa adota abordagem quantitativa, com delineamento exploratório-descritivo e aplicação dirigida à totalidade das IFES participantes do Programa de Privacidade e Segurança da Informação (PPSI). A opção por abranger o universo completo se justifica pelo objetivo de mapear o conjunto de instituições vinculadas ao SISP, evitando vieses de seleção e permitindo a identificação de padrões sistêmicos. No plano epistemológico, a abordagem quantitativa é adequada a investigações com variáveis mensuráveis e ao uso de técnicas estatísticas para interpretação dos dados (Lakatos; Marconi, 2003).

O objetivo central é avaliar a efetividade do PPSI nas IFES, indo além da conformidade normativa. O encadeamento metodológico articula três macro-etapas: (i) Revisão Sistemática da Literatura (RSL), que identifica domínios de capacidade (governança; processos; pessoas/competências; tecnologia/monitoramento; gestão de dados/privacidade; recursos) e de desempenho/efetividade (mitigação de risco; transparência/notificação/conformidade; proteção de dados; confiança/percepção; detecção e resposta; continuidade/disponibilidade); (ii) construção e validação de conteúdo de um instrumento primário aplicado a gestores responsáveis pelo PPSI; e (iii) articulação estatística entre as medidas primárias (escores dos domínios C/E) e os índices de maturidade do PPSI (iBase, iSeg e iPriv) autorrelatados pelos respondentes, tratando o encadeamento ‘maturidade → capacidades → efetividade’ como questão empírica associativa, e não como pressuposto causal.

3.2 REVISÃO SISTEMÁTICA DA LITERATURA (RSL)

3.2.1 Objetivo e pergunta

Esta etapa teve por objetivo identificar e consolidar dimensões, medidas e evidências empíricas empregadas para avaliar a efetividade de políticas, programas e controles de segurança da informação/cibersegurança e privacidade/proteção de dados no setor público, incluindo ensino superior. Pergunta norteadora: quais domínios de capacidade e de desempenho a literatura utiliza para mensurar

efetividade em segurança/privacidade no setor público e nas IFES, e como esses domínios são operacionalizados?

3.2.2 Bases, termos e filtros

A etapa de revisão sistemática foi conduzida de acordo com as diretrizes PRISMA-2020 (Page *et al.*, 2021), com o objetivo de assegurar transparência, reprodutibilidade e rigor metodológico em todas as fases do processo. Foram consultadas a *Scopus* e *Web of Science* (WoS) por sua abrangência internacional e pela cobertura consolidada de estudos sobre governança, tecnologia da informação e políticas públicas digitais. A pesquisa foi feita com a mesma lógica de busca, no mês de setembro de 2025:

("information security" OR cybersecurity OR "data protection" OR privacy) AND (effectiveness OR "program evaluation" OR "policy evaluation" OR assessment OR maturity OR capability OR capabilities OR readiness OR resilience) AND ("public sector" OR government OR "higher education" OR university).

As estratégias de busca foram elaboradas de forma combinada, buscando integrar três conjuntos de descritores:

- (i) termos relacionados à segurança da informação e privacidade;
- (ii) expressões vinculadas à efetividade, avaliação, maturidade ou capacidade;

e

- (iii) indicadores de contexto institucional, como setor público e ensino superior.

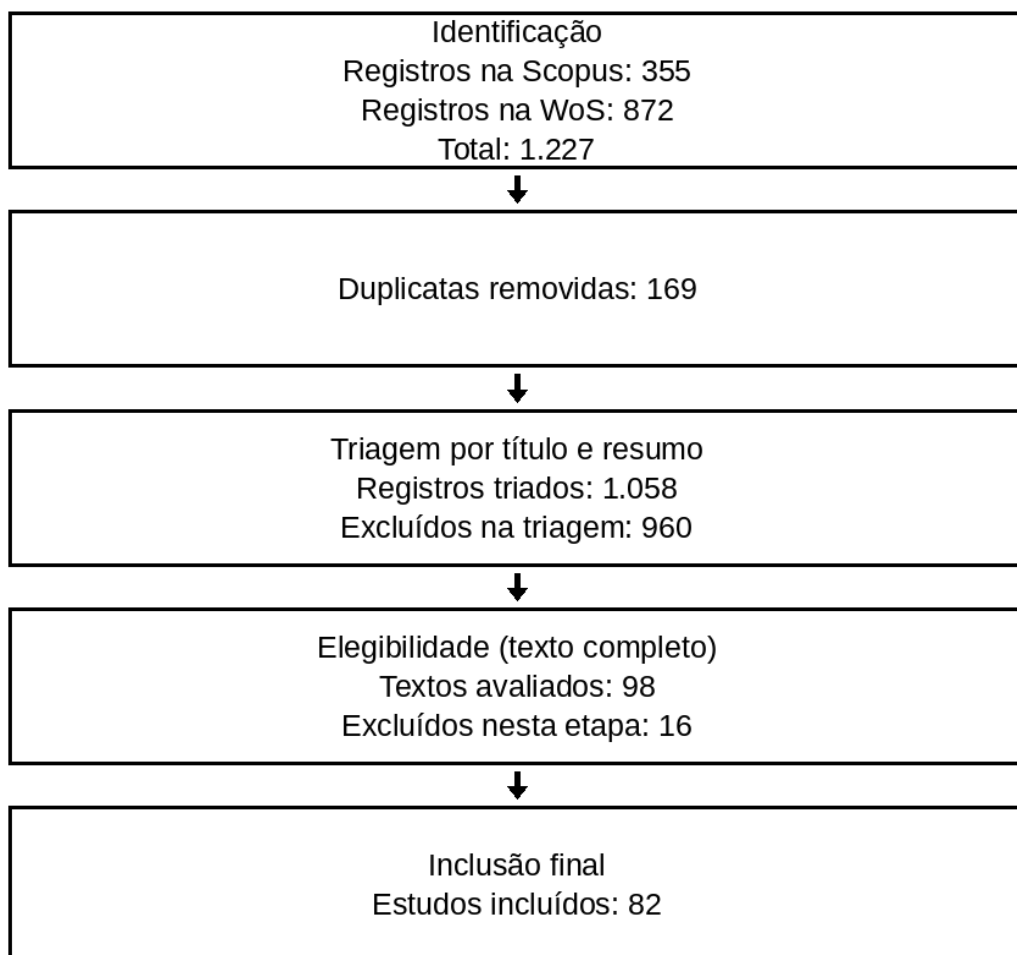
Foram aplicados filtros comuns às duas bases: tipo documental restrito a *Article* e *Review*, idiomas inglês, português e espanhol, e recorte temporal entre 2015 e 2025, abrangendo uma década de produção científica. Esse período foi definido para capturar a consolidação das discussões sobre privacidade e segurança da informação em políticas públicas após a emergência dos marcos regulatórios contemporâneos, como o GDPR (2016) e a LGPD (2018).

Aplicados esses filtros, foi feito um refinamento por áreas dentro das próprias bases, buscando áreas do conhecimento com alguma associação de interesse da presente pesquisa. Foram selecionados para *Scopus*: *Computer Science*; *Social Sciences*; *Decision Sciences*; *Business, Management and Accounting*; *Multidisciplinary*. As demais áreas foram excluídas por predomínio técnico/biomédico sem desfecho organizacional. Refinamento por áreas na WoS: *Computer Science*;

Information Science & Library Science; Public Administration; Business & Economics; Operations Research & Management Science; Government & Law; Education & Educational Research. As demais áreas foram excluídas pelo mesmo critério.

Desta forma, o fluxo PRISMA registrou 355 registros na Scopus e 872 na Web of Science, totalizando 1.227 referências antes da deduplicação. Foram removidas 169 duplicatas, restando 1.058 registros triados por título e resumo, dos quais 960 foram excluídos nessa etapa. 98 textos foram avaliados em texto completo e 82 estudos foram incluídos na síntese final, com 16 exclusões registradas por não alinhamento ao presente trabalho ou por indisponibilidade do texto completo (não localizado ou restrito por *paywall*). O encadeamento no fluxograma PRISMA ficou da seguinte forma (Figura 3):

Figura 3 – Fluxo PRISMA 2020



Fonte: Elaboração própria (2026).

3.2.3 Triagem, elegibilidade e códigos de exclusão

Esgotada a seleção de artigos nas duas bases, a fase seguinte consistiu na exportação em .csv de cada base para confrontação em planilha e remoção de duplicações, etapa em que foram confrontados os filtros de DOI e Título. A seguir, partiu-se para a etapa em que se verificou o maior volume de exclusões, aquela de triagem inicial por título, resumo e palavras-chave, fase em que os critérios de inclusão e exclusão foram aplicados de forma rigorosa. O objetivo foi garantir que os estudos mantidos apresentassem aderência temática à segurança da informação e privacidade no contexto público e institucional, com dimensão avaliativa, de maturidade ou de implementação.

Os critérios de inclusão exigiam, simultaneamente:

(i) menção explícita ao setor público ou a Instituições Federais de Ensino Superior (IFES), com termos como “governo”, “public sector”, “public university”, “universidade federal”, “instituto federal”;

(ii) presença inequívoca do domínio de segurança da informação ou privacidade, com descritores como “information security”, “cybersecurity”, “privacy”, “data protection”, “LGPD”, “GDPR”; e

(iii) caráter avaliativo, observável por termos como “effectiveness”, “evaluation”, “assessment”, “maturity”, “readiness”, “*compliance*”, “resilience”, ou referências a *frameworks* e governança.

A triagem e codificação inicial por título, palavras-chave e resumo foram conduzidas pelo pesquisador com apoio assistido do modelo GPT-5 (OpenAI), empregado para auxiliar na padronização dos critérios de inclusão e exclusão e na verificação de consistência entre registros. Todas as decisões de elegibilidade foram revisadas e validadas manualmente pelo pesquisador, assegurando controle humano integral sobre o processo e rastreabilidade completa das etapas da revisão sistemática.

Quando o título e as palavras-chave não eram suficientes para confirmar esses elementos, procedia-se à leitura do resumo, garantindo uma análise justa antes da decisão de exclusão. Em casos de dúvida persistente, o artigo seguia para leitura em texto completo.

A aplicação desses critérios resultou na utilização de códigos padronizados de exclusão, com um único motivo registrado por artigo:

F1 — fora de setor público ou IFES (ausência de menção explícita em título/*keywords*, como “*university*” genérico sem qualificador público/federal ou de contexto privado);

F2 — foco técnico-operacional (soluções de autenticação, criptografia, biometria, IDS/IPS etc.) sem vínculo com gestão, governança ou políticas públicas;

F3 — fora do domínio de segurança da informação/privacidade (privacidade aparece apenas de forma lateral ou ética, sem foco institucional. Por exemplo: uso ético da IA em educação);

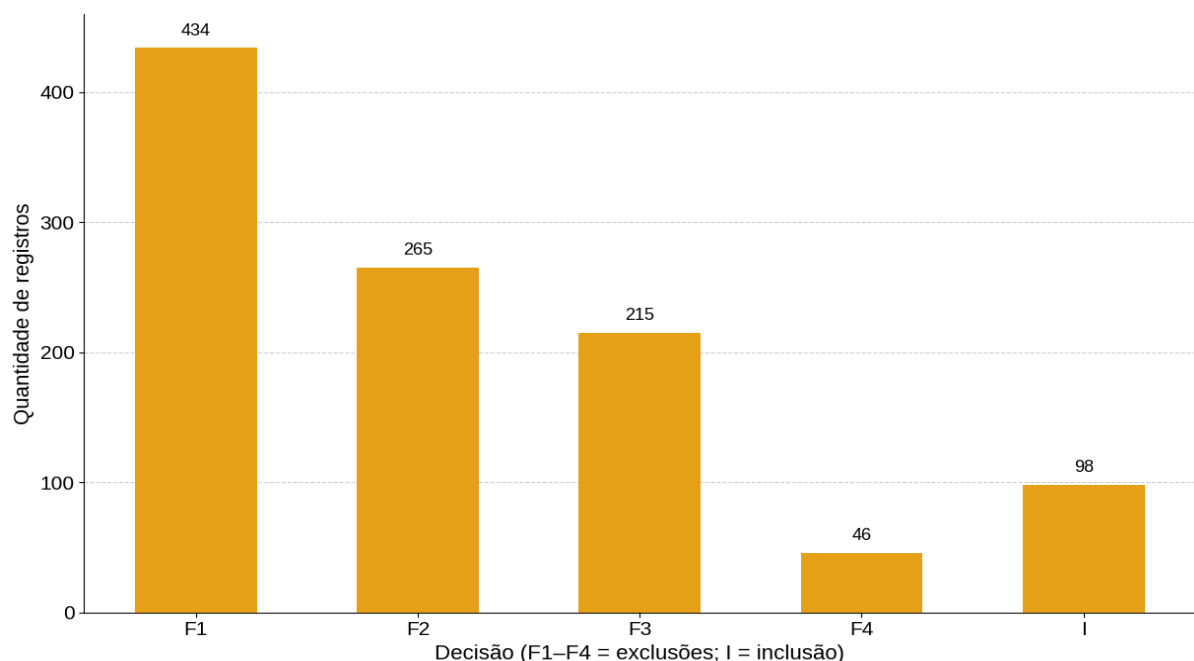
F4 — sem dimensão avaliativa/implementação (ensaios conceituais sem mensuração, diagnóstico ou referência a *frameworks*);

F8 — não localizado ou inacessível (aplicado apenas na etapa de leitura integral dos artigos).

Em alguns casos, os artigos podem se enquadrar em mais de um fator de exclusão, quando isso ocorreu utilizou-se o gradiente $F1 > F2 > F3 > F4$, ou seja: elimina-se primeiro o contexto inadequado (fora do setor público/IFES), em seguida o tecnicismo sem política pública, depois os temas tangenciais à SI/privacidade e, por fim, os casos sem operacionalização avaliativa/implementação.

A aplicação desses critérios resultou em 960 exclusões na etapa de triagem, restando 98 artigos potencialmente elegíveis para leitura integral (Gráfico 1).

Gráfico 1 – Triagem por título, *abstract* e *keywords*



Fonte: Dados da pesquisa (2026).

Essa codificação garantiu transparência e rastreabilidade das decisões. O registro completo das exclusões e inclusões foi mantido em planilha auditável, permitindo reprodutibilidade e conferência futura.

O resultado dessa triagem representa um corpus composto por estudos que, além de tratar de segurança e privacidade em contextos públicos, também incorporam dimensões de avaliação, governança e maturidade, tornando-se o alicerce empírico da análise situacional e da definição dos domínios de capacidade e efetividade apresentados nas seções seguintes.

3.2.4 Leitura integral e extração dos dados

Concluída a triagem inicial, os 98 artigos elegíveis foram submetidos à leitura integral, etapa fundamental para confirmar a aderência teórica e a qualidade metodológica das evidências. Nessa fase, aplicaram-se novamente os mesmos critérios de elegibilidade, agora com base no conteúdo completo dos estudos, assegurando consistência nas decisões.

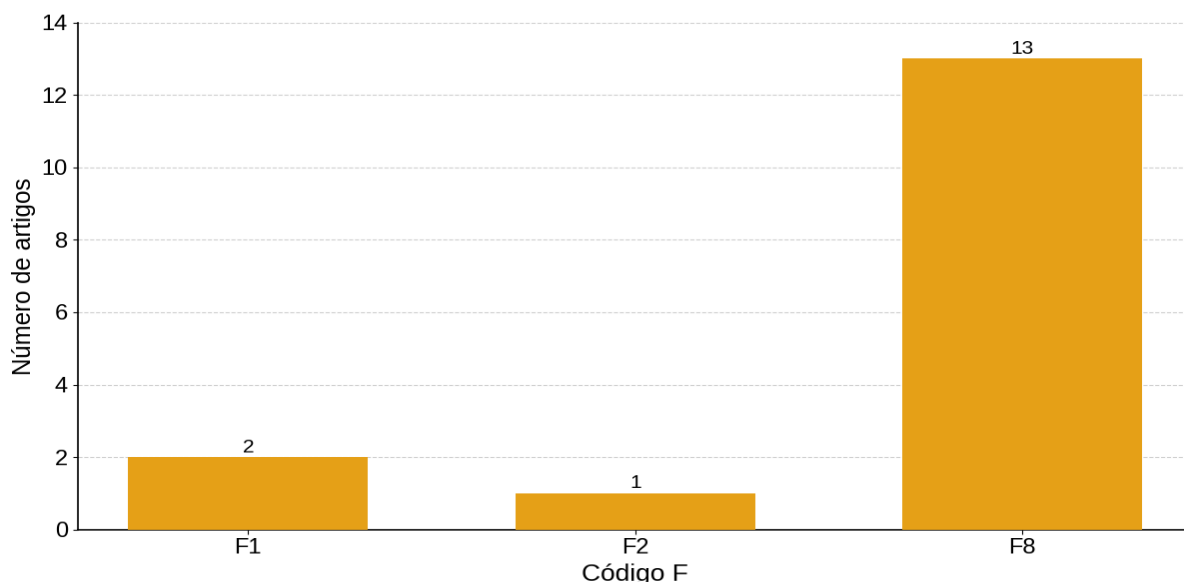
A leitura integral foi conduzida pelo pesquisador com apoio assistido do modelo GPT-5 (OpenAI), utilizado para conferência cruzada de aderência temática, registro sistemático dos códigos de exclusão e inclusão e verificação de consistência entre categorias. Todos os casos de dúvida, especialmente aqueles em que houve divergência de codificação automatizada, foram revisados manualmente pelo pesquisador, que decidiu a inclusão final de cada estudo.

A leitura integral permitiu aprofundar a análise dos objetivos, métodos, contextos institucionais e indicadores de efetividade apresentados em cada publicação, além de verificar o alinhamento dos estudos com a perspectiva organizacional que orienta o PPSI. Os casos de exclusão concentraram-se principalmente no código F8, correspondente a artigos não acessíveis em texto completo, seja por restrição de *paywall* ou ausência de versão pública, totalizando 13 casos. Além disso, foram registrados dois casos de F1 (fora do setor público) e um de F2 (foco técnico-operacional sem dimensão de gestão).

Esse padrão de exclusões, restrito e concentrado em fatores de acesso e contexto, reforça a robustez da triagem inicial, uma vez que a leitura integral não revelou inconsistências relevantes nas decisões anteriores. Contudo, o predomínio de exclusões por F8 evidencia um viés de disponibilidade, característico de revisões em

áreas emergentes, e que deve ser considerado como limitação da pesquisa — especialmente no que se refere ao acesso desigual a determinadas bases e periódicos (Gráfico 2).

Gráfico 2 – Exclusão após leitura completa



Fonte: Dados da pesquisa (2026).

Ao final da leitura integral, 82 estudos permaneceram incluídos na RSL, compondo o corpus definitivo de análise. Esses artigos embasaram a etapa de extração e codificação temática, em que se registraram dados sobre o setor de aplicação, o método utilizado, os domínios de capacidade e os domínios de efetividade abordados em cada estudo. Os resultados descritivos dessas dimensões setoriais, metodológicas e conceituais, são apresentados e discutidos com maior profundidade na seção 4, na qual a RSL é reinterpretada como base empírica do estado da arte sobre segurança e privacidade em instituições públicas.

3.3 DO PORTFÓLIO DA RSL À ETAPA EMPÍRICA

A consolidação do portfólio final da RSL marca o ponto de transição entre a etapa de identificação de evidências científicas e a fase de aplicação empírica da pesquisa. A partir desse corpus, foram delineadas as estratégias subsequentes de investigação, estruturadas em três frentes interdependentes:

- a) construção e codificação da matriz de domínios e instrumento primário de pesquisa, por meio de indicadores identificados na literatura e confirmados pela RSL;

b) iBase, iSeg e iPriv autorrelatados pelas instituições no próprio instrumento, em escala 0,00–1,00: checagem de validade e consistência dos valores e articulação com os escores por domínio.

c) articulação estatística entre as medidas de maturidade, capacidade e efetividade, com síntese analítica orientada pelo encadeamento teórico derivado da literatura, cuja incidência foi verificada na revisão sistemática.

Essa etapa metodológica opera como um elo de translação entre a evidência científica e o diagnóstico institucional aplicado às IFES, permitindo que o estudo avance da revisão sistemática para o exame empírico da efetividade do PPSI.

3.4 MATRIZ DE DOMÍNIOS E INSTRUMENTO PRIMÁRIO: CONSTRUÇÃO, CODIFICAÇÃO, VALIDAÇÃO E COLETA

Os domínios apresentados a seguir não foram definidos de forma indutiva a partir da revisão sistemática, mas resultam de uma síntese teórico-empírica entre literatura prévia, *frameworks* normativos e evidências consolidadas na RSL.

A formulação inicial desses domínios partiu de três fontes complementares:

(i) Programa de Privacidade e Segurança da Informação (PPSI): conjunto de 26 controles. Os controles são multidimensionais e podem combinar governança, processos, pessoas e tecnologia;

(ii) os modelos internacionais de maturidade e capacidade, como ISO/IEC 27001–27004, COBIT 2019 e o NIST Cybersecurity Framework que relacionam níveis de implementação a estágios de desempenho organizacional; e

(iii) a literatura sobre políticas públicas digitais e capacidades estatais, que identifica a relação entre governança, recursos, competências e resultados públicos (Cavalcante; Lotta, 2015; Papi; Seidi; Santos, 2022; Novato; Najberg; Lotta, 2020).

O Quadro 3 apresenta o mapeamento dos domínios conceituais definidos nesta pesquisa, indicando sua correspondência com as fontes normativas e teóricas que lhes dão sustentação.

Quadro 3 – Domínios de capacidade e efetividade e seus referenciais

Dimensão	Código	Domínio conceitual	Descrição sintética	Referenciais normativos e teóricos
----------	--------	--------------------	---------------------	------------------------------------

Efetividade	E1	Continuidade / Disponibilidade	Redução de indisponibilidades e falhas de serviços críticos (SI/TI).	ISO 22301:2019 – <i>Security and resilience — Business continuity management systems — Requirements</i> ; NIST CSF 2.0 – Função <i>Recover</i> .
	E2	Detecção / Resposta a Incidentes	Capacidade de detectar, conter e recuperar-se de incidentes com maior rapidez.	ISO/IEC 27035-1:2023 – <i>Information security incident management</i> ; NIST CSF 2.0 – Funções <i>Detect</i> e <i>Respond</i> ; COBIT 2019 – DSS02 (<i>Managed Service Requests and Incidents</i>).
	E3	Mitigação de Risco	Diminuição de riscos críticos (probabilidade e impacto) após o tratamento.	ISO 31000:2018 – <i>Risk management — Guidelines</i> ; ISO/IEC 27005:2022 – <i>Guidance on managing information security risks</i> ; COBIT 2019 – APO12 (<i>Managed Risk</i>).
	E4	Proteção de Dados / Privacidade	Redução de incidentes envolvendo dados pessoais e maior conformidade com a LGPD.	ISO/IEC 27701:2025 – <i>Privacy Information Management System</i> ; Lei nº 13.709/2018 (LGPD); NIST Privacy Framework 1.0 – Função <i>Protect</i> .
	E5	Transparência / Notificação / Conformidade	Aprimoramento de processos de notificação e conformidade auditável.	ISO/IEC 27701:2025; COBIT 2019 – MEA01 (<i>Managed performance and conformance monitoring</i>).
	E6	Confiança / Percepção	Melhora na percepção da alta administração e das áreas-fim sobre segurança e privacidade.	COBIT 2019 – EDM02 (<i>Ensure Benefits Delivery</i>); literatura sobre capacidades estatais e valor público (Cavalcante; Lotta, 2015; Novato; Najberg; Lotta, 2020).
Capacidade	C1	Governança	Papéis, comitês e integração da gestão de riscos ao planejamento e à tomada de decisão.	ISO/IEC 38500:2024 – <i>Governance of IT for the organization</i> ; COBIT 2019 – EDM01 ao EDM05; NIST CSF 2.0 – Função <i>Govern</i> .
	C2	Pessoas / Competências	Equipe e competências mínimas dedicadas ao PPSI e à privacidade.	ISO/IEC 27001:2022 – cláusula 7.2 (<i>Competence</i>); COBIT 2019 – APO07 (<i>Managed Human Resources</i>).
	C3	Processos	Processos padronizados de segurança e privacidade executados e monitorados.	ISO/IEC 27002:2022; COBIT 2019 – APO13 e DSS05. NIST CSF 2.0 – Função <i>Protect</i> e <i>Respond</i> .
	C4	Tecnologia / Monitoramento	Ferramentas e mecanismos de monitoramento, detecção e resposta proporcionais aos riscos, incluindo	ISO/IEC 27002:2022; NIST CSF 2.0 – Função <i>Identify</i> , <i>Detect</i> e <i>Respond</i> .

			inventário, telemetria e automação	
	C5	Gestão de Dados / Privacidade	Mapeamento de dados, bases legais, DPIA/RIPDs e controles de acesso e qualidade.	ISO/IEC 27701:2025 (<i>PIMS</i>); ISO/IEC 29100:2024 (<i>Privacy framework</i>); ISO/IEC 29134:2023 (<i>PIA/DPIA</i>); LGPD arts. 7–11 (bases legais) e 37–41 (registros, encarregado, RIPD).
	C6	Recursos	Recursos orçamentários e contratuais mínimos para execução do PPSI.	COBIT 2019 – APO06 (<i>Managed Budget and Costs</i>); ISO 22301:2019 – cláusula 7.1 (<i>Resources</i>).

Fonte: Elaboração própria com base em ISO/IEC (2018–2025), COBIT 2019 (ISACA, 2019), NIST CSF 2.0 (NIST, 2024), LGPD (Lei nº 13.709/2018) e literatura sobre capacidades estatais (Cavalcante; Lotta, 2015; Novato; Najberg; Lotta, 2020).

3.4.1 Derivação dos domínios e construção do instrumento

A RSL, portanto, foi desenhada para verificar empiricamente se os domínios previstos nesses referenciais teóricos, aqui denominados domínios de capacidade (governança, processos, pessoas, tecnologia, dados e recursos) e domínios de efetividade (mitigação de risco, conformidade, proteção de dados, confiança e continuidade), são de fato operacionalizados na literatura científica sobre segurança da informação e privacidade em contextos públicos.

Durante a etapa de RSL, foi realizada a codificação de cada estudo selecionado dentro desses domínios. A codificação temática dos artigos incluídos foi complementada com o suporte do NotebookLM (Google), empregado para confrontar trechos textuais e apoiar a consolidação das categorias de capacidades (C1–C6) e efetividade (E1–E6) previamente definidas no *codebook*. Essa etapa manteve supervisão e revisão integral pelo autor, que validou manualmente as classificações e harmonizou eventuais inconsistências detectadas pelas ferramentas de apoio.

Já o questionário deriva diretamente da matriz de domínios codificados na RSL e operacionaliza a lógica inferencial proposta neste estudo, da implementação dos controles (PPSI) às capacidades institucionais e aos resultados de efetividade.

O instrumento final aplicado foi estruturado em blocos sequenciais, contemplando: consentimento livre e esclarecido; qualificação do respondente; identificação da IFES; variáveis institucionais de contexto; capacidades institucionais;

efetividade percebida do PPSI; e campo aberto complementar. Os constructos centrais da pesquisa foram mensurados por 18 itens em escala Likert de 7 pontos, sendo 8 itens relativos às capacidades institucionais (C1–C8) e 10 itens relativos à efetividade percebida (E1–E10). As demais questões tiveram função de qualificação, controle e caracterização contextual, não integrando diretamente os escores centrais de capacidades e efetividade.

Na passagem do *codebook* da RSL para o instrumento aplicado, os seis domínios de capacidade e os seis de efetividade foram refinados em oito itens de capacidade (C1–C8) e dez itens de efetividade (E1–E10). No bloco de capacidades, o domínio Pessoas/Competências foi desdobrado em equipe e competências (C2) e treinamento e conscientização (C7); a integração da gestão de riscos ao planejamento e ao orçamento, originalmente compreendida na descrição do domínio Governança, foi destacada em item próprio (C6); e o domínio Recursos passou a ser mensurado pelo item C8. No bloco de efetividade, os domínios Continuidade/Disponibilidade, Detecção/Resposta, Transparência/Conformidade e Confiança/Percepção foram desdobrados em dois itens cada (E1–E2, E3–E4, E7–E8 e E9–E10), preservando-se itens únicos para Mitigação de Risco (E5) e Proteção de Dados (E6). O Quadro 5, na seção 4, apresenta a correspondência integral entre domínios e itens.

Registre-se, para evitar ambiguidade de leitura, que os códigos C1–C6 e E1–E6 empregados na revisão sistemática designam domínios conceituais, ao passo que os códigos C1–C8 e E1–E10 do instrumento numeram itens, e as duas numerações não coincidem termo a termo: a mitigação de risco, por exemplo, é o terceiro domínio da revisão (E3) e o quinto item do instrumento (E5); no bloco de capacidades, o domínio C6 da revisão corresponde a recursos, enquanto, no instrumento, a integração da gestão de riscos é mensurada pelo item C6 e os recursos, pelo item C8. Nas seções 4 e 5, portanto, os códigos devem ser lidos no contexto do respectivo capítulo, conforme a correspondência do Quadro 5.

O bloco de qualificação do respondente foi incluído para verificar sua relação com o PPSI e seu perfil predominante de atuação institucional. Essa informação permitiu avaliar a consistência da resposta e tratar eventuais duplicidades por IFES, sem caracterizar o respondente individualmente na apresentação dos resultados. A identificação da instituição foi mantida como variável necessária à consolidação da base, à eliminação de duplicidades e à posterior vinculação com variáveis contextuais.

As variáveis de porte institucional foram coletadas por faixas, e não por valores absolutos, com o objetivo de reduzir o esforço de resposta e minimizar erros decorrentes de desconhecimento de números exatos. Foram consideradas faixas para o total aproximado de estudantes regularmente vinculados à instituição, total aproximado de servidores e tamanho aproximado da equipe de TI/TIC. Também foi incluída variável sobre a condição multicampi da IFES, por sua relevância como fator contextual associado à dispersão territorial, complexidade de coordenação e heterogeneidade organizacional.

Os indicadores iBase, iSeg e iPriv foram solicitados em escala de 0,00 a 1,00, em campo de preenchimento facultativo, quando disponíveis ao respondente, como variáveis complementares para articulação analítica com os escores de capacidades e efetividade. Esses indicadores não constituem desfechos da pesquisa, mas medidas de maturidade e estruturação do PPSI, utilizadas para examinar associações entre implementação, capacidades institucionais e resultados percebidos. O campo aberto final teve função complementar, destinado ao registro de observações adicionais sobre o PPSI, sem alterar a natureza quantitativa da pesquisa nem constituir base para análise qualitativa sistemática. A versão integral do instrumento aplicado consta no Apêndice A.

3.4.2 Validação de conteúdo por especialistas

A validação de conteúdo foi conduzida por meio de painel de especialistas, composto por profissionais com experiência em segurança da informação, privacidade de dados, proteção de dados pessoais e governança do PPSI. Os especialistas atuam na Secretaria de Governo Digital (SGD) junto à implementação do PPSI no contexto das IFES, embora o protocolo inicial previsse dez avaliadores, foram obtidos onze retornos válidos. O objetivo dessa etapa foi aferir a validade de conteúdo do questionário, verificando se os itens formulados refletiam de modo adequado os domínios teóricos de capacidade e efetividade identificados na revisão sistemática.

Cada especialista avaliou individualmente a essencialidade de cada item do instrumento, utilizando escala de três pontos: (1) não essencial, (2) útil, mas não essencial, e (3) essencial. Com base nessas avaliações, foi calculado o Content Validity Ratio (CVR), proposto por Lawshe (1975), conforme a fórmula:

$$CVR = (ne - N/2) / (N/2)$$

onde n representa o número de especialistas que consideraram o item “essencial” e N o número total de avaliadores. Na primeira rodada, o critério operacional de retenção adotado foi a exigência mínima de 9 julgamentos como “essencial”, correspondente a $CVR = 0,636$, considerando painel de 11 respondentes válidos.

Os itens que não atingiram esse valor mínimo foram submetidos à etapa complementar de refinamento com especialistas do próprio painel, especialmente entre aqueles que não os haviam classificado como essenciais. Essa etapa teve por objetivo discutir aderência conceitual, clareza semântica e precisão redacional dos itens, com vistas à formulação final do instrumento.

A etapa complementar teve caráter confirmatório e de refinamento, voltado à reapreciação dos itens inicialmente problemáticos, sem reconstituir integralmente o painel inicial. Seu propósito foi verificar se os ajustes promovidos elevavam o grau de convergência entre os especialistas disponíveis para nova apreciação, preservando o núcleo conceitual do instrumento e sua coerência com a matriz derivada da RSL.

Desse modo, a validação por especialistas cumpriu dupla função: aferir a essencialidade dos itens por meio do CVR e apoiar o aprimoramento redacional e operacional do questionário, contribuindo para a consolidação da versão final aplicada na coleta principal.

3.4.3 Aplicação do questionário, qualificação dos respondentes e tratamento de duplicidades

A aplicação foi digital, dirigida a todo o universo de IFES participantes do PPSI, com encaminhamento de convites aos atores institucionais vinculados ao programa. Os convites foram enviados às 110 instituições do universo de referência (69 universidades federais e 41 institutos federais ou instituições equiparadas — Andifes, 2025; Brasil, 2019), com reforços periódicos ao longo do período de coleta, compreendido entre 16 de abril e 22 de maio de 2026. Foram registradas 69 respostas brutas que, após os critérios de depuração descritos na seção 5, resultaram em 58 respostas institucionais válidas, correspondentes a 52,7% do universo. O questionário foi aplicado na plataforma Google Forms, vinculada à conta institucional do pesquisador na Universidade Federal da Fronteira Sul (UFFS), de modo a permitir controle da coleta, exportação dos dados e guarda segura das respostas.

Os convites foram enviados por e-mail institucional, utilizando endereços disponíveis em portais oficiais das IFES e contatos relacionados ao Programa de Privacidade e Segurança da Informação. A mensagem de convite apresentou o objetivo do estudo, sua vinculação acadêmica, o tempo médio estimado de resposta, o Termo de Consentimento Livre e Esclarecido (TCLE) e as garantias de confidencialidade e uso científico dos dados.

A unidade de análise da pesquisa é a IFES. O público-alvo do questionário correspondeu aos atores institucionais formalmente vinculados à implementação, ao acompanhamento ou ao preenchimento do PPSI na instituição, com prioridade para a pessoa que atua como principal responsável institucional pelo programa. Essa delimitação considerou a estrutura de governança do PPSI 2.0, que envolve diferentes papéis institucionais relacionados à alta administração, segurança da informação, tecnologia da informação e proteção de dados pessoais.

Para qualificar a posição institucional do respondente, o questionário incluiu perguntas específicas sobre sua relação com o PPSI e sobre o perfil predominante de atuação em relação ao programa. Essas informações não compõem os constructos centrais de capacidades e efetividade, mas foram utilizadas para controle da consistência da resposta e para tratamento de eventuais duplicidades.

Nos casos em que houve mais de uma resposta da mesma IFES, manteve-se uma única resposta por instituição, selecionada pela proximidade do respondente com o programa: priorizou-se, sucessivamente, quem se declarou principal responsável institucional pelo PPSI, quem declarou atuação direta no programa e o perfil predominante mais próximo do seu objeto (segurança da informação, tecnologia da informação/TIC, privacidade e proteção de dados e gestão institucional, nessa ordem). Empates residuais seriam resolvidos pela resposta mais completa e, por fim, pela mais recente.

Não houve coleta obrigatória de e-mail, preservando-se a identificação institucional como referência necessária à consolidação da base analítica. Ao final do período de coleta, os dados foram exportados em formato .csv e incorporados à base analítica da pesquisa, sendo tratados conforme os procedimentos descritos na Seção 3.6.

3.5 INDICADORES IBASE, ISEG E IPRIV E PLANO DE ARTICULAÇÃO ANALÍTICA

Os indicadores iBase, iSeg e iPriv foram coletados por autorrelato institucional, em escala de 0,00 a 1,00, para fins de análise com capacidades e efetividades. O iBase representa a maturidade associada à estrutura básica do PPSI, enquanto iSeg e iPriv expressam, respectivamente, os níveis de maturidade nos eixos de segurança da informação e privacidade.

A utilização desses indicadores permitiu examinar, de forma exploratória, a associação entre maturidade declarada no PPSI, capacidades institucionais percebidas e resultados de efetividade. Nos casos em que os valores não foram informados, as análises envolvendo iBase, iSeg e iPriv foram realizadas apenas com os casos válidos, preservando-se a base completa para as análises descritivas e inferenciais dos constructos centrais do instrumento.

3.6 TRATAMENTO E ANÁLISE DOS DADOS

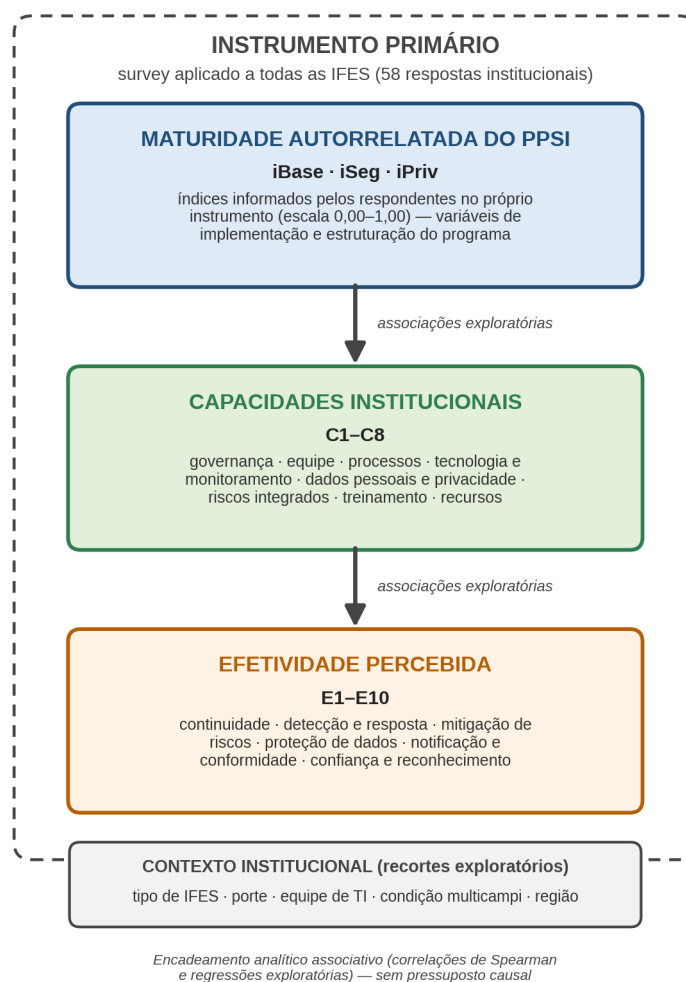
O tratamento quantitativo seguiu rotinas de consistência e verificação de qualidade. Dados ausentes foram tratados por análise de casos completos, sem necessidade de imputação, dada a baixa taxa de ausência — uma variável de porte com um caso omissos e seis casos sem índices de maturidade válidos (Hair *et al.*, 2019; Enders, 2010).

A confiabilidade interna foi estimada por α de Cronbach e ω de McDonald apenas nos domínios multi-itens; domínios de item único tiveram validade de conteúdo (CVR) e evidência convergente (Cronbach, 1951; McDonald, 1999). As estatísticas descritivas foram complementadas por correlações de Spearman entre os domínios de capacidade/efetividade e os índices de maturidade (iBase, iSeg e iPriv), apropriadas para distribuições não-normais e escalas ordinais (Spearman, 1904).

Quando o tamanho amostral o permitiu, foram ajustados modelos de regressão exploratórios com erros-padrão robustos, a fim de corrigir possíveis violações de homocedasticidade e garantir estimativas consistentes (Hayes, 2018). Foram conduzidas verificações de sensibilidade, incluindo o exame de multicolinearidade por meio do fator de inflação da variância (VIF), diagnósticos de influência (distância de Cook e DFBETAS), reestimação *leave-one-out* dos modelos e reestimação por regressão robusta (estimador de Huber), para avaliar a estabilidade dos coeficientes sob diferentes cenários amostrais e reduzir o impacto de observações atípicas.

Embora a literatura metodológica reconheça a modelagem de equações estruturais (SEM) como abordagem de referência para investigar relações entre constructos latentes (Kline, 2016; Hair *et al.*, 2021), o presente estudo não emprega SEM, uma vez que a base de 58 observações institucionais é insuficiente para a estimação estável desse tipo de modelo. Em vez disso, adota-se o encadeamento teórico maturidade → capacidades → efetividade, operacionalizado por meio de regressões lineares e correlações exploratórias, adequadas ao desenho da pesquisa e ao nível de análise institucional desta pesquisa (Hair *et al.*, 2019).

Figura 4 – Fluxo entre maturidade, capacidades e efetividade



Fonte: Elaboração própria (2026).

O modelo representado na Figura 4 sintetiza o encadeamento teórico-analítico adotado na dissertação. A implementação dos controles do PPSI, representada pelos índices de maturidade autorrelatados (iBase, iSeg e iPriv), expressa o grau de estruturação do programa. Essas medidas são tratadas como variáveis de implementação, articuladas às capacidades institucionais mensuradas pelo

instrumento primário, as quais, por sua vez, são analisadas em relação aos resultados de efetividade percebida. Esse encadeamento traduz a hipótese de trabalho de que a implementação, embora necessária, tende a se converter em resultados sustentáveis quando acompanhada do fortalecimento das capacidades organizacionais — tratada nesta pesquisa como questão associativa, e não causal.

3.7 VALIDADE, ÉTICA, LIMITAÇÕES E REPRODUTIBILIDADE

A validade de conteúdo é assegurada pela derivação teórico-empírica a partir da RSL e pela validação de especialistas. A confiabilidade foi estimada pelos coeficientes alfa e ômega. A validade externa é favorecida pela abrangência do universo de IFES, com cobertura de 52,7%, e pela articulação entre as medidas primárias e os índices de maturidade autorrelatados.

Na preparação da base analítica, os indicadores iBase, iSeg e iPriv foram tratados como valores autorrelatados pelos respondentes, informados no âmbito do instrumento de pesquisa em escala de 0 a 1. Valores ausentes ou informados fora desse intervalo foram desconsiderados nas análises envolvendo os índices, preservando-se os demais campos válidos da resposta. A identificação nominal das instituições foi removida da base de análise e substituída apenas pela região geográfica correspondente, de modo a reduzir riscos de reidentificação e preservar a confidencialidade institucional.

Os indicadores iBase, iSeg e iPriv foram utilizados exclusivamente em análises estatísticas agregadas, especialmente correlações e regressões exploratórias envolvendo maturidade autorrelatada, capacidades institucionais e efetividade percebida. Os valores individualizados desses índices por instituição não são apresentados no texto, em quadros, tabelas ou apêndices. A base da pesquisa, quando disponibilizada sob demanda, não conterá identificação nominal das IFES nem valores individualizados dos indicadores de maturidade.

As principais limitações incluem potenciais vieses de não resposta e de método comum, mitigados pela redação equilibrada dos itens, pela ordem dos blocos do questionário e pelo anonimato dos respondentes.

Registre-se que a opção pela efetividade percebida não decorre apenas da indisponibilidade dos registros administrativos do programa. Em cada dimensão avaliada, a medida objetiva correspondente ou não existe em base nacional, ou

pressupõe capacidades que a própria pesquisa identificou como frágeis. Não há consolidação nacional de incidentes por instituição, e o registro interno depende de processos estruturados de detecção e resposta; contagens brutas, ademais, tenderiam a penalizar as instituições que aprimoram a detecção, uma vez que detectar melhor implica registrar mais. Mitigações de risco verificáveis pressupõem gestão de riscos integrada e documentada, uma das capacidades de menor média na amostra. A execução orçamentária em segurança, embora possua trilha documental, raramente é classificada de forma destacada, o que impede sua atribuição sem reconstrução caso a caso. Interrupções de serviços têm causas múltiplas, e desastres de alta severidade têm frequência baixa demais para compor séries comparáveis por instituição. O reconhecimento institucional, por fim, é constructo perceptual por natureza. Nesse estágio de estruturação do campo, a percepção de operadores qualificados constitui a operacionalização disponível mais coerente com o fenômeno avaliado, e a distância entre conformidade declarada e resultado percebido, evidenciada nos dados, ilustra a própria lacuna de mensuração que o estudo problematiza.

Uma limitação da pesquisa decorre do uso de indicadores de maturidade autorrelatados pelos respondentes. Essa opção não foi de desenho, mas de contingência. O acesso à base secundária consolidada dos índices, mantida pelo órgão central, não foi concedido à pesquisa, posteriormente houve classificação da informação por prazo de cinco anos e sem avaliação de risco que distinguisse as camadas de granularidade envolvidas. Essas camadas não carregam o mesmo peso: o índice agregado de um órgão não expõe o que expõem os índices por controle, o grau de implementação de cada medida, as evidências ou os planos de trabalho, e a camada mais agregada tende a apresentar risco reduzido, com valor informacional elevado para fins de avaliação, de coordenação e de controle social. A classificação uniforme, calibrada pela informação mais sensível, inviabilizou a triangulação com registros administrativos prevista no desenho original e conduziu à coleta por autorrelato. Embora iBase, iSeg e iPriv sejam variáveis relevantes para examinar a relação entre maturidade, capacidades e efetividade, seu preenchimento não era obrigatório no formulário e sua coleta por autorrelato pode estar sujeita a erros de preenchimento, desconhecimento do valor atualizado ou diferenças de interpretação quanto ao ciclo de referência do PPSI. Para mitigar esse risco, foram considerados

válidos apenas os valores situados no intervalo previsto entre 0 e 1, e os índices foram utilizados de forma complementar, sem constituir o eixo principal da análise empírica.

Outra limitação refere-se à impossibilidade de análise desagregada por medidas ou controles individuais do PPSI. A pesquisa trabalha com domínios de capacidade e efetividade mensurados por instrumento primário, bem como com indicadores agregados de maturidade autorrelatada. Desse modo, os resultados permitem identificar associações entre capacidades institucionais e efetividade percebida, mas não permitem estimar o efeito específico de medidas ou controles isolados do PPSI. A correspondência entre os domínios do instrumento e os controles do programa deve ser interpretada como aproximação teórica, e não como inferência estatística direta por controle.

A pesquisa foi submetida ao Comitê de Ética em Pesquisa da Universidade Federal da Fronteira Sul (CEP/UFFS), por meio da Plataforma Brasil, tendo sido aprovada sob o CAAE nº 94243825.5.0000.5564 e Parecer CEP/UFFS nº 8.076.502. A participação foi condicionada à leitura e aceite do TCLE, apresentado no início do questionário eletrônico.

Para garantir a rastreabilidade do processo metodológico, a documentação da pesquisa, o protocolo da RSL, as planilhas de deduplicação, triagem e extração, o diagrama PRISMA, o questionário final, o dicionário de variáveis e os scripts de análise, permanecerá sob guarda do pesquisador, em armazenamento vinculado à sua conta institucional na universidade, e poderá ser disponibilizada sob demanda, mediante solicitação fundamentada, para fins de verificação e replicação científica. A base analítica, quando fornecida sob demanda, será entregue sem a identificação nominal das instituições e sem os índices autorrelatados do PPSI (iBase, iSeg e iPriv) que, na fase final da presente pesquisa, foram objeto de classificação nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) (Brasil, 2011).

No desenvolvimento desta pesquisa foram utilizadas, de forma assistiva e pontual, ferramentas baseadas em inteligência artificial, a saber: GPT-5 (OpenAI), no apoio à padronização de critérios e à verificação de consistência nas etapas de triagem e leitura integral da revisão sistemática; NotebookLM (Google), no apoio à codificação temática do portfólio; e Claude (Anthropic), no apoio à sistematização de resultados, à revisão textual e à elaboração de gráficos e figuras. Todo o conteúdo analítico, interpretativo e redacional foi criado, revisado e validado pelo pesquisador,

que responde integralmente pela autoria intelectual e pelo rigor metodológico do trabalho.

4 ANÁLISE SITUACIONAL: RESULTADOS DA REVISÃO SISTEMÁTICA E VALIDAÇÃO DO INSTRUMENTO

Encerradas as etapas metodológicas que conduziram à formação do portfólio final, a pesquisa alcança o ponto de passagem entre o como foi feita a revisão sistemática e o que ela efetivamente revelou. O percurso descrito até aqui permitiu estabelecer identificação, seleção e validação das evidências científicas sobre segurança da informação, privacidade e efetividade em contextos públicos e educacionais.

A RSL cumpriu, portanto, dupla função: consolidou o estado da arte internacional sobre o tema e, ao mesmo tempo, serviu de verificação empírica para a estrutura conceitual adotada nesta dissertação, aquela que distingue e relaciona capacidades institucionais e resultados de efetividade. Ao final desse processo, formou-se um corpus cuja análise permite compreender tanto as tendências setoriais e metodológicas da produção científica recente quanto as combinações de mecanismos organizacionais mais associadas à maturidade e ao desempenho institucional. É a partir desse ponto que se desenvolve a seção 4, dedicada à apresentação e discussão dos resultados da revisão sistemática, que compõem a análise situacional e delineiam o estado da arte em políticas públicas de segurança da informação e privacidade. Nessa seção, são apresentados os padrões observados quanto à evolução temporal das publicações, enfoques temáticos predominantes, distribuição setorial, métodos empregados e, sobretudo, as relações entre capacidades e efetividades que emergem da literatura revisada.

O corpus final da revisão sistemática é composto por 82 estudos (Quadro 4), documentados de forma completa na planilha auditável, constante na seção de Apêndices e sintetizados a seguir.

Quadro 4 – Corpus final da RSL

id	autor	título
R00001	Mohamed Noor, A. F.	Identifying key factors of cybersecurity readiness in organizations: Insights from Malaysian critical infrastructure
R00009	Choudhary, S. K.	Modeling the role of generative AI in organizational privacy and security
R00015	Ogbodo, D. C.	From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection
R00016	Mohsini, M. H.	Framework for Enhancing Effectiveness of Information Security Measures Implemented in Public Institutions in Tanzania
R00019	Gupta, P.	Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis
R00044	Hossain, S.T.	Cybersecurity in local governments: A systematic review and <i>framework</i> of key challenges

R00045	Chahid, A.	Digital Transformation in Higher Education Obstacle Assessment and Development of Strategies against Cybersecurity Threats: The Case of Moroccan Universities
R00046	Durman, M.	Influence Of Digital Technologies On Information Security In The Public Administration System
R00049	Khan, M.A.	Towards the evaluation of cybersecurity threats and challenges in higher education institutions in Saudi Arabia
R00056	Putro, P.A.L.	Validating cybersecurity <i>framework</i> : a case study <i>framework</i> for critical information infrastructure protection
R00059	Šikman, L.	Model For Assessing Measurable Aspects Of Information Security In Higher Education
R00062	Salam, M.	Building Cyber-Resilient Universities: A Tailored Maturity Model for Strengthening Cybersecurity in Higher Education
R00064	Sittitiamjan, K.	Bridging the Gap: How Knowledge, Attitudes, and Practices Shape Cybersecurity Awareness in Thai Education
R00069	Alhawtmeh, O. M.	The role of internal audit as a tool for enhancing cybersecurity effectiveness in Jordanian government agencies
R00075	Gaie, C.	Cybersecurity of Public Sector Institutions
R00077	Sanchez-Zurdo, J.	A Country Risk Assessment from the Perspective of Cybersecurity in Local Entities
R00095	Agashe, N.	Introspecting the digital dynamics: reconnecting the interplay between privacy, surveillance, and governance in the global landscape, with a special focus on India
R00097	Liu, X.	How internet use affects personal privacy risk perception: empirical evidence from China
R00127	Alhanatleh, H. M.	Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel <i>framework</i> in Jordan
R00136	El Rob, M. F. A.	The application of MITRE ATT&CK <i>framework</i> in mitigating cybersecurity threats in the public sector
R00144	Belligoni, S.	Privacy and security concerns with passively collected location data for digital contact tracing among U.S. college students
R00209	Cheng, C.K.E.	Institutional Strategies for Cybersecurity in Higher Education Institutions
R00214	Dewanto, M.R.P.	Comparative Study Of Information Security Evaluation Models For Indonesia Government
R00229	Al Qatawneh, I. S.	A Comparative Study On Surveillance And Privacy Regulations
R00256	Malatji, M.	Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa
R00262	Al-Zahrani, M. S.	Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia
R00277	Van Steen, T.	What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?
R00288	Dutton, W. H.	Cybersecurity Capacity Does It Matter?
R00294	Hale, M. L.	Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards
R00300	Mutimukwe, C.	Information privacy practices in e-government in an African least developing country, Rwanda
R00334	Chinyemba, M. K.	An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector
R00345	Abdelwahed, A. S.	Information security policies and their relationship with the effectiveness of the management information systems of major palestinian universities in the gaza strip
R00365	Magnusson, L.	Information security governance in the public sector: investigations, approaches, measures, and trends
R00366	Allahawiah, S.	The Role of Organizational Culture in Cybersecurity Readiness: An Empirical Study of the Jordanian Ministry of Justice
R00370	Ukeje, N.	Information security and privacy challenges of cloud computing for government adoption: a systematic review
R00373	Chatfield, A. T.	A <i>framework</i> for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government
R00379	Domínguez-Dorado, M.	Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study
R00380	Vestad, A.	From Security Frameworks to Sustainable Municipal Cybersecurity Capabilities
R00382	de Azambuja, A. J. G.	Cybersecurity maturity model for the Brazilian Federal Government Agencies
R00393	Damasceno, L.M.D.	Factors That Influence The Readiness To Follow Information Security Policy In A Higher Education Institution

R00404	Figueroa, V.	Building a holistic cybersecurity <i>framework</i> for e-Government based on a systematic analysis of proposals
R00408	Shaheen, K.	The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain
R00410	Moon, Y.J.	The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations
R00412	Tran, D. V.	Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam
R00413	Park, S.	The Diagnosis and Prescription for Cybersecurity in Korea: Focusing on Policy and System
R00423	Ribeiro, D.	Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications
R00435	Evans, M.	Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector
R00439	Park, S.	A comparative study on data protection legislations and government <i>standards</i> to implement Digital Forensic Readiness as mandatory requirement
R00444	Krishna, B.	Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis
R00447	Granata, D.	Automated threat modelling and risk analysis in e-Government using BPMN
R00448	Martínez, J.J.C.	National cybersecurity outlook for Colombia to 2030
R00453	Hossain, S.T.	Understanding Local Government Cybersecurity Policy: A Concept Map and Framework
R00456	Mwogosi, A.	Digital policy and governance <i>frameworks</i> for EHR systems in Tanzania: a scoping review
R00463	Murah, M.Z.	Web Assessment of Libyan Government e-Government Services
R00469	Zhang, X.S.	A more secure <i>framework</i> for open government data sharing based on federated learning
R00470	Borgman, B.	Cyber security readiness in the South Australian Government
R00483	Green, A.	Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems
R00489	Al Ghaffar, H.T.A.N.	Government Cloud Computing and National Security
R00506	Vatamanu, A.F.	Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities
R00510	Al-Hawamleh, A.M.	Investigate the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA
R00511	Ramtohul, A.	Information security governance for e-services in southern African developing countries e-Government projects
R00514	Le, V. H.	Information Security Risk Management by a Holistic Approach: a Case Study for Vietnamese e-Government
R00515	Li, C. Y.	A Comprehensive Overview of Government Hacking Worldwide
R00520	Frاندell, A.	Cybersecurity Threats in Local Government: A Sociotechnical Perspective
R00521	Saura, J.R.	Assessing behavioral data science privacy issues in government artificial intelligence deployment
R00539	Roehl, U.B.U.	Automated, administrative decision-making and good governance: Synergies, <i>trade-offs</i> , and limits
R00547	Paul, J.A.	Decision support model for cybersecurity risk planning: A two-stage stochastic programming <i>framework</i> featuring firms, government, and attacker
R00549	Masrek, M.N.	Examining The Relationship Between Information Security Effectiveness And Information Security Threats
R00550	Porter, T.	An integrated complex adaptive governmental policy response to cyberthreats
R00578	Yang, X.M.	Understanding the antecedents of privacy fatigue in facial recognition-based m-Gov services: An empirical study from China
R00582	Falowo, O.I.	Enhancing Cybersecurity With Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response
R00592	Karlsson, M.	The effect of perceived organizational culture on employees' information security <i>compliance</i>
R00606	AlAbdali, H.	Privacy Preservation Instruments Influencing the Trustworthiness of e-Government Services
R00637	Mutimukwe, C.	Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior
R00656	Gumzej, N.	DPA powers toward effective and transparent GDPR enforcement: the case of Croatia

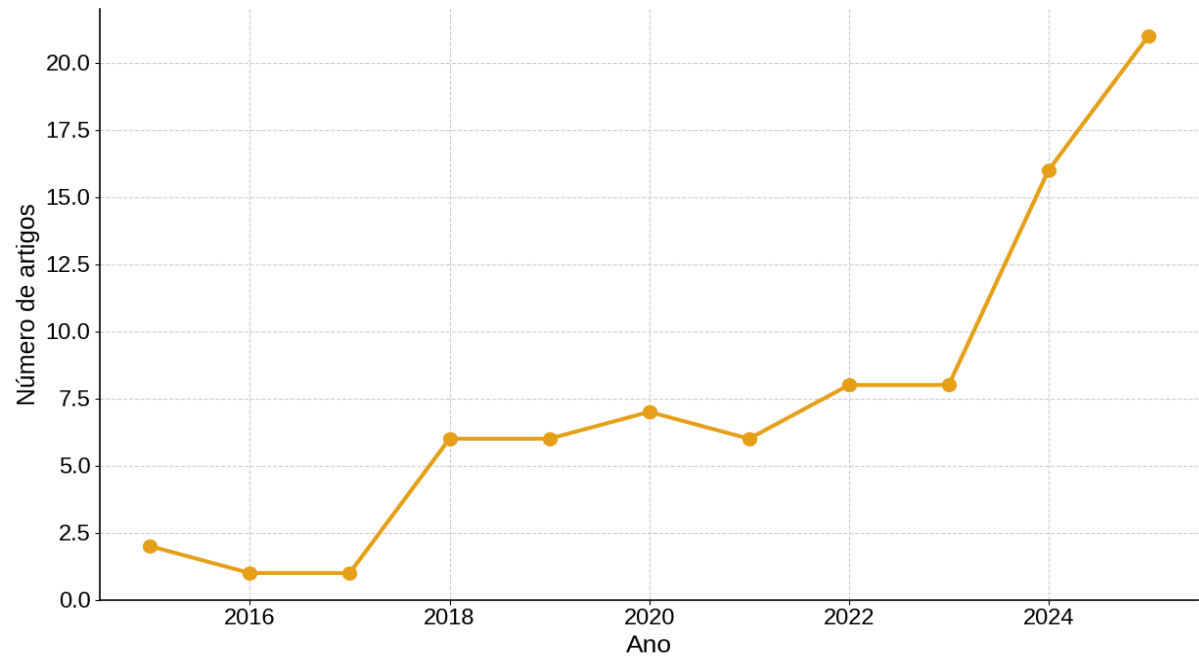
R00662	Munyoka, W.	Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries
R00712	Chorna, V.	Development Of Cybersecurity Of Critical Infrastructure In The Conditions Of Digitalization: Economic Tools For Risks And Investments Assessment
R00802	Esposti, S. D.	What's In It For Us? Benevolence, National Security, and Digital Surveillance
R00893	Benaribi, F.I.	A SPARQL-based <i>framework</i> to preserve privacy of sensitive data on the semantic web
R00965	Alves, G.F.	The diffusion of innovations under normative induction in Brazil
R00981	Zrahia, A.	Navigating vulnerability markets and bug bounty programs: A public policy perspective
R01023	Hosseini, M.B.	Analyzing privacy policies through syntax-driven semantic analysis of information types

Fonte: Dados da pesquisa (2026).

4.1 RESULTADOS DA REVISÃO SISTEMÁTICA

Entrando na análise do corpus final, a primeira característica apresentada é com relação à distribuição temporal das publicações (Gráfico 3), que mostra uma clara aceleração a partir de 2019, com elevada concentração nos anos 2024 e 2025, coerente com o contexto de expansão dos serviços digitais e a consolidação de marcos regulatórios de proteção de dados, como o GDPR e a LGPD.

Gráfico 3 – Distribuição temporal das publicações incluídas (RSL)

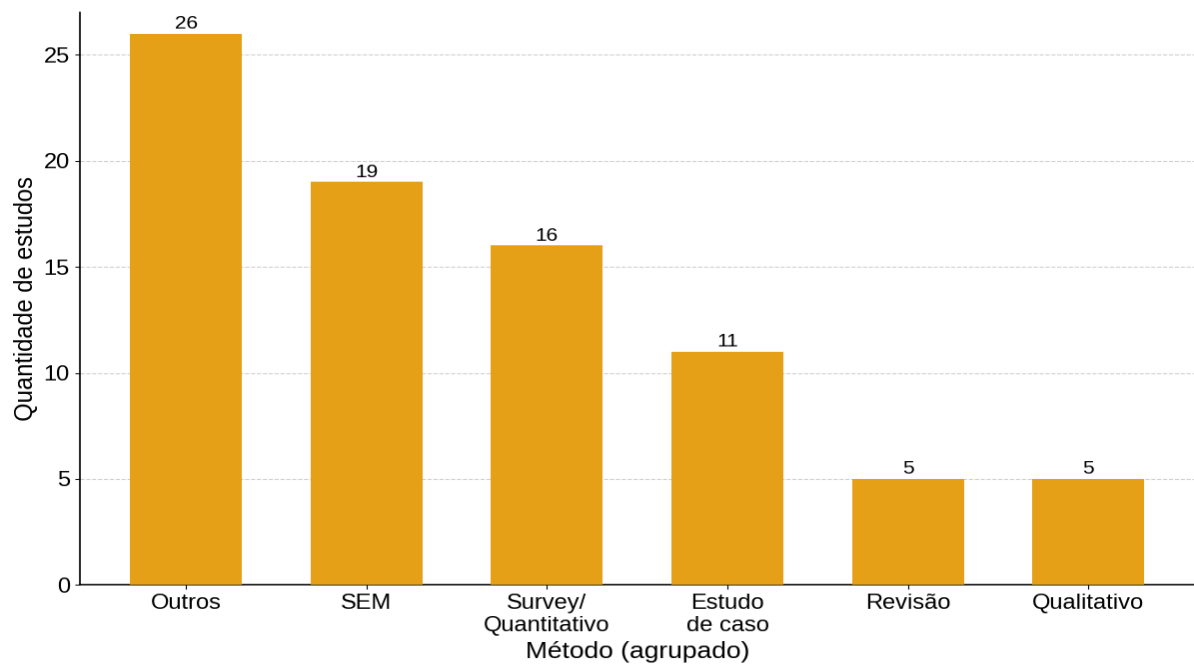


Fonte: Dados da pesquisa (2026).

A diversidade metodológica observada no corpus analisado complementa a compreensão das relações entre capacidades e efetividades.

Os estudos foram classificados conforme a estratégia predominante de pesquisa e pelo tipo de técnica empregada, consolidando o panorama apresentado no Gráfico 4:

Gráfico 4 – Distribuição por método utilizado



Fonte: Dados da pesquisa (2026).

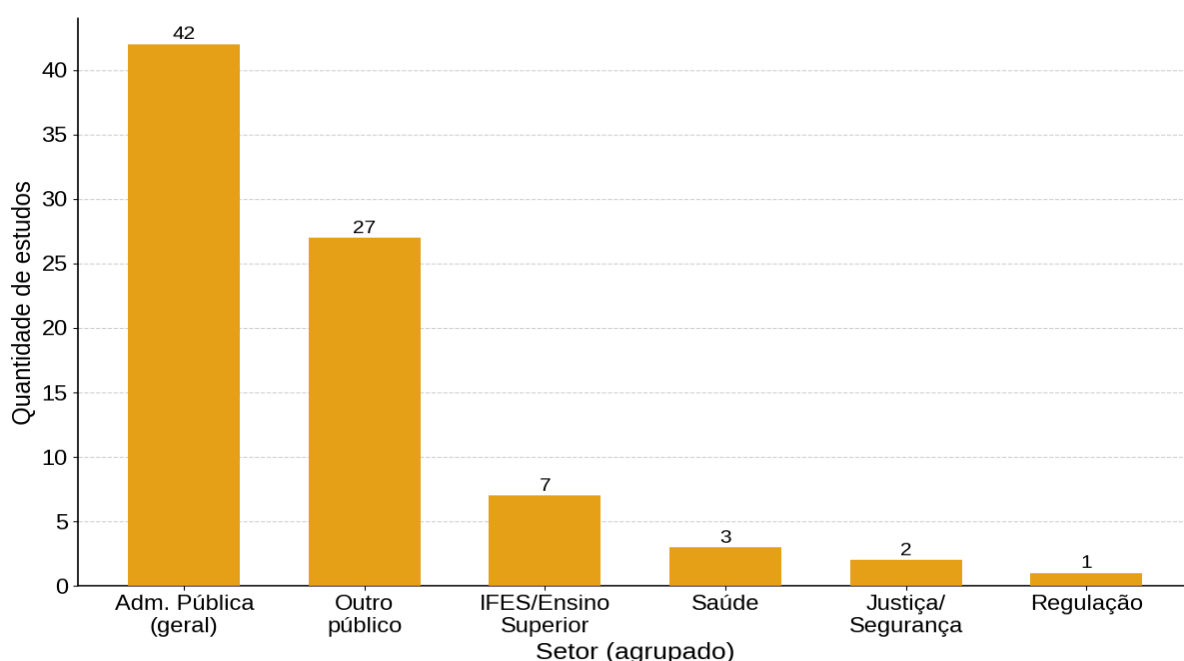
Predominam abordagens *survey*/quantitativas e modelagens de equações estruturais (SEM), frequentemente utilizadas para testar empiricamente as relações entre controles, capacidades e resultados. Em segundo plano, aparecem estudos qualitativos e de caso, voltados a compreender mecanismos de implementação e contextos institucionais que explicam por que determinados controles geram (ou não) efeitos observáveis de efetividade.

Essa composição metodológica sugere um campo em amadurecimento: as abordagens quantitativas fornecem evidências mensuráveis de associação entre construtos, enquanto as qualitativas exploram os processos organizacionais que sustentam essas relações.

No conjunto, o perfil metodológico reforça que maturidade é condição necessária, mas não suficiente. A efetividade depende da combinação entre mensuração técnica e interpretação institucional dos resultados.

Em complemento, a análise setorial dos estudos (Gráfico 5) evidencia a diversidade de contextos públicos em que as políticas de segurança e privacidade foram investigadas.

Gráfico 5 – Distribuição por setor público



Fonte: Dados da pesquisa (2026).

Observa-se maior concentração em Instituições de Ensino Superior (IES) e administrações públicas centrais, seguidas por setores de saúde, justiça e segurança, e ambientes de governo eletrônico e dados abertos.

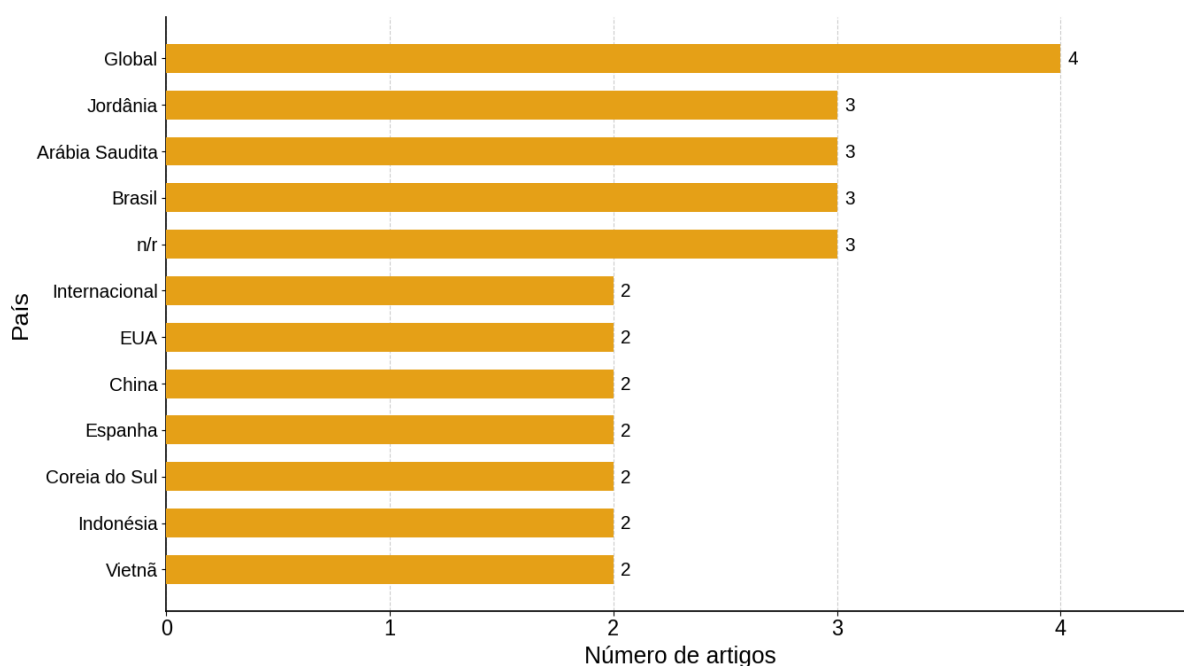
Esse padrão indica que a segurança e a privacidade da informação são tratadas, na literatura, como temas transversais à gestão pública, embora com níveis distintos de maturidade.

Enquanto o ensino superior e a administração central tendem a focar em governança, políticas e conformidade, os estudos de saúde e segurança concentram-se em proteção de dados sensíveis e continuidade operacional.

A distribuição setorial, portanto, confirma a amplitude de aplicação dos domínios de capacidade e efetividade e reforça a pertinência do PPSI como instrumento unificador da política de segurança e privacidade no âmbito do Estado brasileiro.

A distribuição por países e setores revela diversidade geográfica e institucional. Há presença de estudos internacionais e de contextos nacionais como Jordânia, Arábia Saudita, Brasil, Estados Unidos e China, além de recortes setoriais envolvendo administrações públicas centrais e locais, ensino superior, saúde, nuvens governamentais e sistemas de alerta. Essa variedade reforça a transferibilidade dos achados e a utilidade externa do *codebook* adotado para as IFES (Gráfico 6).

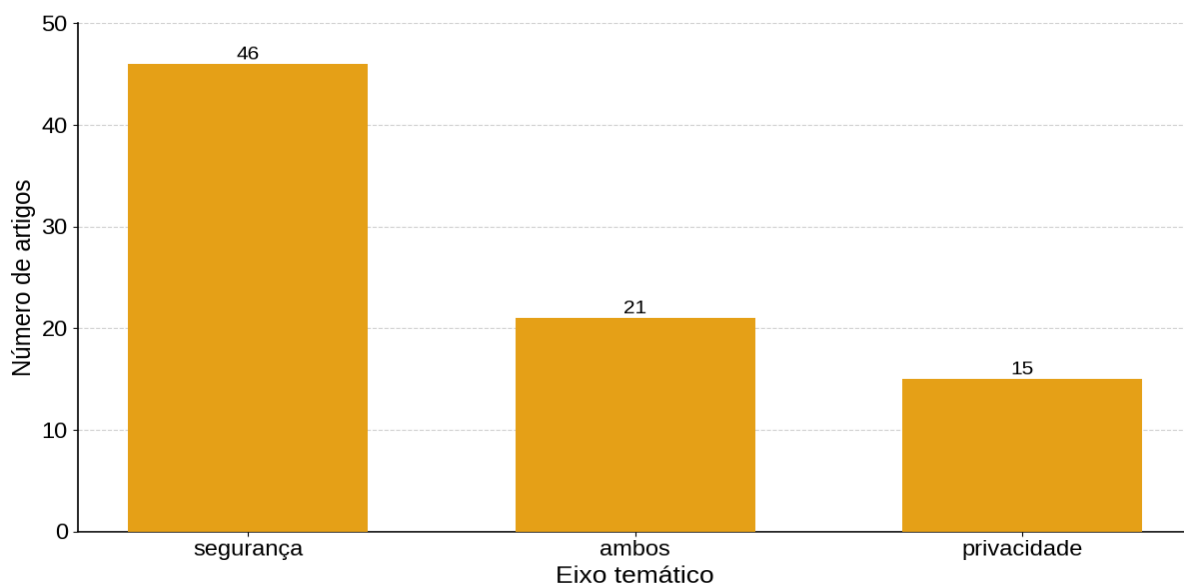
Gráfico 6 – Países mais frequentes



Fonte: Dados da pesquisa (2026).

A caracterização temática por eixo (Gráfico 7) indica predominância do enfoque em segurança da informação, acompanhada por um conjunto expressivo de estudos na interseção entre segurança e privacidade e por um contingente de trabalhos centrados em privacidade. No total, quarenta e seis estudos foram classificados no eixo segurança, vinte e um abordaram conjuntamente segurança e privacidade e quinze foram classificados no eixo privacidade. Essa distribuição confirma a centralidade da segurança como base operacional das políticas de privacidade, mas revela também o avanço de abordagens integradas entre ambos os domínios.

Gráfico 7 – Eixo temático do estudo (segurança, privacidade ou ambos)



Fonte: Dados da pesquisa (2026).

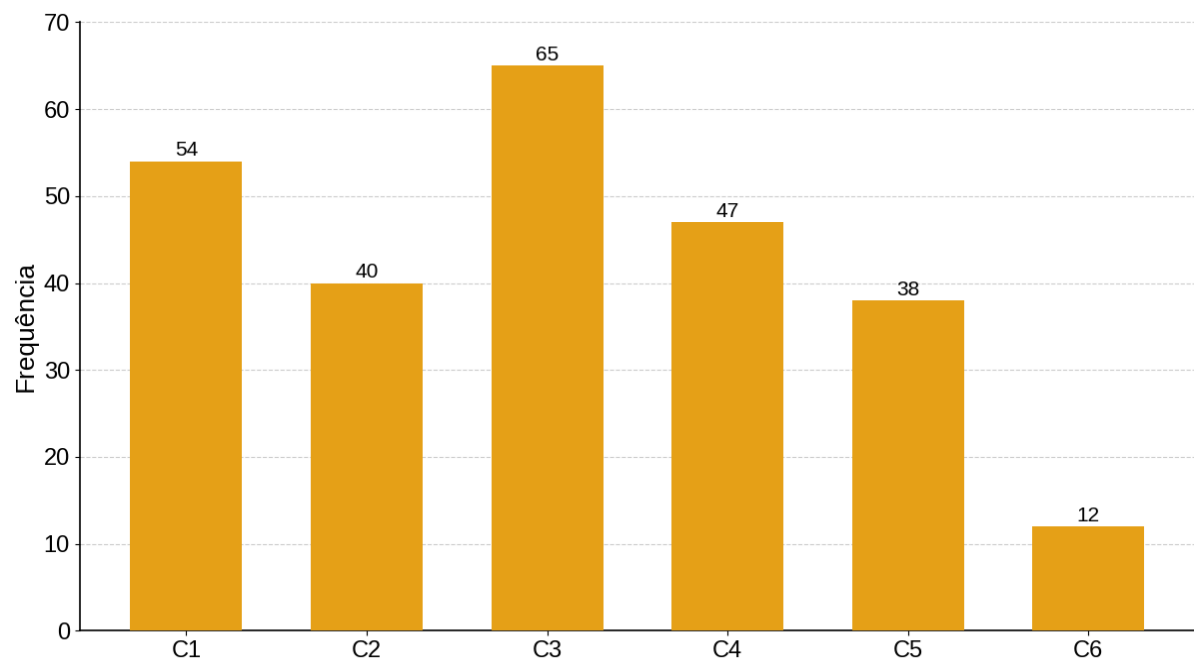
Essa configuração temática observada na literatura cria as condições para compreender como emergem e se consolidam os domínios conceituais adotados nesta pesquisa, que articulam as dimensões de capacidade e efetividade.

O corpus confirmou a presença e a frequência desses domínios: simultaneamente teóricos, derivados da literatura e das normas, e validados empiricamente pela recorrência e coocorrência nos estudos incluídos, eles constituem o elo conceitual entre a fase de revisão e a etapa empírica conduzida junto às IFES.

Na sequência, os mecanismos institucionais e organizacionais identificados na literatura foram agrupados sob o prefixo C, de *capacity*, correspondendo às condições internas necessárias à efetividade. Esses domínios refletem as diferentes dimensões de governança, processos e recursos que estruturam a implementação de políticas de segurança e privacidade.

Os domínios são (Gráfico 8): C1 – Governança; C2 – Pessoas e competências; C3 – Processos; C4 – Tecnologia e monitoramento; C5 – Gestão de dados e privacidade; C6 – Recursos.

Gráfico 8 – Frequência das capacidades



Fonte: Dados da pesquisa (2026).

A tríade formada por governança, processos e tecnologia com monitoramento configura o núcleo sociotécnico mais consistente de implementação. Em Krishna e Sebastian (2021), o compromisso estatal com a segurança do ciberespaço é associado a níveis superiores de governo eletrônico e de uso de TIC. Estratégias nacionais, coordenação interinstitucional e diretrizes de alto nível estruturam a governança (C1), que orienta prioridades e define responsabilidades. Esse mandato é traduzido em processos (C3), nos quais a gestão de riscos atua como função de mediação entre diretrizes e execução, convertendo decisões estratégicas em rotinas operacionais. Essa tradução inclui a atualização de políticas, o registro e a análise sistemática de incidentes e os ciclos de auditoria. A partir dessa base, a tecnologia e o monitoramento (C4) ganham tração com inventário de ativos, telemetria e mecanismos de detecção. Sem tradução do mandato em rotinas, o aparato técnico tende a perder estabilidade. Sem instrumentação, os processos carecem de visibilidade e controle.

No plano organizacional, Green *et al.* (2020) reconstituem a resposta de um órgão público a vulnerabilidades em sistemas de alerta. O encadeamento é explícito. Primeiro, definição de papéis e autoridade decisória, consolidando C1. Em seguida, padronização de C3 com fluxos, *playbooks* e mecanismos de reporte que produzem

repetibilidade e trilhas de evidência. Por fim, estabilização de C4 com monitoramento de serviços críticos e correlação de eventos. O caso evidencia que tecnologias isoladas tendem a gerar ganhos episódicos. Robustez decorre do acoplamento entre governança, processos e telemetria.

No âmbito municipal, Sánchez-Zurdo e San-Martín (2024) aplicam um instrumento de avaliação de risco em entidades locais e identificam associação entre governança (C1), padronização de processos (C3) e cobertura de monitoramento (C4). Normas internas, papéis definidos e coordenação aceleram a institucionalização de rotinas de gestão de riscos e de resposta a incidentes. Essa estabilização processual correlaciona-se com vigilância operacional mais consistente. Onde um dos elementos falta, surgem assimetrias previsíveis. Governança sem processos não escala. Processos sem patrocínio institucional perdem prioridade. Tecnologia sem ambos tende a operar como ilha desconectada.

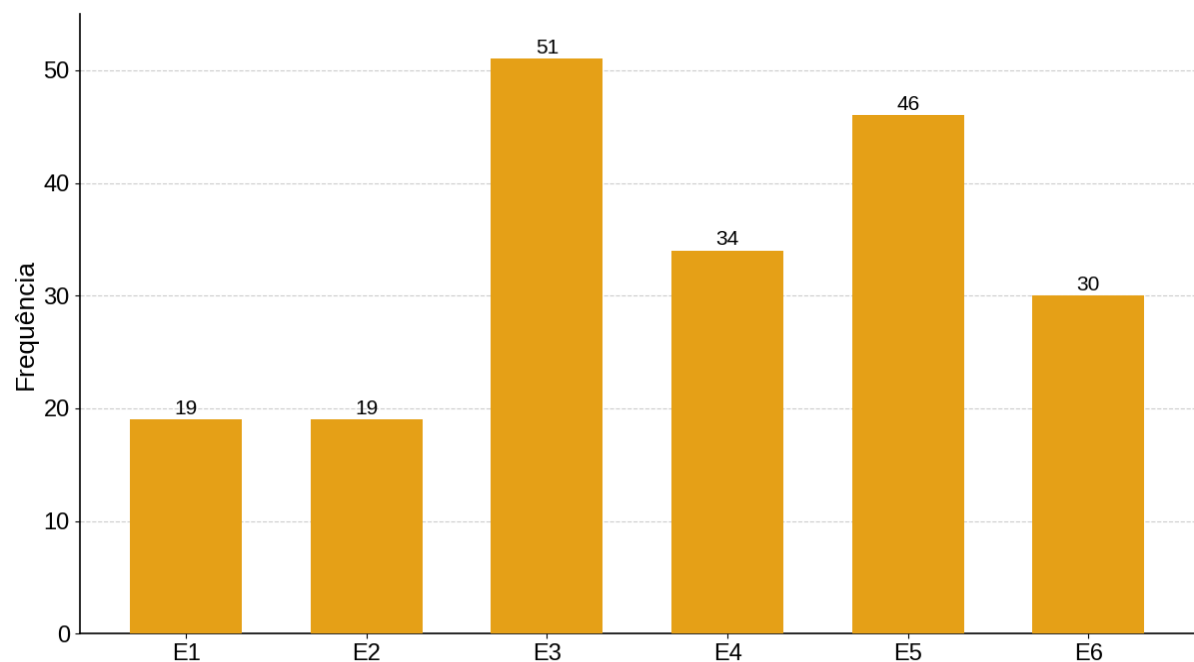
Esses achados alinham-se ao enquadramento teórico já mobilizado. A concepção de governança como “capacidade guarda-chuva” em ambientes públicos complexos formulada por Moon, Choi e Armstrong (2018) explica por que C1 organiza o terreno no qual C3 e C4 funcionam como núcleo. O detalhamento de componentes de política e fluxos organizacionais apresentado por Hossain (2024) explicita a ponte entre diretriz e rotina, condição para auditabilidade. As agendas integradas de Cheng e Wang (2022) e de Saura, Ribeiro-Soriano e Palacios-Marqués (2022) reforçam que a sequência C1–C3–C4 constitui estratégia de implementação, não apenas lógica conceitual. Evidências contemporâneas sobre incorporação de IA generativa em governo, discutidas por Choudhary e Kar (2025), tornam claro o papel de C1 e C3 para que C4 opere com propósito e métricas. Estudos sobre fatores humanos, como Evans *et al.* (2019) e Tran *et al.* (2024), indicam que pessoas e competências (C2) potencializam o núcleo, enquanto gestão de dados e privacidade (C5) agrega coerência regulatória e legitimidade. Em conjunto, consolida-se a leitura de que programas públicos que combinam C1–C3–C4, apoiados por C2 e C5, tendem a apresentar maior consistência operacional, ao passo que recursos (C6) permanecem condicionantes críticos ainda pouco explicitados empiricamente.

Os domínios de efetividade foram apurados por presença em cada estudo incluído. Antes de apresentar os gráficos seguintes, cabe esclarecer que as dimensões de resultado foram sistematizadas no *codebook* da revisão sob o prefixo

E, de *effectiveness*, representando os diferentes tipos de resultados observáveis ou impactos esperados das políticas de segurança e privacidade.

Esses domínios são (Gráfico 9): E1 – Continuidade e disponibilidade de serviços; E2 – Detecção e resposta a incidentes; E3 – Mitigação de risco; E4 – Proteção de dados e privacidade; E5 – Transparência, notificação e conformidade; E6 – Confiança e percepção pública.

Gráfico 9 – Frequência da efetividade



Fonte: Dados da pesquisa (2026).

Os resultados indicam predominância de Mitigação de Risco (E3, n=51), seguida de Transparência/Conformidade (E5, n=46) e Proteção de Dados/Privacidade (E4, n=34). Confiança/Percepção (E6) apresenta 30 ocorrências, enquanto Continuidade/Disponibilidade (E1) e Detecção/Resposta a Incidentes (E2) registram 19 ocorrências cada. O perfil sugere orientação a resultados que combinam gestão de risco operacional com legitimidade institucional ancorada em conformidade e direitos de titulares, além de efeitos percebidos em confiança em parte dos estudos.

A análise de coocorrências evidencia clusters de resultados que tendem a aparecer juntos. Destacam-se E3↔E5 como par mais recorrente (28 estudos), seguido por E3↔E4 (20), E4↔E5 (19), E2↔E3 (18) e E1↔E3 (17). Esses agrupamentos descrevem trajetórias típicas de implementação:

E3↔E5 indica que práticas de mitigação de risco se consolidam quando há capacidade de demonstrar conformidade e prestação de contas, seja por auditorias, trilhas de evidência ou métricas reportáveis. Exemplos incluem estudos que combinam gestão de risco com mecanismos de *accountability* regulatória e organizacional (encontrado nos artigos de *id*: R00444; R00469; R00483; R00489; R00506; R00510; R00515; R00606; R00712; R00981).

E3↔E4 aparece quando mitigação de risco é tratada junto a controles de privacidade e proteção de dados, frequentemente sob o guarda-chuva de políticas de dados e avaliações de impacto (R00001; R00009; R00015; R00019; R00046; R00209; R00214; R00262; R00365; R00380; R00404; R00447; R00469; R00489; R00506; R00510; R00520; R00547; R00606; R00637).

E2↔E3 traduz arranjos onde detecção e resposta se articulam à mitigação de risco em ciclos de melhoria contínua, com ênfase em processos e monitoramento (R00001; R00009; R00016; R00049; R00056; R00062; R00136; R00256; R00294; R00379; R00382; R00404; R00483; R00510; R00515; R00547; R00550; R00582).

E4↔E5 descreve cenários de conformidade orientada a privacidade, nos quais registros, notificações e auditorias acompanham salvaguardas de dados, coerentes com exigências regulatórias (R00001; R00009; R00015; R00095; R00214; R00229; R00365; R00370; R00380; R00404; R00439; R00456; R00469; R00489; R00506; R00510; R00539; R00606; R01023).

E1↔E3 surge quando continuidade e resiliência são tratadas como efeitos esperados da mitigação de risco, notadamente em estudos que incorporam gestão de continuidade, backup e restauração testada (R00001; R00009; R00016; R00049; R00056; R00059; R00062; R00077; R00136; R00294; R00379; R00382; R00423; R00483; R00489; R00510; R00550).

Esse desenho empírico é consistente com a literatura recente em administração pública digital. Resultados de mitigação de risco e conformidade/legitimidade tendem a se reforçar mutuamente, o que se alinha a evidências de que risco percebido, confiança e privacidade são vetores decisivos de adoção e de desempenho de políticas de governo digital (Gupta *et al.*, 2025; Mutimukwe; Kolkowska; Grönlund, 2019, 2020; AlAbdali *et al.*, 2021). No plano regulatório, a proteção de dados permanece estruturante. A literatura que discute o papel de marcos regulatórios robustos, incluindo a inspiração do GDPR em diferentes jurisdições, associa controles de privacidade e mecanismos de prestação de contas a

ganhos de conformidade e a reduções observáveis de risco organizacional, o que explica a frequência de $E4 \leftrightarrow E5$ e seu acoplamento com $E3$ (Agashe; Ghose, 2024; Gumzej, 2023). Em estudos de desenho organizacional e governança de SI, observa-se que capacidade de detecção e resposta ($E2$) tende a emergir integrada a rotinas de gestão de risco e monitoramento, reforçando a coocorrência $E2 \leftrightarrow E3$ quando há processos institucionalizados e telemetria adequada, como nos exemplos acima. Por fim, a presença de $E1$ em parte dos estudos sinaliza o vínculo entre mecanismos de continuidade e efeitos mensuráveis de resiliência, especialmente quando testados por exercícios de restauração ou por métricas de disponibilidade.

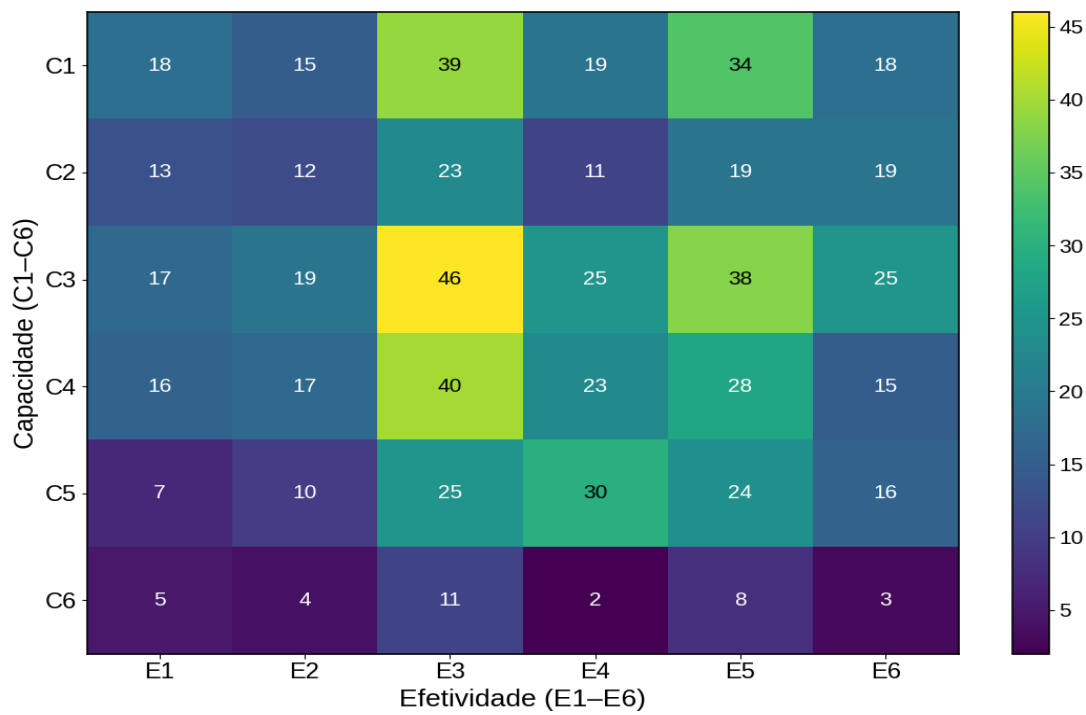
Em síntese, as frequências e coocorrências dentro da própria dimensão apontam um padrão de efetividade composto. $E3$ funciona como eixo organizador ao qual se articulam $E5$ e $E4$, compondo um bloco de gestão de risco, conformidade e privacidade. $E2$ tende a aderir a esse bloco quando há maturidade processual e de monitoramento. $E1$ aparece como consequência operacional desejada desse arranjo, enquanto $E6$ sinaliza a dimensão perceptiva de legitimidade e confiança que acompanha, mas não substitui, os resultados substantivos. Esse padrão dialoga com a arquitetura de capacidades discutida na seção anterior, em especial com a tríade $C1-C3-C4$, que fornece as condições institucionais e operacionais para que os efeitos de efetividade apareçam em conjunto e sejam passíveis de demonstração empírica.

A matriz de coocorrência entre capacidade e efetividade (Gráfico 10) sintetiza os padrões de associação observados nos estudos incluídos. Essa matriz orienta diretamente a priorização de mecanismos institucionais no PPSI, ao situar quais capacidades se combinam mais frequentemente com cada resultado esperado.

A célula mais densa é $C3 \times E3$. Onde há padronização de processos, gestão de vulnerabilidades, gestão de mudanças, backup e restauração testados, registro e revisão sistemática, observam-se quedas de exposição e de riscos críticos. Essa lógica é explicitada em investigações que relacionam “efetividade de segurança” à incidência de ameaças, nas quais a estabilização de rotinas aparece como denominador comum da redução de eventos adversos (Masrek *et al.*, 2020). O mapa também mostra $C4 \times E3$ com intensidade elevada. Inventário completo de ativos, *logging* consistente e sensores analíticos operados de forma regular tendem a encurtar MTTD (*Mean Time To Detect*) e MTTR (*Mean Time To Repair*), o que se converte em redução de risco residual. Avaliações técnico-diagnósticas de serviços públicos on-line reforçam esse resultado ao evidenciar que portais com

monitoramento mais maduro apresentam menor superfície de exposição (Ribeiro *et al.*, 2025).

Gráfico 10 – Matriz de coocorrência (capacidade x efetividade)



Fonte: Dados da pesquisa (2026).

A interseção C3xE5 destaca como processos funcionam como ponte entre norma e prestação de contas. Quando fluxos de notificação, trilhas de evidência e auditorias são institucionalizados, a conformidade torna-se demonstrável e tempestiva. Estudos sobre cultura organizacional e *compliance* mostram que práticas e rotinas internalizadas elevam a adesão às políticas e se refletem em indicadores de conformidade, o que dá materialidade a E5 por meio da combinação C2,C3→E5 (Karlsson *et al.*, 2022). Na dimensão institucional, a matriz exhibe C1xE5 como um eixo de alta coocorrência. Análises da atuação de autoridades de proteção de dados evidenciam que arranjos de governança com poderes sancionatórios, prazos definidos e decisões publicizadas reforçam transparência e *accountability*, produzindo resultados típicos de E5 quando a governança é efetivamente exercida (Gumzej, 2023).

O bloco formado por C1 e C5 tende a aparecer associado a E4 e E5. Em contextos de governança de dados, a ancoragem institucional de mapeamento de operações de tratamento, avaliação de impacto, controle de acesso e revisão de

bases legais é decisiva para reduzir violações envolvendo dados pessoais e, ao mesmo tempo, para produzir registros que sustentam a prestação de contas. A combinação $C1, C5 \rightarrow E4, E5$ sintetiza esse mecanismo ao mostrar que proteção de dados e transparência caminham juntas quando a governança organiza o ciclo de dados como processo verificável e não apenas como diretriz abstrata (Agashe; Ghose, 2024). Em paralelo, o caminho $C2-C4 \rightarrow E2$ aparece nos estudos que conectam competências e treinamento a uma instrumentação de monitoramento efetiva. A presença de equipe habilitada, aliada a telemetria operante e a planos de resposta utilizáveis, eleva a capacidade de detecção e contenção e pode repercutir em salvaguardas de privacidade quando os controles técnicos impactam diretamente os vetores de exfiltração e vazamento, aproximando $E2$ de $E4$ em determinados arranjos decisórios e de investimento (Paul; Zhang, 2021).

Em conjunto, a matriz e o quadro-síntese descrevem um desenho coerente com o restante da revisão. Processos e tecnologia/monitoramento funcionam como motores técnico-operacionais da mitigação de risco. Governança estabelece o mandato e a responsabilização que sustentam conformidade. Gestão de dados traduz privacidade em rotinas auditáveis. Pessoas e competências dão tração a detecção e resposta e fortalecem a adesão às políticas. É nessas cadeias: $C3 \times E3$, $C4 \times E3$, $C3 \times E5$, $C1 \times E3$, $C1 \times E5$, e nos exemplos articulados $C1, C5 \rightarrow E4, E5$, $C2-C4 \rightarrow E2$ e $C2, C3 \rightarrow E5$, que a coocorrência concentra as maiores intensidades, oferecendo orientação direta para a priorização de mecanismos institucionais no PPSI e um roteiro verificável para a obtenção de resultados de efetividade.

A análise situacional delinea um estado da arte que integra conformidade regulatória e governança de dados a uma perspectiva orientada a resultados. Os estudos convergem para a necessidade de mecanismos de governança que alinhem papéis e decisões, de processos padronizados e monitoramento contínuo, e de competências organizacionais que sustentem detecção, resposta e continuidade. A partir desse mapeamento, a etapa subsequente do estudo emprega o instrumento primário para mensurar, nas IFES, a efetividade percebida e sua associação com a maturidade do PPSI e com variáveis contextuais, avançando da síntese secundária para a inferência empírica no campo.

A partir da coocorrência entre os domínios de capacidade e efetividade, derivou-se a matriz de indicadores que fundamenta o instrumento primário de pesquisa. O questionário operacionaliza os constructos identificados na revisão

sistemática em variáveis mensuráveis, adaptadas ao contexto das Instituições Federais de Ensino Superior (IFES) e alinhadas aos eixos do Programa de Privacidade e Segurança da Informação (PPSI). A correspondência entre domínios teóricos e itens do instrumento é apresentada no Quadro 5, preservando a coerência conceitual entre os eixos analíticos e as dimensões empíricas. Para captar nuances complementares dentro de um mesmo domínio, alguns indicadores foram desdobrados em dois itens, resultando em dezoito variáveis principais e dois itens contextuais, T1 (porte institucional, nas faixas de servidores, estudantes e equipe de TI) e T2 (condição multicampi e região da sede), voltados à caracterização institucional das respostas.

No caso das capacidades (C1–C8), optou-se por representar cada domínio com um único item sintético, dada a natureza estrutural e relativamente estável desses constructos. Diferentemente dos domínios de efetividade, que descrevem resultados observáveis e demandam desdobramento para captar variações de desempenho, as capacidades referem-se a funções institucionais cujos componentes já se encontram delineados nas normas e *frameworks* de referência. A inclusão de C6 e C7 ampliou a granularidade conceitual sem comprometer a parcimônia do instrumento.

Quadro 5 – Estrutura do instrumento de pesquisa derivada dos domínios teóricos

Domínio	Código e item do instrumento	Descrição resumida
Efetividade: Continuidade e Disponibilidade	E1. <i>Serviços digitais essenciais apresentaram menor indisponibilidade nos últimos 12 meses.</i> E2. <i>Planos de continuidade foram testados com melhor desempenho.</i>	Mede a continuidade operacional e a capacidade de resposta preventiva.
Efetividade: Detecção e Resposta a Incidentes	E3. <i>O tempo de detecção de incidentes de segurança diminuiu.</i> E4. <i>O tempo de contenção/recuperação após incidentes diminuiu.</i>	Avalia a prontidão e a eficiência das ações corretivas.
Efetividade: Mitigação de Risco	E5. <i>Riscos críticos de TI/Segurança foram mitigados após planos de tratamento.</i>	Mede a efetividade das ações de mitigação de riscos relevantes.
Efetividade: Proteção de Dados e Privacidade	E6. <i>Incidentes envolvendo dados pessoais tornaram-se menos frequentes/graves.</i>	Avalia o grau de segurança e conformidade no tratamento de dados pessoais.
Efetividade: Transparência e Conformidade	E7. <i>Processos de notificação (titulares/ANPD) estão maduros e tempestivos.</i> E8. <i>Auditorias e monitoramentos indicam conformidade crescente em privacidade.</i>	Representa o cumprimento das exigências legais e a transparência institucional.

Efetividade: Confiança e Percepção	E9. A confiança das áreas-fim na segurança/privacidade aumentou. E10. A alta administração percebe ganhos concretos decorrentes do PPSI.	Reflete a legitimidade e a percepção institucional de seus resultados.
Capacidade: Governança	C1. Papéis e governança do PPSI estão definidos e atuantes.	Estrutura e integração decisória.
Capacidade: Pessoas e Competências	C2. Existe equipe e competências mínimas dedicadas ao PPSI/privacidade.	Capacidade técnica e de pessoal.
Capacidade: Processos	C3. Processos de gestão de vulnerabilidades e de backup/restauração são executados e testados.	Procedimentos estruturados e testados regularmente.
Capacidade: Tecnologia e Monitoramento	C4. Inventário de ativos e as ferramentas de monitoramento (como logging, EDR ou SIEM) são adequados à complexidade e aos riscos da instituição.	Nível tecnológico e abrangência de monitoramento.
Capacidade: Gestão de Dados e Privacidade	C5. Gestão de dados/privacidade (mapeamento, bases legais, RIPD) está operante.	Maturidade na aplicação dos instrumentos da LGPD.
Capacidade: Gestão de Riscos	C6. Gestão de riscos está integrada ao planejamento e orçamento.	Integração de riscos à governança institucional.
Capacidade: Treinamento e Conscientização	C7. Treinamentos e conscientização atingem públicos críticos (TI e áreas-fim).	Disseminação da cultura de segurança e privacidade.
Capacidade: Recursos Institucionais	C8. Recursos orçamentários/contratuais permitem executar o PPSI.	Sustentação orçamentária e contratual.
Contexto: Porte Institucional	T1. Porte da IFES: faixas de estudantes, de servidores e da equipe de TI (três campos).	Controla heterogeneidade estrutural entre instituições.
Contexto: Estrutura e Localização	T2. A IFES é multicampi? (Sim/Não) e região da sede.	Caracteriza o ambiente e a dispersão geográfica institucional.

Fonte: Elaboração própria (2026), derivada do Quadro 3 e da RSL.

4.2 VALIDAÇÃO DE CONTEÚDO DO INSTRUMENTO POR ESPECIALISTAS

Após a derivação do instrumento a partir da Revisão Sistemática da Literatura e da consolidação dos domínios teóricos apresentados no Quadro 5, procedeu-se à validação de conteúdo por especialistas. Essa etapa teve por finalidade verificar a aderência entre domínio teórico, descrição resumida e item do instrumento, conforme a lógica explicitada no formulário de validação, no qual os participantes foram orientados a julgar se cada item era essencial para representar o domínio ao qual havia sido associado, considerando aderência conceitual, clareza da redação e adequação como medida do constructo.

A validação foi realizada de forma remota e assíncrona, por meio de formulário eletrônico, com especialistas atuantes no contexto da Secretaria de Governo Digital, todos com experiência em segurança da informação, privacidade, proteção de dados e apoio à implementação do PPSI. A versão submetida ao painel correspondeu à redação revisada do instrumento, distinta da formulação preliminar originalmente

registrada no Quadro 5, e já refletiu os ajustes semânticos realizados antes da rodada de validação.

Conforme previsto na metodologia, cada especialista avaliou individualmente a essencialidade de cada item em escala de três pontos: não essencial, útil, mas não essencial, e essencial, permitindo o cálculo do Content Validity Ratio (CVR) proposto por Lawshe (1975). Embora o protocolo inicial previsse um painel com 10 especialistas, a etapa contou com 11 respondentes válidos. Em razão desse quantitativo, adotou-se como critério operacional de retenção a exigência mínima de 9 julgamentos “essencial”, o que corresponde a $CVR = 0,636$. Os itens abaixo desse valor foram classificados para revisão e nova rodada com o mesmo painel, preservando o procedimento já previsto no delineamento metodológico.

Os resultados indicaram retenção de 13 dos 18 itens avaliados na primeira rodada, correspondendo a 72,2% do instrumento submetido ao painel. No bloco de capacidades institucionais, todos os oito itens atingiram o critério de retenção, com CVRs entre 0,818 e 1,000. No bloco de efetividade, cinco dos dez itens atingiram o limiar estabelecido. Os itens que não alcançaram o critério mínimo concentraram-se nos domínios de continuidade e disponibilidade, transparência e conformidade, e confiança e percepção, sinalizando necessidade de refinamento adicional da redação ou de melhor ajuste entre item e domínio.

Entre os itens de efetividade, o menor consenso ocorreu em E9, referente ao aumento da confiança das áreas-fim na segurança da informação e na privacidade, com seis julgamentos de essencialidade e cinco classificações como útil, mas não essencial, resultando em $CVR = 0,091$. Em seguida, os itens E1 e E7 apresentaram $CVR = 0,273$, enquanto E2 e E10 obtiveram $CVR = 0,455$. Esses resultados não indicaram inadequação absoluta dos itens, mas sugeriram necessidade de refinamento adicional de redação e de maior aderência entre domínio, descrição resumida e item.

Os resultados da primeira rodada estão sintetizados a seguir (Quadro 6).

Quadro 6 – Síntese da primeira rodada de validação de conteúdo por especialistas

Código	Item submetido ao painel	Essencial	Útil, mas não essencial	Não essencial	CVR	Situação
C1	Papéis, responsabilidades e instâncias de governança do PPSI estão formalizados e em funcionamento.	11	0	0	1,000	Retido

C2	A instituição dispõe de equipe e competências adequadas para conduzir ações de segurança da informação e privacidade.	11	0	0	1,000	Retido
C3	Processos de segurança da informação e privacidade, incluindo gestão de vulnerabilidades e backup/restauração, são executados e testados regularmente.	10	1	0	0,818	Retido
C4	A instituição dispõe de recursos tecnológicos compatíveis com sua complexidade e perfil de risco para manter visibilidade sobre seus ativos e apoiar o monitoramento, a detecção e a resposta a eventos de segurança.	11	0	0	1,000	Retido
C5	A gestão de dados pessoais e privacidade, incluindo mapeamento de tratamentos, bases legais e RIPD, está implementada e em funcionamento.	11	0	0	1,000	Retido
C6	A gestão de riscos de segurança da informação e privacidade está integrada ao planejamento e ao orçamento institucional.	11	0	0	1,000	Retido
C7	A instituição promove ações de treinamento e conscientização em segurança da informação e privacidade com alcance entre diferentes públicos institucionais.	10	1	0	0,818	Retido
C8	A instituição dispõe de recursos orçamentários e contratuais suficientes para sustentar ações de segurança da informação e privacidade previstas no PPSI.	11	0	0	1,000	Retido
E1	Nos últimos 12 meses, os serviços digitais essenciais apresentaram menor indisponibilidade.	7	4	0	0,273	Revisão e nova rodada
E2	Nos últimos 12 meses, a instituição demonstrou maior capacidade de manter e recuperar serviços críticos diante de interrupções.	8	3	0	0,455	Revisão e nova rodada
E3	Nos últimos 12 meses, a instituição tornou-se mais ágil na detecção de incidentes de segurança.	10	1	0	0,818	Retido
E4	Nos últimos 12 meses, a instituição tornou-se mais ágil na contenção e recuperação após incidentes de segurança.	10	1	0	0,818	Retido
E5	Nos últimos 12 meses, a exposição da instituição a riscos críticos de segurança da informação e privacidade diminuiu.	9	2	0	0,636	Retido
E6	Nos últimos 12 meses, incidentes envolvendo dados pessoais tornaram-se menos frequentes ou menos graves.	9	2	0	0,636	Retido

E7	Nos últimos 12 meses, quando aplicáveis, as notificações a titulares e à ANPD ocorreram de forma tempestiva e com registros completos.	7	3	1	0,273	Revisão e nova rodada
E8	Nos últimos 12 meses, auditorias e monitoramentos indicaram avanço na conformidade em segurança da informação e privacidade, inclusive quanto às exigências da LGPD.	10	1	0	0,818	Retido
E9	Nos últimos 12 meses, a confiança das áreas-fim na segurança da informação e na privacidade aumentou.	6	5	0	0,091	Revisão e nova rodada
E10	Nos últimos 12 meses, a alta administração passou a perceber ganhos institucionais associados ao PPSI.	8	3	0	0,455	Revisão e nova rodada

Fonte: Elaboração própria com base nas rodadas de validação de conteúdo com especialistas.

Com base nas observações qualitativas do painel, os cinco itens abaixo do limiar foram submetidos a uma etapa intermediária de refinamento semântico e conceitual. Para isso, foram convidados quatro especialistas que, na primeira rodada, não haviam classificado como essencial pelo menos um dos itens que ficaram abaixo do critério mínimo de retenção. A reunião foi realizada por videoconferência e gravada para fins de registro metodológico, tendo como objetivo discutir os pontos de ambiguidade, aderência ao domínio teórico e precisão redacional das formulações originalmente submetidas.

A partir dessa discussão, os itens E1, E2, E7, E9 e E10 foram reformulados e submetidos a uma segunda rodada de validação, de caráter complementar, voltada à confirmação da aderência conceitual das novas redações. Essa etapa não teve por objetivo reconstituir integralmente o painel inicial, mas verificar se os ajustes promovidos elevavam o grau de convergência entre os especialistas disponíveis para reapreciação dos itens revisados.

Na segunda rodada, obteve-se retorno válido de 6 especialistas. Considerando-se a natureza confirmatória dessa etapa e a manutenção do critério operacional de retenção adotado no estudo, os itens que alcançaram pelo menos 5 julgamentos como “essencial” foram considerados satisfatórios para permanência no instrumento. Nessa configuração, o CVR correspondente é de 0,667, valor superior ao limiar operacional adotado para esta etapa complementar. Na reapreciação, o item E9 foi julgado essencial pelos seis avaliadores (CVR = 1,000), e os itens E1, E2, E7 e E10 receberam, cada um, cinco julgamentos de essencialidade e um de utilidade (CVR =

0,667), de modo que todos os itens revisados atingiram o critério de retenção estabelecido. Optou-se por não realizar rodadas adicionais, tendo em vista a convergência qualitativa observada na reunião com especialistas, o resultado obtido na reapreciação dos itens revisados, a suficiência analítica do refinamento promovido e a necessidade de preservar a viabilidade empírica da pesquisa.

Assim, a reunião de refinamento e a segunda rodada foram tratadas como etapas complementares de consolidação final dos itens originalmente problemáticos, e não como procedimento autônomo de revalidação integral do instrumento. Essa decisão implica limitação metodológica, uma vez que a confirmação dos itens revisados ocorreu com subconjunto do painel inicial. Ainda assim, entende-se que o instrumento alcançou grau satisfatório de consistência conceitual e clareza semântica para aplicação na coleta principal, especialmente porque os itens reapresentados já haviam sido previamente examinados pelo painel completo e foram reformulados a partir das críticas recebidas e da discussão dirigida com especialistas que haviam indicado menor essencialidade na primeira rodada.

O Quadro 7 apresenta a consolidação das alterações promovidas nos itens que não atingiram o limiar mínimo de retenção na primeira rodada, após refinamento orientado pelas observações qualitativas dos especialistas e reapreciação na rodada complementar.

Quadro 7 – Itens revisados após a rodada complementar com especialistas

Item	Redação da 1ª rodada	Redação final aplicada (2ª rodada)
E1	Nos últimos 12 meses, os serviços digitais essenciais apresentaram menor indisponibilidade.	Após o início da implementação do PPSI, as interrupções em serviços digitais essenciais tiveram menor frequência.
E2	Nos últimos 12 meses, a instituição demonstrou maior capacidade de manter e recuperar serviços críticos diante de interrupções.	Após o início da implementação do PPSI, serviços críticos passaram a ser restabelecidos com maior rapidez após interrupções.
E7	Nos últimos 12 meses, quando aplicáveis, as notificações a titulares e à ANPD ocorreram de forma tempestiva e com registros completos.	Após o início da implementação do PPSI, quando aplicáveis, as notificações de incidentes a titulares e à ANPD ocorreram de forma tempestiva e adequadamente documentada.
E9	Nos últimos 12 meses, a confiança das áreas-fim na segurança da informação e na privacidade aumentou.	Nos últimos 12 meses, cresceu, entre as áreas-fim, a percepção de que a instituição protege informações e dados pessoais.
E10	Nos últimos 12 meses, a alta administração passou a perceber ganhos institucionais associados ao PPSI.	Nos últimos 12 meses, a alta administração reconheceu ganhos institucionais associados ao PPSI.

Fonte: Elaboração própria com base nas rodadas de validação de conteúdo com especialistas.

Após a validação de conteúdo e a rodada complementar de refinamento, a versão final do instrumento foi consolidada e aplicada aos respondentes das IFES. O questionário completo, incluindo TCLE, blocos de qualificação, variáveis institucionais, itens de capacidades, itens de efetividade e campo aberto complementar, encontra-se disponível no Apêndice A.

5 RESULTADOS DA PESQUISA EMPÍRICA COM AS IFES

Esta seção apresenta os resultados da etapa empírica da pesquisa, desenvolvida a partir da aplicação do instrumento junto a atores institucionais vinculados ao Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior (IFES). Enquanto a seção anterior consolidou a revisão sistemática da literatura, a validação de conteúdo do instrumento e a estrutura conceitual dos domínios de capacidade e efetividade, esta etapa examina os dados primários coletados no campo.

A análise parte da premissa metodológica de que a efetividade do PPSI não pode ser inferida apenas pela existência formal de controles ou pelo nível de maturidade aferido nos indicadores do programa. Nesta pesquisa, a efetividade é tratada como resultado percebido da implementação, observável a partir de dimensões como continuidade dos serviços digitais, detecção e resposta a incidentes, mitigação de riscos, proteção de dados pessoais, conformidade, notificação, confiança institucional e reconhecimento pela alta administração. As capacidades institucionais, por sua vez, são compreendidas como condições organizacionais que podem sustentar ou limitar esses resultados, abrangendo governança, pessoas, processos, tecnologia, gestão de dados, gestão de riscos, treinamento e recursos.

A apresentação segue sequência progressiva: preparação da base e composição da amostra; caracterização dos respondentes e das instituições; estatística descritiva dos blocos de capacidades institucionais e de efetividade percebida; e, por fim, associações entre capacidades, efetividade e indicadores de maturidade do PPSI, por meio de correlações e modelos exploratórios de regressão, interpretados como relações associativas.

Dessa forma, a seção busca responder empiricamente à questão central da dissertação: como a implementação do PPSI nas IFES se traduz em efetividade, em termos de desempenho organizacional e valor público, examinando padrões, associações e contrastes que permitam compreender como capacidades institucionais, contexto organizacional e indicadores de implementação se relacionam com a efetividade percebida do programa.

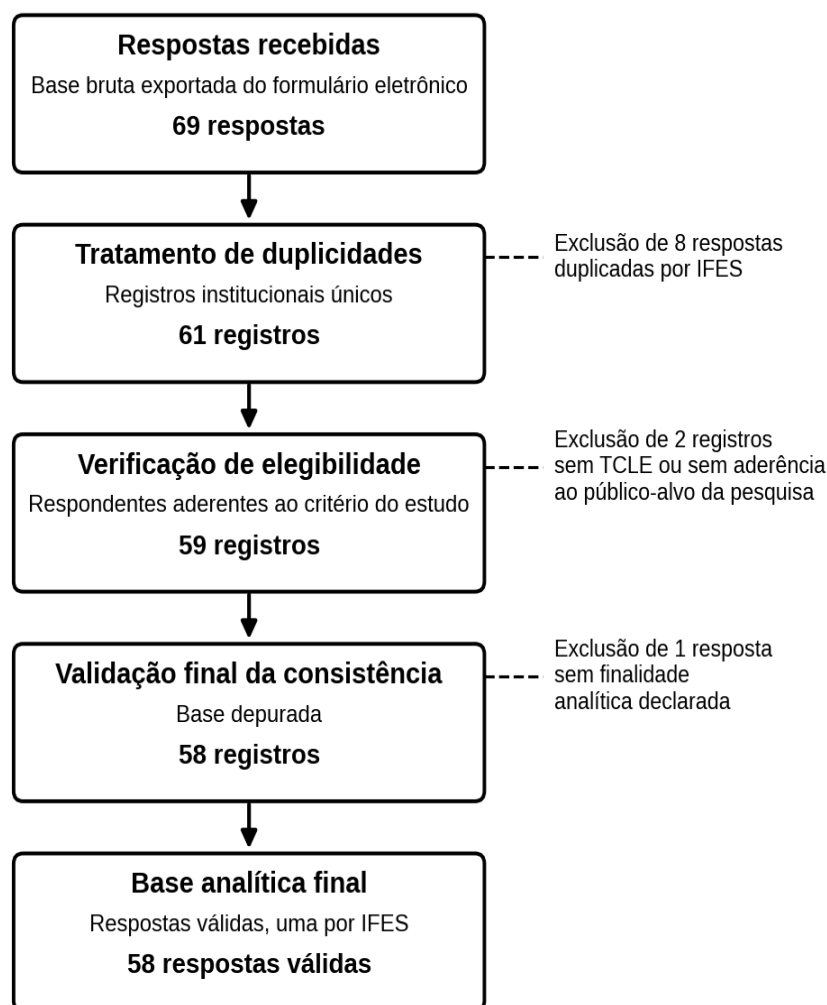
5.1 PREPARAÇÃO DA BASE E COMPOSIÇÃO DA AMOSTRA

A base empírica da pesquisa foi constituída a partir das respostas ao questionário aplicado de forma digital junto às Instituições Federais de Ensino Superior. A unidade de análise adotada foi a IFES, e não o respondente individual, uma vez que o objetivo da pesquisa consiste em avaliar capacidades institucionais e resultados percebidos do Programa de Privacidade e Segurança da Informação (PPSI) no nível organizacional. Por esse motivo, antes da análise estatística, a base bruta foi submetida a procedimentos de consistência, eliminação de duplicidades e verificação de elegibilidade dos respondentes.

Ao final da coleta, foram registradas 69 respostas brutas. A primeira etapa de tratamento consistiu na identificação de respostas duplicadas por instituição. Como a pesquisa trabalha com uma única observação por IFES, foram removidas 8 respostas duplicadas, preservando-se, em cada caso, a resposta considerada mais aderente ao critério de qualificação do estudo. Após essa etapa, permaneceram 61 registros institucionais únicos.

Em seguida, foram aplicados os critérios de elegibilidade do respondente. O instrumento foi direcionado preferencialmente ao principal responsável institucional pelo acompanhamento ou preenchimento do PPSI. Na ausência desse perfil, admitiu-se a participação de ator diretamente envolvido com o programa. Nessa etapa, foram excluídos 2 registros: um de participante que não aceitou o Termo de Consentimento Livre e Esclarecido (TCLE), condição exigida pelo protocolo aprovado pelo CEP/UFFS, e um de respondente que declarou não atuar diretamente no PPSI, sem aderência ao público-alvo da pesquisa. Também foi excluída uma resposta cujo próprio preenchimento indicou ausência de finalidade analítica, preservando-se a consistência da base principal. Após esses procedimentos, a base analítica final ficou composta por 58 respostas válidas, cada uma correspondente a uma IFES (Figura 5).

Figura 5 – Fluxo de composição da base analítica



Fonte: Elaboração própria com base nos dados da pesquisa.

Nos casos de duplicidade institucional, adotou-se a regra de prevalência definida na seção 3.4.3, orientada pela proximidade do respondente com o objeto da pesquisa; o Quadro 8 sintetiza o conjunto de critérios de composição da base analítica.

Quadro 8 – Critérios de composição da base analítica

Dimensão de tratamento	Critério adotado	Justificativa metodológica
Unidade de análise	IFES	A pesquisa avalia capacidades institucionais e efetividade percebida no nível organizacional, e não percepções individuais isoladas.
Consentimento	Manutenção apenas de respostas com aceite ao TCLE	Assegura aderência aos procedimentos éticos aprovados para a pesquisa.
Duplicidades	Manutenção de uma única resposta por IFES	Evita que uma mesma instituição tenha peso superior na análise.

Perfil prioritário	Principal responsável institucional pelo acompanhamento ou preenchimento do PPSI	Preserva a resposta com maior aderência ao conhecimento requerido pelo instrumento.
Perfil alternativo admitido	Ator diretamente envolvido com o PPSI, ainda que não seja o principal responsável	Permite incluir respostas qualificadas quando não há responsável único identificado ou quando outro ator possui atuação direta no programa.
Perfil excluído	Respondente sem atuação direta no PPSI	Reduz erro de mensuração em itens que exigem conhecimento sobre capacidades, processos, recursos e resultados do programa.
Regra de prevalência em duplicidades	Prioridade ao principal responsável; em seguida, ao respondente com atuação direta; persistindo duplicidade, ao perfil mais aderente ao PPSI	Garante critério uniforme para seleção da resposta institucional mantida na base.
Resposta inconsistente	Exclusão de registro cujo próprio preenchimento indicou ausência de finalidade analítica	Preserva a consistência e a validade da base empírica.
Base final	58 respostas válidas, uma por IFES	Constitui o conjunto analítico utilizado para as estatísticas descritivas e análises associativas.

Fonte: Elaboração própria com base nos dados da pesquisa.

Os itens de capacidades e efetividade foram mensurados em escala Likert de sete pontos, variando de 1, “discordo totalmente”, a 7, “concordo totalmente”. Para cada bloco, foram calculados escores agregados pela média dos itens válidos, preservando-se a escala original do instrumento. Essa decisão buscou manter a interpretação dos resultados diretamente vinculada à métrica utilizada pelos respondentes, evitando transformações adicionais de escala. Os indicadores iBase, iSeg e iPriv, por sua vez, foram informados pelos respondentes em escala de 0 a 1 e mantidos em sua métrica original. Valores ausentes ou informados fora desse intervalo foram desconsiderados nas análises envolvendo os respectivos índices, preservando-se os demais campos válidos da resposta.

Na preparação da base analítica, a identificação nominal das instituições foi removida e substituída apenas pela região geográfica correspondente. Essa anonimização buscou reduzir riscos de reidentificação e assegurar que os resultados fossem apresentados apenas de forma agregada. Os valores individualizados de iBase, iSeg e iPriv não são apresentados no texto, em quadros, tabelas ou apêndices, tendo sido utilizados apenas para correlações e regressões exploratórias em nível agregado.

Dessa forma, a preparação da base seguiu três princípios: unicidade da resposta por IFES, aderência do respondente ao PPSI e consistência analítica dos

registros. Esses procedimentos permitem que os resultados apresentados nas seções seguintes sejam interpretados como evidências agregadas sobre a percepção qualificada de atores institucionais envolvidos com a implementação do PPSI nas IFES.

5.2 PERFIL DOS RESPONDENTES E DAS INSTITUIÇÕES PARTICIPANTES

A caracterização da amostra foi realizada a partir das variáveis de qualificação do respondente e das variáveis institucionais incluídas no instrumento. Essas questões tiveram a finalidade de verificar a aderência do participante ao público-alvo da pesquisa, identificar o tipo de vínculo com o PPSI e descrever o contexto organizacional das IFES participantes. Conforme previsto no questionário, a pesquisa foi direcionada preferencialmente ao principal responsável institucional pelo acompanhamento ou preenchimento do PPSI ou, alternativamente, a ator diretamente envolvido com o programa.

A base analítica final foi composta por 58 respostas válidas, correspondentes a 58 IFES. Considerando o universo de referência de 110 instituições, composto por 69 universidades federais e 41 institutos federais ou instituições equiparadas (Andifes, 2025; Brasil, 2019), a amostra corresponde a 52,7% do universo total. Entre as universidades federais, foram obtidas 37 respostas, o que representa 53,6% desse grupo. Entre os institutos federais e instituições equiparadas, foram obtidas 21 respostas, correspondentes a 51,2% do respectivo grupo. Esse equilíbrio indica que a composição da amostra preserva proporção semelhante entre os dois principais segmentos institucionais analisados (Tabela 1).

Tabela 1 – Composição da amostra por tipo de IFES

Tipo de IFES	Universo de referência	Respostas válidas	Cobertura
Universidades federais	69	37	53,6%
Institutos federais e equiparados	41	21	51,2%
Total	110	58	52,7%

Fonte: Elaboração própria com base nos dados da pesquisa.

Quanto à relação declarada com o PPSI, a amostra apresentou distribuição equilibrada entre responsáveis institucionais e demais atores diretamente envolvidos com o programa. Das 58 respostas válidas, 29 foram prestadas por participantes que se identificaram como principais responsáveis institucionais pelo acompanhamento ou

preenchimento do PPSI, e 29 por participantes que declararam atuar diretamente no programa, embora não se identifiquem como os principais responsáveis (Tabela 2).

Tabela 2 – Relação do respondente com o PPSI

Relação com o PPSI	n	%
Principal responsável institucional pelo acompanhamento ou preenchimento do PPSI	29	50,0
Atua diretamente no PPSI, mas não é o principal responsável	29	50,0
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

Esse resultado reforça a aderência da base ao público-alvo do estudo. Embora nem todos os respondentes ocupem a posição de principal responsável institucional, todos os registros mantidos na base final correspondem a participantes com atuação direta no PPSI. Essa condição é relevante porque os itens do instrumento exigem conhecimento sobre governança, processos, recursos, tecnologias, gestão de riscos, privacidade e resultados percebidos do programa.

Em relação ao perfil predominante de atuação, observa-se maior participação de respondentes vinculados à segurança da informação, seguidos por privacidade e proteção de dados, tecnologia da informação/TIC e gestão institucional. Esse padrão indica que a amostra não se limita a uma percepção exclusivamente técnica de TI, embora mantenha forte presença de atores diretamente relacionados à segurança da informação e à operação do PPSI (Tabela 3).

Tabela 3 – Perfil predominante de atuação do respondente

Perfil predominante	n	%
Segurança da Informação	24	41,4
Privacidade e proteção de dados	12	20,7
Tecnologia da Informação/TIC	11	19,0
Gestão institucional	10	17,2
Outro perfil diretamente envolvido com o PPSI	1	1,7
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

A distribuição por região geográfica revela participação de IFES de todas as regiões do país. A maior concentração ocorreu no Sudeste e no Nordeste, seguidos pelas regiões Sul, Norte e Centro-Oeste. Essa composição é compatível com a dispersão nacional das IFES e contribui para captar diferentes contextos institucionais de implementação do PPSI. Considerado o universo de referência de cada região, a

cobertura amostral variou de 38,9% no Norte a 58,1% no Sudeste, com as demais regiões entre 52,9% e 54,8% e cobertura global de 52,7%, o que indica representação regional razoavelmente proporcional, um pouco menor na região Norte (Tabela 4).

Tabela 4 – Distribuição regional das IFES participantes

Região	Universo de referência	Respostas válidas	Cobertura
Sudeste	31	18	58,1%
Nordeste	31	17	54,8%
Sul	17	9	52,9%
Norte	18	7	38,9%
Centro-Oeste	13	7	53,8%
Total	110	58	52,7%

Fonte: Elaboração própria com base nos dados da pesquisa.

A caracterização de porte indica heterogeneidade relevante entre as instituições respondentes. Quanto ao número de servidores, predominam IFES na faixa de 1.001 a 2.000 servidores, mas há presença expressiva de instituições com até 1.000 servidores e de instituições com mais de 4.000 servidores. Essa variação reforça a necessidade de interpretar a implementação do PPSI considerando diferentes capacidades administrativas, estruturas organizacionais e graus de complexidade institucional (Tabela 5).

Tabela 5 – Porte das IFES por número aproximado de servidores

Faixa de servidores	n	%
Até 1.000	11	19,0
De 1.001 a 2.000	22	37,9
De 2.001 a 3.000	6	10,3
De 3.001 a 4.000	7	12,1
Acima de 4.000	12	20,7
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

Em relação ao tamanho da equipe de TI/TIC, a maior parte das instituições situa-se na faixa de 21 a 40 profissionais. Também há presença relevante de IFES com equipes entre 11 e 20 profissionais, entre 41 e 60 profissionais e entre 61 e 100 profissionais. Apenas três instituições declararam possuir equipes superiores a 100 profissionais de TI/TIC (Tabela 6).

Tabela 6 – Porte das IFES por tamanho aproximado da equipe de TI/TIC

Faixa da equipe de TI/TIC	n	%
----------------------------------	----------	----------

Até 10	0	0,0
De 11 a 20	11	19,0
De 21 a 40	21	36,2
De 41 a 60	12	20,7
De 61 a 100	11	19,0
Acima de 100	3	5,2
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

Quanto ao número aproximado de estudantes, a maior frequência concentrou-se nas faixas até 10.000 estudantes e de 10.001 a 20.000 estudantes. Ainda assim, há instituições de maior porte, incluindo 11 IFES com mais de 40.000 estudantes. Uma resposta válida não informou essa variável, contabilizada na categoria “Não informado” da tabela (Tabela 7).

Tabela 7 – Porte das IFES por número aproximado de estudantes

Faixa de estudantes	n	%
Até 10.000	18	31,0
De 10.001 a 20.000	17	29,3
De 20.001 a 30.000	9	15,5
De 30.001 a 40.000	2	3,4
Acima de 40.000	11	19,0
Não informado	1	1,7
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

A condição multicampi apareceu como característica predominante da amostra. Das 58 IFES participantes, 55 declararam possuir estrutura multicampi, enquanto apenas três indicaram não possuir essa característica. Esse resultado é relevante para a análise do PPSI porque a dispersão territorial tende a ampliar a complexidade de coordenação, padronização de processos, governança, monitoramento de ativos, resposta a incidentes e implementação de práticas de privacidade (Tabela 8).

Tabela 8 – Condição multicampi das IFES participantes

Condição multicampi	n	%
Sim	55	94,8
Não	3	5,2
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

Em síntese, a amostra apresenta três características relevantes para a interpretação dos resultados. Primeiro, há equilíbrio entre universidades federais e institutos federais quando comparados ao universo de referência. Segundo, os respondentes mantêm aderência ao público-alvo do estudo, uma vez que todos os casos válidos correspondem a responsáveis institucionais ou atores diretamente envolvidos com o PPSI. Terceiro, a amostra reúne instituições heterogêneas em termos de porte, região, estrutura multicampi e tamanho das equipes de TI/TIC. Essas características reforçam a pertinência de analisar a efetividade do PPSI não apenas por médias agregadas, mas também considerando assimetrias institucionais que podem influenciar capacidades, implementação e resultados percebidos, exercício realizado, em caráter exploratório, nos recortes das Tabelas 11, 12 e 14 e retomado na discussão da seção 6.6.

5.3 ESTATÍSTICA DESCRITIVA DAS CAPACIDADES INSTITUCIONAIS

Esta seção apresenta a estatística descritiva dos itens referentes às capacidades institucionais associadas à implementação do PPSI nas IFES. Os itens foram mensurados em escala Likert de sete pontos, variando de 1, correspondente a “discordo totalmente”, a 7, correspondente a “concordo totalmente”. Para a interpretação dos resultados, considera-se o valor 4 como ponto intermediário da escala, representando posição neutra. Valores médios superiores a 4 indicam tendência de concordância, enquanto valores inferiores a 4 indicam menor consolidação percebida da capacidade avaliada.

A Tabela 9 apresenta as médias dos oito itens de capacidades institucionais. Os resultados indicam uma assimetria relevante entre a formalização da governança do PPSI e as capacidades necessárias à sua sustentação material, operacional e integrativa. A maior média foi observada em C1, referente à governança formalizada e em funcionamento. Em sentido oposto, as menores médias concentraram-se em C8, C6 e C5, correspondentes, respectivamente, a recursos orçamentários e contratuais, integração da gestão de riscos ao planejamento e ao orçamento, e gestão de dados pessoais e privacidade.

Tabela 9 – Estatística descritiva dos itens de capacidades institucionais

Código	Capacidade avaliada	Média	Mediana	Desvio-padrão	Concordância (5–7)	Discordância (1–3)
C1	Governança	4,72	5,00	1,44	58,6%	25,9%

C3	Processos	4,00	4,00	1,57	43,1%	37,9%
C2	Pessoas e competências	3,88	4,00	1,51	37,9%	41,4%
C7	Treinamento e conscientização	3,81	4,00	1,55	31,0%	39,7%
C4	Tecnologia e monitoramento	3,74	4,00	1,57	37,9%	41,4%
C5	Gestão de dados pessoais e privacidade	3,17	3,00	1,45	22,4%	63,8%
C6	Gestão de riscos integrada ao planejamento e orçamento	3,05	3,00	1,53	13,8%	67,2%
C8	Recursos orçamentários e contratuais	2,71	3,00	1,35	12,1%	72,4%

Fonte: Elaboração própria com base nos dados da pesquisa.

O item C1 apresentou a maior média do bloco, com 4,72. Esse resultado sugere que a governança é a dimensão de capacidade relativamente mais consolidada entre as IFES participantes. Em termos substantivos, C1 representa a existência de papéis, responsabilidades e instâncias de governança formalizadas e em funcionamento. Trata-se, portanto, da dimensão mais diretamente associada à arquitetura institucional do PPSI: designações, responsabilidades, comitês, fluxos de responsabilização e estruturas mínimas de coordenação.

Esse resultado, contudo, não deve ser interpretado como evidência de plena consolidação da governança em todas as instituições. Embora C1 apresente a maior média, 15 das 58 IFES, correspondentes a 25,9% da amostra, atribuíram valores inferiores ao ponto neutro da escala. Esse grupo é composto por respostas nos valores 2 e 3, indicando que aproximadamente um quarto das instituições participantes ainda percebe fragilidade na própria estrutura de governança do PPSI. Assim, a governança aparece como a capacidade mais avançada em termos relativos, mas não como uma dimensão universalmente consolidada.

A Tabela 10 apresenta a distribuição das respostas do item C1. Observa-se que não houve respostas no valor 1, mas há concentração relevante nos valores 5 e 6, ambos com 14 respostas. Ainda assim, o grupo com respostas inferiores ao ponto neutro permanece expressivo, reforçando que a formalização da governança não se encontra distribuída de maneira uniforme entre as IFES participantes.

Tabela 10 – Distribuição das respostas do item C1

Resposta em C1	n	%
1	0	0,0
2	3	5,2
3	12	20,7

4	9	15,5
5	14	24,1
6	14	24,1
7	6	10,3
Total	58	100,0

Fonte: Elaboração própria com base nos dados da pesquisa.

A análise exploratória desse grupo com C1 abaixo do ponto neutro sugere concentração maior entre universidades, instituições de menor porte administrativo e instituições com equipes de TI menores. Entre as universidades federais, 12 de 37 respostas situaram-se abaixo do ponto neutro em C1, enquanto entre institutos federais foram 3 de 21. Também se observou maior proporção de avaliações inferiores em C1 entre instituições com até 1.000 servidores e entre aquelas com equipes de TI de 11 a 20 profissionais, enquanto a região do país com maior proporção de casos foi o Norte, com 3 de 7. Esses recortes devem ser interpretados com cautela, em razão do tamanho das subamostras, mas indicam que a fragilidade de governança pode estar associada a contextos institucionais com menor capacidade administrativa ou menor densidade técnico-organizacional (Tabela 11).

Tabela 11 – Recortes exploratórios das IFES com C1 inferior ao ponto neutro

Recorte	C1 abaixo de 4 / total % abaixo de 4	
Universidades federais	12 / 37	32,4
Institutos federais	3 / 21	14,3
Norte	3 / 7	42,9
Sul	3 / 9	33,3
Nordeste	5 / 17	29,4
Centro-Oeste	2 / 7	28,6
Sudeste	2 / 18	11,1
Até 1.000 servidores	5 / 11	45,5
Equipe TI de 11 a 20	5 / 11	45,5
Equipe TI de 21 a 40	7 / 21	33,3
Acima de 100 profissionais de TI/TIC	0 / 3	0,0

Fonte: Elaboração própria com base nos dados da pesquisa.

O item C3, com média de 4,00, ocupa a segunda posição entre as capacidades avaliadas. Ele representa aquilo que a instituição efetivamente faz: processos de segurança da informação e privacidade, incluindo gestão de vulnerabilidades, backup, restauração, execução de rotinas e testes periódicos. O resultado situa C3 junto ao ponto neutro da escala, indicando condição intermediária. Em outras palavras, os

processos aparecem menos consolidados do que a governança formal, mas ainda acima das dimensões mais frágeis do bloco.

A diferença entre C1 e C3 é relevante para a interpretação da implementação do PPSI. Enquanto C1 expressa a existência de arranjos formais de governança, C3 representa a tradução desses arranjos em práticas recorrentes. A distância entre os dois itens sugere que a formalização institucional do programa tende a avançar antes da estabilização de processos executados e testados. Essa leitura é compatível com programas públicos de implementação descentralizada, nos quais a criação de papéis e instâncias pode ocorrer mais rapidamente do que a consolidação de rotinas operacionais consistentes.

O item C4, referente aos recursos tecnológicos, visibilidade, monitoramento e apoio à detecção e resposta, apresentou média de 3,74, ligeiramente abaixo do ponto neutro. Esse item expressa aquilo de que a instituição dispõe para operacionalizar parte das exigências do PPSI. Diferentemente de C3, que focaliza processos executados e testados, C4 aborda a base tecnológica necessária para sustentar visibilidade sobre ativos, monitoramento, detecção e resposta a eventos de segurança. Sua média abaixo do ponto neutro indica que a capacidade tecnológica permanece como dimensão parcialmente insuficiente ou desigual entre as IFES.

A comparação entre C3 e C4 permite distinguir duas camadas complementares da implementação. C3 representa a capacidade processual, isto é, a existência de rotinas organizadas. C4 representa a capacidade instrumental, isto é, a disponibilidade de recursos tecnológicos e mecanismos de visibilidade. O fato de C3 apresentar média ligeiramente superior a C4 sugere que algumas instituições podem estar formalizando ou executando processos mesmo sem dispor, de maneira plenamente adequada, dos instrumentos tecnológicos necessários para dar escala, rastreabilidade e capacidade de resposta a essas práticas.

Os itens C2 e C7, relacionados à dimensão humana da implementação, apresentaram médias de 3,88 e 3,81, respectivamente. Esses resultados indicam percepção intermediária, mas ainda inferior ao ponto de concordância. C2 trata da existência de equipe e competências adequadas para conduzir ações de implementação e operação de segurança da informação e privacidade, com alcance mais especializado. C7, por sua vez, avalia ações de treinamento e conscientização com alcance mais amplo entre diferentes públicos institucionais. Em conjunto, esses itens sugerem que pessoas, competências e cultura organizacional constituem

capacidades parcialmente desenvolvidas, mas ainda insuficientes para sustentar de forma ampla a implementação do PPSI.

Esse ponto é relevante porque pessoas e competências funcionam como capacidade transversal. Sem equipe suficiente e qualificada, processos tendem a se tornar formais, mas frágeis na execução. Sem treinamento e conscientização, a segurança da informação e a privacidade permanecem concentradas em áreas técnicas ou especializadas, com baixa capilaridade nas áreas-fim. Assim, as médias de C2 e C7 reforçam a leitura de que a implementação do PPSI depende não apenas de governança formal, mas também da disseminação de capacidades institucionais entre atores técnicos, administrativos e finalísticos.

As três menores médias do bloco foram observadas em C5, C6 e C8. O item C5, referente à gestão de dados pessoais e privacidade, apresentou média de 3,17. Esse resultado sugere fragilidade na operacionalização da privacidade, especialmente em práticas como mapeamento de tratamentos, definição de bases legais e elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Embora a privacidade seja eixo estruturante do PPSI, os dados indicam que sua institucionalização prática ainda se encontra em patamar inferior ao da governança geral do programa.

A baixa média de C5 pode ser interpretada como indício de maior complexidade organizacional da privacidade. Diferentemente de algumas práticas de segurança da informação, frequentemente vinculadas à área de TI ou segurança, a gestão de dados pessoais exige articulação entre múltiplos atores: encarregado, áreas finalísticas, setor jurídico, gestão documental, tecnologia da informação, segurança da informação e alta administração. Essa natureza transversal pode dificultar a transformação de diretrizes gerais em rotinas operantes, especialmente quando não há processos maduros de governança de dados.

O item C6, com média de 3,05, revela fragilidade ainda mais estratégica: a integração da gestão de riscos de segurança da informação e privacidade ao planejamento e ao orçamento institucional. Esse resultado indica que, em parte expressiva das IFES, riscos de segurança e privacidade podem estar sendo identificados ou tratados em alguma medida, mas ainda não incorporados de forma suficiente aos instrumentos decisórios da instituição. Trata-se de uma dimensão crítica, pois a gestão de riscos só produz efeitos institucionais consistentes quando informa prioridades, decisões, investimentos e alocação de recursos.

A posição de C6 entre as menores médias ajuda a qualificar a leitura de C1. A existência de governança formalizada não significa, necessariamente, que a gestão de riscos esteja integrada ao ciclo de planejamento e orçamento. Esse descompasso sugere que o PPSI pode estar institucionalmente reconhecido, mas ainda não plenamente incorporado ao núcleo decisório das IFES. Em outros termos, a governança existe com maior frequência como estrutura, mas nem sempre se converte em capacidade de priorização.

O item C8 apresentou a menor média do bloco, com 2,71. Ele avalia a suficiência de recursos orçamentários e contratuais para sustentar ações de segurança da informação e privacidade previstas no PPSI. Esse resultado aponta a principal fragilidade percebida pelas IFES participantes. A baixa pontuação em C8 sugere que a implementação do programa pode estar limitada por restrições materiais, especialmente aquelas relacionadas a orçamento, contratações, soluções tecnológicas, serviços especializados e manutenção de capacidades permanentes.

A relação entre C1 e C8 é particularmente reveladora. Ainda que a governança seja a dimensão mais bem avaliada, os recursos orçamentários e contratuais aparecem como a dimensão mais frágil. Isso indica que a formalização de papéis e instâncias não resolve, por si só, o problema da sustentação material do PPSI. Mesmo instituições que percebem governança em funcionamento podem continuar enfrentando limitações para contratar soluções, ampliar equipes, manter ferramentas, executar planos de tratamento de riscos ou implementar controles de privacidade.

Essa oposição entre C1 e C8 permite formular uma das principais interpretações da seção: o PPSI parece avançar mais no plano da institucionalização formal do que no plano da capacidade material de execução. Em vez de indicar mera ausência de governança, os dados sugerem um problema mais complexo: há governança em parte relevante das instituições, mas sua capacidade de transformar diretrizes em recursos, decisões orçamentárias e execução sustentada ainda é limitada.

A comparação entre as instituições com C1 abaixo e acima do ponto neutro reforça essa interpretação. Nas IFES que avaliaram C1 abaixo de 4, as médias das demais capacidades também tendem a ser menores, especialmente em C5, C6 e C8. Isso sugere que a governança pode funcionar como capacidade estruturante: quando ela é percebida como ausente ou insuficiente, as demais capacidades também aparecem mais fragilizadas. Contudo, mesmo entre instituições com C1 igual ou

superior ao ponto neutro, C8 permanece baixo, indicando que a insuficiência de recursos orçamentários e contratuais é uma limitação transversal, e não apenas consequência de governança frágil.

Tabela 12 – Médias das capacidades segundo avaliação de C1

Capacidade	C1 abaixo de 4 (n = 15)	C1 igual ou acima de 4 (n = 43)
C2 – Equipe e competências adequadas	2,73	4,28
C3 – Processos executados e testados	3,73	4,09
C4 – Recursos tecnológicos e monitoramento	3,07	3,98
C5 – Gestão de dados pessoais e privacidade	2,27	3,49
C6 – Gestão de riscos integrada ao planejamento/orçamento	2,20	3,35
C7 – Treinamento e conscientização	2,93	4,12
C8 – Recursos orçamentários e contratuais	2,20	2,88

Fonte: Elaboração própria com base nos dados da pesquisa.

A Tabela 12 evidencia que a baixa percepção de governança se associa a menores médias nas demais capacidades institucionais. A diferença é mais pronunciada em C2, C5, C6 e C7, indicando que instituições com governança percebida como insuficiente também tendem a avaliar de forma mais crítica suas equipes, práticas de privacidade, integração de riscos e ações de treinamento. Entretanto, o resultado de C8 merece destaque: mesmo no grupo com C1 igual ou superior ao ponto neutro, a média permanece abaixo de 3. Esse achado reforça que a limitação orçamentária e contratual atravessa diferentes níveis de governança, funcionando como restrição estrutural à implementação do PPSI.

Dessa forma, os resultados descritivos apontam para um padrão de implementação em camadas. A primeira camada, mais avançada, refere-se à formalização da governança. A segunda, intermediária, envolve processos, pessoas, treinamento e tecnologia, dimensões necessárias para transformar governança em prática institucional. A terceira, mais frágil, envolve recursos, integração da gestão de riscos ao planejamento e operacionalização da privacidade. É justamente nessa terceira camada que se concentram os maiores desafios para a conversão do PPSI em capacidades institucionais robustas.

Em síntese, a estatística descritiva das capacidades institucionais evidencia uma assimetria central: as IFES participantes tendem a reconhecer maior avanço na governança formal do PPSI, mas apontam fragilidades importantes na sustentação orçamentária, na integração da gestão de riscos ao planejamento e na gestão efetiva

de dados pessoais e privacidade. Essa configuração sugere que o desafio do PPSI não se limita a instituir estruturas de governança, mas envolve transformar essas estruturas em capacidade organizacional efetiva, com recursos, processos, tecnologia, competências e integração decisória suficientes para sustentar resultados institucionais.

5.4 ESTATÍSTICA DESCRITIVA DA EFETIVIDADE PERCEBIDA

Esta seção apresenta a estatística descritiva dos itens de efetividade percebida do PPSI nas IFES, mensurados na mesma escala e interpretados segundo os mesmos critérios do bloco de capacidades (seção 5.3).

A apresenta as médias dos dez itens de efetividade percebida. Os resultados indicam que os maiores valores se concentram em dimensões operacionais associadas à detecção, contenção e recuperação após incidentes de segurança. Em contrapartida, os menores valores aparecem em dimensões ligadas à percepção institucional e ao reconhecimento da alta administração, sugerindo que os efeitos do PPSI são percebidos de forma mais clara nas rotinas técnicas e operacionais do que na sua tradução em valor organizacional reconhecido pela gestão superior.

Tabela 13 – Estatística descritiva dos itens de efetividade percebida

Código	Dimensão	Média	Mediana	Desvio-padrão	Concordância (5–7)	Discordância (1–3)
E3	Maior agilidade na detecção de incidentes de segurança	4,59	5,00	1,36	55,2%	15,5%
E4	Maior agilidade na contenção e recuperação após incidentes	4,48	4,00	1,39	48,3%	15,5%
E7	Notificações a titulares e à ANPD tempestivas e documentadas	4,45	4,50	1,52	50,0%	20,7%
E5	Redução da exposição a riscos críticos de segurança e privacidade	4,36	4,00	1,36	48,3%	19,0%
E6	Incidentes com dados pessoais menos frequentes ou menos graves	4,31	4,00	1,45	37,9%	15,5%
E8	Avanço em conformidade em segurança, privacidade e LGPD	4,21	4,00	1,48	48,3%	25,9%
E9	Percepção das áreas-fim de que a instituição protege informações e dados pessoais	4,19	5,00	1,52	51,7%	31,0%
E2	Restabelecimento mais rápido de serviços críticos após interrupções	4,10	4,00	1,52	32,8%	25,9%

E1	Menor frequência de interrupções em serviços digitais essenciais	4,05	4,00	1,52	34,5%	27,6%
E10	Reconhecimento de ganhos institucionais pela alta administração	3,91	4,00	1,49	36,2%	37,9%

Fonte: Elaboração própria com base nos dados da pesquisa.

O item com maior média foi E3, relativo à maior agilidade na detecção de incidentes de segurança, com média de 4,59 e mediana 5,00. Esse resultado sugere que a detecção é o aspecto de efetividade mais reconhecido pelos respondentes. Além disso, 55,2% das respostas situaram-se entre 5 e 7, indicando tendência majoritária de concordância quanto à melhora dessa capacidade após a implementação do PPSI ou no período recente analisado.

Em seguida, aparece E4, referente à maior agilidade na contenção e recuperação após incidentes de segurança, com média de 4,48. Em conjunto, E3 e E4 formam o núcleo operacional mais forte da efetividade percebida. Essa combinação indica que os efeitos mais visíveis do PPSI, segundo os respondentes, estão ligados à capacidade de perceber, conter e recuperar-se de eventos de segurança. Trata-se de um resultado coerente com a própria estrutura do programa, que mobiliza controles, processos e práticas voltadas à melhoria da resposta institucional a incidentes.

A posição de E3 e E4 no topo da distribuição sugere que a efetividade do PPSI é percebida de maneira mais concreta quando associada a rotinas técnicas e operacionais. Detecção, contenção e recuperação são dimensões relativamente observáveis para equipes de segurança da informação, tecnologia da informação e atores diretamente envolvidos com o programa. Diferentemente de resultados mais difusos, como confiança institucional ou reconhecimento estratégico, essas dimensões podem ser percebidas a partir de práticas, fluxos, ferramentas, registros de incidentes e experiências operacionais recentes.

Na sequência, aparecem E7, E5 e E6, que podem ser interpretados como resultados intermediários entre a operação técnica e a conformidade institucional. O item E7, relativo à tempestividade e documentação das notificações de incidentes a titulares e à ANPD, apresentou média de 4,45, com 50,0% de concordância. Esse resultado indica percepção relativamente positiva quanto à capacidade de formalizar

e documentar respostas quando há incidentes aplicáveis, embora ainda com dispersão relevante entre as instituições.

O item E5, referente à redução da exposição a riscos críticos de segurança da informação e privacidade, apresentou média de 4,36. Esse resultado sugere que parte dos respondentes percebe diminuição da exposição institucional a riscos críticos, mas sem que essa percepção alcance o mesmo patamar observado em detecção e contenção. A diferença é importante: detectar e responder melhor a incidentes não equivale, necessariamente, a reduzir estruturalmente a exposição a riscos. A redução de risco depende de processos mais amplos, que envolvem tratamento, priorização, recursos, monitoramento contínuo e integração ao planejamento institucional.

O item E6, relativo à menor frequência ou gravidade de incidentes envolvendo dados pessoais, apresentou média de 4,31. Embora acima do ponto neutro, esse resultado deve ser interpretado com cautela. A elevada proporção de respostas neutras sugere que, em parte das IFES, a avaliação sobre incidentes de dados pessoais pode ser limitada por baixa ocorrência, subnotificação, ausência de registros consolidados ou dificuldade de comparação temporal. Assim, E6 aponta tendência positiva, mas menos afirmativa do que os itens diretamente relacionados à detecção e resposta a incidentes de segurança.

Os itens E1 e E2, vinculados à continuidade e disponibilidade de serviços digitais, apresentaram médias de 4,05 e 4,10, respectivamente. Esses resultados situam a continuidade em posição intermediária, próxima ao ponto neutro da escala. Em E1, referente à menor frequência de interrupções em serviços digitais essenciais, a concordância foi de 34,5%, enquanto 37,9% das respostas permaneceram no ponto neutro. Em E2, referente ao restabelecimento mais rápido de serviços críticos após interrupções, a concordância foi de 32,8%, com 41,4% de respostas neutras.

Esse padrão sugere que os efeitos do PPSI sobre continuidade e disponibilidade são percebidos de forma menos intensa ou menos direta do que seus efeitos sobre detecção e resposta a incidentes. Uma possível interpretação é que a continuidade de serviços digitais depende de múltiplos fatores além do PPSI, como infraestrutura de TI, contratos, redundância, arquitetura de sistemas, capacidade de operação, conectividade e processos de continuidade de negócio. Assim, ainda que o PPSI possa contribuir para a resiliência institucional, sua contribuição específica para a redução de interrupções e para a recuperação de serviços críticos pode ser mais difícil de isolar na percepção dos respondentes.

Os itens E8 e E9 ocupam posição intermediária. E8, referente ao avanço em conformidade em segurança da informação e privacidade, inclusive quanto às exigências da LGPD, apresentou média de 4,21. Esse resultado indica tendência moderada de percepção positiva, mas inferior aos itens operacionais de detecção, contenção e notificação. A conformidade aparece, portanto, como resultado em desenvolvimento, possivelmente condicionado à maturidade de processos, registros, auditorias, monitoramentos e práticas de governança de dados.

O item E9, referente à ampliação, entre as áreas-fim, da percepção de que a instituição protege informações e dados pessoais, apresentou média de 4,19 e mediana 5,00. Apesar da média próxima à de E8, sua distribuição é mais polarizada: 51,7% dos respondentes indicaram concordância, mas 31,0% indicaram discordância. Esse resultado é relevante porque sugere que a percepção das áreas-fim não acompanha de forma homogênea os avanços operacionais percebidos pelas áreas mais diretamente envolvidas com o PPSI. Em algumas instituições, a segurança e a privacidade podem estar mais visíveis para as áreas finalísticas; em outras, permanecem restritas ao circuito técnico ou de governança.

O item com menor média foi E10, relativo ao reconhecimento, pela alta administração, de ganhos institucionais associados ao PPSI. A média foi de 3,91, abaixo do ponto neutro da escala, e a proporção de discordância foi ligeiramente superior à de concordância: 37,9% contra 36,2%. Esse resultado é um dos achados mais relevantes da seção, pois indica que os ganhos do PPSI podem estar sendo percebidos em dimensões operacionais, mas ainda não se traduzem de forma consistente em reconhecimento estratégico pela alta administração.

A posição de E10 como menor média reforça uma tensão central da pesquisa: o PPSI pode produzir melhorias percebidas em detecção, resposta, notificação e redução de riscos, mas tais resultados nem sempre se convertem em valor institucional reconhecido pela cúpula decisória. Essa lacuna é especialmente importante em políticas de segurança da informação e privacidade, pois a sustentação de longo prazo do programa depende de reconhecimento estratégico, priorização, recursos e incorporação ao planejamento institucional.

A comparação com o bloco de capacidades ajuda a interpretar esse resultado. Na seção anterior, C8, relativo aos recursos orçamentários e contratuais, foi a capacidade com menor média. Isso sugere que a baixa percepção de reconhecimento pela alta administração pode estar relacionada a uma dificuldade mais ampla de

converter o PPSI em prioridade institucional dotada de recursos e sustentação decisória. Em outras palavras, quando o programa não é plenamente reconhecido como gerador de ganhos institucionais, tende a ser mais difícil justificar investimentos, contratos, ampliação de equipes e integração ao planejamento.

Para explorar essa relação, a Tabela 14 compara os resultados de efetividade entre IFES que avaliaram C8 abaixo do ponto neutro e aquelas que avaliaram C8 igual ou acima de 4. O recorte é exploratório e não deve ser interpretado como evidência causal, mas permite observar diferenças relevantes na percepção de efetividade segundo a suficiência percebida de recursos orçamentários e contratuais.

Tabela 14 – Efetividade percebida segundo a avaliação de recursos (C8)

Indicador de efetividade	C8 abaixo de 4 (n = 42)	C8 igual ou acima de 4 (n = 16)
Escore geral de efetividade percebida	3,94	5,13
E1 – Menor frequência de interrupções em serviços essenciais	3,69	5,00
E2 – Restabelecimento mais rápido de serviços críticos	3,76	5,00
E3 – Maior agilidade na detecção de incidentes	4,31	5,31
E4 – Maior agilidade na contenção e recuperação	4,14	5,38
E5 – Redução da exposição a riscos críticos	4,07	5,13
E6 – Incidentes com dados pessoais menos frequentes ou menos graves	4,00	5,13
E7 – Notificações tempestivas e documentadas	4,26	4,94
E8 – Avanço em conformidade em segurança, privacidade e LGPD	3,90	5,00
E9 – Percepção das áreas-fim	3,76	5,31
E10 – Reconhecimento da alta administração	3,45	5,13

Fonte: Elaboração própria com base nos dados da pesquisa.

Os resultados desse recorte indicam que instituições com avaliação mais favorável em C8 também apresentam médias superiores nos principais itens de efetividade. A diferença é especialmente expressiva em E9 e E10. Enquanto o grupo com C8 abaixo de 4 apresenta média de 3,76 em E9 e 3,45 em E10, o grupo com C8 igual ou superior ao ponto neutro apresenta médias de 5,31 e 5,13, respectivamente. Esse achado sugere que a suficiência percebida de recursos orçamentários e contratuais está associada não apenas a resultados operacionais, mas também à percepção das áreas-fim e ao reconhecimento pela alta administração.

Essa associação deve ser interpretada com prudência. Não se trata de afirmar que recursos causam reconhecimento ou que reconhecimento causa recursos. A

leitura mais adequada é que recursos, percepção organizacional e reconhecimento estratégico parecem compor um mesmo circuito institucional. Onde o PPSI dispõe de maior sustentação orçamentária e contratual, seus resultados tendem a ser mais visíveis, comunicáveis e reconhecidos. Onde essa sustentação é frágil, a efetividade percebida tende a permanecer mais restrita e menos traduzida em valor institucional.

Em síntese, a estatística descritiva da efetividade percebida indica que os efeitos mais reconhecidos do PPSI nas IFES estão associados à detecção, contenção e recuperação após incidentes de segurança. Resultados ligados à notificação, redução de riscos, proteção de dados pessoais e conformidade aparecem em patamar intermediário. Já a continuidade de serviços digitais apresenta percepção mais moderada, possivelmente por depender de fatores estruturais que extrapolam o escopo direto do programa. Por fim, o reconhecimento de ganhos institucionais pela alta administração aparece como o ponto mais frágil do bloco, sugerindo que a efetividade operacional do PPSI ainda não se converte, de forma homogênea, em reconhecimento estratégico e sustentação institucional.

5.5 ASSOCIAÇÕES ENTRE CAPACIDADES E EFETIVIDADE PERCEBIDA

Após a análise descritiva dos itens de capacidades institucionais e efetividade percebida, foi verificada a consistência interna dos constructos centrais do instrumento. Essa etapa é necessária porque as análises associativas subsequentes utilizam escores agregados de capacidade total e efetividade total, calculados a partir da média dos itens que compõem cada bloco.

O bloco de capacidades institucionais, composto pelos itens C1 a C8, apresentou consistência interna adequada, com α de Cronbach = 0,84 e ω de McDonald = 0,84. O bloco de efetividade percebida, composto pelos itens E1 a E10, apresentou consistência interna elevada, com α de Cronbach = 0,93 e ω de McDonald = 0,93. Esses resultados indicam coerência interna satisfatória entre os itens de cada constructo e respaldam seu uso como escores agregados nas análises subsequentes.

Ressalta-se que essa evidência de confiabilidade não elimina a multidimensionalidade substantiva dos constructos. As capacidades C1–C8 representam dimensões institucionais distintas, como governança, pessoas, processos, tecnologia, privacidade, riscos, treinamento e recursos. Do mesmo modo, os itens E1–E10 abrangem diferentes manifestações da efetividade percebida do

PPSI, incluindo continuidade, resposta a incidentes, mitigação de riscos, proteção de dados, conformidade, percepção das áreas-fim e reconhecimento pela alta administração. Assim, os coeficientes de confiabilidade indicam consistência suficiente para compor medidas agregadas de capacidade total e efetividade total, sem reduzir a análise à interpretação unidimensional dos domínios.

Após essa verificação, foram estimadas correlações de Spearman com o objetivo de examinar a associação entre os constructos centrais da pesquisa. A opção por Spearman decorre da natureza ordinal dos itens mensurados em escala Likert de sete pontos e do interesse em verificar associações monotônicas entre as variáveis, sem pressupor normalidade das distribuições ou relação causal entre os constructos. Os escores agregados foram calculados pela média dos itens válidos de cada bloco, preservando-se a escala original do instrumento. O bloco de capacidades compreende os itens C1 a C8, enquanto o bloco de efetividade percebida compreende os itens E1 a E10, conforme estrutura do questionário aplicado às IFES.

A primeira análise examinou a correlação entre capacidade total e efetividade total. O resultado indicou associação positiva, estatisticamente significativa e de magnitude moderada a forte entre os dois constructos ($\rho = 0,627$; $p < 0,001$). Esse achado sugere que instituições com maior percepção de capacidades institucionais também tendem a relatar maior efetividade percebida do PPSI. Em termos substantivos, o resultado reforça a tese analítica de que a efetividade do programa não depende apenas da existência formal de controles, mas da presença de capacidades organizacionais capazes de transformar diretrizes, processos e recursos em resultados institucionais percebidos (Tabela 15).

Tabela 15 – Correlação entre capacidade total e efetividade percebida total

Variável	n	ρ com a efetividade total
Capacidade total	58	0,627***

Fonte: Elaboração própria com base nos dados da pesquisa.

Nota: ρ = coeficiente de correlação de Spearman. * $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$.

Na segunda análise, foram correlacionadas as capacidades específicas C1–C8 com o escore agregado de efetividade total. Todas as capacidades apresentaram associação positiva com a efetividade percebida, embora com magnitudes distintas. As maiores correlações foram observadas em C6, referente à integração da gestão de riscos ao planejamento e ao orçamento institucional ($\rho = 0,612$; $p < 0,001$), C4,

relativa à disponibilidade de recursos tecnológicos, visibilidade, monitoramento, detecção e resposta ($p = 0,586$; $p < 0,001$), e C8, referente à suficiência de recursos orçamentários e contratuais para sustentar as ações previstas no PPSI ($p = 0,553$; $p < 0,001$). Também se destacou C3, associada à execução e testagem regular de processos de segurança da informação e privacidade ($p = 0,479$; $p < 0,001$). Esses resultados indicam que a efetividade percebida se associa de forma mais intensa a capacidades operacionais, materiais e de integração institucional, especialmente riscos, tecnologia, processos e recursos. A governança formal, representada por C1, apresentou associação positiva e estatisticamente significativa, porém de menor magnitude ($p = 0,292$; $p < 0,05$). Esse resultado não reduz a relevância da governança, mas sugere que sua contribuição para a efetividade depende de sua conversão em práticas sustentadas, recursos, instrumentos tecnológicos, gestão de riscos e rotinas executadas. De modo semelhante, C5, referente à gestão de dados pessoais e privacidade, também apresentou associação positiva, mas mais baixa ($p = 0,298$; $p < 0,05$), o que pode indicar que esse domínio ainda se encontra em processo de consolidação nas IFES respondentes (Tabela 16).

Tabela 16 – Correlações entre capacidades específicas e efetividade total

Variável	ETOTAL
ETOTAL	—
C1	0,292*
C2	0,432***
C3	0,479***
C4	0,586***
C5	0,298*
C6	0,612***
C7	0,339**
C8	0,553***

Fonte: Elaboração própria com base nos dados da pesquisa.

Nota: p = coeficiente de correlação de Spearman. * $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$.

A terceira análise examinou a associação entre capacidade total e os domínios de efetividade percebida. Foram considerados seis domínios: continuidade/disponibilidade, detecção/resposta, mitigação de risco, proteção de

dados/privacidade, transparência/conformidade e confiança/percepção. A capacidade total apresentou correlações positivas e estatisticamente significativas com todos os domínios de efetividade. As maiores associações ocorreram com confiança/percepção ($\rho = 0,551$; $p < 0,001$), proteção de dados/privacidade ($\rho = 0,547$; $p < 0,001$), transparência/conformidade ($\rho = 0,530$; $p < 0,001$) e continuidade/disponibilidade ($\rho = 0,529$; $p < 0,001$). Também foram observadas associações relevantes com detecção/resposta ($\rho = 0,520$; $p < 0,001$) e mitigação de risco ($\rho = 0,458$; $p < 0,001$). Esse padrão sugere que as capacidades institucionais não se associam apenas a resultados técnico-operacionais, como detecção de incidentes, contenção, recuperação ou continuidade de serviços digitais. Elas também se relacionam a dimensões institucionais mais amplas, como conformidade, proteção de dados, percepção das áreas-fim e reconhecimento dos ganhos associados ao PPSI. Esse achado é relevante porque aproxima a discussão da efetividade do programa da literatura sobre valor público, na medida em que os resultados percebidos envolvem não apenas a operação técnica da segurança da informação, mas também legitimidade institucional, confiança e capacidade de demonstrar conformidade (Tabela 17).

Tabela 17 – Correlações entre capacidade total e domínios de efetividade percebida

Variável CTOTAL	
CTOTAL	—
E1-E2	0,529***
E3-E4	0,520***
E5	0,458***
E6	0,547***
E7-E8	0,530***
E9-E10	0,551***

Fonte: Elaboração própria com base nos dados da pesquisa.

Nota: ρ = coeficiente de correlação de Spearman. * $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$.

A quarta análise consistiu na matriz de correlações entre cada capacidade específica e cada domínio de efetividade. Essa matriz permite observar padrões mais finos de associação entre capacidades e resultados. C4, referente à tecnologia e monitoramento, apresentou associações particularmente elevadas com continuidade/disponibilidade, detecção/resposta, mitigação de risco e proteção de dados/privacidade. Esse resultado sugere que a capacidade tecnológica não deve ser

compreendida apenas como disponibilidade de infraestrutura, mas como condição de visibilidade operacional, monitoramento contínuo e resposta a eventos de segurança. A associação com proteção de dados também indica que recursos tecnológicos adequados podem apoiar a prevenção, detecção e contenção de incidentes envolvendo informações e dados pessoais. C6, referente à gestão de riscos integrada ao planejamento e orçamento, apresentou correlações consistentes com todos os domínios de efetividade, com destaque para confiança/percepção, continuidade/disponibilidade e proteção de dados/privacidade. Esse padrão sugere que a gestão de riscos atua como capacidade transversal, capaz de conectar diretrizes estratégicas, priorização orçamentária e ações operacionais. Quando a gestão de riscos está integrada ao planejamento institucional, a segurança da informação e a privacidade tendem a deixar de ser tratadas como ações isoladas ou reativas, passando a compor o processo decisório e a agenda de gestão. C8, relativa aos recursos orçamentários e contratuais, também apresentou associações expressivas com a efetividade total e com diferentes domínios de resultado, especialmente confiança/percepção, proteção de dados, detecção/resposta e continuidade. Esse achado dialoga com a estatística descritiva, na qual C8 apareceu como uma das capacidades mais frágeis. A combinação entre baixa média descritiva e correlação elevada com a efetividade percebida indica um ponto crítico para interpretação: os recursos constituem uma fragilidade relevante, mas também uma capacidade fortemente associada aos resultados do programa. Portanto, a insuficiência orçamentária e contratual pode representar obstáculo importante à consolidação do PPSI nas IFES. C3, associada aos processos executados e testados regularmente, apresentou correlações positivas com todos os domínios de efetividade. Esse resultado reforça a importância da proceduralização das práticas de segurança da informação e privacidade. A existência de processos regulares de gestão de vulnerabilidades, backup, restauração, monitoramento e resposta contribui para transformar diretrizes e controles em rotinas institucionais verificáveis. Nesse sentido, os processos funcionam como ponte entre a formalização da política e a produção de resultados percebidos. Em síntese, as correlações indicam que a efetividade percebida do PPSI está positivamente associada ao conjunto das capacidades institucionais, mas com maior intensidade nos domínios ligados à gestão de riscos, tecnologia/monitoramento, recursos e processos. Esses resultados sustentam a interpretação de que a efetividade percebida do PPSI está associada à

conversão da implementação do programa em capacidades organizacionais operantes, dotadas de recursos, instrumentos, rotinas e integração ao planejamento institucional. A governança formal permanece relevante, mas seus efeitos parecem depender da capacidade de se materializar em práticas sustentadas e em condições institucionais concretas de execução (Tabela 18).

Tabela 18 – Correlações entre capacidades específicas e domínios de efetividade

Capacidade	E1-E2 Continuidade	E3-E4 Detecção /resposta	E5 Mitigação de risco	E6 Proteção de dados	E7-E8 Conformidade	E9-E10 Confiança/ percepção
C1 Governança	0,220	0,266*	0,225	0,169	0,273*	0,325*
C2 Pessoas/competências	0,385**	0,401**	0,241	0,424***	0,285*	0,368**
C3 Processos	0,456***	0,419**	0,385**	0,437***	0,397**	0,324*
C4 Tecnologia/monitoramento	0,590***	0,499***	0,458***	0,592***	0,392**	0,421***
C5 Dados/privacidade	0,267*	0,258	0,236	0,269*	0,301*	0,255
C6 Gestão de riscos	0,507***	0,436***	0,419**	0,504***	0,433***	0,592***
C7 Treinamento/conscientização	0,145	0,292*	0,247	0,232	0,487***	0,336**
C8 Recursos	0,431***	0,444***	0,409**	0,462***	0,349**	0,605***

Fonte: Elaboração própria com base nos dados da pesquisa.

Nota: ρ = coeficiente de correlação de Spearman. * $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$.

5.6 ASSOCIAÇÕES COM OS ÍNDICES DE MATURIDADE DO PPSI

Esta seção examina as associações entre os índices de maturidade autorrelatada do PPSI (iBase, iSeg e iPriv) e os constructos centrais da pesquisa: capacidades institucionais e efetividade percebida. Conforme delimitado na metodologia, esses índices são tratados como medidas de implementação, e não como desfechos. Os indicadores foram informados pelos respondentes em escala de 0 a 1 e utilizados exclusivamente em análises agregadas, sem divulgação individualizada, conforme informado expressamente no questionário.

As análises restringiram-se aos 52 casos com os três índices válidos. Cinco instituições não informaram os indicadores e uma resposta apresentou valores incompatíveis com a escala prevista, superiores a 1, tendo sido desconsiderada nas

análises envolvendo maturidade. Em coerência com a opção metodológica adotada para variáveis ordinais e distribuições não necessariamente normais, foram estimadas correlações de Spearman.

Os três índices foram considerados de duas formas: de modo agregado, por meio de um indicador de maturidade total autorrelatada, definido como a média aritmética de iBase, iSeg e iPriv; e de modo desagregado, para fins de transparência analítica. A agregação foi adotada como decisão analítica parcimoniosa, voltada a representar a maturidade autorrelatada geral do PPSI. Contudo, como iBase, iSeg e iPriv expressam dimensões distintas — estrutura básica, segurança da informação e privacidade —, os resultados desagregados também são reportados (Tabela 19).

Tabela 19 – Correlações da maturidade com capacidade e efetividade percebidas

Índice de maturidade	n	ρ com capacidade total	ρ com efetividade total
Maturidade total	52	0,41**	0,22 n.s.
iBase	52	0,32*	0,25 n.s.
iSeg	52	0,38**	0,23 n.s.
iPriv	52	0,25 n.s.	-0,01 n.s.

Fonte: Elaboração própria com base nos dados da pesquisa.

Nota: ρ = coeficiente de Spearman. * $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$; n.s. = não significativo.

A maturidade total autorrelatada apresentou associação positiva e estatisticamente significativa com a capacidade total ($\rho = 0,41$; $p < 0,01$), indicando que instituições com maiores índices autorrelatados de maturidade tendem a relatar maiores capacidades institucionais. Entretanto, a associação entre maturidade total e efetividade total não alcançou significância estatística ($\rho = 0,22$; n.s.). Em contraste, conforme apresentado na seção anterior, a correlação entre capacidade total e efetividade total foi positiva, mais elevada e estatisticamente significativa ($\rho = 0,627$; $p < 0,001$).

Esse padrão reforça a distinção analítica entre maturidade e efetividade. Os índices de maturidade autorrelatada parecem se aproximar mais da dimensão de estruturação institucional e capacidade percebida do que dos resultados de efetividade propriamente ditos. Em outros termos, maior maturidade declarada no PPSI não se traduz automaticamente em maior efetividade percebida, ao menos no conjunto de respostas analisado. A efetividade parece estar mais fortemente associada à presença de capacidades institucionais operantes do que aos índices agregados de maturidade considerados isoladamente.

A análise desagregada qualifica esse resultado. Nenhum dos três índices, isoladamente, apresentou associação estatisticamente significativa com a efetividade total ao nível de 5%. Com as capacidades, as associações significativas concentraram-se em iSeg ($p = 0,38$; $p < 0,01$) e iBase ($p = 0,32$; $p < 0,05$), enquanto iPriv apresentou associação positiva, mas não significativa ($p = 0,25$; n.s.). O resultado mais distintivo refere-se ao iPriv, cuja correlação com a efetividade percebida foi praticamente nula ($p = -0,01$; n.s.). Esse achado sugere que, nesta amostra, a maturidade autorrelatada em privacidade se encontra menos associada aos resultados percebidos de efetividade do que os demais componentes da maturidade.

Essas associações devem ser interpretadas com cautela. Os índices foram informados por autorrelato, não foram divulgados individualmente e apresentaram casos faltantes. Além disso, as correlações são de natureza associativa, não autorizando inferência causal. A ausência de associação significativa entre maturidade e efetividade não deve ser interpretada como evidência de irrelevância da implementação do PPSI, mas como indício de que a maturidade declarada, isoladamente, não acompanha os resultados percebidos com a mesma intensidade observada nas capacidades institucionais.

5.7 MODELOS EXPLORATÓRIOS DE REGRESSÃO

Para examinar de forma complementar o encadeamento teórico que orienta a pesquisa (maturidade autorrelatada, capacidades institucionais e efetividade percebida), foram ajustados modelos exploratórios de regressão linear com erros-padrão robustos à heterocedasticidade, por meio do estimador HC3. Os coeficientes são apresentados de forma padronizada, permitindo comparação entre variáveis mensuradas em métricas distintas. Para preservar a comparabilidade entre os modelos, todas as estimações desta seção restringem-se aos 52 casos com valores válidos para iBase, iSeg e iPriv. Dada a dimensão amostral e o delineamento transversal da pesquisa, os resultados são interpretados em chave associativa, e não causal (Tabela 20).

Tabela 20 – Modelos exploratórios de regressão para capacidade e efetividade

Modelo	Variável dependente	Preditor	β	EP HC3	p	R ²	R ² ajust.
M0	Capacidade total	Maturidade total	0,33	0,18	0,069	0,106	0,088
M1	Efetividade total	Maturidade total	0,13	0,18	0,487	0,016	-0,004

M2	Efetividade total	Capacidade total	0,61	0,13	< 0,001	0,374	0,361
M3	Efetividade total	Maturidade total	-0,08	0,13	0,545	0,380	0,354
M3	Efetividade total	Capacidade total	0,64	0,15	< 0,001	0,380	0,354

Fonte: Elaboração própria com base nos dados da pesquisa.

Nota: β = coeficiente padronizado; EP HC3 = erro-padrão robusto à heterocedasticidade. No modelo M3, o VIF foi de 1,12, indicando ausência de multicolinearidade relevante.

No modelo M0, a maturidade total apresentou coeficiente positivo em relação à capacidade total, mas com significância apenas marginal sob erros-padrão robustos ($\beta = 0,33$; $p = 0,069$; $R^2 = 0,106$). Esse resultado deve ser lido em conjunto com a correlação de Spearman apresentada na seção anterior, na qual a associação entre maturidade total e capacidade total foi positiva e estatisticamente significativa. A diferença entre os resultados sugere sensibilidade ao método de estimação, comportamento esperado em amostras de menor porte e que reforça a necessidade de interpretação cautelosa.

No modelo M1, a maturidade total não apresentou associação estatisticamente significativa com a efetividade percebida ($\beta = 0,13$; $p = 0,487$), respondendo por parcela muito reduzida da variação observada ($R^2 = 0,016$). Em contraste, no modelo M2, a capacidade total apresentou associação positiva e estatisticamente significativa com a efetividade percebida ($\beta = 0,61$; $p < 0,001$), com $R^2 = 0,374$. No modelo conjunto M3, a capacidade total permaneceu como o único preditor estatisticamente significativo ($\beta = 0,64$; $p < 0,001$), enquanto a maturidade total não apresentou associação significativa ($\beta = -0,08$; $p = 0,545$). A inclusão da maturidade praticamente não alterou o poder explicativo do modelo em relação ao modelo com capacidade total, com R^2 passando de 0,374 para 0,380.

As verificações de sensibilidade respaldaram a estabilidade desses resultados. A distância de Cook máxima foi de 0,38, abaixo do limiar convencional de 1,0. Na reestimação *leave-one-out*, retirando-se uma instituição por vez, o coeficiente padronizado da capacidade total variou entre 0,56 e 0,71 no modelo M2 e entre 0,59 e 0,76 no modelo M3, mantendo significância estatística em todas as reestimações, enquanto o coeficiente da maturidade total permaneceu entre -0,15 e -0,03, sem alcançar significância em nenhum cenário. Sob o mesmo procedimento, a correlação de Spearman entre capacidade total e efetividade total oscilou entre 0,61 e 0,69. Por fim, a reestimação por regressão robusta com o estimador de Huber, que repondera observações atípicas, produziu coeficientes de 0,66 no modelo M2 e de 0,70 para capacidade e -0,13 para maturidade no modelo M3, na mesma direção e em

magnitude próxima às dos modelos originais. Nenhuma observação isolada altera, portanto, a direção, a magnitude aproximada ou a significância das associações reportadas.

Em conjunto, os modelos reforçam a interpretação de que, nesta amostra, a efetividade percebida do PPSI está mais fortemente associada às capacidades institucionais do que à maturidade autorrelatada do programa. Esse achado é coerente com a distinção teórica adotada na dissertação entre maturidade, entendida como medida de implementação e estruturação, e efetividade, compreendida como dimensão de resultados percebidos. A tradução da maturidade em efetividade parece depender, de modo mais imediato, da presença de capacidades institucionais operantes.

5.8 SÍNTESE DOS ACHADOS EMPÍRICOS

Esta seção apresentou os resultados da pesquisa empírica com as 58 IFES da base analítica, abrangendo o perfil da amostra, as estatísticas descritivas, a confiabilidade dos constructos, as associações entre capacidades e efetividade e os modelos exploratórios.

Em conjunto, os resultados desenham um quadro heterogêneo: a governança formal é a capacidade mais consolidada, enquanto recursos orçamentários e contratuais, gestão de riscos integrada ao planejamento e gestão de dados pessoais são as mais frágeis; a efetividade percebida concentra-se nas dimensões operacionais e encontra seu ponto mais baixo no reconhecimento pela alta administração; e as capacidades institucionais, sobretudo gestão de riscos, tecnologia e monitoramento, recursos e processos, associam-se de forma consistente à efetividade, ao passo que a maturidade autorrelatada se associa às capacidades, mas não aos resultados percebidos.

Em síntese, a seção 5 evidencia que a avaliação da efetividade do PPSI nas IFES não pode ser reduzida à mensuração da maturidade declarada do programa. Os achados sugerem que a passagem da implementação para os resultados percebidos depende da conversão da maturidade em capacidades organizacionais concretas, especialmente nos domínios de recursos, gestão de riscos, tecnologia, monitoramento e processos. Essa interpretação será aprofundada na seção seguinte, na qual os resultados empíricos aqui apresentados serão confrontados com os achados da

revisão sistemática da literatura e convertidos em implicações analíticas, recomendações e produto técnico voltado ao aprimoramento do PPSI nas IFES.

6 DISCUSSÃO, RECOMENDAÇÕES E PRODUTO TÉCNICO

Esta seção discute os resultados empíricos apresentados na seção 5, tomando-os como fio condutor da argumentação, e os confronta com a literatura reunida na revisão sistemática consolidada na seção 4. O movimento analítico é duplo. De um lado, retoma-se cada achado central da pesquisa de campo e examina-se em que medida ele converge, diverge ou tensiona o que a literatura internacional sobre segurança da informação e privacidade no setor público tem evidenciado. De outro, retorna-se diretamente aos estudos do portfólio da revisão, inclusive a trabalhos que não haviam sido mobilizados na análise situacional, para aprofundar a interpretação dos resultados e evitar que a discussão fique circunscrita ao mesmo conjunto de autores já explorado anteriormente. É nesse encontro, entre a experiência internacional documentada pela literatura e a primeira avaliação empírica de efetividade do *framework* brasileiro nas Instituições Federais de Ensino Superior, que reside a contribuição central desta seção.

Cabe reiterar que os dados da seção 5 são transversais e perceptuais, não autorizando leituras causais, e que os estudos do portfólio provêm de contextos heterogêneos, exigindo prudência na transposição e cautela na generalização dos resultados. A discussão opera, portanto, em chave sugestiva: padrões, mecanismos plausíveis e explicações candidatas.

Um esclarecimento de leitura é necessário antes do confronto. Entre a revisão sistemática e a pesquisa de campo, os domínios de análise foram refinados. Na codificação da literatura, a governança tinha definição ampla, abrangendo estratégias, coordenação, definição de papéis e, com frequência, a própria função de gestão de riscos, e a dimensão humana formava um único domínio de pessoas e competências. No instrumento, essas categorias foram desdobradas em oito capacidades. A governança foi recortada para seu núcleo formal, os papéis, responsabilidades e instâncias em funcionamento (C1); a gestão de riscos ganhou domínio próprio, com foco na integração ao planejamento e ao orçamento (C6); o treinamento e a conscientização destacaram-se de pessoas e competências (C7); e os recursos passaram a ser medidos em sua expressão orçamentária e contratual (C8). No bloco de efetividade, os seis domínios da revisão foram preservados, mas quatro deles desdobraram-se em dois itens, e a numeração dos dez itens do questionário não coincide com os códigos de domínio da revisão: a mitigação de risco, por exemplo, é

o terceiro domínio na revisão e o quinto item no instrumento. Por isso, ao longo da seção, os constructos serão nomeados por extenso, com os códigos do instrumento indicados quando a precisão o exigir. Essa expansão, longe de ser um detalhe técnico, é um recurso analítico. Estudos que a revisão codificou como governança dialogam, no vocabulário do instrumento, tanto com a face formal quanto com o núcleo integrativo da gestão de riscos, e é justamente essa decomposição, como se verá, que permite identificar qual componente da governança acompanha os resultados.

A estrutura segue os achados: das assimetrias de implementação (6.1 a 6.2) à distinção entre maturidade, capacidades e efetividade (6.3); dos elos frágeis de privacidade, riscos e recursos (6.4 a 6.6) à dimensão humana (6.7); e da síntese interpretativa (6.8) às recomendações e à ancoragem do produto técnico-tecnológico (6.9–6.10).

6.1 O DESCOMPASSO ENTRE INSTITUCIONALIZAÇÃO FORMAL E CAPACIDADE DE EXECUÇÃO

O primeiro achado estruturante da pesquisa empírica é a assimetria entre a formalização da governança do PPSI e as capacidades que a sustentam materialmente. A governança, entendida como papéis, responsabilidades e instâncias formalizados e em funcionamento (C1), obteve a maior média do bloco de capacidades, 4,72, enquanto o polo mais frágil reuniu a suficiência de recursos orçamentários e contratuais (C8), com 2,71, a integração da gestão de riscos ao planejamento e ao orçamento (C6), com 3,05, e a gestão de dados pessoais e privacidade (C5), com 3,17. O padrão sugere que o programa avança primeiro no plano dos papéis, dos comitês e das instâncias, e só depois, e de forma incompleta, no plano das rotinas executadas, dos instrumentos tecnológicos e da sustentação orçamentária. Mesmo a governança, contudo, não é universal: um quarto das instituições participantes (25,9%) avaliou a própria estrutura de governança abaixo do ponto neutro da escala.

Esse padrão encontra respaldo direto na evidência brasileira sobre difusão de práticas de gestão por indução normativa. Alves e Santos (2022), ao acompanharem por uma década a adoção de práticas de gestão de riscos, integridade e segurança da informação em mais de duzentos órgãos federais, concluíram que as instruções normativas expedidas por instâncias hierarquicamente superiores são eficazes em

propagar a adoção formal dessas práticas, mas que sua mera edição não é suficiente para institucionalizá-las. Nenhuma das práticas avaliadas atingiu nível de saturação superior a 75% no período analisado. O PPSI, instituído por portaria e monitorado por índices reportados ao órgão central, é um caso típico de indução normativa. Os resultados da seção 5 sugerem que as IFES reproduzem exatamente o comportamento previsto por esse mecanismo: a adesão formal, na designação de papéis e na constituição de instâncias, avança à frente da conversão em capacidade operante.

A literatura internacional sobre governança de segurança da informação no setor público reforça essa leitura. No mapeamento sistemático de Magnusson *et al.* (2025), a adesão a *frameworks* reconhecidos, como a ISO/IEC 27001, o GDPR e a diretiva NIS, convive com uma escassez generalizada de práticas efetivas de conformidade: faltam indicadores de desempenho, medidas sistemáticas de avaliação de risco, modelos de maturidade aplicados e auditorias regulares. Os autores identificam ainda que processos de governança abaixo do padrão figuram entre as causas comuns de medidas de segurança frágeis e que a adoção de procedimentos adequados de governança está, em alguma medida, vinculada aos recursos orçamentários disponíveis em cada organização. O quadro descrito espelha o das IFES, com estruturas formais razoavelmente difundidas, instrumentação e verificação escassas, e restrição material como pano de fundo.

Vestad e Yang (2025) oferecem a formulação conceitual mais próxima do que os dados das IFES indicam. Ao estudarem municípios noruegueses, organizações públicas com mandato amplo e recursos restritos, os autores argumentam que *frameworks* como o NIST CSF e a ISO/IEC 27001 fornecem práticas padronizadas, mas que essas práticas precisam ser implementadas por pessoas com competências adequadas e sustentadas por soluções tecnológicas efetivas, o que denominam capacidades de cibersegurança sustentáveis. Os desafios que identificam, ambiguidade na formalização de papéis, lacunas de competências, dificuldade de implantar tecnologias de segurança avançadas e barreiras de comunicação entre a TI central e as áreas funcionais, correspondem, quase termo a termo, à camada intermediária observada nas IFES, na qual equipe e competências, base tecnológica de monitoramento e treinamento apresentaram médias entre 3,74 e 3,88. A convergência sugere que o fenômeno não é idiossincrático do PPSI, mas

característico de organizações públicas que recebem mandatos normativos amplos sem o correspondente reforço de capacidades.

Evidências de programas estruturados em outras jurisdições apontam na mesma direção, ao mostrarem que mesmo iniciativas maduras convivem com lacunas persistentes de implementação. Borgman, Mubarak e Choo (2015), ao avaliarem a implantação do *framework* de gestão de segurança da informação no governo do Sul da Austrália, registraram ganhos reconhecidos pelos participantes na estruturação do programa, mas identificaram áreas críticas pendentes que exigiriam fases sucessivas de implantação ao longo de anos. A implementação de políticas de segurança, nessa leitura, é menos um ato de adesão e mais um processo prolongado de acumulação de capacidades, no qual a formalização inicial é apenas a etapa de menor custo político e orçamentário.

No setor de educação superior, a literatura acrescenta um alerta interpretativo relevante para o resultado da governança. Šikman *et al.* (2025) observam que as organizações universitárias exibem níveis variados de comprometimento com a segurança da informação, o que se traduz em variações significativas no desenvolvimento e na implementação de seus sistemas de gestão, e defendem modelos com critérios mensuráveis justamente porque a existência formal do sistema pouco informa sobre seu funcionamento. Salam, Abu Bakar e Aman (2025) constatarem que muitas instituições de ensino superior não dispõem de estruturas adequadas para avaliar e aprimorar suas práticas de segurança, a despeito da criticidade de seus ativos. Khan, Almulhim e Alkati (2025) acrescentam o alerta de que universidades tendem a considerar sua infraestrutura segura sem compreender a extensão real de sua vulnerabilidade. Em conjunto, esses estudos recomendam cautela com leituras excessivamente otimistas da governança formal: percebê-la como existente e atuante é condição de partida, mas pode mascarar fragilidades que só a instrumentação, o teste e a verificação revelariam.

O confronto com a seção 4 exige, neste ponto, a mediação conceitual apresentada na abertura da seção. A revisão sistemática apontava a tríade formada por governança, processos e tecnologia com monitoramento como núcleo consistente de implementação, com a governança operando como capacidade organizadora do terreno em que as demais funcionam, inclusive por meio da gestão de riscos, então descrita como função de mediação entre diretrizes e execução. A governança da literatura, porém, é o constructo amplo; o item do instrumento mede apenas seu

núcleo formal, enquanto a função de mediação foi emancipada no domínio de gestão de riscos e sua expressão operacional habita, em parte, o domínio de processos. Lidos isoladamente, os resultados poderiam sugerir uma contradição com a literatura: a capacidade mais consolidada, a governança formal, foi também a de menor associação com a efetividade percebida (0,292). Lidas em conjunto, porém, as duas faces do constructo dissolvem a contradição em uma especificação. A face formal está relativamente instalada, mas fracamente associada aos resultados, ao passo que a face integrativa e decisória, justamente a que a literatura credita como mecanismo ativo da governança, permanece frágil nas IFES (média 3,05) e é a mais fortemente associada à efetividade (0,612).

Colocada nesses termos, a comparação confirma a direção do encadeamento da tríade. Os processos executados e testados (média 4,00) e a base tecnológica de monitoramento (3,74) ocupam posições intermediárias, acima do polo mais frágil. Mas revela um elo incompleto, em que o mandato existe com mais frequência do que as rotinas, e as rotinas existem com mais frequência do que a instrumentação, a integração decisória e os recursos. Em outras palavras, o que falta às IFES não é diretriz nem desenho institucional, mas tração material e integrativa, exatamente a camada que a literatura de *frameworks* tende a pressupor como dada e que estudos como os de Vestad e Yang (2025) e Magnusson *et al.* (2025) recolocam no centro do problema. O achado empírico, viabilizado pela decomposição do constructo no instrumento, acrescenta à revisão uma precisão que ela, agregando estudos com codificações amplas, não tinha como oferecer: dentro da governança, é o componente que conecta riscos, planejamento e orçamento, e não o que formaliza papéis e instâncias, que acompanha os resultados percebidos do programa.

6.2 EFETIVIDADE OPERACIONAL SEM RECONHECIMENTO ESTRATÉGICO

O segundo achado estruturante diz respeito à topografia da efetividade percebida. Os maiores escores concentraram-se nas dimensões operacionais: a agilidade na detecção de incidentes de segurança (E3) alcançou média 4,59, a agilidade na contenção e recuperação (E4), 4,48, e a tempestividade das notificações a titulares e à ANPD (E7), 4,45. Na extremidade oposta, o reconhecimento de ganhos institucionais pela alta administração (E10) obteve a única média abaixo do ponto neutro do bloco, 3,91, com discordância superior à concordância, e a percepção das

áreas-fim de que a instituição protege informações e dados pessoais (E9) apresentou distribuição polarizada, com 51,7% de concordância e 31,0% de discordância. O PPSI, na percepção de quem o operacionaliza, melhora a capacidade de perceber e responder a eventos de segurança, mas esses ganhos não se convertem, na mesma medida, em valor reconhecido pela cúpula decisória.

Uma primeira chave interpretativa para essa assimetria é a da visibilidade diferencial dos resultados. Detecção, contenção e recuperação são observáveis por quem opera o programa, pois se materializam em ferramentas, fluxos, registros de incidentes e experiências recentes. Já o principal produto da segurança bem-sucedida é um não-evento, o incidente que deixou de ocorrer, e não-eventos não geram evidência espontânea. Dutton *et al.* (2019) identificam esse problema na escala das nações: é difícil justificar compromissos com a construção de capacidade em cibersegurança quando seus benefícios se apoiam em raciocínio lógico, estudos de caso limitados e opinião de especialistas, e não em evidência sistemática. A mesma lógica parece operar na escala organizacional das IFES. Sem métricas que traduzam riscos evitados, exposição reduzida e continuidade preservada em linguagem de valor institucional, a alta administração carece de matéria-prima para reconhecer ganhos, ainda que eles existam no plano operacional.

A segunda chave é relacional, e aqui o retorno a Moon, Choi e Armstrong (2018) permite extrair do estudo um conteúdo mais específico do que o mobilizado na seção 4. Com dados de 102 organizações governamentais coreanas, os autores mostram que a liderança relacional do responsável pela segurança impulsiona o alinhamento social entre dirigentes de negócio e de tecnologia, que esse alinhamento produz conhecimento integrado entre as partes e que é essa integração que se converte em efetividade do sistema de segurança e, na sequência, em desempenho organizacional. O mecanismo descrito é preciso. A efetividade estratégica da segurança não decorre automaticamente da operação técnica competente, mas da qualidade dos vínculos entre quem opera e quem decide. Lido a partir desse modelo, o baixo reconhecimento pela alta administração nas IFES sugere um déficit menos de desempenho e mais de alinhamento: o programa funciona operacionalmente, mas o circuito relacional que converteria esse funcionamento em reconhecimento e prioridade institucional está interrompido ou é frágil.

A centralidade do patrocínio da alta administração para resultados de segurança é um dos pontos de maior convergência do portfólio. Shaheen e Zolait

(2023), ao avaliarem o programa Cyber-Trust do Bahrein, destacam o papel da alta administração como fator explícito de sucesso da implementação. Chinyemba e Phiri (2018), a partir do setor público zambiano, recomendam que a alta administração demonstre comprometimento aprovando políticas e assegurando o orçamento requerido para o sistema de gestão de segurança. Abdelwahed, Mahmoud e Bdair (2017), em estudo com universidades palestinas, incluem o apoio da alta administração entre as dimensões da política de segurança associadas à efetividade dos sistemas de informação institucionais. Frandell e Feeney (2022), com dados de 500 cidades norte-americanas, mostram que a adesão e as percepções dos gestores interagem com os fatores técnicos na explicação dos incidentes reportados, evidenciando que a proteção é irredutivelmente sociotécnica. O que os dados das IFES acrescentam a essa convergência é a direção do problema no caso brasileiro: não se trata apenas de obter patrocínio prévio para implementar, mas de comunicar resultados já produzidos para sustentar o patrocínio ao longo do tempo.

Nesse ponto, o portfólio oferece uma pista institucional pouco explorada na análise situacional, a dos mecanismos formais de tradução entre a operação de segurança e a linguagem da gestão. Alhawtmeh (2025) encontra influência estatisticamente significativa da auditoria interna sobre a efetividade da cibersegurança em agências governamentais jordanianas, sugerindo que estruturas de avaliação independentes funcionam como correia de transmissão entre o desempenho técnico e o processo decisório. Esse achado dialoga com um resultado específico da seção 5: as ações de treinamento e conscientização correlacionaram-se mais fortemente com o domínio de transparência e conformidade (0,487) do que com qualquer outro, e a conformidade demonstrável é precisamente o formato de resultado que auditorias, relatórios executivos e prestação de contas conseguem processar. Instituições que dispõem de canais como auditoria interna, comitês com participação da alta administração e relatórios periódicos de risco tendem a ter mais oportunidades de converter desempenho operacional em reconhecimento estratégico.

Os dados sugerem, ainda, que reconhecimento e recursos formam um circuito. No recorte exploratório da Tabela 14, as IFES que avaliaram favoravelmente seus recursos orçamentários e contratuais apresentaram médias superiores justamente nas dimensões perceptivas (5,31 contra 3,76 na percepção das áreas-fim; 5,13 contra 3,45 no reconhecimento pela alta administração). A correlação entre recursos e o domínio de confiança e percepção, de 0,605, foi a mais alta de toda a matriz que cruza

capacidades e efetividades. A leitura não é causal, mas a configuração é consistente com um ciclo que se retroalimenta: onde há sustentação material, o programa produz resultados mais visíveis e comunicáveis, o que favorece o reconhecimento, o qual, por sua vez, facilita a alocação de novos recursos; onde a sustentação falta, a efetividade permanece confinada ao circuito técnico e o programa perde a disputa por prioridade. Al-Hawamleh (2024) descreve o elo final desse circuito no plano do valor público: práticas robustas de cibersegurança correlacionam-se fortemente com a qualidade percebida dos serviços de governo eletrônico, alimentando confiança e satisfação dos usuários. O risco simétrico, para as IFES no polo frágil, é o de um ciclo vicioso em que invisibilidade, despriorização e subfinanciamento se reforçam mutuamente.

6.3 MATURIDADE NÃO É EFETIVIDADE: AS CAPACIDADES COMO ELO

O achado de maior densidade teórica da pesquisa é a dissociação empírica entre maturidade declarada e efetividade percebida. O conjunto das capacidades institucionais correlacionou-se de forma expressiva com a efetividade total ($p = 0,627$, significativo a 0,1%), ao passo que a maturidade autorrelatada do programa, embora associada às capacidades (0,41), não apresentou associação estatisticamente significativa com a efetividade (0,22). Nos modelos de regressão exploratórios, a capacidade total foi o único preditor relevante da efetividade percebida ($\beta = 0,64$), e a inclusão da maturidade nada acrescentou ao poder explicativo. O caso extremo é o índice de privacidade, o iPriv, cuja correlação com a efetividade foi praticamente nula (-0,01). Em síntese, o quanto a instituição declara ter implementado não acompanha o quanto ela percebe colher de resultados; o que acompanha são as capacidades operantes.

Esse resultado converge com a evidência internacional de que capacidade, em sentido amplo, importa para desfechos de segurança. Dutton *et al.* (2019), combinando bases transnacionais, encontraram correlações significativas entre indicadores de capacidade em cibersegurança e menores indicadores de comprometimento das máquinas dos usuários finais, um dos poucos testes empíricos disponíveis de que o investimento em capacidade se traduz em resultados observáveis. É relevante notar o que os autores entendem por capacidade: um conjunto multidimensional de iniciativas gerenciais, técnicas, sociais, jurídicas e

regulatórias, construído por um ecossistema de atores. Trata-se de um constructo mais próximo do bloco de capacidades desta dissertação do que de um índice declaratório de implementação de controles. A distinção conceitual ajuda a explicar por que, nas IFES, as capacidades predizem a efetividade percebida e a maturidade autorrelatada, não.

A literatura recente sobre prontidão organizacional oferece o vocabulário teórico para essa distinção. Mohamed Noor, Moghavvemi e Tajudeen (2025), estudando operadores de infraestrutura crítica na Malásia à luz da teoria das capacidades dinâmicas, descrevem a prontidão em cibersegurança não como um estoque de controles implantados, mas como um feixe de capacidades adaptativas de percepção do ambiente de ameaças, de aproveitamento de oportunidades de proteção e de transformação organizacional contínua. Sob essa lente, os índices de maturidade do PPSI fotografam o estoque, enquanto os itens de capacidade do instrumento desta pesquisa aproximam-se do fluxo: processos executados e testados, riscos integrados à decisão, recursos que sustentam a operação. A dissociação encontrada na seção 5 é exatamente a que a teoria prevê quando estoque e fluxo se descolam.

Há também um problema de mensuração, e o portfólio é incisivo nesse ponto. Dewanto, Oktavia e Sundaram (2022), ao compararem modelos de avaliação de segurança utilizados pelo governo indonésio, questionam a confiabilidade e a acurácia de índices baseados em autoavaliação e argumentam que a robustez só se alcança mediante avaliação rigorosa de desempenho e efetividade, e não apenas de aderência declarada. Ribeiro *et al.* (2025) fornecem a demonstração em escala global: ao auditarem tecnicamente 3.068 plataformas de serviços públicos digitais em 193 países, encontraram lacunas substanciais entre os padrões internacionais formalmente adotados e a postura de segurança efetivamente verificável nas plataformas. A implicação para o PPSI é direta porque a autodeclaração não é um traço acidental dos dados, mas o próprio desenho de mensuração do programa. As organizações preenchem, em autodiagnóstico, o grau de implantação de cada medida, e essas declarações compõem os índices por controle e, por agregação, os índices iBase, iSeg e iPriv, historicamente sem exigência de evidências que as sustentassem. Índices assim construídos podem capturar formalização e esforço, mas tendem a superestimar a proteção efetiva na ausência de verificação, o que ajudaria a explicar sua fraca associação com os resultados percebidos.

O próprio ecossistema de controle do programa reconheceu essa limitação. Ao fiscalizar os dois primeiros ciclos de autoavaliação de controles coletados pela Secretaria de Governo Digital junto às organizações do SISP, bem como o *framework* do PPSI, o Tribunal de Contas da União evidenciou a baixa maturidade agregada do sistema e formulou apontamentos sobre a confiabilidade do modelo declaratório e a necessidade de sustentação das respostas em evidências (Brasil, 2024b). Em consonância com esse apontamento, a segunda versão do programa, instituída pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, passou a disponibilizar campo para registro de evidências no sistema de autodiagnóstico e a prever, em seu normativo, que tais evidências poderão vir a ser exigidas (Brasil, 2025c). Trata-se de um primeiro passo, ainda no plano da possibilidade, exatamente na direção que a literatura internacional recomenda e que os dados desta pesquisa reforçam: aproximar a medição declarada da verificação e complementar a régua de implementação com indicadores de capacidade e de resultado. Os achados da seção 5 oferecem, nesse sentido, evidência empírica nacional que corrobora a pertinência dessa inflexão do desenho do programa. A operacionalização da exigência comporta cuidados de desenho, como a separação entre implementação e verificação e a proteção graduada das informações, retomados nas recomendações ao órgão central (seção 6.9).

O contraponto do portfólio impede, contudo, uma conclusão apressada contra os modelos de maturidade em si. Shaheen e Zolait (2023) documentam que o programa de maturidade do Bahrein produziu impactos significativos na garantia de segurança das entidades participantes, elevando a conscientização, reduzindo ataques e otimizando recursos. A diferença relevante não está no instrumento, mas no arranjo. Trata-se de programa com acompanhamento próximo do órgão central, verificação e forte envolvimento da alta administração, e não de autodeclaração periódica. No mesmo sentido, Azambuja e Souza Neto (2020), ao proporem um modelo de maturidade de segurança cibernética para a administração pública federal brasileira, o concebem como ferramenta diagnóstica para orientar planos de melhoria, e não como métrica de resultado. A tensão entre esses estudos e os achados desta pesquisa se resolve, portanto, em uma síntese: a maturidade é útil como mapa de implementação; torna-se problemática quando é tomada como proxy de efetividade, uso que os dados das IFES desautorizam.

A analogia macro reforça a centralidade dos mecanismos intermediários. Krishna e Sebastian (2021), em análise entre países, mostram que o compromisso

nacional com a cibersegurança não gera prosperidade econômica diretamente; seus efeitos são mediados pelo uso efetivo das tecnologias pelas empresas. Transposto para o plano organizacional, o resultado sugere que indicadores agregados de compromisso ou implementação só produzem desfechos por meio de mecanismos que os convertem em prática, no caso das IFES, as capacidades institucionais. Essa é, em essência, a cadeia que os modelos exploratórios da seção 5 desenham: a maturidade associa-se às capacidades, as capacidades associam-se à efetividade, e a maturidade perde relevância quando ambas entram no mesmo modelo.

Registre-se, por fim, uma divergência instrutiva. Mohsini, Toke e Rashidi (2025), ao investigarem instituições públicas tanzanianas, encontraram capacidade técnica e financeira suficientes convivendo com carência de pessoal de TI qualificado, configuração quase inversa à das IFES, nas quais o gargalo declarado é material e integrativo, recursos e integração de riscos, com a dimensão de pessoas em posição intermediária (média 3,88). A comparação sugere que o elo fraco da corrente que liga implementação a resultados depende do contexto, o que tem uma implicação metodológica importante: instrumentos de avaliação de programas como o PPSI precisam ser capazes de localizar o gargalo específico de cada organização, em vez de presumir uma hierarquia universal de carências. Essa implicação será retomada na especificação do produto técnico-tecnológico, na seção 6.10.

Também merece aprofundamento o próprio conceito de efetividade adotado. Masrek *et al.* (2020), ao examinarem 292 agências federais malaias, operacionalizam a efetividade da política de segurança como constructo perceptual multidimensional e demonstram sua associação significativa com as ameaças experimentadas pelas organizações, validando a percepção qualificada de atores institucionais como medida legítima de resultado em segurança da informação. Esse precedente metodológico sustenta a opção desta dissertação por mensurar efetividade percebida, ao mesmo tempo em que delimita seu alcance: percepções qualificadas capturam resultados que indicadores técnicos não alcançam, como reconhecimento e confiança, mas não substituem métricas objetivas de incidentes, disponibilidade e exposição, cuja construção permanece como agenda para as IFES e para o órgão central do programa.

6.4 A PRIVACIDADE COMO ELO FRÁGIL: ENTRE A CONFORMIDADE EPISÓDICA E A GESTÃO OPERANTE DE DADOS

O terceiro conjunto de achados desenha um paradoxo. A privacidade é um dos dois eixos constitutivos do PPSI, mas a gestão de dados pessoais e privacidade (C5) figurou entre as capacidades mais frágeis, com média 3,17 e discordância de 63,8% dos respondentes; sua correlação com a efetividade total foi das mais baixas do bloco (0,298); e o índice de maturidade em privacidade foi o único indicador com associação praticamente nula com a efetividade percebida. Ao mesmo tempo, a notificação de incidentes a titulares e à ANPD alcançou a terceira maior média de efetividade (4,45), e o avanço em conformidade situou-se acima do ponto neutro (4,21). O programa, portanto, parece produzir respostas formais e episódicas de privacidade com mais facilidade do que privacidade como função de gestão contínua.

A defasagem entre a agenda técnica de digitalização e a institucionalização da privacidade não é exclusividade brasileira. Mutimukwe, Kolkowska e Grönlund (2019), ao avaliarem práticas de proteção da privacidade da informação no governo eletrônico de Ruanda, constataram que o desenvolvimento dos serviços priorizava a expansão técnica acelerada, enquanto as práticas de privacidade permaneciam incipientes, a ponto de os autores questionarem sua eficácia na proteção efetiva dos usuários. Guardadas as distâncias de contexto, o padrão é análogo ao das IFES, com a transformação digital correndo à frente da governança de dados que deveria acompanhá-la. Trata-se de um achado com sabor estrutural, e não conjuntural, o que sugere que a fragilidade da gestão de dados não se resolverá espontaneamente com o amadurecimento natural do programa.

Ogbodo *et al.* (2025) dão a esse fenômeno uma formulação que interessa diretamente à interpretação dos dados: no setor de saúde digital, os autores identificam lacunas significativas entre as expectativas regulatórias e as realidades operacionais das organizações, e propõem um *framework* sociotécnico explicitamente desenhado para construir a ponte entre exigência normativa e implementação prática, validando empiricamente os elos entre governança, práticas de segurança e conformidade. A situação das IFES descrita pela seção 5 é a de organizações posicionadas exatamente sobre essa lacuna. A LGPD e o PPSI definem o que se espera, e os controles de privacidade do framework (19 a 25) preveem expressamente essa infraestrutura administrativa: o mapeamento de tratamentos, as bases legais

definidas e os relatórios de impacto. As notificações tempestivas e a conformidade auditável mostram que as respostas exigíveis acontecem; a fragilidade da capacidade de gestão de dados revela, porém, que o prescrito ainda não se consolidou como prática operante nas instituições.

Por que a notificação avança e a gestão de dados não? Uma explicação plausível articula a natureza das tarefas aos incentivos institucionais. Notificar um incidente é uma tarefa episódica, com gatilho claro, rito definido e cobrança externa identificável; mapear tratamentos e manter relatórios de impacto atualizados é uma função contínua, transversal, que exige a cooperação de áreas finalísticas, jurídicas, de documentação e de tecnologia, sem gatilho externo equivalente. Gumzej (2023) acrescenta a dimensão do *enforcement*: ao analisar a atuação da autoridade croata de proteção de dados, evidencia que os poderes corretivos sobre o setor público são estruturalmente mais brandos, órgãos públicos frequentemente não estão sujeitos a multas, e que a efetividade da fiscalização depende de prazos, transparência e publicização das decisões. No Brasil, a ANPD igualmente opera com sanções atenuadas sobre entes públicos. O resultado é um sistema de incentivos que torna racional responder bem ao que é exigível e visível, a notificação, a resposta a fiscalizações, e postergar o que é contínuo e silencioso, a governança de dados, exatamente o padrão que os dados das IFES exibem.

As consequências dessa configuração extrapolam o risco jurídico. A síntese meta-analítica de Gupta *et al.* (2025) mostra que percepções de privacidade e segurança alimentam a confiança no governo eletrônico e, por essa via, a intenção de uso dos serviços. Mutimukwe, Kolkowska e Grönlund (2020) demonstram que as garantias organizacionais de privacidade moldam as percepções de risco e controle dos usuários e que a confiança no governo eletrônico tem natureza mais complexa que em outros serviços, e AlAbdali *et al.* (2021) associam instrumentos de preservação de privacidade à confiabilidade percebida dos serviços governamentais. No polo oposto dessa cadeia, Yang, Mei e Zheng (2023), em levantamento com 3.436 usuários de serviços móveis de governo com reconhecimento facial na China, mostram que a percepção de perda de controle sobre os próprios dados é o principal antecedente da fadiga de privacidade, estado de exaustão emocional e cinismo em que o usuário se sente impotente para proteger a própria privacidade e tende ao desengajamento e à desconfiança no governo. Para instituições cuja atividade-fim envolve dados de estudantes, pesquisadores e servidores em larga escala, a

fragilidade persistente da gestão de dados representa, portanto, um passivo de confiança em formação, ainda que não se manifeste imediatamente em incidentes.

Resta interpretar o resultado mais anômalo, a correlação nula entre a maturidade declarada em privacidade e a efetividade percebida. Três leituras se complementam. A primeira é a da formalização documental: o índice pode estar capturando a produção de artefatos, políticas publicadas, inventários declarados, que ainda não alteram práticas, hipótese coerente com a lacuna entre adoção declarada e postura verificável demonstrada por Ribeiro *et al.* (2025). A segunda é a da imaturidade do próprio campo: se a gestão de dados é a capacidade menos consolidada, as instituições podem simplesmente ainda não ter atingido o patamar mínimo a partir do qual a implementação começa a gerar resultados perceptíveis, uma não-linearidade que dados transversais não capturam. A terceira é a da mensurabilidade: resultados de privacidade são menos observáveis que resultados de segurança, incidentes com dados pessoais podem passar despercebidos ou não ser registrados, como sugere a alta proporção de respostas neutras no item sobre a frequência e a gravidade desses incidentes, de modo que nem o índice nem a percepção dispõem de bons sinais. As três leituras convergem para a mesma implicação prática. A privacidade requer, mais do que qualquer outro eixo do PPSI, instrumentos específicos de gestão e de mensuração de resultados.

6.5 A GESTÃO DE RISCOS COMO CAPACIDADE-PONTE: O MAIOR POTENCIAL, UM DOS MENORES DESENVOLVIMENTOS

A integração da gestão de riscos ao planejamento e ao orçamento institucional (C6) apresentou a mais alta correlação com a efetividade total entre todas as capacidades mensuradas (0,612) e, de modo singular, associou-se de forma consistente a todos os seis domínios de resultado, da continuidade dos serviços digitais (0,507) à proteção de dados pessoais (0,504), com destaque para o domínio de confiança e percepção (0,592). É, pelos dados, a capacidade que mais acompanha a efetividade do programa em todas as suas frentes. E, no entanto, é uma das menos desenvolvidas nas IFES, com média de 3,05, 67,2% de discordância e apenas 13,8% de concordância, à frente somente da suficiência de recursos orçamentários. Mesmo no grupo de instituições que percebem sua governança formal como atuante, a integração de riscos permanece abaixo do ponto neutro da escala (média 3,35). O

programa convive, portanto, com a sua alavanca mais promissora praticamente desativada.

Essa posição singular deixa de surpreender quando se recupera o papel que a literatura reserva à gestão de riscos. Na síntese da seção 4, ela aparecia como função de mediação entre diretrizes e execução, o mecanismo pelo qual o mandato da governança se converte em prioridades operacionais, e a mitigação de risco era o eixo em torno do qual os demais resultados de efetividade se agrupavam nos estudos revisados. A pesquisa empírica devolve a mesma imagem pelo avesso: onde a mediação existe, os resultados melhoram em conjunto, o que se expressa nas correlações consistentes com todos os domínios; onde falta, falta ao conjunto. Le, Phung e Nguyen (2020) demonstram a viabilidade dessa função integradora ao consolidar avaliações qualitativas e quantitativas de risco em estruturas administrativas compostas do governo vietnamita, e Mohamed Noor, Moghavvemi e Tajudeen (2025) oferecem o correlato teórico. Nas organizações prontas, a percepção do ambiente de ameaças se converte em decisão e em transformação organizacional, e a gestão de riscos integrada é precisamente a institucionalização desse trajeto, o elo entre perceber e agir.

Há também uma razão plausível para sua associação particularmente alta com o domínio de confiança e percepção: o risco funciona como língua franca do núcleo decisório. Registros de risco, matrizes de priorização e declarações de apetite são formatos que conselhos, comitês, auditorias e órgãos de controle processam com naturalidade, ao contrário de métricas técnicas de detecção ou vulnerabilidade. Paul e Zhang (2021) formalizam essa função ao modelar o planejamento de riscos como o cálculo que ordena os investimentos entre prevenção, detecção e contenção sob restrição orçamentária, e Chorna, Bohdan e Gaponov (2025) propõem instrumentos econômicos com o mesmo propósito, dimensionar o investimento a partir do risco. Nos dados das IFES, a integração de riscos e a suficiência de recursos caminham juntas (correlação de 0,498), configuração coerente com a hipótese de que é pela via do risco que a segurança entra na disputa orçamentária, embora a direção dessa relação não possa ser estabelecida com dados transversais. A leitura conecta esta seção ao circuito descrito na seção 6.2: onde os riscos entram no planejamento, o programa entra na agenda da direção.

Se a alavanca é tão promissora, por que está desativada? Três explicações sugestivas se combinam. A primeira é a transversalidade, pois integrar riscos ao

planejamento não é tarefa que a equipe de segurança execute sozinha, exige a cooperação das áreas de planejamento e orçamento e o engajamento do núcleo decisório, e não por acaso as três capacidades mais frágeis da amostra, ou seja, recursos, integração de riscos e gestão de dados, compartilham essa dependência de atores externos ao circuito técnico. A segunda é o desenho da indução. O *framework* do PPSI deriva de catálogos de controles, e a lógica do autodiagnóstico convida a implementar e reportar medida a medida. Uma organização pode cumprir controles durante anos sem jamais construir a ponte entre riscos e decisão, porque a ponte não é uma medida a implantar, é uma rotina a sustentar, e a indução normativa tende a produzir aquilo que é verificável e reportável (Alves; Santos, 2022), enquanto a escassez de práticas sistemáticas de avaliação de risco figura entre as lacunas típicas de conformidade no setor público (Magnusson *et al.*, 2025). A terceira é conjuntural. Com orçamentos discricionários comprimidos e ciclos orçamentários rígidos, informar o orçamento pelo risco pressupõe uma margem de manobra que muitas IFES não têm, o que remete à sustentação material tratada na seção seguinte.

A implicação é direta e será retomada nas recomendações e no produto técnico-tecnológico: se os dados apontam uma aposta com maior potencial de retorno institucional, ela é o desenvolvimento da capacidade de gestão de riscos integrada, hoje quase inativa. Os dados não permitem afirmar que desenvolvê-la causará efetividade; permitem afirmar que, entre todas as capacidades mensuradas, é a que mais acompanha os resultados percebidos, em todas as suas dimensões, e que seu estágio atual é incompatível com o papel de mediação que tanto a literatura internacional quanto o desenho de qualquer política madura de segurança lhe reservam.

6.6 RECURSOS E HETEROGENEIDADE INSTITUCIONAL: A SUSTENTAÇÃO MATERIAL DA POLÍTICA

A capacidade com menor média de todo o instrumento foi a suficiência de recursos orçamentários e contratuais (C8), com 2,71 e discordância de 72,4% dos respondentes, e essa fragilidade mostrou-se transversal. Mesmo entre as IFES que percebem sua governança como consolidada, a média de recursos permaneceu abaixo de 3. Ao mesmo tempo, os recursos apresentaram correlação elevada com a efetividade total (0,553) e a maior correlação de toda a matriz com o domínio de

confiança e percepção (0,605). Repete-se, agora em chave material, o paradoxo da seção anterior: a dimensão mais frágil do programa é também uma das mais associadas aos seus resultados.

Esse é, possivelmente, o ponto de convergência mais forte entre os achados empíricos e a literatura sobre organizações públicas subnacionais e setoriais. Na revisão sistemática de Hossain *et al.* (2025) sobre cibersegurança em governos locais, as restrições de recursos financeiros aparecem como o primeiro dos quatro grupos de desafios-chave, ao lado de vulnerabilidades tecnológicas, fatores humanos e quadro regulatório, e associam-se a sistemas desatualizados, treinamento insuficiente e erosão da confiança pública. Frandell e Feeney (2022) partem do mesmo diagnóstico para o caso norte-americano, o de governos locais cronicamente subdotados e subpreparados diante de ameaças crescentes. Vestad e Yang (2025) constroem seu conceito de capacidades sustentáveis precisamente para organizações com essa restrição. As IFES ocupam posição estruturalmente análoga, pois recebem um mandato nacional uniforme, mas o executam com orçamentos discricionários comprimidos e estruturas de TI de porte muito variável, de 11 a mais de 100 profissionais na amostra.

A literatura de governança acrescenta que essa não é uma correlação acidental. Magnusson *et al.* (2025) registram que a própria adoção de procedimentos de governança de segurança está vinculada aos recursos orçamentários disponíveis, e Dutton *et al.* (2019) lembram que a construção de capacidade é intensiva em recursos por definição, exigindo atenção simultânea a múltiplas dimensões. Al-Hawamleh (2024) fecha o argumento no plano organizacional, ao evidenciar que o investimento financeiro figura entre os preditores significativos de práticas robustas de cibersegurança, ao lado de treinamento e aderência regulatória. Contra esse pano de fundo, a leitura dos dados das IFES ganha precisão: a indução normativa do PPSI encontrou nas instituições um teto material, e políticas induzidas por norma sem correspondente estratégia de financiamento tendem a estacionar na camada formal, como discutido na seção 6.1.

O retorno a Paul e Zhang (2021) permite extrair implicações que a seção 4 não explorou. O modelo de otimização dos autores, que aloca investimentos entre prevenção, detecção e contenção considerando governo e organizações, produz dois resultados relevantes para o desenho do PPSI. Primeiro, o investimento do ator central em inteligência eleva a efetividade da detecção dos entes, o que sugere

complementaridade, e não substituição, entre gasto central e gasto local. Segundo, há externalidades positivas do investimento agregado, uma vez que a proteção de cada organização beneficia as demais, o que justifica economicamente arranjos coordenados de investimento em vez de decisões isoladas. Chorna, Bohdan e Gaponov (2025) seguem linha semelhante ao proporem instrumentos econômicos para dimensionar riscos e investimentos em infraestruturas críticas, combinando regulação estatal, padrões internacionais e estímulo ao investimento. A mensagem conjunta é que a lacuna de recursos não se resolve por exortação normativa nem por esforço isolado de cada IFES: requer engenharia financeira da política.

O portfólio também documenta estratégias viáveis sob escassez, particularmente pertinentes para o polo mais frágil da amostra. Hossain *et al.* (2025) sistematizam abordagens não convencionais para mitigar limitações financeiras e de competências: ferramentas de código aberto, terceirização seletiva de funções específicas de segurança e colaborações com agências especializadas, instituições acadêmicas e setor privado. Domínguez-Dorado *et al.* (2023), a partir de um caso público espanhol, propõem o centro de operações de segurança terceirizado de amplo escopo como solução para organizações que não conseguem constituir equipes próprias completas, documentando inclusive os requisitos de contratação para preservar o alinhamento com as necessidades do ente público. Para o sistema das IFES, essas evidências apontam para arranjos cooperativos, centros de operação compartilhados, contratações conjuntas, reuso de soluções e comunidades de prática, como caminho de escala que orçamentos individuais não alcançam, hipótese que será retomada nas recomendações.

A heterogeneidade institucional é a outra face da sustentação material. Os recortes exploratórios da seção 5 indicaram que a fragilidade de governança se concentra em universidades (12 de 37, contra 3 de 21 entre institutos), em instituições com até mil servidores e equipes de TI de 11 a 20 profissionais (45,5% abaixo do ponto neutro em ambos os grupos). Ainda que as subamostras exijam cautela, o padrão é coerente com a literatura de governos locais, na qual porte e densidade técnico-administrativa condicionam sistematicamente a capacidade de resposta (Hossain *et al.*, 2025; Frandell; Feeney, 2022). Chahid *et al.* (2025) acrescentam, para universidades marroquinas, que as barreiras de cibersegurança na transformação digital são interdependentes e exigem priorização estruturada, e Salam, Abu Bakar e Aman (2025) defendem modelos de maturidade desenhados sob medida para a

educação superior. A implicação para o PPSI é clara. Um programa uniforme aplicado a um universo desigual tende a reproduzir, e possivelmente ampliar, as desigualdades de partida, a menos que incorpore mecanismos explícitos de apoio diferenciado.

Um traço contextual agrava esse quadro nas IFES: 94,8% das instituições da amostra são multicampi. A dispersão territorial multiplica os custos de coordenação de inventário, monitoramento, resposta a incidentes e padronização de processos, desafios que a literatura associa a estruturas governamentais multiníveis. Le, Phung e Nguyen (2020), ao aplicarem uma abordagem holística de gestão de riscos ao governo eletrônico vietnamita, mostram a viabilidade de integrar avaliação qualitativa e quantitativa de riscos em estruturas administrativas compostas, do ministério à província, oferecendo um paralelo metodológico para instituições que precisam consolidar riscos de múltiplos campi em uma única visão institucional, exatamente a integração que se revelou incipiente nas IFES.

6.7 A DIMENSÃO HUMANA: COMPETÊNCIAS, CULTURA E OS LIMITES DA CONSCIENTIZAÇÃO

As capacidades ligadas a pessoas ocuparam a faixa intermediária do bloco: a existência de equipe e competências adequadas (C2) obteve média 3,88, e o alcance do treinamento e da conscientização entre os públicos institucionais (C7), 3,81, ambas abaixo do ponto neutro. Cabe lembrar que, na matriz da revisão sistemática, essas duas capacidades formavam um único domínio de pessoas e competências, desdobrado no instrumento justamente para distinguir a disponibilidade de equipe qualificada do alcance das ações de conscientização; a literatura sobre fatores humanos mobilizada nesta seção dialoga, portanto, com ambas. Mais revelador que as médias, porém, é o perfil de correlações do treinamento. Sua associação mais forte foi com o domínio de transparência e conformidade (0,487), e a mais fraca, com continuidade e disponibilidade de serviços (0,145). O treinamento, tal como praticado, parece produzir mais conformidade demonstrável do que resiliência operacional, e o desdobramento do domínio permite enxergar essa nuance, que ficaria oculta em uma medida única da dimensão humana.

Esse perfil encontra explicação na crítica de Van Steen *et al.* (2020) às campanhas governamentais de conscientização. Ao codificarem 17 campanhas com base em taxonomias de mudança comportamental, os autores constataram que as

iniciativas se concentram em educação e aumento de consciência, sob a premissa implícita de que informação suficiente gera mudança de comportamento, e que praticamente inexistem avaliações publicadas de sua efetividade comportamental. Se o mesmo desenho prevalece nas ações das IFES, o resultado esperado é justamente o observado: públicos capazes de responder corretamente a auditorias e requisitos formais, sem alteração proporcional nas práticas que sustentam continuidade e resposta. A recomendação decorrente, desenhar ações por comportamento-alvo e medir efeito comportamental, e não apenas alcance, será incorporada à seção 6.9.

A segmentação de públicos é o segundo refinamento que o portfólio sugere. Sittitiamjan e Wuttidittachotti (2025), aplicando o modelo de conhecimentos, atitudes e práticas a estudantes tailandeses, encontraram diferenças significativas de conscientização por gênero, idade e domínio de conhecimento, concluindo pela necessidade de programas culturalmente adaptados e segmentados. A comunidade das IFES é radicalmente heterogênea, docentes, técnicos, estudantes, terceirizados, gestores, e o instrumento pergunta precisamente pelo alcance do treinamento entre esses diferentes públicos. A leitura conjunta sugere que o desafio não é ofertar mais do mesmo treinamento, mas diferenciar conteúdo, formato e métrica por público crítico.

O aprofundamento de Karlsson *et al.* (2022) conecta a dimensão humana à discussão de reconhecimento estratégico da seção 6.2. Os autores mostram que a cultura organizacional percebida, mais do que a formalmente declarada, condiciona a adesão dos servidores às políticas de segurança. Cultura percebida se forma, em larga medida, pelos sinais que a organização emite: prioridade orçamentária, envolvimento da alta administração, consequências reais de não conformidade. Nas IFES em que o PPSI é visível apenas no circuito técnico, o sinal cultural transmitido às áreas-fim é o de baixa prioridade, o que retroalimenta tanto a polarização da percepção das áreas-fim quanto o alcance limitado do treinamento. Evans *et al.* (2019) complementam ao demonstrar, com a técnica IS-CHEC, que o erro humano no setor público se concentra em causas nucleares recorrentes e tratáveis por desenho de processos, e Tran *et al.* (2024) identificam os fatores que moldam o comportamento de segurança de servidores públicos, reforçando que comportamento seguro é produto de rotina, desenho organizacional e contexto, mais do que de exposição a conteúdo informativo.

6.8 SÍNTESE INTERPRETATIVA: UM MODELO EM CAMADAS DA EFETIVIDADE DO PPSI

O confronto entre os achados empíricos e a literatura do portfólio permite consolidar uma leitura integrada. Registre-se, desde já, que se trata de leitura interpretativa, apoiada em dados transversais e perceptuais, cuja generalização pede a cautela detalhada ao final desta seção. A implementação do PPSI nas IFES organiza-se em três camadas de profundidade crescente e consolidação decrescente. A primeira, mais avançada, é a da institucionalização formal: papéis, comitês, instâncias e adesão normativa, a camada que a indução normativa produz com eficácia (Alves; Santos, 2022), mas que pouco prediz, por si, os resultados percebidos. A segunda é a camada sociotécnica de operação: processos executados e testados, tecnologia e monitoramento, pessoas e treinamento, na qual as IFES apresentam consolidação intermediária e desigual, o padrão que Vestad e Yang (2025) descrevem como o desafio de converter *frameworks* em capacidades. A terceira, mais frágil e mais fortemente associada à efetividade, é a camada de sustentação material e integração decisória: recursos orçamentários e contratuais, gestão de riscos integrada ao planejamento e gestão operante de dados pessoais. Note-se que, pela correspondência conceitual apresentada na abertura da seção, o constructo amplo de governança da literatura atravessa as três camadas, com a face formal na primeira, a expressão processual na segunda e o núcleo integrativo-decisório na terceira, onde se concentra a associação com os resultados percebidos.

Sobre essas camadas opera um circuito perceptivo que os dados sugerem e a literatura ajuda a nomear: resultados operacionais que não são traduzidos em linguagem de valor não geram reconhecimento estratégico; sem reconhecimento, a sustentação material não se renova; sem sustentação, os resultados se estreitam e se tornam ainda menos visíveis. A efetividade do PPSI, nessa síntese, não é uma função direta da maturidade declarada, mas o produto da conversão de maturidade em capacidades operantes, conversão que depende criticamente da camada material-integrativa e do circuito de reconhecimento. A seção 4 já antecipava, a partir da literatura, que a maturidade é condição necessária, mas não suficiente; os dados da seção 5 especificam onde a suficiência falha, e o portfólio, revisitado nesta discussão, explica por quê. O Quadro 9 sintetiza o confronto.

Quadro 9 – Síntese do confronto entre achados empíricos e literatura do portfólio

Achado empírico (Capítulo 5)	Convergências na literatura	Tensões e qualificações	Leitura sugerida
Governança formal consolidada (média 4,72) convive com fragilidade de recursos (2,71), de integração de riscos (3,05) e de gestão de dados (3,17)	Indução normativa difunde adoção formal sem garantir institucionalização (Alves; Santos, 2022); <i>frameworks</i> não se convertem automaticamente em capacidades (Vestad; Yang, 2025); escassez de práticas de conformidade apesar da adesão a padrões (Magnusson <i>et al.</i> , 2025)	Programas estruturados com verificação e patrocínio geram ganhos reais (Shaheen; Zolait, 2023; Borgman; Mubarak; Choo, 2015)	O PPSI avançou na camada de menor custo; a decomposição da governança mostra que é seu núcleo integrativo (0,612), e não sua face formal (0,292), que acompanha os resultados
Gestão de riscos integrada: a maior associação com a efetividade (0,612), consistente em todos os domínios, e uma das menores médias (3,05)	Risco como função de mediação entre diretriz e execução e como eixo organizador dos resultados (Capítulo 4); integração holística viável em estruturas compostas (Le; Phung; Nguyen, 2020); planejamento de riscos ordena investimentos (Paul; Zhang, 2021; Chorna; Bohdan; Gaponov, 2025)	Indução por catálogo de controles produz o reportável, não o integrativo (Alves; Santos, 2022); escassez de avaliação sistemática de riscos como lacuna típica do setor (Magnusson <i>et al.</i> , 2025)	Capacidade-ponte com a maior alavancagem potencial do programa; prioridade natural de desenvolvimento
Efetividade concentrada na operação, detecção (4,59) e contenção (4,48), e frágil no reconhecimento pela alta administração (3,91)	Alinhamento relacional entre segurança e direção como mecanismo de efetividade (Moon; Choi; Armstrong, 2018); apoio da alta administração como fator crítico (Shaheen; Zolait, 2023; Chinyemba; Phiri, 2018; Abdelwahed; Mahmoud; Bdair, 2017); adesão gerencial interage com o técnico (Frاندell; Feeney, 2022)	Benefícios preventivos são estruturalmente difíceis de evidenciar (Dutton <i>et al.</i> , 2019); auditoria interna como canal de tradução (Alhawtmeh, 2025)	Déficit de tradução e alinhamento, mais que de desempenho operacional
Capacidades predizem efetividade (0,627); maturidade autorrelatada, não (0,22 n.s.; índice de privacidade nulo)	Capacidade multidimensional associa-se a desfechos (Dutton <i>et al.</i> , 2019); prontidão como capacidade dinâmica, não estoque	Autoavaliação tem confiabilidade limitada (Dewanto; Oktavia; Sundaram, 2022); adoção declarada supera postura verificável (Ribeiro <i>et</i>	Maturidade mapeia implementação; não deve ser tomada como proxy de resultado

Achado empírico (Capítulo 5)	Convergências na literatura	Tensões e qualificações	Leitura sugerida
	(Mohamed Noor; Moghavvemi; Tajudeen, 2025); efeitos de indicadores agregados são mediados (Krishna; Sebastian, 2021)	<i>al.</i> , 2025); maturidade é útil como diagnóstico (Azambuja; Souza Neto, 2020); PPSI 2.0 inicia a exigência de evidências (Brasil, 2024b, 2025c)	
Privacidade como elo frágil: gestão de dados em 3,17 e maturidade de privacidade sem associação com resultados, mas notificação avança (4,45)	Digitalização corre à frente das práticas de privacidade (Mutimukwe; Kolkowska; Grönlund, 2019); lacuna entre expectativa regulatória e realidade operacional (Ogbodo <i>et al.</i> , 2025); <i>enforcement</i> brando sobre o setor público (Gumzej, 2023)	Privacidade percebida sustenta confiança e uso (Gupta <i>et al.</i> , 2025; Mutimukwe; Kolkowska; Grönlund, 2020; AlAbdali <i>et al.</i> , 2021); fadiga de privacidade erode engajamento (Yang; Mei; Zheng, 2023)	Conformidade episódica avança; a gestão contínua de dados exige instrumentos e incentivos próprios
Recursos como restrição transversal (2,71) e fortemente associados aos resultados (0,553; 0,605 com confiança e percepção)	Restrição financeira como desafio central no setor público local (Hossain <i>et al.</i> , 2025; Frandell; Feeney, 2022); governança condicionada a orçamento (Magnusson <i>et al.</i> , 2025); investimento como preditor de práticas (Al-Hawamleh, 2024)	Externalidades justificam investimento coordenado e apoio central (Paul; Zhang, 2021); estratégias sob escassez: cooperação, terceirização seletiva, código aberto (Hossain <i>et al.</i> , 2025; Domínguez-Dorado <i>et al.</i> , 2023)	A lacuna material requer engenharia financeira da política, não apenas cobrança normativa
Heterogeneidade: fragilidade concentrada em universidades, menor porte e equipes pequenas; 94,8% multicampi	Porte e densidade técnica condicionam capacidade (Hossain <i>et al.</i> , 2025); barreiras interdependentes em universidades (Chahid <i>et al.</i> , 2025); modelos sob medida para o setor (Salam; Abu Bakar; Aman, 2025)	Comprometimento e implementação variam entre instituições do mesmo setor (Šikman <i>et al.</i> , 2025); autopercepção de segurança pode ser ilusória (Khan; Almulhim; Alkati, 2025)	Programa uniforme sobre universo desigual tende a reproduzir desigualdades; apoio diferenciado é necessário
Treinamento associado à conformidade (0,487), não à continuidade (0,145); equipe e treinamento em faixa intermediária	Campanhas centradas em informação, sem evidência de mudança comportamental (Van Steen <i>et al.</i> , 2020); necessidade de segmentação por público (Sittitiamjan; Wuttidittachotti, 2025)	Cultura percebida condiciona adesão (Karlsson <i>et al.</i> , 2022); erro humano tratável por desenho de processos (Evans <i>et al.</i> , 2019; Tran <i>et al.</i> , 2024)	Conscientização deve ser desenhada por comportamento-alvo e medida por efeito, não por alcance

Fonte: Elaboração própria (2026).

Registrem-se, por fim, os limites dessa síntese. O delineamento transversal impede ordenar temporalmente as camadas e o circuito descritos; a medida de efetividade é perceptual e proveniente, em cada IFES, de um único respondente qualificado; a amostra, embora expressiva (52,7% do universo), não permite desagregações robustas; e os estudos do portfólio, produzidos em contextos distintos, sustentam analogias, não generalizações. O modelo em camadas deve ser lido, portanto, como estrutura interpretativa a ser testada por pesquisas longitudinais e por medidas objetivas de resultado, e não como descrição acabada do funcionamento do programa.

6.9 RECOMENDAÇÕES FUNDAMENTADAS PARA A GESTÃO

Em uma dissertação de Mestrado Profissional em Administração Pública, recomendações não são um apêndice retórico, mas parte do compromisso do gênero: traduzir evidência em orientação acionável para a prática. Entende-se, assim, que sua inclusão é pertinente, desde que respeitados dois limites que os próprios dados impõem. As recomendações derivam de associações, e não de relações causais demonstradas, e devem ser lidas como hipóteses de intervenção priorizadas pela evidência, cuja implementação requer adaptação a cada contexto institucional. Elas se organizam em dois planos, o das IFES e o do órgão central do programa, e cada uma se ancora explicitamente em um achado e em seu respaldo na literatura, conforme sistematiza o Quadro 10.

No plano das IFES, cinco linhas de ação emergem dos resultados. A primeira é integrar a gestão de riscos de segurança e privacidade aos instrumentos de planejamento e orçamento, do plano de desenvolvimento institucional à proposta orçamentária, dado que essa integração foi simultaneamente uma das capacidades mais frágeis e a mais correlacionada com a efetividade, o paradoxo dissecado na seção 6.5; a viabilidade de consolidar riscos em estruturas administrativas compostas tem precedentes metodológicos documentados (Le; Phung; Nguyen, 2020; Paul; Zhang, 2021). A segunda é institucionalizar a comunicação executiva de resultados do programa, com relatórios periódicos à alta administração que traduzam não-eventos em linguagem de valor, riscos mitigados, exposição reduzida, conformidade demonstrada, mobilizando canais como a auditoria interna e os comitês de governança, em resposta direta ao elo mais frágil da efetividade percebida

(Alhawtmeh, 2025; Moon; Choi; Armstrong, 2018; Dutton *et al.*, 2019). A terceira é priorizar a visibilidade tecnológica, inventário de ativos, registro e monitoramento proporcionais ao risco, uma vez que a base tecnológica combinou média baixa (3,74) com forte associação à efetividade (0,586), padrão que a seção 4 já identificara na coocorrência entre tecnologia e mitigação de risco. A quarta é converter a privacidade de resposta episódica em função de gestão, com mapeamento de tratamentos priorizado por criticidade, rede de pontos focais nas áreas-fim e metas de gestão de dados pactuadas com a direção (Ogbodo *et al.*, 2025; Mutimukwe; Kolkowska; Grönlund, 2019). A quinta é redesenhar a capacitação por público e por comportamento-alvo, com medição de efeito comportamental e não apenas de alcance (Van Steen *et al.*, 2020; Sittitiamjan; Wuttidittachotti, 2025).

No plano do órgão central, quatro linhas de ação decorrem dos achados. A primeira é complementar os índices de maturidade autorrelatada com indicadores de capacidades institucionais e de efetividade percebida, dado que a maturidade declarada, isoladamente, não acompanhou os resultados, e que a autoavaliação sem verificação tende a superestimar a proteção (Dewanto; Oktavia; Sundaram, 2022; Ribeiro *et al.*, 2025). A segunda é consolidar o movimento iniciado no PPSI 2.0 quanto às evidências, convertendo progressivamente a possibilidade normativa em exigência e agregando verificação amostral, avaliações técnicas externas e auditorias temáticas (Brasil, 2024b, 2025c), o que aproximaria o desenho do programa de iniciativas com acompanhamento ativo, cujo impacto sobre maturidade e resultados está documentado (Shaheen; Zolait, 2023).

No desenho dessa exigência, cabe a separação entre os ambientes de implementação e de verificação, na linha do que consagram os referenciais internacionais: o ecossistema do CIS Controls publica, separadamente das salvaguardas (CIS, 2021), especificação própria do que deve ser medido para verificar sua implementação, operacionalizada em ferramental dedicado de aferição, como o CIS-CAT (CIS, 2025), e a família ISO/IEC dedica normas apartadas ao código de práticas de controles (ISO/IEC 27002) e à sua medição e avaliação (ISO/IEC 27004). A guarda segregada das evidências justifica-se porque evidências de implementação podem detalhar configurações técnicas específicas, elevando a criticidade do ambiente que as concentra junto a autodiagnóstico, plano de trabalho e índices. Cabe, ainda, que a proteção das informações do sistema como um todo seja graduada por análise de risco que distinga suas camadas de granularidade, entre autoavaliação de

medidas, planos de trabalho, índices por controle e índices agregados, em lugar da classificação uniforme calibrada pela informação mais sensível, cujos custos para a avaliação, a coordenação, o controle social e a própria pesquisa sobre o programa foram registrados na seção 3.7. Essa graduação conecta-se diretamente aos achados: a indisponibilidade das camadas agregadas de baixo risco impede a comparabilidade entre instituições, em contraste com os levantamentos públicos de governança conduzidos pelo próprio ecossistema de controle (Brasil, 2024c), e inibe que dirigentes máximos comuniquem resultados mensuráveis do programa, retirando dele um dos poucos incentivos capazes de alcançar o circuito decisório, exatamente onde esta pesquisa localizou o elo mais frágil da efetividade percebida, o reconhecimento pela alta administração, único item abaixo do ponto neutro (3,91).

A terceira é criar trilhas de apoio diferenciadas por porte e segmento, com prioridade para instituições de menor densidade técnica e para as regiões com maior fragilidade relativa, em resposta direta à heterogeneidade identificada (Salam; Abu Bakar; Aman, 2025; Hossain et al., 2025). A quarta é fomentar arranjos cooperativos de escala, centros de operação de segurança compartilhados, contratações conjuntas, reuso de soluções e comunidades de prática entre IFES, estratégia economicamente justificada pelas externalidades positivas do investimento coordenado (Paul; Zhang, 2021) e operacionalmente respaldada pelas experiências de terceirização de amplo escopo e colaboração interinstitucional (Domínguez-Dorado et al., 2023; Hossain et al., 2025).

Quadro 10 – Recomendações, achados e respaldo na literatura

Recomendação	Achado que a fundamenta	Respaldo na literatura
IFES 1. Integrar riscos de segurança e privacidade ao planejamento e ao orçamento (PDI, plano de riscos, proposta orçamentária)	Integração de riscos entre as menores médias (3,05) e com a maior correlação com a efetividade (0,612)	Le, Phung e Nguyen (2020); Paul e Zhang (2021)
IFES 2. Institucionalizar comunicação executiva de resultados (relatórios de valor, auditoria interna, comitês)	Reconhecimento pela alta administração como menor média de efetividade (3,91); circuito recursos-reconhecimento	Alhawtmeh (2025); Moon, Choi e Armstrong (2018); Dutton <i>et al.</i> (2019)
IFES 3. Priorizar visibilidade tecnológica proporcional ao risco (inventário, registro, monitoramento, detecção)	Base tecnológica com média 3,74 e correlação de 0,586 com a efetividade	Coocorrência tecnologia-mitigação do Capítulo 4; Vestad e Yang (2025)

Recomendação	Achado que a fundamenta	Respaldo na literatura
IFES 4. Converter a privacidade em função de gestão contínua (mapeamento priorizado, pontos focais, metas pactuadas)	Gestão de dados com média 3,17 e 63,8% de discordância; maturidade de privacidade sem associação com resultados	Ogbodo <i>et al.</i> (2025); Mutimukwe, Kolkowska e Grönlund (2019)
IFES 5. Redesenhar a capacitação por público e comportamento-alvo, medindo efeito e não alcance	Treinamento com média 3,81, associado à conformidade (0,487) e não à continuidade (0,145)	Van Steen <i>et al.</i> (2020); Sittitiamjan e Wuttidittachotti (2025); Karlsson <i>et al.</i> (2022)
Órgão central 1. Complementar a maturidade autorrelatada com indicadores de capacidade e efetividade	Maturidade sem associação com a efetividade; capacidades como único preditor relevante ($\beta = 0,64$)	Dewanto, Oktavia e Sundaram (2022); Ribeiro <i>et al.</i> (2025)
Órgão central 2. Consolidar a exigência de evidências do PPSI 2.0, com verificação independente amostral, separação entre os ambientes de implementação e de verificação e classificação graduada por análise de risco por camada de granularidade	Limites do modelo declaratório (seção 6.3); classificação uniforme restringiu as camadas agregadas de baixo risco (seção 3.7)	Brasil (2024b, 2024c, 2025c); CIS (2021, 2025); Shaheen e Zolait (2023); Ribeiro <i>et al.</i> (2025)
Órgão central 3. Criar trilhas de apoio diferenciadas por porte, segmento e região	Fragilidade concentrada em instituições menores e equipes reduzidas	Salam, Abu Bakar e Aman (2025); Hossain <i>et al.</i> (2025); Chahid <i>et al.</i> (2025)
Órgão central 4. Fomentar arranjos cooperativos de escala (SOC compartilhado, contratações conjuntas, comunidades de prática)	Recursos como restrição transversal (2,71) fortemente associada aos resultados	Paul e Zhang (2021); Domínguez-Dorado <i>et al.</i> (2023); Hossain <i>et al.</i> (2025)

Fonte: Elaboração própria (2026).

6.10 ANCORAGEM DO PRODUTO TÉCNICO-TECNOLÓGICO

O produto técnico-tecnológico desta dissertação deve transferir seus achados para a prática das organizações estudadas. A discussão desenvolvida nesta seção indica com precisão qual lacuna esse produto deve preencher: o PPSI dispõe de um instrumento consolidado para medir implementação, os índices de maturidade, mas não dispõe de instrumento para avaliar as capacidades institucionais que sustentam o programa nem os resultados que ele produz na percepção de quem o opera, exatamente as dimensões que, nos dados desta pesquisa, distinguem instituições com maior e menor efetividade percebida.

Propõe-se, assim, como produto técnico-tecnológico, o Guia de Avaliação de Capacidades e Efetividade do PPSI nas IFES (GACE-PPSI), instrumento autoaplicável de diagnóstico complementar à medição de maturidade. A caracterização completa do produto (componentes, protocolo de uso, roteiro de

implantação e público-alvo) é apresentada na seção 6.11, na estrutura da proposta contextualizada da Rede PROFIAP.

A ancoragem do produto nos achados é o seu diferencial em relação a guias genéricos de boas práticas, e cada decisão de desenho responde a um resultado da pesquisa:

- a) como a maturidade declarada não acompanhou a efetividade (seção 6.3), o Guia não replica a lógica de checagem de controles, mas mede capacidades e resultados percebidos;
- b) como o gargalo é heterogêneo entre instituições (seções 6.3 e 6.6), o diagnóstico é posicional, comparando a instituição consigo mesma ao longo do tempo e com o padrão agregado das IFES aqui documentado;
- c) como o reconhecimento estratégico é o elo mais frágil da cadeia de valor do programa (seção 6.2), o produto dedica um componente específico à tradução dos resultados para o processo decisório;
- d) como a evidência internacional e o próprio ciclo de aprendizado do PPSI recomendam verificação e acompanhamento em vez de autodeclaração isolada (Dewanto; Oktavia; Sundaram, 2022; Shaheen; Zolait, 2023; Brasil, 2024b), o protocolo prevê o uso do Guia como insumo de conversas estruturadas entre a gestão de segurança, a auditoria interna e os comitês de governança, e não como formulário adicional de conformidade.

Encerrada a discussão, a seção seguinte formaliza a proposta contextualizada do produto técnico-tecnológico, na estrutura preconizada pela Rede PROFIAP; na sequência, as considerações finais retomam os objetivos da pesquisa e as questões norteadoras para apresentar a síntese conclusiva, os limites do estudo e a agenda de pesquisas futuras.

6.11 PROPOSTA CONTEXTUALIZADA DO PRODUTO TÉCNICO-TECNOLÓGICO

Em conformidade com a estrutura de trabalhos de conclusão da Rede PROFIAP, esta seção apresenta a proposta contextualizada do produto técnico-tecnológico (PTT) derivado da pesquisa, sintetizando seu contexto de aplicação, o público-alvo, a situação-problema com a linha de intervenção adotada, o objetivo e a proposta de intervenção. A versão integral da proposta, elaborada no modelo editável

da Rede, constitui o relatório técnico conclusivo que acompanha esta dissertação e cuja entrega aos praticantes-líderes é registrada em protocolo próprio.

6.11.1 Contexto de aplicação da proposta

A administração pública federal brasileira digitalizou a quase totalidade de seus serviços e, com isso, tornou a proteção de dados e a segurança da informação condições de continuidade do próprio serviço público. Nesse cenário, o PPSI, instituído pela Portaria SGD/MGI nº 852/2023 e reformulado pela Portaria SGD/MGI nº 9.511/2025 (PPSI 2.0), passou a orientar os órgãos do SISP por meio de um framework de controles cuja implementação é medida por autodiagnóstico, expresso nos índices iBase, iSeg e iPriv. O Tribunal de Contas da União, ao fiscalizar os primeiros ciclos do programa (Acórdão nº 2.387/2024-Plenário), evidenciou a baixa maturidade agregada do sistema e a necessidade de sustentar as autoavaliações em evidências (Brasil, 2024b).

A proposta insere-se nesse tempo social e no espaço institucional específico das 110 IFES: organizações que custodiam dados pessoais de milhões de estudantes, servidores e pesquisadores, operam estruturas multicampi de alta complexidade e executam o mandato nacional do PPSI com orçamentos discricionários comprimidos e equipes de TI de porte muito variável. A pesquisa que origina o produto avaliou nacionalmente a efetividade do programa nesse universo e constatou que a régua oficial de maturidade não capta as dimensões que efetivamente distinguem as instituições com melhores resultados.

A proposição alinha-se aos Objetivos de Desenvolvimento Sustentável (ODS) da ONU, em especial ao ODS 16 (paz, justiça e instituições eficazes), metas 16.6, desenvolver instituições eficazes, responsáveis e transparentes, e 16.10, proteger liberdades fundamentais e o acesso à informação, e, de forma complementar, ao ODS 9 (infraestrutura resiliente e inovação) e ao ODS 4, ao contribuir para a continuidade e a confiabilidade dos serviços digitais que sustentam a educação superior pública.

6.11.2 Público-alvo da proposta

O produto destina-se aos praticantes-líderes que respondem pelo PPSI dentro de cada IFES: o gestor de segurança da informação, o encarregado pelo tratamento de dados pessoais e o dirigente de tecnologia da informação, atuando junto às

instâncias de governança a que se reportam, como o comitê de segurança da informação e privacidade e o comitê de governança digital. São atores que reúnem, simultaneamente, a competência técnica para aplicar o instrumento e a autonomia institucional para converter o diagnóstico em pauta de comitê, proposta orçamentária e comunicação à alta administração, exatamente os usos para os quais o aplicativo foi desenhado.

Em plano secundário, o produto interessa à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, órgão central do PPSI, para a qual a aplicação agregada do instrumento pode compor um painel complementar aos índices de maturidade, e às redes de colaboração entre IFES, que podem adotá-lo como linguagem comum de diagnóstico. Por essa razão, o relatório técnico que formaliza esta proposta é redigido na linguagem do gestor, e não na do pesquisador. Cada elemento do produto responde a uma tarefa concreta de quem administra o programa na ponta.

6.11.3 Situação-problema: diagnóstico, análise e linha de intervenção

O diagnóstico que fundamenta a proposta resulta da pesquisa nacional apresentada nas seções 4 e 5, conduzida com 58 IFES (52,7% do universo) por meio de instrumento derivado de revisão sistemática de 82 estudos e validado em conteúdo por painel de especialistas. Três achados desenharam a situação-problema.

Primeiro, a implementação do PPSI nas IFES avança em camadas desiguais. A governança formal do programa (papéis, comitês e instâncias) é a capacidade mais consolidada (média 4,72 em escala de sete pontos), enquanto a sustentação material e integrativa é a mais frágil: recursos orçamentários e contratuais em 2,71, integração da gestão de riscos ao planejamento e ao orçamento em 3,05 e gestão de dados pessoais em 3,17. O programa institucionalizou-se no papel antes de se converter em capacidade operante, comportamento típico de políticas induzidas por norma, nas quais a adoção formal corre à frente da institucionalização real.

Segundo, a efetividade percebida concentra-se na operação e não alcança o núcleo decisório. Os respondentes reconhecem ganhos em detecção (4,59) e em contenção e recuperação de incidentes (4,48), mas o reconhecimento de ganhos institucionais pela alta administração é o item mais frágil de todo o bloco (3,91), o único abaixo do ponto neutro. Sem métricas que traduzam riscos evitados em

linguagem de valor, o principal produto da segurança bem-sucedida, o incidente que não ocorreu, permanece invisível para quem decide orçamento e prioridade.

Terceiro, e central para a linha de intervenção, a maturidade declarada não acompanha os resultados. O conjunto das capacidades institucionais correlacionou-se de forma expressiva com a efetividade percebida ($p = 0,627$), ao passo que os índices oficiais de maturidade não apresentaram associação estatisticamente significativa com ela, e o índice de privacidade mostrou correlação praticamente nula. A capacidade mais associada à efetividade (a gestão de riscos integrada ao planejamento, $p = 0,612$) é justamente uma das menos desenvolvidas. Em síntese, as IFES medem o que implementaram, mas não dispõem de instrumento para medir as capacidades que sustentam o programa nem os resultados que ele produz — e é nesse vazio de mensuração que a efetividade se perde entre a operação técnica e a decisão institucional.

A análise desses achados à luz da literatura internacional e do quadro normativo converge para o mesmo ponto. Estudos sobre governança de segurança no setor público mostram que a adesão a frameworks convive com escassez de indicadores e verificação; a evidência sobre autoavaliações governamentais indica que a adoção declarada tende a superestimar a postura efetiva, limitação reconhecida pelo próprio ecossistema do PPSI, que a partir da versão 2.0 passou a prever campo de evidências; e a pesquisa comparada demonstra que resultados de segurança acompanham capacidades multidimensionais, e não estoques declarados de controles.

Entre as linhas de intervenção possíveis (propor novo normativo ao órgão central, contratar consultorias externas de avaliação ou aguardar a evolução do próprio programa), escolheu-se a que atua diretamente sobre o elo que o diagnóstico revelou mais frágil e que está ao alcance imediato do praticante, a de dotar cada IFES de um instrumento de autodiagnóstico complementar, que mede capacidades e efetividade percebida, compara a instituição ao padrão nacional, prioriza o desenvolvimento de capacidades pela evidência empírica e traduz o resultado em relatório executivo para a alta administração. É uma intervenção de baixo custo, implementável sem autorização externa, que respeita a autonomia institucional e produz efeito onde a pesquisa localizou o gargalo: na mensuração e no reconhecimento.

6.11.4 Objetivo da proposta

O objetivo da proposta é disponibilizar aos responsáveis pelo PPSI nas IFES um instrumento autoaplicável, gratuito e de execução local que avalie, anualmente, as capacidades institucionais que sustentam o programa e a efetividade percebida que ele produz, convertendo essa avaliação em três entregas de gestão: o posicionamento da instituição frente ao padrão nacional das 58 IFES pesquisadas; a priorização fundamentada das capacidades a desenvolver, ordenada pelas associações empíricas observadas na pesquisa; e o relatório executivo que traduz o diagnóstico em linguagem de valor institucional para apresentação à alta administração.

De forma específica, o produto materializa a linha de intervenção ao mensurar as oito capacidades e os dez itens de efetividade do instrumento validado; posicionar os resultados na leitura em camadas do modelo interpretativo da dissertação, identificando o gargalo específico de cada instituição em vez de presumir uma hierarquia universal de carências; orientar a decisão com recomendações vinculadas a cada capacidade frágil; institucionalizar a comparação entre ciclos anuais, por meio da exportação e importação de avaliações; e preservar a confidencialidade institucional, uma vez que nenhum dado sai do computador do gestor.

6.11.5 A proposta de intervenção: o GACE-PPSI

O produto é o GACE-PPSI, software na categoria aplicativo (programa de computador), uma das doze possibilidades admitidas pela CAPES para a Área 27 (CAPES, 2019). O documento completo do Produto Técnico-Tecnológico, no modelo preconizado pela Rede PROFIAP, é apresentado no Apêndice D. Trata-se de aplicação web contida em um único arquivo, aberto diretamente no navegador, sem instalação, sem servidor, sem custo e sem transmissão de dados: as respostas permanecem na máquina da instituição, decisão de arquitetura coerente com o objeto do programa que o produto avalia. O código-fonte é aberto, auditável e de livre adaptação pelo setor público, com atribuição.

O aplicativo organiza-se em seis folhas. A primeira apresenta o protocolo de uso: respondente qualificado (o principal responsável pelo PPSI ou ator diretamente envolvido), aplicação anual antes do ciclo de planejamento e orçamento, e emprego do resultado como insumo de conversas estruturadas com a auditoria interna e os comitês. A segunda registra, apenas localmente, a identificação institucional. A

terceira e a quarta aplicam os dezoito itens validados, oito de capacidades e dez de efetividade, em escala de sete pontos. A quinta entrega o diagnóstico: escores comparados ao padrão nacional, leitura em camadas, prioridades calculadas pela combinação entre a fragilidade do escore e a associação de cada capacidade com a efetividade e, quando houver avaliação anterior importada, a evolução entre ciclos. A sexta documenta método, origem, limites e forma de citação. O relatório executivo, gerado em uma página para impressão ou PDF, encerra o ciclo de uso levando o diagnóstico à mesa da alta administração.

O roteiro de implantação pelo praticante-líder tem quatro passos e cabe em uma manhã de trabalho: abrir o arquivo e responder ao instrumento; validar o diagnóstico com a equipe e o comitê; apresentar o relatório executivo à alta administração, preferencialmente junto à proposta orçamentária; e arquivar a exportação da avaliação para comparação no ciclo seguinte. Não há pré-requisitos técnicos além de um navegador moderno, nem dependência de fornecedores, redes ou autorizações externas.

Quanto aos atributos qualificadores previstos pela Rede, a proposta caracteriza-se pelo impacto potencial imediato sobre as 110 IFES e, por extensão, sobre os demais órgãos do SISP, ao converter diagnóstico em priorização de investimentos e em comunicação qualificada com a alta administração; pela aplicabilidade imediata e de custo zero, com replicabilidade a outros órgãos mediante recalibração do padrão de referência; pela inovação de constituir, até onde a pesquisa pôde apurar, o primeiro instrumento de avaliação orientado a capacidades e efetividade percebida construído especificamente para o PPSI, com régua interpretativa calibrada por evidência empírica nacional; e pela complexidade da cadeia que o sustenta (revisão sistemática, derivação da matriz de domínios, validação por especialistas, aplicação nacional, modelo interpretativo em camadas e algoritmo de priorização), documentada nas seções 3 a 6 desta dissertação.

7 CONSIDERAÇÕES FINAIS

Esta dissertação partiu de uma pergunta avaliativa situada no encontro entre a política pública digital e a gestão universitária: como a implementação do Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior se traduz em efetividade, em termos de desempenho organizacional e valor público? Para respondê-la, o estudo percorreu um encadeamento deliberado: a revisão sistemática de 82 estudos consolidou os domínios de capacidade e de efetividade empregados pela literatura internacional (seção 4); esses domínios foram operacionalizados em um instrumento de 18 itens, submetido a validação de conteúdo por 11 especialistas e aplicado a todo o universo de IFES, com 58 respostas institucionais válidas, correspondentes a 52,7% do universo (seção 5); os resultados foram, por fim, confrontados com o portfólio da revisão e traduzidos em recomendações e em um produto técnico-tecnológico (seção 6).

A resposta ao problema central pode ser enunciada de forma direta: a implementação do PPSI não se traduz em efetividade de maneira automática. A tradução ocorre, e é empiricamente observável, quando a estruturação formal do programa se converte em capacidades institucionais operantes. Três resultados sustentam essa conclusão. Primeiro, a maturidade autorrelatada associou-se positivamente às capacidades institucionais ($p = 0,41$; $p < 0,01$), mas não apresentou associação estatisticamente significativa com a efetividade percebida ($p = 0,22$; n.s.). Segundo, as capacidades institucionais associaram-se de forma consistente à efetividade percebida ($p = 0,627$; $p < 0,001$), padrão confirmado nos modelos exploratórios de regressão ($\beta = 0,61$; $R^2 = 0,374$). Terceiro, no modelo conjunto, a capacidade total permaneceu associada à efetividade ($\beta = 0,64$; $p < 0,001$), enquanto a maturidade perdeu qualquer poder explicativo ($\beta = -0,08$; n.s.). Em síntese, maturidade declarada não é efetividade; capacidades são o elo que conecta uma à outra.

Em relação à primeira questão norteadora, as capacidades que mais se associaram à efetividade percebida foram a integração da gestão de riscos ao planejamento e ao orçamento institucional (C6; $p = 0,612$), a base tecnológica de monitoramento, detecção e resposta (C4; $p = 0,586$), a suficiência de recursos orçamentários e contratuais (C8; $p = 0,553$) e os processos executados e testados regularmente (C3; $p = 0,479$). O achado carrega um paradoxo relevante para a gestão:

as capacidades com maior potencial de conversão em resultados estão entre as menos desenvolvidas nas IFES. C6 obteve média 3,05 e C8, a menor do instrumento, 2,71. É precisamente nessa distância entre potencial e desenvolvimento que residem as apostas de maior retorno institucional, base das recomendações formuladas na seção 6.

Quanto à segunda questão, os recortes exploratórios indicaram que capacidades e efetividade não se distribuem de maneira uniforme entre contextos institucionais. A fragilidade de governança concentrou-se em instituições de menor porte administrativo e com equipes de TI reduzidas; entre as universidades federais, 32,4% avaliaram a governança abaixo do ponto neutro, proporção superior à observada nos institutos federais. A condição multicampi, presente em 94,8% da amostra, opera como multiplicador de complexidade de coordenação. O recorte por suficiência de recursos foi o mais ilustrativo: instituições com avaliação favorável em C8 apresentaram efetividade percebida sistematicamente superior, com diferenças mais expressivas justamente nas dimensões de confiança e reconhecimento estratégico (E9 e E10). Esses contrastes devem ser lidos como exploratórios, mas delineiam com nitidez a heterogeneidade que qualquer política uniforme de segurança e privacidade encontrará no sistema federal de ensino superior.

O objetivo geral, avaliar a efetividade percebida do PPSI nas IFES e identificar as capacidades institucionais que mais se associam a esses resultados, foi atendido pelo conjunto das seções 4 a 6, nos termos sintetizados acima. O primeiro objetivo específico foi cumprido pela revisão sistemática, que delimitou seis domínios de capacidade e seis de efetividade recorrentes na literatura sobre segurança e privacidade no setor público, verificando sua operacionalização e coocorrência. O segundo foi cumprido com a construção do instrumento de 18 itens e sua validação de conteúdo pelo método de Lawshe, com retenção de 13 itens na primeira rodada, refinamento qualitativo e rodada complementar dos cinco itens restantes, e posterior confirmação da consistência interna dos blocos ($\alpha = 0,84$ e $\omega = 0,84$ para capacidades; $\alpha = 0,93$ e $\omega = 0,93$ para efetividade). O terceiro objetivo foi atendido pela pesquisa de campo com 58 IFES e pelas análises descritivas, correlacionais e de regressão da seção 5. O quarto materializou-se nas cinco linhas de ação propostas às IFES, nas quatro dirigidas ao órgão central e no produto técnico-tecnológico ancorado nos achados (seção 6, subseções 6.9 a 6.11, e Apêndice D).

As contribuições da pesquisa podem ser lidas em quatro planos. No plano teórico, o estudo oferece evidência empírica, em contexto brasileiro, para a distinção entre maturidade declarada, capacidades institucionais e efetividade percebida, tríade que a literatura internacional vinha tratando de modo fragmentado, e a organiza em um modelo interpretativo em camadas: institucionalização formal, execução sociotécnica e sustentação material, atravessadas por um circuito de reconhecimento e recursos. No plano metodológico, entrega um instrumento curto, validado e replicável, capaz de capturar dimensões que os índices de conformidade não alcançam, ao custo de poucos minutos de resposta. No plano gerencial, próprio de um Mestrado Profissional em Administração Pública, converte os achados em recomendações acionáveis e no Guia de Avaliação de Capacidades e Efetividade do PPSI nas IFES (GACE-PPSI), instrumento autoaplicável de diagnóstico que posiciona cada instituição nas camadas do modelo e orienta a priorização de investimentos. No plano da política pública, sugere ao órgão central um aperfeiçoamento concreto do ciclo avaliativo do PPSI: complementar os índices declaratórios de maturidade com indicadores de capacidade e de resultado, deslocando o foco do quanto foi implementado para o que a implementação produz.

Os limites do estudo foram reiterados ao longo das seções e devem balizar a leitura das conclusões. O delineamento é transversal, o que impede ordenar temporalmente maturidade, capacidades e efetividade ou sustentar inferências causais; as associações reportadas são compatíveis com o encadeamento teórico proposto, mas não o demonstram. A efetividade foi mensurada por percepção qualificada de um respondente institucional por IFES, estratégia que assegura conhecimento direto do programa, mas expõe os resultados a vieses de método comum e de desejabilidade. Os índices iBase, iSeg e iPriv foram autorrelatados, com casos ausentes ou inválidos, em coleta anterior à classificação das informações do programa, e não puderam ser confrontados com os registros administrativos do órgão central, cujo acesso não foi concedido à pesquisa. A cobertura de 52,7% do universo, embora expressiva para levantamentos institucionais, não afasta viés de não resposta, pois é plausível que instituições menos estruturadas estejam sub-representadas. Por fim, a pesquisa não permite estimar efeitos de controles ou medidas individuais do PPSI: a unidade analítica são capacidades e resultados agregados, e os recortes contextuais têm natureza exploratória.

Como agenda de pesquisas futuras, cinco desdobramentos decorrem diretamente deste trabalho. Primeiro, um desenho longitudinal que acompanhe os ciclos anuais do PPSI, permitindo observar a dinâmica temporal entre maturidade, capacidades e efetividade, inclusive com a aplicação periódica do instrumento aqui validado. Segundo, a articulação com dados administrativos oficiais do órgão central, substituindo o autorrelato dos índices e viabilizando a triangulação originalmente idealizada, o que pressupõe a revisão do regime de acesso aos índices agregados. Terceiro, a validação estrutural do instrumento com amostras maiores ou acumuladas entre ciclos, incluindo análise fatorial confirmatória e, quando o tamanho da base permitir, modelagem de equações estruturais. Quarto, estudos qualitativos de mecanismo, examinando como a gestão de riscos entra, ou deixa de entrar, no planejamento e no orçamento das IFES e como resultados operacionais são traduzidos em linguagem de valor para a alta administração. Quinto, a extensão do desenho a outros segmentos do SISP, testando a transferibilidade do modelo em camadas para além do ensino superior, e a avaliação de adoção e efeitos do próprio GACE-PPSI.

Ao fim do percurso, a conclusão que esta dissertação oferece à Administração Pública é menos uma sentença sobre o PPSI e mais um deslocamento de olhar: a efetividade de uma política de segurança da informação e privacidade não se decide nos formulários de conformidade, mas na capacidade concreta das instituições de transformar mandatos em rotinas, riscos em decisões orçamentárias e proteção de dados em confiança. Nas IFES, que guardam dados de milhões de estudantes, servidores e pesquisas, essa conversão é condição de legitimidade da própria universidade pública digital. Medi-la, como aqui se propôs, é o primeiro passo para governá-la.

REFERÊNCIAS

- ABDELWAHED, A. S.; MAHMOUD, A. Y.; BDAIR, R. A. Information security policies and their relationship with the effectiveness of the management information systems of major Palestinian universities in the Gaza Strip. **International Journal of Information Science and Management**, v. 15, n. 1, p. 1-26, 2017. Disponível em: https://ijism.isc.ac/article_698242.html. Acesso em: 06 out. 2025.
- AGASHE, N.; GHOSE, A. Introspecting the Digital Dynamics: Reconnecting the Interplay between Privacy, Surveillance, and Governance in the Global Landscape, with a Special Focus on India. **Braz. J. Pub. Pol'y**, v. 14, p. 377, 2024. DOI: <https://doi.org/10.5102/rbpp.v14i2.9408>. Acesso em: 06 out. 2025.
- ALABDALI, H. et al. Privacy Preservation Instruments influencing the trustworthiness of e-government services. **Computers**, v. 10, n. 9, p. 114, 2021. DOI: <https://doi.org/10.3390/computers10090114>. Acesso em: 06 out. 2025.
- ALEXEI, A.; ALEXEI, A. The difference between cyber security vs information security. **Journal of Engineering Science**, v. 29, n. 4, p. 72–83, 2022. [https://doi.org/10.52326/jes.utm.2022.29\(4\).08](https://doi.org/10.52326/jes.utm.2022.29(4).08). Acesso em: 10 jul. 2025.
- AL-HAWAMLEH, A. M. Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. **Digital Policy, Regulation and Governance**, v. 26, n. 3, p. 317-336, 2024. DOI: <https://doi.org/10.1108/DPRG-11-2023-0168>. Acesso em: 06 out. 2025.
- ALHAWTMEH, O. M. The role of internal audit as a tool for enhancing cybersecurity effectiveness in Jordanian government agencies. **Heritage and Sustainable Development**, v. 7, n. 1, p. 317-328, 2025. DOI: <https://doi.org/10.37868/hsd.v7i1.1130>. Acesso em: 06 out. 2025.
- ALVES, G. F.; SANTOS, C. D. dos. The diffusion of innovations under normative induction in Brazil. **RAUSP Management Journal**, v. 57, n. 2, p. 149-164, 2022. DOI: <https://doi.org/10.1108/RAUSP-10-2020-0250>. Acesso em: 06 out. 2025.
- ARAÚJO NETO, A. C. de. Política de segurança da informação nas universidades: teoria e prática. In: Workshop de Tecnologia da Informação e Comunicação das Instituições Federais de Ensino Superior, 10., 2016, Gramado. Anais [...]. Gramado: [s.n.], 2016. Disponível em: <https://lume.ufrgs.br/handle/10183/142252>. Acesso em: 10 jul. 2025.
- 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.
- ASSOCIAÇÃO NACIONAL DOS DIRIGENTES DAS INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR (ANDIFES). **Brasil tem 69 universidades federais; conheça cada uma**. Brasília, DF: Andifes, 2025. Disponível em:

<https://www.andifes.org.br/2025/01/16/brasil-tem-69-universidades-federais-conheca-cada-uma/>. Acesso em: 24 jul. 2026.

AZAMBUJA, A. J.; SOUZA NETO, J. Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal. **Revista do Serviço Público**, v. 71, n. 3, p. 660-712, 2020. DOI: <https://doi.org/10.21874/rsp.v71i3.3210>. Acesso em: 06 out. 2025.

BERENGUER, G. Modeling approaches and metrics to evaluate nonprofit operations. In: ZOBEL, C.; ALTAY, N.; HASELKORN, M. (org.). **Advances in managing humanitarian operations**. Cham: Springer International Publishing, 2016. p. 9–31. DOI: https://doi.org/10.1007/978-3-319-24418-1_2. Acesso em: 10 nov. 2024.

BORGMAN, B.; MUBARAK, S.; CHOO, K.-K. R. Cyber security readiness in the South Australian Government. **Computer Standards & Interfaces**, v. 37, p. 1-8, 2015. DOI: <https://doi.org/10.1016/j.csi.2014.06.002>. Acesso em: 06 out. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações [...]. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 19 set. 2026.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. Brasília, DF, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 07 set. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre o tratamento de dados pessoais [...]. Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 set. 2025.

BRASIL. Ministério da Educação. **Instituições da Rede Federal**. Brasília, DF: MEC, 2019. Disponível em: <http://portal.mec.gov.br/rede-federal-inicial/instituicoes>. Acesso em: 24 jul. 2026.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Estratégia de Governo Digital 2020–2022. Brasília, DF, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm. Acesso em: 07 set. 2025.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital. Brasília, DF, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 07 set. 2025.

BRASIL. Tribunal de Contas da União. **Lista de alto risco na administração pública federal**. 1. ed. Brasília: TCU, 2022. Disponível em: <https://sites.tcu.gov.br/listadealtorisco2022/>. Acesso em: 24 jul. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia do Framework de Privacidade e Segurança da Informação**. Brasília, DF: Secretaria de Governo Digital, 2023a. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework>. Acesso em: 03 out. 2024.

BRASIL. **Portaria SGD/MGI nº 852, de 28 de março de 2023**. Institui o Programa de Privacidade e Segurança da Informação – PPSI. Brasília, DF, 2023b. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908>. Acesso em: 07 set. 2025.

BRASIL. **Decreto nº 12.198, de 24 de setembro de 2024**. Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Diário Oficial da União: Seção 1, Brasília, DF, 25 set. 2024a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12198.htm. Acesso em: 20 ago. 2025.

BRASIL. Tribunal de Contas da União. Acórdão nº 2.387/2024 – TCU – Plenário. Processo TC 010.390/2024-3. Relator: Ministro Augusto Nardes. Sessão de 6 de novembro de 2024. Brasília, DF: TCU, 2024b. Disponível em: <https://pesquisa.apps.tcu.gov.br/doc/acordao-completo/2387/2024/Plen%C3%A1rio>. Acesso em: 26 jul. 2026.

BRASIL. Tribunal de Contas da União. **Levantamento iESGo 2024: relatório de levantamento**. Brasília, DF: TCU, 2024c. Disponível em: https://iesgo.tcu.gov.br/wp-content/uploads/sites/12/iesgo2024/iESGo2024_Relatorio_tecnico.pdf. Acesso em: 24 jul. 2026.

BRASIL. **Decreto nº 12.572, de 4 de agosto de 2025**. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. Diário Oficial da União: Seção 1, Brasília, DF, 5 ago. 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12572.htm. Acesso em: 26 jul. 2026.

BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança. Diário Oficial da União: Seção 1, Brasília, DF, 5 ago. 2025b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 20 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. Institui o Programa de Privacidade e Segurança da Informação (PPSI 2.0). Diário Oficial da União: seção 1, Brasília, DF, ed. 208, p. 91, 31 out. 2025c. Disponível em: <https://www.in.gov.br/web/dou/-/>

/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 26 jul. 2026.

BRYSON, J. M.; CROSBY, B. C.; BLOOMBERG, L. Public value governance: moving beyond traditional public administration and the new public management. **Public Administration Review**, v. 74, n. 4, p. 445–456, 2014. DOI: <https://doi.org/10.1111/puar.12238>. Acesso em: 06 de out. 2025.

CARVALHO, D. S.; CASTRO, P. A. de; FERNANDES-SOBRINHO, M. Políticas públicas na era do governo digital: revisão de literatura. **Revista GeTeC: Gestão, Tecnologia e Ciências**, v. 20, p. 169-188, 2024. Disponível em: <https://www.revistas.fucamp.edu.br/index.php/getec/article/view/3681>. Acesso em: 13 jul. 2026.

CAVALCANTE, P.; LOTTA, G. **Burocracia de médio escalão**: perfil, trajetória e atuação. Brasília, DF: ENAP, 2015. URI: <http://repositorio.enap.gov.br/handle/1/2063>. Acesso em: 13 jul. 2026.

CENTER FOR INTERNET SECURITY. **CIS Controls v8**. East Greenbush, NY: CIS, 2021. Disponível em: <https://www.cisecurity.org>. Acesso em: 24 nov. 2024.

CENTER FOR INTERNET SECURITY. CIS Controls Assessment Specification: for CIS Controls v8. Versão 2025 Q1. East Greenbush, NY: CIS, 2025. Disponível em: <https://cas8.docs.cisecurity.org>. Acesso em: 25 jul. 2026.

CEPIK, M. A. C.; CANABARRO, D. R.; POSSAMAI, A. J. Do novo gerencialismo público à governança na era digital. In: CEPIK, M. A. C.; CANABARRO, D. R. (org.). **Governança de TI**: transformando a administração pública no Brasil. Porto Alegre: UFRGS, 2014. p. 11–26. URI: <http://hdl.handle.net/10183/79095>. Acesso em: 13 jul. 2026.

CHAHID, A.; AHRIZ, S.; EL GUEMMAT, K.; MANSOURI, K. Digital transformation in higher education: obstacle assessment and development of strategies against cybersecurity threats. **Engineering, Technology & Applied Science Research**, v. 15, n. 1, p. 19809-19815, 2025. DOI: <https://doi.org/10.48084/etasr.8853>. Acesso em: 06 de out. 2025.

CHENG, E. C. K.; WANG, T. Institutional strategies for cybersecurity in higher education institutions. **Information**, v. 13, n. 4, p. 192, 2022. DOI: <https://doi.org/10.3390/info13040192>. Acesso em: 06 de out. 2025.

CHINYEMBA, M. K.; PHIRI, J. An investigation into information security threats from insiders and how to mitigate them: a case study of Zambian public sector. **Journal of Computer Science**, v. 14, n. 10, p. 1389-1400, 2018. DOI: <https://doi.org/10.3844/jcssp.2018.1389.1400>. Acesso em: 06 de out. 2025.

CHORNA, V.; BOHDAN, B.; GAPONOV, O. Development of cybersecurity of critical infrastructure in the conditions of digitalization: economic tools for risks and investments assessment. **Baltic Journal of Economic Studies**, v. 11, n. 3, p. 330–

338, 2025. DOI: <https://doi.org/10.30525/2256-0742/2025-11-3-330-338>. Acesso em: 06 de out. 2025.

CHOUDHARY, S. K.; KAR, A. K. Modeling the role of generative AI in organizational privacy and security. **Decision Support Systems**, v. 196, art. 114500, 2025. DOI: <https://doi.org/10.1016/j.dss.2025.114500>. Acesso em: 06 de out. 2025.

COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR (CAPES). **Documento de área — Área 27: Administração Pública e de Empresas, Ciências Contábeis e Turismo**. Brasília, DF: CAPES, 2019. Disponível em: <https://www.gov.br/capes/pt-br/centrais-de-conteudo/adm-pdf>. Acesso em: 26 jul. 2026.

CRONBACH, L. J. Coefficient alpha and the internal structure of tests. **Psychometrika**, v. 16, n. 3, p. 297–334, 1951. DOI: <https://doi.org/10.1007/BF02310555>. Acesso em: 06 de out. 2025.

CULOT, G. et al. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. **The TQM Journal**, v. 33, n. 7, p. 76–105, 2021. DOI: <https://doi.org/10.1108/TQM-09-2020-0202>. Acesso em: 06 de out. 2025.

DEDEKE, A.; MASTERSON, K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. **Information and Computer Security**, v. 27, n. 3, p. 373–392, 2019. DOI: <https://doi.org/10.1108/ICS-10-2018-0122>. Acesso em: 06 de out. 2025.

DE HAES, S.; VAN GREMBERGEN, W. IT governance structures, processes and relational mechanisms: achieving IT/business alignment in a major Belgian financial group. In: Hawaii International Conference on System Sciences, 38., 2005, Honolulu. Proceedings [...]. Honolulu: IEEE, 2005. p. 237b–237b. DOI: <https://doi.org/10.1109/HICSS.2005.362>. Acesso em: 20 de nov. 2024.

DE HAES, S.; VAN GREMBERGEN, W. An exploratory study into IT governance implementations and its impact on business/IT alignment. **Information Systems Management**, v. 26, n. 2, p. 123–137, 2009. DOI: <https://doi.org/10.1080/10580530902794786>. Acesso em: 20 de nov. 2024.

DEWANTO, M. R. P.; OKTAVIA, T.; SUNDARAM, D. Comparative study of information security evaluation models for Indonesia government. **Journal of Theoretical and Applied Information Technology**, v. 100, n. 4, 2022. Disponível em: <https://www.jatit.org/volumes/Vol100No4/1Vol100No4.pdf>. Acesso em: 06 de out. 2025.

DINIZ, E. H.; BARBOSA, A. F.; JUNQUEIRA, A. R. B.; PRADO, O. O governo eletrônico no Brasil: perspectiva histórica a partir de um modelo estruturado de análise. **Revista de Administração Pública**, v. 43, n. 1, p. 23-48, 2009. DOI: <https://doi.org/10.1590/S0034-76122009000100003>. Acesso em: 06 de out. 2025.

DOMÍNGUEZ-DORADO, M. et al. Boosting holistic cybersecurity awareness with outsourced wide-scope CyberSOC: a generalization from a Spanish public organization study. **Information**, v. 14, n. 11, art. 586, 2023. DOI: <https://doi.org/10.3390/info14110586>. Acesso em: 06 de out. 2025.

DUNLEAVY, P.; MARGETTS, H. Data science, artificial intelligence and the third wave of digital era governance. **Public Policy and Administration**, v. 40, n. 2, p. 185–214, 2023. DOI: <https://doi.org/10.1177/09520767231198737>. Acesso em: 06 de out. 2025.

DUTTON, W. H. et al. Cybersecurity capacity: does it matter? **Journal of Information Policy**, v. 9, p. 280-306, 2019. DOI: <https://doi.org/10.5325/jinfopoli.9.2019.0280>. Acesso em: 06 de out. 2025.

ENDERS, C. K. **Applied missing data analysis**. New York: Guilford Press, 2010.

ESWARAN, R.; VINAYAGAMOORTHY, G. Cyber security and information security. **International Journal of Recent Technology and Engineering**, v. 8, n. 3, p. 372–374, 2019. DOI: <https://doi.org/10.35940/IJRTE.C1079.1083S19>. Acesso em: 06 de out. 2025.

EUROPEAN UNION. **Tallinn Declaration on eGovernment**: at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017. Brussels: European Commission, 2017. Disponível em: <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>. Acesso em: 23 set. 2025.

EUROPEAN UNION. **Berlin Declaration on Digital Society and Value-Based Digital Government**: at the ministerial meeting during the German Presidency of the Council of the EU on 8 December 2020. Brussels: European Commission, 2020. Disponível em: <https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government>. Acesso em: 26 jul. 2026.

EVANS, M. et al. Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. **International journal of medical informatics**, v. 127, p. 109-119, 2019. DOI: <https://doi.org/10.1016/j.ijmedinf.2019.04.019>. Acesso em: 06 de out. 2025.

FRANDELL, A.; FEENEY, M. K. Cybersecurity threats in local government: a sociotechnical perspective. **The American Review of Public Administration**, v. 52, n. 8, p. 558-572, 2022. DOI: <https://doi.org/10.1177/02750740221125432>. Acesso em: 06 de out. 2025.

GOMIDE, A. de Á.; PIRES, R. R. C. Capacidades estatais e democracia: a abordagem do Ipea. In: GOMIDE, A. de Á.; PIRES, R. R. C. (org.). **Capacidades estatais e democracia**: arranjos institucionais de políticas públicas. Brasília, DF: Ipea, 2014. p. 13–34. URL: <http://repositorio.ipea.gov.br/handle/11058/3098> Acesso em: 13 jul. 2026.

GREEN, A. W. et al. Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems. **Communications of the Association for Information Systems**, v. 46, 2020. DOI: <https://doi.org/10.17705/1CAIS.04608>. Acesso em: 06 de out. 2025.

GUMZEJ, N. DPA powers toward effective and transparent GDPR enforcement: the case of Croatia. **Tribuna Juridică**, v. 13, n. 2, p. 192-223, 2023. DOI: <https://doi.org/10.24818/tbj/2023/13/2.03>. Acesso em: 06 de out. 2025.

GUPTA, P. et al. Trust, risk, privacy and security in e-Government use: Insights from a MASEM analysis. **Information Systems Frontiers**, v. 27, n. 3, p. 1089-1105, 2025. DOI: <https://doi.org/10.1007/s10796-024-10497-8>. Acesso em: 06 de out. 2025.

HAIR, J. F.; BLACK, W. C.; BABIN, B. J.; ANDERSON, R. E. **Multivariate Data Analysis**. 8. ed. Boston: Cengage, 2019. ISBN: 978-1-4737-5654-0.

HAIR, J. F.; HULT, G. T. M.; RINGLE, C. M.; SARSTEDT, M. **A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)**. 3. ed. Thousand Oaks: Sage, 2021. ISBN: 978-1-5443-9640-8.

HAYES, A. F. **Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach**. 2. ed. New York: Guilford Press, 2018. ISBN: 9781462534654.

HOSSAIN, S. T. et al. **Understanding local government cybersecurity policy: A concept map and framework**. *Information*, v. 15, n. 6, p. 342, 2024. DOI: <https://doi.org/10.3390/info15060342>. Acesso em: 06 de out. 2025.

HOSSAIN, S. T. et al. Cybersecurity in local governments: a systematic review and framework of key challenges. **Urban Governance**, v. 5, n. 1, p. 1-19, 2025. DOI: <https://doi.org/10.1016/j.ugj.2024.12.010>. Acesso em: 06 de out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 31000:2018** – Risk management – Guidelines. Geneva: ISO, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 22301:2019** – Security and resilience – Business continuity management systems – Requirements. Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 38500:2024** – Information technology — Governance of IT for the organization. Geneva: ISO, 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 29100:2011** — Information technology — Security techniques — Privacy framework. Geneva: ISO, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27004:2016** — Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. Geneva: ISO, 2016.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 29151:2017** — Information technology — Security techniques — Code of practice for personally identifiable information protection. Geneva: ISO, 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27000:2018** — Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001:2022** — Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27002:2022** — Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27005:2022** — Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27032:2023** — Cybersecurity — Guidelines for internet security. Geneva: ISO, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27035-1:2023** — **Information technology — Information security incident management — Part 1: Principles and process**. Geneva: ISO, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 29134:2023** — Information technology — Security techniques — Guidelines for privacy impact assessment. Geneva: ISO, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 29100:2024** — Information technology — Security techniques — Privacy framework. Geneva: ISO, 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27018:2025** — Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors. Geneva: ISO, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27701:2025** — Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance. Geneva: ISO, 2025.

ISACA. COBIT 2019: **Governance and management objectives**. Rolling Meadows, IL: ISACA, 2019.

KARLSSON, M. et al. The effect of perceived organizational culture on employees' information security compliance. **Information and Computer Security**, v. 30, n. 3, p. 382–401, 2022. DOI: <https://doi.org/10.1108/ICS-06-2021-0073>. Acesso em: 06 de out. 2025.

KHAN, M. A.; ALMULHIM, A. A.; ALKATI, S. S. Towards the evaluation of cybersecurity threats and challenges in higher education institutions in Saudi Arabia. **Edelweiss Applied Science and Technology**, v. 9, n. 2, p. 657-669, 2025. DOI: <https://doi.org/10.55214/25768484.v9i2.4564>. Acesso em: 06 de out. 2025.

KLINE, R. B. **Principles and Practice of Structural Equation Modeling**. 4. ed. New York: Guilford Press, 2016. ISBN: 978-1-4625-2335-1

KRISHNA, B.; SEBASTIAN, M. P. Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis. **Information and Computer Security**, v. 29, n. 5, p. 737–760, 2021. DOI: <https://doi.org/10.1108/ICS-12-2020-0205>. Acesso em: 06 de out. 2025.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2003.

LAWSHE, C. H. A quantitative approach to content validity. **Personnel Psychology**, v. 28, n. 4, p. 563–575, 1975. DOI: <https://doi.org/10.1111/j.1744-6570.1975.tb01393.x>. Acesso em: 06 de out. 2025.

LE, V. H.; PHUNG, V. O.; NGUYEN, N. H. Information security risk management by a holistic approach: a case study for Vietnamese e-Government. **IJCSNS International Journal of Computer Science and Network Security**, v. 20, n. 6, p. 72-82, 2020.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. Impacto da adoção de mecanismos de governança de Tecnologia de Informação (TI) no desempenho da gestão da TI: uma análise baseada na percepção dos executivos. **Revista de Ciências da Administração**, v. 12, n. 28, p. 11-39, 2010. DOI: <https://doi.org/10.5007/2175-8077.2010v12n28p11>. Acesso em: 06 de out. 2025.

MAGNUSSON, L. et al. Information security governance in the public sector: investigations, approaches, measures, and trends. **International Journal of Information Security**, v. 24, art. 177, 2025. DOI: <https://doi.org/10.1007/s10207-025-01097-x>. Acesso em: 06 de out. 2025.

MARCHIORI, D. M. et al. O papel das capacidades de TI, capacidade de reconfiguração de TI e inovatividade no desempenho organizacional: evidências do setor público brasileiro. **Revista de Administração Pública**, v. 57, n. 2, F2022-0221, 2023. DOI: <https://doi.org/10.1590/0034-761220220221>. Acesso em: 06 de out. 2025.

MARGETTS, H.; DUNLEAVY, P. The second wave of digital-era governance: a quasi-paradigm for government on the web. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, v. 371, n. 1987, 20120382, 2013. DOI: <https://doi.org/10.1098/rsta.2012.0382>. Acesso em: 06 de out. 2025.

MASREK, M. N. et al. Examining the relationship between information security effectiveness and information security threats. **International Journal of Business & Society**, v. 21, n. 3, 2020. DOI: <https://doi.org/10.33736/ijbs.3335.2020>. Acesso em: 06 de out. 2025.

MATLAND, R. E. Synthesizing the implementation literature: the ambiguity–conflict model of policy implementation. **Journal of Public Administration Research and Theory**, v. 5, n. 2, p. 145–174, 1995. DOI: <https://doi.org/10.1093/oxfordjournals.jpart.a037242>. Acesso em: 20 de out. 2024

MCDONALD, R. P. **Test Theory: A Unified Treatment**. Mahwah: Lawrence Erlbaum Associates, 1999.

MCINTOSH, T. R. et al. From COBIT to ISO 42001: evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. **arXiv**, 2024. (arXiv:2402.15770). Acesso em: 20 de out. 2024

MOHAMED NOOR, A. F.; MOGHAVVEMI, S.; TAJUDEEN, F. P. Identifying key factors of cybersecurity readiness in organizations: insights from Malaysian critical infrastructure. **Computers & Security**, v. 159, art. 104674, 2025. DOI: <https://doi.org/10.1016/j.cose.2025.104674>. Acesso em: 06 de out. 2025.

MOHSINI, M.; TOKE, F. V.; RASHIDI, F. Framework for enhancing effectiveness of information security measures implemented in public institutions in Tanzania. **The Electronic Journal of Information Systems in Developing Countries**, v. 91, n. 4, e70017, 2025. DOI: <https://doi.org/10.1002/isd2.70017>. Acesso em: 06 de out. 2025.

MÖLLER, D. P. F. **Cybersecurity in digital transformation: scope and applications**. Cham: Springer, 2020. DOI: <https://doi.org/10.1007/978-3-030-60570-4>. Acesso em: 06 de out. 2025.

MOON, Y. J.; CHOI, M.; ARMSTRONG, D. J. The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. **International Journal of Information Management**, v. 40, p. 54-66, 2018. DOI: <https://doi.org/10.1016/j.ijinfomgt.2018.01.001>. Acesso em: 06 de out. 2025.

MOORE, M. H. **Creating public value: strategic management in government**. Cambridge, MA: Harvard University Press, 1995. ISBN 9780674175587

MOREIRA, F. R. et al. Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. **IEEE Access**, 9, 129605–129618, 2021. DOI: <https://doi.org/10.1109/ACCESS.2021.3113178>. Acesso em: 06 de out. 2025.

MUTIMUKWE, C.; KOLKOWSKA, E.; GRÖNLUND, Å. Information privacy practices in e-government in an African least developing country, Rwanda. **The Electronic Journal of Information Systems in Developing Countries**, v. 85, n. 2, p. e12074, 2019. DOI: <https://doi.org/10.1002/isd2.12074>. Acesso em: 06 de out. 2025.

MUTIMUKWE, C.; KOLKOWSKA, E.; GRÖNLUND, Å. Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. **Government Information Quarterly**, v. 37, n. 1, p. 101413, 2020. DOI: <https://doi.org/10.1016/j.giq.2019.101413>. Acesso em: 06 de out. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Privacy Framework**: a tool for improving privacy through enterprise risk management (Version 1.0). Gaithersburg, MD: NIST, 2020. (NIST CSWP 01162020). DOI: <https://doi.org/10.6028/NIST.CSWP.01162020>. Acesso em: 04 de abr. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The NIST Cybersecurity Framework (CSF) 2.0**. Gaithersburg, MD: NIST, 2024. (NIST CSWP 29). DOI: <https://doi.org/10.6028/NIST.CSWP.29>. Acesso em: 04 de abr. 2025.

NOVATO, V. O. L.; NAJBERG, E.; LOTTA, G. S. O burocrata de médio escalão na implementação de políticas públicas. **Revista de Administração Pública**, v. 54, p. 416-432, 2020. Acesso em: 04 de abr. 2025.

OECD. **Digital Government Index**: 2019 results. (OECD Public Governance Policy Papers, n. 3). Paris: OECD Publishing, 2020b. DOI: <https://doi.org/10.1787/4de9f5bb-en>. Acesso em: 04 de abr. 2025.

OECD. **The OECD Digital Government Policy Framework**: six dimensions of a digital government. (OECD Public Governance Policy Papers, n. 2). Paris: OECD Publishing, 2020a. DOI: <https://doi.org/10.1787/f64fed2a-en>. Acesso em: 04 de abr. 2025.

OGBODO, D. C. et al. From regulation to reality: a framework to bridge the gap in digital health data protection. **Electronics**, v. 14, art. 2629, 2025. DOI: <https://doi.org/10.3390/electronics14132629>. Acesso em: 06 out. 2025.

PAGE, M. J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. **BMJ**, v. 372, n. 71, p. 1–9, 2021. DOI: <https://doi.org/10.1136/bmj.n71>. Acesso em: 06 out. 2025.

PAPI, L. P.; SEIDI, M.; SANTOS, G. T. Burocracia de médio escalão e capacidade burocrática: uma pesquisa de escopo. In: ENCONTRO BRASILEIRO DE ADMINISTRAÇÃO PÚBLICA (EBAP), 9., 2022, São Paulo. Anais [...]. São Paulo: Sociedade Brasileira de Administração Pública, 2022. Disponível em: <https://sbap.org.br/ebap/index.php/home/article/view/812>. Acesso em: 10 nov. 2025.

PAUL, J. A.; ZHANG, M. Decision support model for cybersecurity risk planning: a two-stage stochastic programming framework featuring firms, government, and attacker. **European Journal of Operational Research**, v. 291, n. 1, p. 349–364, 2021. DOI: <https://doi.org/10.1016/j.ejor.2020.09.013>. Acesso em: 06 out. 2025.

POISTER, T. H. **Measuring performance in public and nonprofit organizations**. San Francisco: Jossey-Bass, 2003. ISBN 0-7879-4999-X.

POLLITT, C.; BOUCKAERT, G. **Public management reform: a comparative analysis**. 3. ed. Oxford: Oxford University Press, 2011.

REID, R.; VAN NIEKERK, J. From information security to cyber security cultures. In: **Information Security For South Africa (ISSA)**, 2014, Johannesburg. Proceedings [...]. Johannesburg: IEEE, 2014. p. 1–7. DOI: <https://doi.org/10.1109/ISSA.2014.6950492>. Acesso em: 06 out. 2025.

RIBEIRO, D. et al. Assessing the information security posture of online public services worldwide: technical insights, trends, and policy implications. **Government Information Quarterly**, v. 42, n. 2, 102031, 2025. DOI: <https://doi.org/10.1016/j.giq.2025.102031>. Acesso em: 06 out. 2025.

ROSSI, P. H.; LIPSEY, M. W.; FREEMAN, H. E. **Evaluation: a systematic approach**. 7. ed. Thousand Oaks, CA: Sage Publications, 2004.

SABATIER, P. A. Top-down and bottom-up approaches to implementation research: a critical analysis and suggested synthesis. **Journal of Public Policy**, v. 6, n. 1, p. 21–48, 1986. DOI: <https://doi.org/10.1017/S0143814X00003846>. Acesso em: 10 nov. 2024.

SALAM, M.; ABU BAKAR, K. A.; AMAN, A. H. M. Building cyber-resilient universities: a tailored maturity model for strengthening cybersecurity in higher education institutions. **International Journal of Advanced Computer Science and Applications**, v. 16, n. 5, 2025. DOI: <https://doi.org/10.14569/IJACSA.2025.0160510>. Acesso em: 06 out. 2025.

- SÁNCHEZ-ZURDO, J.; SAN-MARTÍN, J. A Country Risk Assessment from the Perspective of Cybersecurity in Local Entities. **Applied Sciences**, v. 14, n. 24, p. 12036, 2024. DOI: <https://doi.org/10.3390/app142412036>. Acesso em: 06 out. 2025.
- SAURA, J. R.; RIBEIRO-SORIANO, D.; PALACIOS-MARQUÉS, D. Assessing behavioral data science privacy issues in government artificial intelligence deployment. **Government Information Quarterly**, v. 39, n. 4, p. 101679, 2022. DOI: <https://doi.org/10.1016/j.giq.2022.101679>. Acesso em: 06 out. 2025.
- SHAHEEN, K.; ZOLAIT, A. H. The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. **Information & Computer Security**, v. 31, n. 5, p. 529-544, 2023. DOI: <https://doi.org/10.1108/ICS-06-2022-0108>. Acesso em: 06 out. 2025.
- SHAH, S.; MEHTRE, B. M. A modern approach to cyber security analysis using vulnerability assessment and penetration testing. **International Journal of Electronics Communication and Computer Engineering**, v. 4, n. 6, p. 47–52, 2013. Acesso em: 06 out. 2025.
- ŠIKMAN, L. et al. Model for assessing measurable aspects of information security in higher education. **Comptes Rendus de l'Académie Bulgare des Sciences**, v. 78, n. 7, p. 1008-1019, 2025. DOI: <https://doi.org/10.7546/CRABS.2025.07.07>. Acesso em: 06 out. 2025.
- SITTITIAMJAN, K.; WUTTIDITTACHOTTI, P. Bridging the gap: how knowledge, attitudes, and practices shape cybersecurity awareness in Thai education. **Educational Process: International Journal**, v. 16, e2025236, 2025. DOI: <https://doi.org/10.22521/edupij.2025.16.236>. Acesso em: 06 out. 2025.
- SOUZA NETO, J.; CARVALHO, L. E. M. de. A avaliação da governança de TI da administração pública sob a ótica dos princípios da governança corporativa. **Revista do Serviço Público**, v. 71, n. esp. 3, p. 345–374, dez. 2020. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/5994/1/4426-Texto%20do%20artigo17169-1-10-20201211.pdf>. Acesso em: 01 set. 2025.
- SPEARMAN, C. The proof and measurement of association between two things. **The American Journal of Psychology**, v. 15, n. 1, p. 72–101, 1904.
- STOKER, R. P. A regime framework for implementation analysis: cooperation and reconciliation of federalist imperatives. **Policy Studies Review**, v. 9, n. 1, p. 29–49, 1989. DOI: <https://doi.org/10.1111/j.1541-1338.1989.tb01019.x>. Acesso em: 10 nov. 2024.
- TAHERDOOST, H. Understanding cybersecurity frameworks and information security standards — a review and comprehensive overview. **Electronics**, v. 11, n. 14, p. 2181, 2022. DOI: <https://doi.org/10.3390/electronics11142181>. Acesso em: 10 nov. 2024.

TONELLI, A. O. et al. IT governance in the public sector: a conceptual model. **Information Systems Frontiers**, v. 19, n. 3, p. 593–610, 2017. DOI: <https://doi.org/10.1007/s10796-015-9614-x>. Acesso em: 10 nov. 2024.

TRAN, D. V. et al. Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam. **Journal of Asia Business Studies**, v. 18, n. 6, p. 1445-1464, 2024. DOI: <https://doi.org/10.1108/JABS-01-2024-0058>. Acesso em: 06 out. 2025.

VAN DOOREN, W.; BOUCKAERT, G.; HALLIGAN, J. **Performance management in the public sector**. 2. ed. London: Routledge, 2015. DOI: <https://doi.org/10.4324/9781315817590>. Acesso em: 10 nov. 2024.

VAN STEEN, T. et al. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? **Journal of Cybersecurity**, v. 6, n. 1, tyaa019, 2020. DOI: <https://doi.org/10.1093/cybsec/tyaa019>. Acesso em: 06 out. 2025.

VESTAD, A.; YANG, B. From security frameworks to sustainable municipal cybersecurity capabilities. **Journal of Cybersecurity and Privacy**, v. 5, n. 2, art. 19, 2025. DOI: <https://doi.org/10.3390/jcp5020019>. Acesso em: 06 out. 2025.

VOIGT, P.; VON DEM BUSSCHE, A. **The EU General Data Protection Regulation (GDPR): a practical guide**. Cham: Springer, 2017. DOI: <https://doi.org/10.1007/978-3-319-57959-7>. Acesso em: 06 out. 2025.

VON SOLMS, B.; VON SOLMS, R. Cybersecurity and information security — what goes where? **Information & Computer Security**, v. 26, n. 1, p. 2–9, 2018. DOI: <https://doi.org/10.1108/ICS-04-2017-0025>. Acesso em: 10 nov. 2024.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security**, v. 38, p. 97–102, 2013. DOI: <https://doi.org/10.1016/j.cose.2013.04.004>. Acesso em: 10 nov. 2024.

WEILL, P.; ROSS, J. W. **IT governance: how top performers manage IT decision rights for superior results**. Boston: Harvard Business School Press, 2004. ISBN: 978-1591392538. Acesso em: 10 nov. 2024.

WORLD ECONOMIC FORUM. **The Global Risks Report**: 18th edition. Geneva: WEF, 2023. Disponível em: <https://www.weforum.org/reports/global-risks-report-2023/>. Acesso em: 13 out. 2024.

WU, X.; RAMESH, M.; HOWLETT, M. Policy capacity: a conceptual framework for understanding policy competences and capabilities. **Policy and Society**, v. 34, n. 3–4, p. 165–171, 2015. DOI: <https://doi.org/10.1016/j.polsoc.2015.09.001>. Acesso em: 10 nov. 2024.

YANG, X.; MEI, H.; ZHENG, Y. Understanding the antecedents of privacy fatigue in facial recognition-based m-Gov services: an empirical study from China.

Government Information Quarterly, v. 40, n. 4, 101827, 2023. DOI:
<https://doi.org/10.1016/j.giq.2023.101827>. Acesso em: 06 out. 2025.

APÊNDICE A – INSTRUMENTO DE PESQUISA (VERSÃO APLICADA)

O instrumento foi aplicado por meio de formulário eletrônico (Google Forms), vinculado à conta institucional do pesquisador na UFFS. Reproduz-se, a seguir, a íntegra do formulário aplicado, incluindo o Termo de Consentimento Livre e Esclarecido (TCLE), os blocos de qualificação do respondente, de identificação e contexto institucional, os indicadores de maturidade (iBase, iSeg e iPriv), os itens de capacidades institucionais (C1–C8) e de efetividade percebida (E1–E10), mensurados em escala Likert de sete pontos (1 = discordo totalmente; 7 = concordo totalmente), e o campo aberto complementar. As capturas tiveram o cabeçalho e o rodapé de impressão do navegador (data de impressão e URL de edição do formulário) suprimidos por tarja; o conteúdo reproduzido corresponde integralmente à versão aplicada aos respondentes.

Pesquisa sobre a efetividade do Programa de Privacidade e Segurança da Informação (PPSI) nas IFES

Este questionário integra a pesquisa **“Avaliação da efetividade do Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior (IFES)”**, desenvolvida no âmbito do **Mestrado Profissional em Administração Pública da Universidade Federal da Fronteira Sul (PROFIAP/UFFS)**.

O objetivo do estudo é compreender como a implementação do PPSI se relaciona a capacidades institucionais e a resultados percebidos em segurança da informação e privacidade nas IFES.

Solicita-se, preferencialmente, a resposta da pessoa que atua como principal responsável institucional pelo acompanhamento ou preenchimento do PPSI. Na ausência dessa definição, o questionário poderá ser respondido por ator diretamente envolvido com o programa.

As informações fornecidas serão tratadas com confidencialidade e utilizadas exclusivamente para fins acadêmicos. Os resultados serão analisados e apresentados apenas de forma agregada, sem divulgação individualizada de respondentes ou de instituições. Eventuais informações institucionais solicitadas no formulário não se caracterizam como divulgação pública, ampla ou irrestrita, mas como insumos restritos à análise científica do estudo. Não há coleta de dados pessoais.

Tempo médio para preenchimento: 8 minutos.

Esta pesquisa foi aprovada pelo Comitê de Ética em Pesquisa da UFFS, por meio da Plataforma Brasil:

CAAE: 94243825.5.0000.5564
Parecer CEP/UFFS nº 8.076.502

Leia o [Termo de Consentimento Livre e Esclarecido \(TCLE\)](#) antes de prosseguir.

* Indica uma pergunta obrigatória

1. **Você leu e concorda com o Termo de Consentimento Livre e Esclarecido (TCLE)?** *

Marcar apenas uma oval.

- ☐ Sim, li e concordo
- ☐ Não concordo

Bloco 0 - Qualificação do Respondente

As questões abaixo servem apenas para qualificar o vínculo do respondente com o PPSI na instituição.

2. **No momento, qual é sua relação com o PPSI na instituição?** *

Marcar apenas uma oval.

- ☐ Sou o principal responsável institucional pelo acompanhamento ou preenchimento do PPSI
- ☐ Atuo diretamente no PPSI, mas não sou o principal responsável
- ☐ Não atuo diretamente no PPSI

3. **Qual perfil melhor descreve sua atuação predominante em relação ao PPSI na instituição?** *

Marcar apenas uma oval.

- ☐ Segurança da Informação
- ☐ Tecnologia da Informação/TIC
- ☐ Privacidade e proteção de dados
- ☐ Gestão institucional
- ☐ Outro perfil diretamente envolvido com o PPSI

Bloco 1 – Identificação da Instituição

Informe o nome da sua instituição.

Nota: as páginas 4 a 8 da impressão do formulário, que continham exclusivamente a lista de seleção das 110 IFES do campo de identificação da instituição, foram suprimidas neste apêndice por economia de espaço. A relação completa das instituições do universo de referência será mantido sob guarda do pesquisador em repositório institucional e disponibilizado sob demanda, nos termos da seção 3.7.

Bloco 2 – Variáveis Institucionais

As informações a seguir auxiliam na caracterização institucional da IFES. Os campos referentes aos índices do PPSI de estrutura básica (iBase), segurança da informação (iSeg) e privacidade (iPriv) serão utilizados exclusivamente para fins analíticos da pesquisa e não serão exibidos individualmente. Os resultados serão apresentados apenas de forma agregada e consolidada, de modo a impedir a identificação de respondentes e a divulgação isolada dos índices de qualquer instituição.

5. **Considerando o total aproximado de servidores da instituição, em qual faixa sua IFES se enquadra?**

Marcar apenas uma oval.

- ☐ Até 1.000
- ☐ De 1.001 a 2.000
- ☐ De 2.001 a 3.000
- ☐ De 3.001 a 4.000
- ☐ Acima de 4.000

6. **Considerando total aproximado da equipe de TI/TIC da instituição, em qual faixa sua IFES se enquadra?**

Marcar apenas uma oval.

- ☐ Até 10
- ☐ De 11 a 20
- ☐ De 21 a 40
- ☐ De 41 a 60
- ☐ De 61 a 100
- ☐ Acima de 100

7. **Considerando o total aproximado de estudantes regularmente vinculados à instituição, em qual faixa sua IFES se enquadra?**

Marcar apenas uma oval.

- ☐ Até 10.000
- ☐ De 10.001 a 20.000
- ☐ De 20.001 a 30.000
- ☐ De 30.001 a 40.000
- ☐ Acima de 40.000

8. **Sua IFES é multicampi?**

Marcar apenas uma oval.

- ☐ Sim
- ☐ Não

9. **Indicador de Maturidade da Estrutura Básica (iBase) do PPSI - valor entre 0,00 e 1,00**

10. **Indicador de Maturidade em Segurança da Informação (iSeg) do PPSI - valor entre 0,00 e 1,00**

11. **Indicador de Maturidade em Privacidade (iPriv) do PPSI - valor entre 0,00 e 1,00**

Bloco 3 – Capacidades Institucionais

Avalie as capacidades de sua instituição em relação ao Programa de Privacidade e Segurança da Informação (PPSI). Indique seu nível de concordância conforme a escala: 1 = Discordo totalmente, 2 = Discordo, 3 = Discordo um pouco, 4 = Não concordo nem discordo, 5 = Concordo um pouco, 6 = Concordo, 7 = Concordo totalmente.

12. **Papéis, responsabilidades e instâncias de governança do PPSI estão formalizados e em funcionamento.**

Marcar apenas uma oval.

[illegible]

13. **A instituição dispõe de equipe e competências adequadas para conduzir ações de segurança da informação e privacidade.**

Marcar apenas uma oval.

[illegible]

14. **Processos de segurança da informação e privacidade, incluindo gestão de vulnerabilidades e backup/restauração, são executados e testados regularmente.**

Marcar apenas uma oval.

[illegible]

15. A instituição dispõe de recursos tecnológicos compatíveis com sua complexidade e perfil de risco para manter visibilidade sobre seus ativos e apoiar o monitoramento, a detecção e a resposta a eventos de segurança.

Marcar apenas uma oval.

1 2 3 4 5 6 7

Discordo totalmente Concordo totalmente

16. **A gestão de dados pessoais e privacidade, incluindo mapeamento de tratamentos, bases legais e RIPD, está implementada e em funcionamento.**

Marcar apenas uma oval.

[illegible]

17. A gestão de riscos de segurança da informação e privacidade está integrada ao planejamento e ao orçamento institucional. *

Marcar apenas uma oval.

[illegible]

18. A instituição promove ações de treinamento e conscientização em segurança da informação e privacidade com alcance entre diferentes públicos institucionais. *

Marcar apenas uma oval.

[illegible]

19. A instituição dispõe de recursos orçamentários e contratuais suficientes para sustentar ações de segurança da informação e privacidade previstas no PPSI. *

Marcar apenas uma oval.

[illegible]

Bloco 4 – Efetividade do PPSI

Avalie os resultados alcançados pela sua instituição em relação à efetividade do PPSI. Indique seu nível de concordância conforme a escala: 1 = Discordo totalmente, 2 = Discordo, 3 = Discordo um pouco, 4 = Não concordo nem discordo, 5 = Concordo um pouco, 6 = Concordo, 7 = Concordo totalmente.

20. Após o início da implementação do PPSI, as interrupções em serviços digitais essenciais tornaram-se menos frequentes.

Marcar apenas uma oval.

[illegible]

21. Após o início da implementação do PPSI, serviços críticos passaram a ser restabelecidos mais rapidamente após interrupções. *

Marcar apenas uma oval.

[illegible]

22. Nos últimos 12 meses, a instituição tornou-se mais ágil na detecção de incidentes de segurança.

Marcar apenas uma oval.

[illegible]

23. Nos últimos 12 meses, a instituição tornou-se mais ágil na contenção e recuperação após incidentes de segurança.

Marcar apenas uma oval.

[illegible]

24. Nos últimos 12 meses, a exposição da instituição a riscos críticos de segurança da informação e privacidade diminuiu.

Marcar apenas uma oval.

1 2 3 4 5 6 7

Discordo totalmente Concordo totalmente

25. Nos últimos 12 meses, incidentes envolvendo dados pessoais tornaram-se menos frequentes ou menos graves.

Marcar apenas uma oval.

[illegible]

26. Após o início da implementação do PPSI, quando aplicáveis, as notificações de incidentes a titulares e à ANPD passaram a ocorrer de forma tempestiva e adequadamente documentada. *

Marcar apenas uma oval.

[illegible]

27. Nos últimos 12 meses, auditorias e monitoramentos indicaram avanço na conformidade em segurança da informação e privacidade, inclusive quanto às exigências da LGPD.

Marcar apenas uma oval.

[illegible]

28. Nos últimos 12 meses, ampliou-se, entre as áreas-fim, a percepção de que a instituição protege informações e dados pessoais.

Marcar apenas uma oval.

[illegible]

29. Nos últimos 12 meses, a alta administração passou a reconhecer ganhos institucionais associados ao PPSI. ★

Marcar apenas uma oval.

[illegible]

Consideração Adicional

30. **Caso tenha mais alguma colocação sobre o PPSI da sua instituição, ou geral sobre o assunto, escreva no espaço abaixo.**

Este conteúdo não foi criado nem aprovado pelo Google.

Google Formulários

APÊNDICE B – DOCUMENTAÇÃO DA REVISÃO SISTEMÁTICA

O corpus final da revisão sistemática (82 estudos) está apresentado no Quadro 4 (Capítulo 4), e o diagrama PRISMA integra o corpo da dissertação (Figura 3). A documentação do processo é composta pelos arquivos de exportação (.csv) das buscas realizadas na Scopus e na Web of Science e por planilha auditável única, organizada em abas sequenciais que registram a deduplicação, a triagem por título, resumo e palavras-chave com o código de exclusão atribuído a cada registro (F1–F4 e F8), a leitura integral e a extração e codificação temática do portfólio final nos domínios de capacidade e efetividade. O protocolo da revisão, com pergunta norteadora, estratégias de busca, filtros e critérios de elegibilidade, corresponde aos procedimentos descritos na seção 3.2 e foi consolidado em documento próprio. Esse conjunto compõe o pacote de reprodutibilidade da pesquisa, a ser disponibilizado em repositório institucional quando do depósito final da dissertação.

APÊNDICE C – APROVAÇÃO ÉTICA

A pesquisa foi aprovada pelo Comitê de Ética em Pesquisa da Universidade Federal da Fronteira Sul (CEP/UFFS), sob o CAAE nº 94243825.5.0000.5564 e Parecer nº 8.076.502. Reproduz-se, a seguir, o parecer consubstanciado emitido pela Plataforma Brasil.

UNIVERSIDADE FEDERAL DA
FRONTEIRA SUL - UFFS



PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: AVALIAÇÃO DA EFETIVIDADE DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI) NAS INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR

Pesquisador: Débora Regina Schneider Locatelli

Área Temática:

Versão: 2

CAAE: 94243825.5.0000.5564

Instituição Proponente: UNIVERSIDADE FEDERAL DA FRONTEIRA SUL - UFFS

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 8.076.502

Apresentação do Projeto:

Resumo:

O objetivo central é avaliar a efetividade do PPSI nas IFES, buscando ir além da verificação de mera conformidade normativa. A pesquisa proposta adota uma abordagem quantitativa com delineamento exploratório-descritivo e estratégia censitária, abrangendo todas as Instituições Federais de Ensino Superior (IFES) participantes do Programa de Privacidade e Segurança da Informação (PPSI). O método se estrutura em três etapas principais: a) Revisão Sistemática da Literatura (RSL): Identificou seis domínios de capacidade (governança, processos, pessoas/competências, tecnologia/monitoramento, gestão de dados/privacidade e recursos) e seis domínios de desempenho/efetividade (redução de risco, transparência/notificação/conformidade, proteção de dados, confiança/percepção, detecção e resposta, e continuidade/disponibilidade); b) Construção e Validação do Instrumento: Desenvolvimento e validação de conteúdo de um questionário primário aplicado a gestores responsáveis pelo PPSI; c) Triangulação Estatística: Comparação dos escores primários dos domínios de Capacidade e Efetividade (C/E) com dados secundários de maturidade do PPSI (índices ISeg e IPriv). Essa etapa trata a relação `maturidade &

Endereço: Rodovia SC 484 Km 02, Fronteira Sul - Bloco da Biblioteca - sala 310, 3º andar

Bairro: Área Rural

CEP: 89.815-899

UF: SC

Município: CHAPECÓ

Telefone: (49)2049-3745

E-mail: cep.uffs@uffs.edu.br

Nota: reproduzem-se a primeira página do parecer consubstanciado, com a identificação do projeto, o CAAE e o número do parecer, e a página final, com a situação de aprovação. As páginas intermediárias (2 a 8) foram suprimidas por economia de espaço; o documento integral compõe o pacote de reprodutibilidade da pesquisa.

**UNIVERSIDADE FEDERAL DA
FRONTEIRA SUL - UFFS**



Continuação do Parecer: 8.076.502

Contate a "central de suporte" da Plataforma Brasil, clicando no ícone no canto superior direito da página eletrônica da Plataforma Brasil. O atendimento é online.

Boa pesquisa!

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2705162.pdf	16/12/2025 16:36:41		Aceito
Outros	Carta_Pendencias_CEP_Aval_PPCI_2025.pdf	16/12/2025 16:36:12	Débora Regina Schneider Locatelli	Aceito
Outros	Questionario_print_Forms.pdf	29/11/2025 16:07:44	Débora Regina Schneider Locatelli	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE_online.pdf	29/11/2025 16:07:18	Débora Regina Schneider Locatelli	Aceito
Projeto Detalhado / Brochura Investigador	Projeto_CEP_PPSI.pdf	29/11/2025 16:07:03	Débora Regina Schneider Locatelli	Aceito
Folha de Rosto	folhaDeRosto_Flavio_CEP_assinadoassinado.pdf	29/11/2025 16:06:42	Débora Regina Schneider Locatelli	Aceito

Situação do Parecer:

Aprovado

Necessita Apreciação da CONEP:

Não

CHAPECO, 19 de Dezembro de 2025

Assinado por:
Renata dos Santos Rabello
(Coordenador(a))

Endereço: Rodovia SC 484 Km 02, Fronteira Sul - Bloco da Biblioteca - sala 310, 3º andar
Bairro: Área Rural **CEP:** 89.815-899
UF: SC **Município:** CHAPECO
Telefone: (49)2049-3745 **E-mail:** cep.uffs@uffs.edu.br

APÊNDICE D – PRODUTO TÉCNICO-TECNOLÓGICO (GACE-PPSI)

Apresenta-se, neste apêndice, o documento completo do Produto Técnico-Tecnológico (PTT) GACE-PPSI, o Guia de Avaliação de Capacidades e Efetividade do PPSI nas IFES, elaborado conforme o modelo de relatório técnico da Rede PROFIAP.



GACE-PPSI: APLICATIVO DE AVALIAÇÃO DE CAPACIDADES E EFETIVIDADE DO PPSI NAS INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR

Software de diagnóstico complementar aos índices de maturidade:
execução local, gratuito e de código aberto

**GACE-PPSI: APLICATIVO DE AVALIAÇÃO DE
CAPACIDADES E EFETIVIDADE DO PROGRAMA DE
PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO NAS
INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR**

Relatório técnico apresentado pelo mestrando Flavio Humberto Testa ao Mestrado Profissional em Administração Pública em Rede Nacional (PROFIAP), instituição associada Universidade Federal da Fronteira Sul (UFFS), sob orientação da Prof.^a Dr.^a Débora Regina Schneider Locatelli, como parte dos requisitos para obtenção do título de Mestre em Administração Pública.



SUMÁRIO	Contexto de aplicação da proposta	04
	Público-alvo da proposta	05
	Situação-problema	06
	Objetivo da proposta	10
	PTT – Proposta de Intervenção	12
	Autoria da Proposta	17
	Referências	18
	Protocolo de Entrega	19
	Atributos e Evidenciação de Impacto	20

CONTEXTO DE APLICAÇÃO DA PROPOSTA

A administração pública federal digitalizou a quase totalidade de seus serviços. Nesse cenário, o Programa de Privacidade e Segurança da Informação (PPSI) — instituído pela Portaria SGD/MGI nº 852/2023 e reformulado pela Portaria SGD/MGI nº 9.511/2025 (PPSI 2.0) — passou a orientar os órgãos do SISP por meio de um framework de controles cuja implementação é medida por autodiagnóstico, expresso nos índices iBase, iSeg e iPriv (Brasil, 2026).

Ao fiscalizar os primeiros ciclos do programa (Acórdão nº 2.387/2024-Plenário), o Tribunal de Contas da União evidenciou a baixa maturidade agregada do sistema e a necessidade de sustentar as autoavaliações em evidências.

A proposta insere-se no espaço institucional das 110 Instituições Federais de Ensino Superior: organizações que custodiam dados pessoais de milhões de estudantes, servidores e pesquisadores, operam estruturas multicampi de alta complexidade e executam o mandato nacional do PPSI com orçamentos comprimidos e equipes de TI de porte muito variável.

A proposição alinha-se aos Objetivos de Desenvolvimento Sustentável da ONU: ao ODS 16 (instituições eficazes), metas 16.6 e 16.10, e, de forma complementar, aos ODS 9 e 4, ao contribuir para a continuidade e a confiabilidade dos serviços digitais que sustentam a educação superior pública.



Serviços públicos digitalizados fizeram da proteção de dados e da segurança da informação condições de continuidade do próprio serviço público.



PÚBLICO-ALVO DA PROPOSTA

O produto destina-se aos praticantes-líderes que respondem pelo PPSI em cada IFES: o gestor de segurança da informação, o encarregado pelo tratamento de dados pessoais e o dirigente de tecnologia da informação, atuando junto às instâncias de governança a que se reportam, como o comitê de segurança da informação e privacidade e o comitê de governança digital.

São atores que reúnem a competência técnica para aplicar o instrumento e a autonomia institucional para converter o diagnóstico em pauta de comitê, proposta orçamentária e comunicação à alta administração — exatamente os usos para os quais o aplicativo foi desenhado.

PRATICANTES-LÍDERES

Gestores de segurança da informação, encarregados de dados pessoais e dirigentes de TI, com os comitês de SI e privacidade e de governança digital de cada IFES.

Em plano secundário, o produto interessa à Secretaria de Governo Digital (SGD/MGI), órgão central do PPSI, e às redes de colaboração entre IFES, que podem adotá-lo como linguagem comum de diagnóstico.

Por essa razão, este relatório é redigido na linguagem do gestor, e não na do pesquisador: cada elemento do produto responde a uma tarefa concreta de quem administra o programa na ponta.



PÚBLICO SECUNDÁRIO

A Secretaria de Governo Digital (SGD/MGI), órgão central do PPSI, e as redes de colaboração entre IFES, como linguagem comum de diagnóstico.

QUEM RESPONDEU À PESQUISA

➤ 58 IFES participantes

52,7% do universo de 110

94,8% com estrutura multicampi

IFES de todas as regiões do país

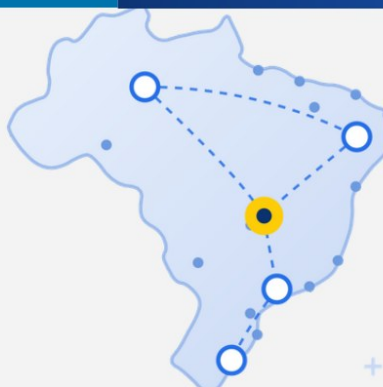
➤ Perfil dos respondentes

Segurança da Informação: 41,4%

Privacidade e proteção de dados: 20,7%

TI/TIC: 19,0%

Gestão: 17,2%



SITUAÇÃO-PROBLEMA

Diagnóstico, análise e linha de intervenção

O diagnóstico que fundamenta esta proposta resulta de pesquisa nacional realizada em 2026 com 58 IFES, 52,7% do universo, por meio de instrumento derivado de revisão sistemática de 82 estudos internacionais e validado em conteúdo por painel de especialistas.

Três achados desenharam a situação-problema, detalhados nas páginas seguintes: a implementação avança em camadas desiguais; a efetividade concentra-se na operação e não alcança o núcleo decisório; e a maturidade declarada não acompanha os resultados.

O instrumento aplicado deriva de revisão sistemática da literatura internacional (2015–2025), foi validado em conteúdo por painel de especialistas (CVR de Lawshe) e aplicado nacionalmente em 2026.

As 58 respostas válidas, uma por instituição, cobrem todas as regiões do país e todos os portes de IFES, o que permite usar os resultados como padrão nacional de referência para o autodiagnóstico local.

Primeiro achado: a implementação avança em camadas desiguais. A governança formal do programa — papéis, comitês e instâncias — é a capacidade mais consolidada, com média 4,72 em escala de 7 pontos. A sustentação material e integrativa é a mais frágil: recursos orçamentários e contratuais em 2,71, integração da gestão de riscos ao planejamento e ao orçamento em 3,05 e gestão de dados pessoais em 3,17.

O programa institucionalizou-se no papel antes de se converter em capacidade operante, comportamento típico de políticas induzidas por norma, nas quais a adoção formal corre à frente da institucionalização real (Alves; Santos, 2022; Vestad; Yang, 2025).

Vistas em conjunto, as oito capacidades formam degraus: no alto, as que dependem sobretudo de formalização; na base, as que exigem orçamento, integração e rotina continuada. O gargalo do programa, portanto, não é normativo — é de sustentação: a estrutura formal existe, mas disputa recursos escassos com as demais prioridades institucionais.

Segundo achado: a efetividade percebida concentra-se na operação e não alcança o núcleo decisório. Os respondentes reconhecem ganhos em detecção (4,59) e em contenção e recuperação de incidentes (4,48). O reconhecimento de ganhos institucionais pela alta administração, porém, é o item mais frágil de todo o bloco (3,91), o único abaixo do ponto neutro.

Sem métricas que traduzam riscos evitados em linguagem de valor, o principal produto da segurança bem-sucedida, o incidente que não ocorreu, permanece invisível para quem decide orçamento e prioridade (Moon; Choi; Armstrong, 2018; Dutton et al., 2019).

Os demais itens do bloco distribuem-se entre esses dois extremos, decrescendo à medida que se afastam da rotina técnica: o esforço de segurança produz resultados concretos, mas eles perdem visibilidade no percurso institucional, exatamente o trajeto que a proposta busca encurtar.

Encurtar esse trajeto exige tornar visível, em linguagem de decisão, o que a operação já entrega, função que esta proposta assume.

Terceiro achado, decisivo para a linha de intervenção: a maturidade declarada não acompanha os resultados. As capacidades institucionais correlacionaram-se de forma expressiva com a efetividade percebida ($p = 0,627$; $p < 0,001$); os índices oficiais de maturidade não apresentaram associação significativa com a efetividade, e o índice de privacidade teve correlação praticamente nula.

E a capacidade mais associada à efetividade, a gestão de riscos integrada ao planejamento (0,612), é justamente uma das menos desenvolvidas.

Os índices oficiais seguem necessários, cumprem função de conformidade perante o órgão central, mas, isoladamente, não informam a dimensão que mais importa à gestão local: onde investir para converter estrutura em resultado.

A análise à luz da literatura internacional e do quadro normativo converge para o mesmo ponto: a adesão a frameworks convive com escassez de indicadores e de verificação; autoavaliações governamentais tendem a superestimar a postura efetiva (Dewanto et al., 2022; Ribeiro et al., 2025), limitação que o próprio PPSI 2.0 reconheceu ao prever campo de evidências; e os resultados de segurança acompanham capacidades multidimensionais, não estoques declarados de controles (Dutton et al., 2019), ao passo que programas de maturidade acompanhados de verificação e de patrocínio próximo do órgão central produzem ganhos reais (Shaheen; Zolait, 2023).

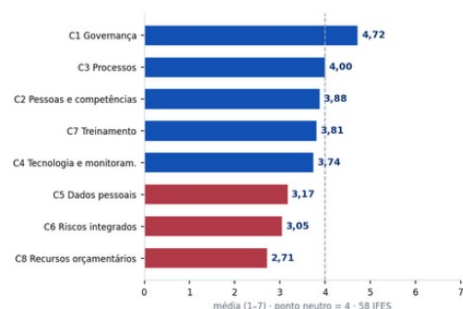
Para o gestor, a consequência é direta: acompanhar o programa apenas pela conformidade declarada sustenta decisões sobre uma fotografia incompleta. Incorporar capacidades e efetividade percebida à avaliação devolve ao diagnóstico aquilo que ele existe para informar: o resultado.

Em síntese: as IFES medem o que implementaram, mas não dispõem de instrumento para medir as capacidades que sustentam o programa nem os resultados que ele produz.

É nesse vazio de mensuração que a efetividade se perde entre a operação técnica e a decisão institucional.

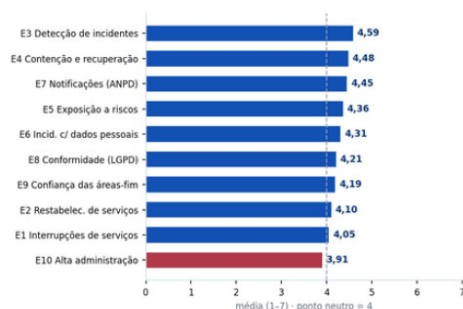
Os gráficos desta página resumem a evidência da pesquisa nacional: a implementação em camadas desiguais, os ganhos percebidos que param antes da alta administração e a associação entre capacidades e resultados.

Capacidades institucionais: camadas desiguais



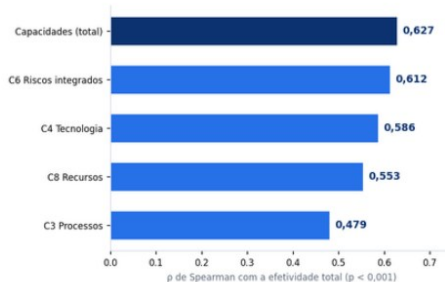
Leitura: a governança formal consolidou-se (4,72), mas a sustentação material — dados pessoais, riscos e recursos — permanece abaixo do ponto neutro.

Efetividade percebida: ganhos param antes da decisão



Leitura: os ganhos concentram-se na operação (detecção e resposta); o reconhecimento pela alta administração (3,91) é o único item abaixo do ponto neutro.

O que se associa à efetividade: capacidades



Leitura: as capacidades associam-se fortemente aos resultados ($p = 0,627$); os índices oficiais de maturidade não apresentaram associação significativa (Ipriv $p = -0,01$).

A base do padrão nacional



Leitura: as 58 respostas válidas — uma por instituição — cobrem todas as regiões e portes, permitindo usar os resultados como régua nacional de referência.

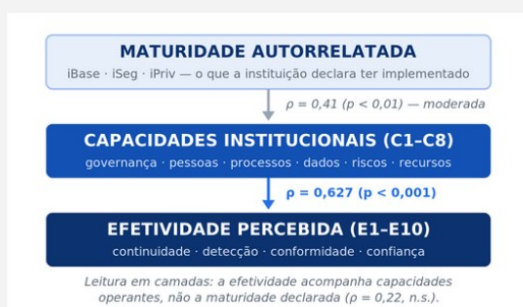
Entre as linhas de intervenção possíveis: propor novo normativo ao órgão central, contratar consultorias externas de avaliação ou aguardar a evolução do próprio programa, escolheu-se a que atua diretamente sobre o elo que o diagnóstico revelou mais frágil e que está ao alcance imediato do praticante.

A linha de intervenção é dotar cada IFES de um instrumento de autodiagnóstico complementar, que mede capacidades e efetividade percebida, compara a instituição ao padrão nacional, prioriza o desenvolvimento de capacidades pela evidência empírica e traduz o resultado em relatório executivo para a alta administração.

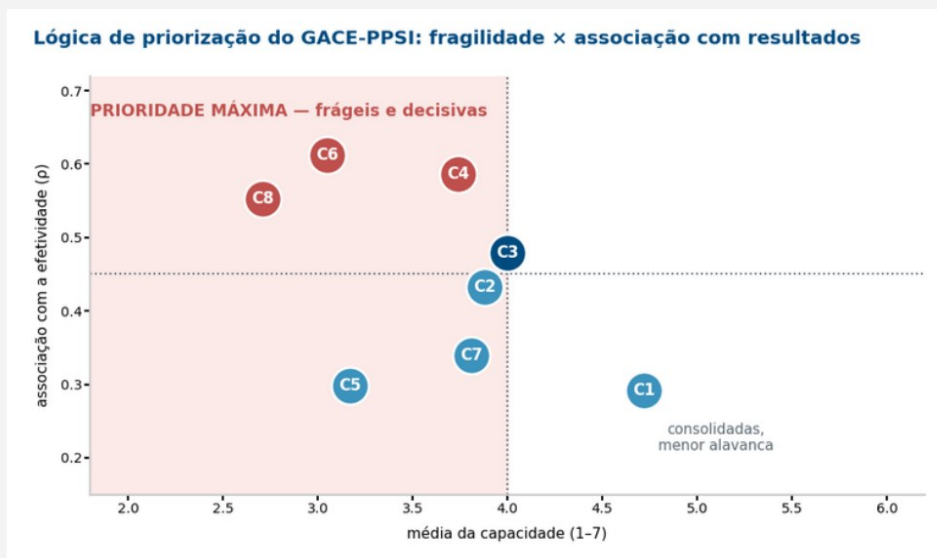
É uma intervenção de baixo custo, implementável sem autorização externa, que respeita a autonomia institucional e produz efeito onde a pesquisa localizou o gargalo: na mensuração e no reconhecimento.

A leitura em camadas do modelo interpretativo orienta a intervenção: o contexto e a maturidade situam a instituição; as capacidades sustentam o programa; a efetividade é o resultado que se busca.

O GACE-PPSI aplica ao diagnóstico local a régua construída com a evidência nacional, identificando o gargalo específico de cada instituição em vez de presumir uma hierarquia universal de carências.



O diagrama ao lado resume essa leitura; o quadrante abaixo ordena as oito capacidades pela combinação entre fragilidade (eixo horizontal) e associação com a efetividade (eixo vertical), quanto mais alto e mais à esquerda, maior a prioridade de desenvolvimento.



OBJETIVO DA PROPOSTA

O objetivo da proposta é disponibilizar aos responsáveis pelo PPSI nas IFES um instrumento autoaplicável, gratuito e de execução local que avalie, anualmente, as capacidades institucionais que sustentam o programa e a efetividade percebida que ele produz, convertendo essa avaliação em três entregas de gestão.

➤ Posicionar, priorizar e comunicar: do diagnóstico à decisão

As três entregas: o posicionamento da instituição frente ao padrão nacional das 58 IFES pesquisadas; a priorização fundamentada das capacidades a desenvolver, ordenada pelas associações empíricas observadas; e o relatório executivo que traduz o diagnóstico em linguagem de valor institucional para a alta administração.

Do diagnóstico à decisão: as três entregas de gestão



Ciclo anual, autoaplicável e de execução local.

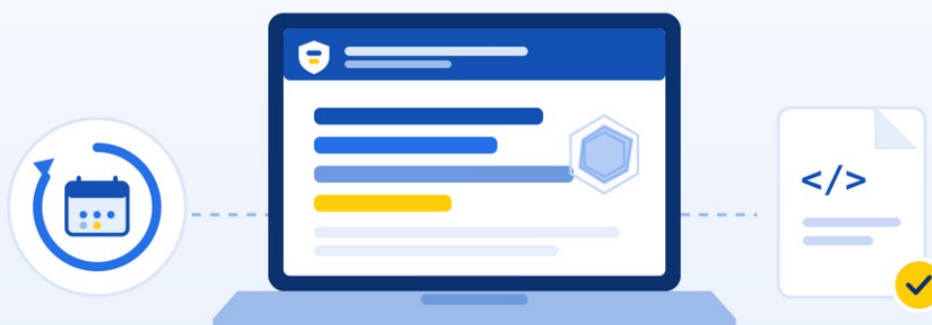
De forma específica, o produto materializa a linha de intervenção ao: mensurar as oito capacidades e os dez itens de efetividade do instrumento validado; posicionar os resultados na leitura em camadas do modelo interpretativo da dissertação, identificando o gargalo específico de cada instituição; e orientar a decisão com recomendações vinculadas a cada capacidade frágil.



O aplicativo institucionaliza a comparação entre ciclos anuais, por meio da exportação e importação de avaliações, permitindo acompanhar a evolução da instituição ao longo do tempo e documentar o efeito das ações priorizadas.



A confidencialidade institucional é preservada integralmente: nenhum dado sai do computador do gestor, decisão de arquitetura coerente com o objeto do programa que o produto avalia.



PTT – PROPOSTA DE INTERVENÇÃO



GACE-PPSI

CAPACIDADES · EFETIVIDADE · PPSI

O produto é o GACE-PPSI, software na categoria aplicativo (programa de computador), uma das doze possibilidades admitidas pela CAPES para a Área 27.

Trata-se de aplicação web contida em um único arquivo, aberto diretamente no navegador: sem instalação, sem servidor, sem custo e sem transmissão de dados, as respostas permanecem na máquina da instituição.

O aplicativo organiza-se em seis folhas, que conduzem o gestor do protocolo de uso ao relatório executivo, detalhadas nas páginas seguintes. O ciclo completo de aplicação cabe em uma manhã de trabalho.

O código-fonte é aberto, auditável e de livre adaptação, com atribuição, licença CC BY 4.0.

Distribuição pública com DOI (Zenodo), verificação de integridade e aviso de novas versões no próprio aplicativo.

Requisito único: um navegador moderno.

Download oficial e código-fonte: github.com/flaviotesta/gace-ppsi

Seis folhas, um arquivo — sem instalação, sem servidor, sem envio de dados

1 · Protocolo

como aplicar, quem responde, quando

2 · Identificação

dados institucionais (apenas local)

3 · Capacidades

8 itens validados (C1–C8), escala 1–7

4 · Efetividade

10 itens validados (E1–E10), escala 1–7

5 · Diagnóstico

padrão nacional, camadas, prioridades, evolução

6 · Método

origem, limites e forma de citação



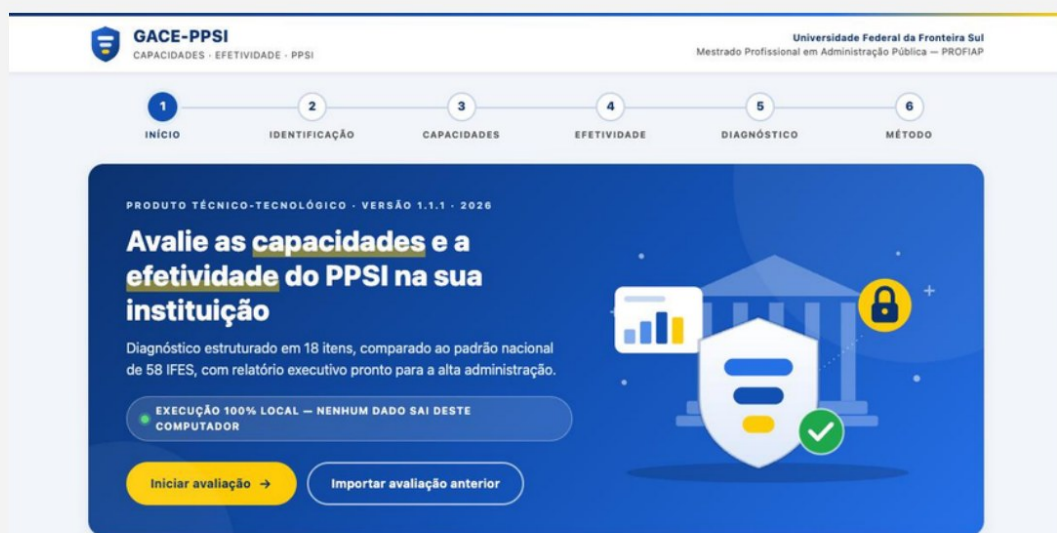
RELATÓRIO EXECUTIVO — 1 página (impressão/PDF) para a alta administração

A porta de entrada do aplicativo apresenta o produto, a versão em uso e o protocolo de aplicação: respondente qualificado, ciclo anual antes do planejamento e emprego do resultado em conversas estruturadas com a auditoria interna e os comitês.

É a primeira das seis folhas: as demais são percorridas na ordem indicada pelo próprio aplicativo.

➤ O indicador de progresso no topo, Início, Identificação, Capacidades, Efetividade, Diagnóstico e Método, torna o percurso completo visível desde o primeiro contato.

➤ Dois caminhos partem daqui: “Iniciar avaliação”, para um ciclo novo, e “Importar avaliação anterior”, que retoma a série histórica exportada no ciclo passado.



Tela inicial do GACE-PPSI, com o protocolo de uso e os dois caminhos de entrada: avaliação nova ou importação do ciclo anterior.

A segunda folha registra, apenas localmente, a identificação institucional: por desenho, o aplicativo não solicita índices de maturidade nem outros dados de conformidade da instituição.

A terceira e a quarta aplicam os dezoito itens validados: oito de capacidades e dez de efetividade, em escala de sete pontos.

➤ Cada item traz o enunciado completo e a escala de sete pontos com âncoras verbais, o mesmo instrumento validado da pesquisa nacional.

➤ O preenchimento segue a ordem das folhas, e o diagnóstico é calculado a partir das respostas registradas nesses dois blocos.

GACE-PPSI
CAPACIDADES - EFETIVIDADE - PPSI

Universidade Federal da Fronteira Sul
Mestrado Profissional em Administração Pública - PROFAP

Bloco I - Capacidades institucionais

Assinale, para cada enunciado, o ponto da escala que melhor descreve a situação atual da instituição, de 1 — discordo totalmente a 7 — concordo totalmente. O ponto 4 é neutro.

8 de 8 itens respondidos

C1 — GOVERNANÇA

Papéis, responsabilidades e instâncias de governança do PPSI estão formalizados e em funcionamento.

1 2 3 4 5 6 7
DISCORDO TOTALMENTE NEUTRO CONCORDO TOTALMENTE

C2 — PESSOAS E COMPETÊNCIAS

A instituição dispõe de equipe e competências adequadas para conduzir ações de segurança da informação e privacidade.

1 2 3 4 5 6 7
DISCORDO TOTALMENTE NEUTRO CONCORDO TOTALMENTE

C3 — PROCESSOS

Processos de segurança da informação e privacidade, incluindo gestão de vulnerabilidades e backup/restauração, são executados e testados regularmente.

1 2 3 4 5 6 7

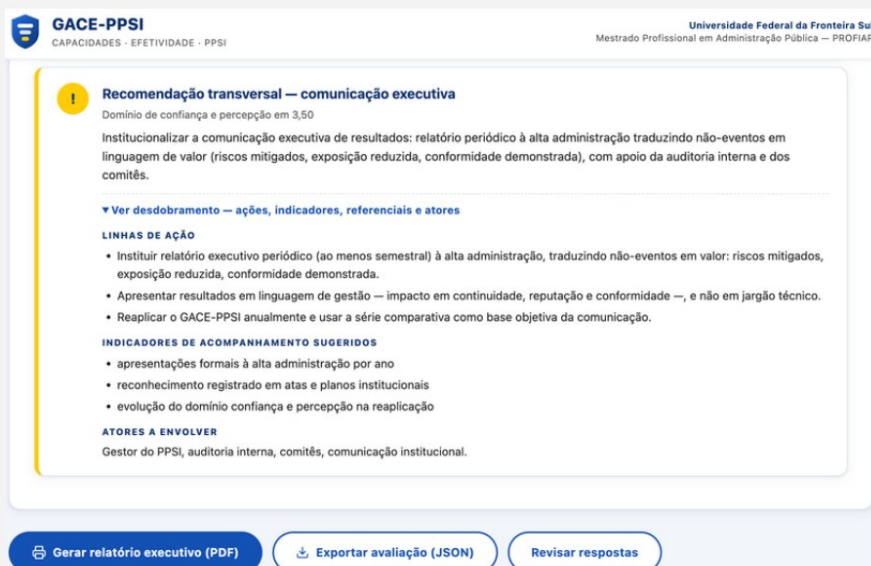
Folha de resposta do GACE-PPSI
Bloco I - Capacidades institucionais, com dados de demonstração.

A quinta folha entrega o diagnóstico: escores comparados ao padrão nacional, leitura em camadas, prioridades calculadas pela combinação entre fragilidade e associação com a efetividade, evolução entre ciclos e recomendações.

A sexta documenta método, origem, limites e forma de citação.



Tela ilustrativa do diagnóstico gerado pelo GACE-PPSI

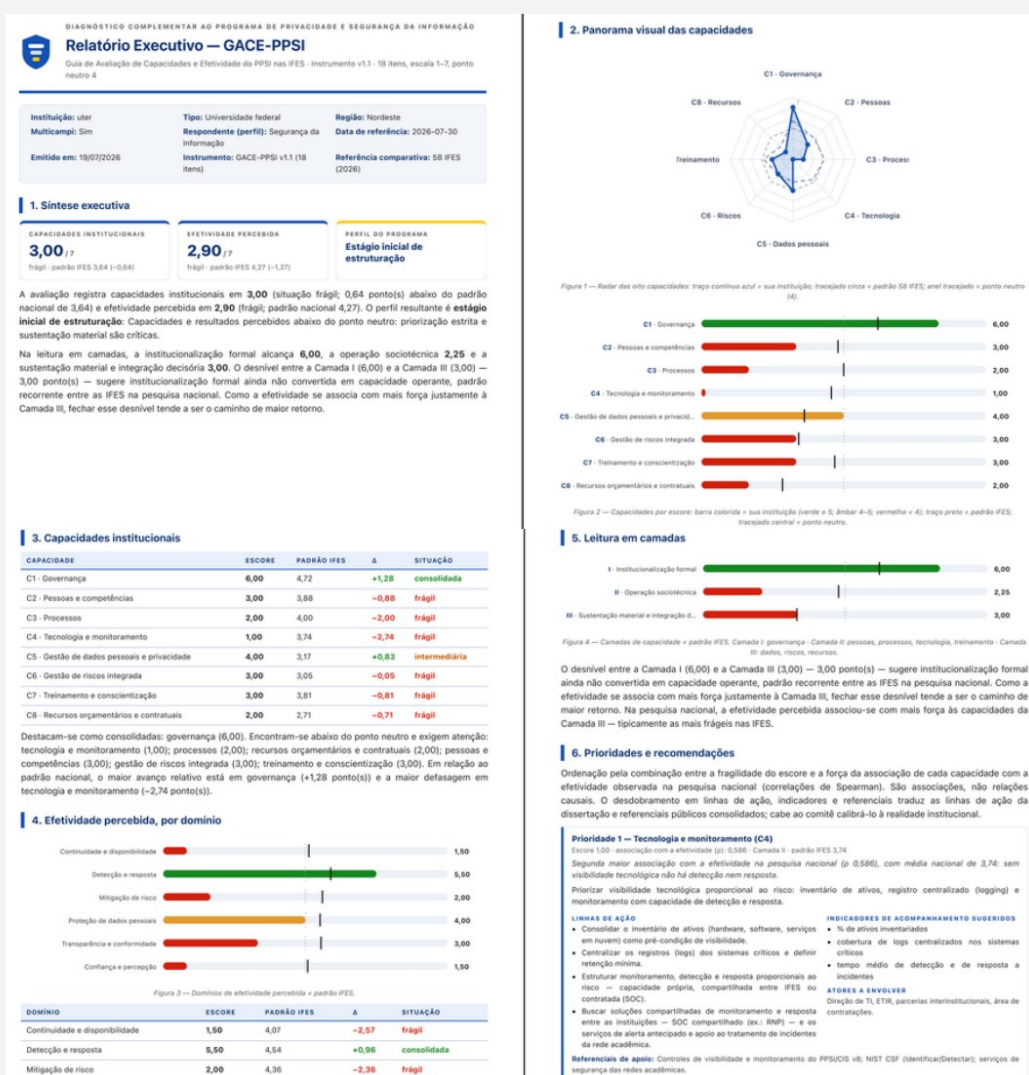


Tela ilustrativa do diagnóstico gerado pelo GACE-PPSI

➤ O relatório executivo, gerado em uma página para impressão ou PDF, encerra o ciclo de uso levando o diagnóstico à mesa da alta administração.

➤ A captura abaixo mostra a síntese executiva com dados de demonstração: escores, comparação com o padrão nacional e prioridades prontas para apreciação.

Roteiro de implantação em quatro passos: (1) baixar o aplicativo no repositório público e responder ao instrumento; (2) validar o diagnóstico com a equipe e o comitê; (3) apresentar o relatório executivo à alta administração, junto à proposta orçamentária; (4) arquivar a exportação para comparação no ciclo seguinte.



Telas ilustrativas do relatório gerado pelo GACE-PPSI

AUTORIA DA PROPOSTA

Flavio Humberto Testa

Mestrando do Mestrado Profissional em Administração Pública em Rede Nacional (PROFIAP), instituição associada UFFS, campus Chapecó.

E-mail: flavio.testa@uffs.edu.br · ORCID: <https://orcid.org/0009-0004-8965-0065>

Débora R. S. Locatelli

Orientadora. Prof.^a Dr.^a Débora Regina Schneider Locatelli, docente do PROFIAP/UFFS.

E-mail: debora.locatelli@uffs.edu.br · ORCID: <https://orcid.org/0000-0002-7488-4879>

Sobre este documento

Relatório técnico conclusivo do produto técnico-tecnológico GACE-PPSI, derivado da dissertação “Avaliação da efetividade do Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior” (Testa, 2026).

O título do PTT designa o produto (o aplicativo), e não o estudo que o originou, conforme orientação do modelo (ABNT NBR 6023).

DOI 10.5281/zenodo.21433368

Download: github.com/flaviotesta/gace-ppi

Data de finalização: 19 de julho de 2026.



REFERÊNCIAS

- ALVES, G. F.; SANTOS, C. D. The diffusion of innovations under normative induction in Brazil. *RAUSP Management Journal*, v. 57, n. 2, p. 149-164, 2022.
- BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. Institui o Programa de Privacidade e Segurança da Informação (PPSI). Brasília: MGI, 2023.
- BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. Institui o PPSI 2.0. Brasília: MGI, 2025.
- BRASIL. Secretaria de Governo Digital. Guia do Framework de Privacidade e Segurança da Informação: PPSI 2.0. Versão 1.2. Brasília: SGD/MGI, 2026.
- BRASIL. Tribunal de Contas da União. Acórdão nº 2.387/2024 – TCU – Plenário. Relator: Ministro Augusto Nardes. Brasília: TCU, 2024.
- DEWANTO, M. R. P.; OKTAVIA, T.; SUNDARAM, D. Comparative study of information security evaluation models for Indonesia government. *Journal of Theoretical and Applied Information Technology*, v. 100, n. 4, 2022.
- DUTTON, W. H.; CREESE, S.; SHILLAIR, R.; BADA, M. Cybersecurity capacity: does it matter? *Journal of Information Policy*, v. 9, 2019.
- MOON, Y. J.; CHOI, M.; ARMSTRONG, D. J. The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, v. 40, p. 54-66, 2018.
- RIBEIRO, D.; FONTE, V.; RAMOS, L. F.; SILVA, J. M. Assessing the information security posture of online public services worldwide. *Government Information Quarterly*, v. 42, 102031, 2025.
- SHAHEEN, K.; ZOLAIT, A. H. The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. *Information & Computer Security*, v. 31, n. 5, p. 529-544, 2023.
- TESTA, F. H. Avaliação da efetividade do Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior. Dissertação (Mestrado Profissional em Administração Pública) – Universidade Federal da Fronteira Sul, Chapecó, 2026.
- TESTA, F. H. GACE-PPSI: aplicativo de avaliação de capacidades e efetividade do PPSI nas IFES. Versão 1.2.0 Software. Chapecó: PROFIAP/UFS, 2026. DOI: 10.5281/zenodo.21433368.
- VESTAD, A.; YANG, B. From security frameworks to sustainable municipal cybersecurity capabilities. *Journal of Cybersecurity and Privacy*, v. 5, n. 2, 19, 2025.

PROTOCOLO DE ENTREGA DA PROPOSTA AOS PRATICANTES

MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA EM REDE NACIONAL —
PROFIAP

UNIVERSIDADE FEDERAL DA FRONTEIRA SUL — UFFS

Encaminhamento e protocolo de entrega de Produto Técnico-Tecnológico nº
02/2026

Ao Senhor
Sérgio Begnini
Encarregado pelo Tratamento de Dados Pessoais
Universidade Federal da Fronteira Sul (UFFS)

Pelo presente, encaminhamos o produto técnico-tecnológico intitulado "GACE-PPSI: aplicativo de avaliação de capacidades e efetividade do Programa de Privacidade e Segurança da Informação nas Instituições Federais de Ensino Superior", derivado da dissertação de mestrado "Avaliação da Efetividade do Programa de Privacidade e Segurança da Informação (PPSI) nas Instituições Federais de Ensino Superior", de autoria de Flavio Humberto Testa, defendida e aprovada no âmbito do Mestrado Profissional em Administração Pública em Rede Nacional (PROFIAP), instituição associada Universidade Federal da Fronteira Sul (UFFS).

A solução é apresentada sob a forma de software/aplicativo (programa de computador), uma das doze possibilidades admitidas pela CAPES para a Área 27, e seu propósito é disponibilizar à instituição um diagnóstico anual e autoaplicável das capacidades institucionais e da efetividade percebida do PPSI, com comparação ao padrão nacional, priorização fundamentada em evidência e relatório executivo para a alta administração.

O aplicativo é gratuito, de código aberto (licença CC BY 4.0) e de execução local. Download: <https://github.com/flaviotesta/gace-ppsi>. DOI: 10.5281/zenodo.21433368.

Solicitamos, por gentileza, a devolução deste documento com o registro de recebimento ao final preenchido e assinado, bem como que ações voltadas à implementação desta proposição sejam informadas ao pesquisador, pelo endereço flavio.testa@uffs.edu.br, com cópia à Coordenação Local do PROFIAP/UFFS (posq.profiap@uffs.edu.br). O registro assinado integra a documentação de evidencição do produto técnico-tecnológico junto à Rede PROFIAP.

Chapecó, 15 de setembro de 2026.

Flavio Humberto Testa
Mestre em Administração Pública — PROFIAP/UFFS

REGISTRO DE RECEBIMENTO

Referente ao Encaminhamento e protocolo de entrega de Produto Técnico-Tecnológico nº 02/2026 (GACE-PPSI), de 15 de setembro de 2026.

Assinatura:



Documento assinado digitalmente
SERGIO BEGNINI
Data: 16/09/2026 17:38:37-0300
Verifique em <https://validar.iti.gov.br>

Nome:

Cargo:

Data (dd/mm/aaaa):

Observação: o registro de recebimento pode ser feito pela devolução deste documento com o campo acima assinado, inclusive com assinatura eletrônica gov.br, ou por documento de teor equivalente, elaborado e assinado no sistema oficial da instituição recebedora.

Discente: Flavio Humberto Testa
Orientadora: Prof.^a Dr.^a Débora Regina
Schneider Locatelli
Universidade Federal da Fronteira Sul (UFFS)
Data de finalização do documento: 19/07/2026



ATRIBUTOS QUALIFICADORES DO PTT

Impacto. Potencial de alcance imediato sobre as 110 IFES e, por extensão, sobre cerca de 250 órgãos do SISP: conversão do diagnóstico em priorização de investimentos e em comunicação qualificada com a alta administração — o elo que a pesquisa identificou como o mais frágil da efetividade do programa.

Aplicabilidade. Imediata e de custo zero: um arquivo aberto em qualquer navegador, sem instalação, rede ou autorização externa, aplicável em uma única sessão de trabalho e desenhado para o ciclo anual de planejamento. Replicável aos demais órgãos do SISP mediante recalibração do padrão de referência; o código aberto permite adaptação por qualquer ente. O produto está publicado em repositório público, com DOI (Zenodo), hash de integridade e mecanismo de aviso de novas versões.

Inovação. Até onde a pesquisa pôde apurar, é o primeiro instrumento de avaliação orientado a capacidades institucionais e efetividade percebida construído especificamente para o PPSI, com régua interpretativa calibrada por evidência empírica nacional (58 IFES) e priorização baseada nas associações observadas.

Complexidade. Reside na cadeia que sustenta o produto: revisão sistemática de 82 estudos, derivação da matriz de domínios, validação de conteúdo por especialistas (CVR de Lawshe), aplicação nacional, modelo interpretativo em camadas e algoritmo de priorização, documentados nos Capítulos 3 a 6 da dissertação. O código, deliberadamente simples e auditável, é a face visível dessa cadeia.

EVIDENCIAÇÃO DE IMPLEMENTAÇÃO E IMPACTO DA PROPOSTA

Impacto potencial. O produto ataca diretamente os dois resultados mais frágeis medidos pela pesquisa nacional: o reconhecimento de ganhos pela alta administração (média 3,91, única dimensão abaixo do ponto neutro) e a integração da gestão de riscos ao planejamento e ao orçamento (média 3,05, a capacidade mais associada à efetividade 0,612).

Cada aplicação institucional do GACE-PPSI produz, por construção, um relatório executivo dirigido à alta administração e uma lista de prioridades vinculada ao ciclo orçamentário: o uso do produto é, em si, a ativação do circuito de reconhecimento e priorização cuja ausência a pesquisa diagnosticou.

Evidências de impacto real. Campo a ser atualizado ao longo de até três quadriênios avaliativos, com: registros de recebimento do protocolo de entrega; declarações de uso emitidas pelas IFES adotantes; atas de comitês que apreciaram o relatório executivo; eventuais menções do órgão central; e métricas públicas do repositório de distribuição (downloads e adoções).

Evidências serão inseridas à medida que forem produzidas.