Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Programa de Privacidade e Segurança da Informação (PPSI) aplicado ao Governo Digital do Brasil

Leonardo Rodrigo Ferreira

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. Marcio de Carvalho Victorino

Brasília
2025

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

FF383p

Ferreira, Leonardo Rodrigo
Programa de Privacidade e Segurança da Informação (PPSI) aplicado ao Governo Digital do Brasil. / Leonardo Rodrigo Ferreira; orientador Marcio de Carvalho Victorino. Brasília, 2025.
140 p.

Dissertação(Mestrado Profissional em Computação Aplicada) Universidade de Brasília, 2025.

1. Privacidade.. 2. Proteção de Dados Pessoais.. 3. Segurança da Informação.. 4. Segurança Cibernética.. 5. Governo Digital.. I. Victorino, Marcio de Carvalho , orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Programa de Privacidade e Segurança da Informação (PPSI) aplicado ao Governo Digital do Brasil

Leonardo Rodrigo Ferreira

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. Marcio de Carvalho Victorino (Orientador)
Faculdade de Ciência da Informação

Prof. Dr. Milton Morais de Lima
Centro Integrado de Segurança em Sistemas Avançados (CISSA)

Prof. Dr. Andrei Lima Queiroz
Secretaria de TIC (UNB)

Prof. Dr. Edna Dias Canedo
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 12 de maio de 2025

Dedicatória

Dedico este trabalho a Deus, fonte de força e sabedoria em minha trajetória. Aos meus pais, pelo exemplo de integridade, dedicação e pelo suporte incondicional ao longo da minha vida. À minha esposa, companheira incansável, cujo amor, paciência e incentivo foram essenciais nesta jornada. À minha filha e ao meu filho, inspirações constantes, que me motivam a buscar sempre o melhor. A todos, minha mais profunda gratidão por estarem ao meu lado em cada desafio e conquista.

Agradecimentos

Agradeço ao Prof. Dr. Marcio de Carvalho Victorino pela dedicação, incentivo e paciência ao longo da jornada de orientação e construção desta dissertação. Seu comprometimento e valiosas contribuições foram fundamentais para a realização deste trabalho, motivo pelo qual expresso minha sincera gratidão.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

O presente trabalho apresenta a proposta de um Programa de Privacidade e Segurança da Informação (PPSI) voltado para os 254 órgãos que compõem o Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP) do governo federal do Brasil. A pesquisa percorreu um caminho que contextualiza a transformação digital do governo brasileiro, destacando a privacidade e a segurança da informação como pilares essenciais para o êxito desse processo. A reflexão inicial levou à definição do problema de pesquisa, seguida pelo delineamento metodológico, baseado na Teoria do Enfoque Meta-Analítico Consolidado (TEMAC) e em um estudo de caso confirmatório. Em seguida, realizou-se uma ampla revisão dos principais estudos sobre privacidade e segurança da informação, contribuindo para a construção do referencial teórico. Essa etapa permitiu aprofundar a compreensão dos conceitos de privacidade, proteção de dados, segurança da informação e segurança cibernética, além de explorar os principais frameworks aplicáveis. Os estágios iniciais da pesquisa serviram de base para o desenvolvimento da metodologia de construção do PPSI, cuja proposta foi testada e validada por meio da modelagem, aplicação e análise dos resultados obtidos junto aos órgãos do SISP. Para interpretar os dados, foi utilizado um modelo de avaliação de maturidade, que serviu como base para a análise crítica e permitiu compreender o nível de prontidão e evolução das instituições em relação à privacidade e à segurança da informação. Os resultados da aplicação do modelo evidenciaram avanços, desafios e oportunidades de aprimoramento, contribuindo para o fortalecimento da governança em privacidade e segurança no contexto governamental.

Palavras-chave: PPSI, Privacidade, Proteção de Dados Pessoais, Segurança da Informação, Segurança Cibernética, Governança, Maturidade, Metodologia, Governo Digital.

Abstract

This dissertation presents the proposal for a Privacy and Information Security Program (PISP) aimed at the 254 agencies that make up the Integrated System for the Administration of Information Technology Resources (SISP) of the Brazilian federal government. The research contextualizes the digital transformation of the Brazilian government, highlighting privacy and information security as essential pillars for the success of this process. The initial reflection led to the definition of the research problem, followed by the methodological design based on the Consolidated Meta-Analytical Approach Theory (TEMAC) and a confirmatory case study. A comprehensive review of key studies on privacy and information security was carried out, contributing to the construction of the theoretical framework. This stage deepened the understanding of concepts such as privacy, data protection, information security, and cybersecurity, as well as the main applicable frameworks. The initial stages of the research provided the foundation for developing the PISP methodology, which was tested and validated through modeling, implementation, and analysis of the results obtained with SISP agencies. To interpret the data, a maturity assessment model was applied, serving as a reference for critical analysis and enabling an understanding of the institutions' level of readiness and progress in privacy and information security. The results of the model's application revealed significant advancements, challenges, and opportunities for improvement, contributing to the strengthening of governance in privacy and security within the governmental context.

Keywords: PISP, Privacy, Personal Data Protection, Information Security, Cybersecurity, Governance, Maturity, Methodology, Digital Government.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

DATAPREV Empresa de Tecnologia e Informações da Previdência.

DEPSI Departamento de Privacidade e Segurança da Informação.

GDPR General Data Protection Regulation.

LGPD Lei Geral de Proteção de Dados.

MGI Ministério de Gestão e Inovação em Serviços Públicos.

PNSI Política Nacional de Segurança da Informação.

PPSI Programa de Privacidade e Segurança da Informação.

SCOPUS SCOPUS.

SERPRO Serviço Federal de Processamento de Dados.

SGD Secretaria de Governo Digital.

SISP Sistema Integrado de Administração de Recursos de Tecnologia da Informação.

TEMAC Teoria do Enfoque Meta-Analítico Consolidado.

WoS Web of Science.

Capítulo 1

Introdução

1.1 Contextualização

Atualmente, organizações públicas e privadas enfrentam um cenário repleto de oportunidades e desafios decorrentes do fenômeno da transformação digital. Esse fenômeno, sob uma perspectiva macro, refere-se às profundas mudanças ocorridas na sociedade, na indústria e nos governos a partir do uso intensivo das tecnologias digitais [1]. No âmbito governamental, pode ser conceituado como uma transformação acelerada de atividades, processos, competências e modelos de negócio, visando potencializar os impactos e oportunidades gerados pelas tecnologias digitais, de forma estratégica, humanizada e orientada às prioridades públicas [2].

No Brasil, esse movimento é liderado pela Secretaria de Governo Digital(SGD), vinculada ao Ministério da Gestão e da Inovação em Serviços Públicos (MGI), que tem entre suas atribuições a definição de diretrizes, a normatização e a coordenação de projetos de simplificação de serviços, transformação digital de políticas públicas, governança e compartilhamento de dados, bem como o uso de canais digitais [3].

Essa estratégia de transformação digital tem sido amplamente reconhecida por diferentes setores da sociedade, da indústria, dos governos e da academia. Esse reconhecimento foi recentemente reforçado pelo *GovTech Maturity Index* (GTMI), publicado pelo Banco Mundial, que é considerado a medida mais abrangente de maturidade em transformação digital no setor público. O índice avalia quatro áreas centrais: o suporte aos principais sistemas governamentais, a melhoria da prestação de serviços públicos, a integração do cidadão nos processos digitais e a presença de facilitadores tecnológicos. Em sua edição de 2022, o Brasil foi apontado como o segundo país mais maduro entre as 198 economias analisadas, ficando atrás apenas da Coreia do Sul [4].

Esse é, portanto, um cenário bastante promissor para o governo digital brasileiro, para a sociedade e, em última instância, para o cidadão. Contudo, surgem também importan-

tes desafios relacionados à privacidade, à proteção de dados pessoais e à segurança da informação e à segurança cibernética, especialmente no que diz respeito ao tratamento de dados governamentais e dos cidadãos sob custódia do Estado. O relatório *Global Cybersecurity Outlook* 2023, publicado pelo Fórum Econômico Mundial, destaca como principais preocupações dos líderes empresariais e cibernéticos aspectos como a instabilidade geopolítica, o rápido amadurecimento das tecnologias emergentes, a escassez de profissionais qualificados nas áreas de privacidade e segurança da informação, o aumento das expectativas da sociedade e dos reguladores, além dos efeitos persistentes da pandemia e da digitalização acelerada [5].

Esse conjunto de fatores evidencia a necessidade de estruturação, por parte da SGD, de um conjunto articulado de medidas preventivas, detectivas e corretivas voltadas à privacidade, à proteção de dados, à segurança da informação e à segurança cibernética, especialmente no contexto da estratégia federal de governo digital. Essa estratégia é composta por um ecossistema robusto de plataformas, soluções e serviços digitais oferecidos a cidadãos, empresas e à sociedade em geral.

Atualmente, a Plataforma Gov.br conta com mais de 165 milhões de usuários ativos e oferece cerca de 4.500 serviços digitais, provendo soluções por meio de mais de 250 órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do governo federal, além das empresas públicas de tecnologia da informação e comunicação, como (SERPRO e DATAPREV) [6].

1.2 Definição do Problema

A recente publicação do Decreto nº 12.102, de 08 de julho de 2024, consolidou a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da SGD/MGI. O referido decreto atribui à SGD/MGI a importante missão de atuar como órgão central SISP. Cabendo-lhe o papel de apoiar ações de fomento à segurança da informação e proteção a dados pessoais no âmbito da administração pública federal, em articulação com os órgãos responsáveis por essas políticas no âmbito do governo federal. [7].

A implementação dessas atribuições está sob responsabilidade da Diretoria de Privacidade e Segurança da Informação (DEPSI), unidade integrante da SGD. Competindo ao DEPSI:

1. Planejar e implementar projetos de privacidade e proteção de dados pessoais, no âmbito da administração pública federal direta, autárquica e fundacional, observadas as atribuições da Autoridade Nacional de Proteção de Dados, nos termos do disposto na Lei nº 13.709, de 2018.

2. Planejar e implementar projetos de segurança da informação baseados na eficiência, na eficácia e na qualidade dos serviços públicos federais, no âmbito da administração pública federal direta, autárquica e fundacional, observadas as atribuições dos demais órgãos do Poder Executivo Federal.

3. Adotar medidas de comunicação, diagnóstico, engajamento, capacitação e compartilhamento de competências sobre privacidade e segurança da informação, direcionadas aos órgãos do SISP e aos demais órgãos e entidades da administração pública federal direta, autárquica e fundacional.

4. Apoiar ações de fomento a privacidade, proteção de dados pessoais e segurança da informação no âmbito da administração pública federal, em articulação com os órgãos e as entidades responsáveis por essas ações.

5. Atuar em iniciativas, projetos e programas relacionados às temáticas de privacidade e segurança da informação, em conjunto com outros órgãos e entidades da administração pública e com instituições, públicas ou privadas, nacionais ou internacionais.

Essas temáticas estão fundamentadas em normativos estratégicos como a Lei Geral de Proteção de Dados(LGPD), a Política Nacional de Segurança da Informação (PNSI) e a Política Nacional de Cibersegurança (PNCiber, os quais estabelecem diretrizes claras para as organizações públicas brasileiras sobre como tratar adequadamente dados pessoais, garantir a segurança da informação e promover práticas cibernéticas responsáveis.

Tais diretrizes impactam diretamente a estratégia de Governo Digital do Brasil, tornando urgente o fortalecimento da maturidade e da resiliência dos órgãos integrantes do SISP. Esses órgãos são os principais responsáveis pela disponibilização de mais de 4.500 serviços públicos digitais acessados diariamente por milhões de cidadãos brasileiros. O crescimento exponencial desse ecossistema digital exige das instituições públicas não apenas conformidade normativa, mas também capacidade institucional contínua de adaptação, resposta e prevenção a riscos digitais.

Dessa forma, o problema de pesquisa que orienta este trabalho pode ser assim sintetizado:

Como a SGD/MGI poderá contribuir com ações nas temáticas de privacidade e segurança da informação para o aumento da maturidade e resiliência dos 254 órgãos do SISP provedores de serviços do Governo Digital do Brasil?

1.3 Justificativa do Tema

As pesquisas sobre as temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética vem crescendo de forma exponencial no cenário internacional, como constata-se em pesquisa exploratória realizada nas bases de conhecimento *Web Of Science (WOS)* [8] e *SCOPUS* [9] . Tais pesquisas concentram-se no estudo isolado das temáticas acima apontadas, geralmente, com a proposição de conceitos, programas, frameworks e ou modelos para as organizações públicas ou privadas.

Por outro lado, quando buscamos conectar pesquisas com as temáticas de privacidade e segurança da informação, objetivando identificar programas, modelos e frameworks de privacidade e segurança da informação, construídos dentro de uma visão unificada, abrangente e complementar, os resultados retornados nas bases referenciadas são bastante escassos, e em alguns poucos casos, um tanto superficiais quanto à perspectiva de aplicabilidade prática.

Dessa forma, considerando-se que as bases de dados *Web Of Science (WOS)* e *SCOPUS*, com publicações de elevado rigor científico, qualidade e abrangência, vislumbra-se que o objeto desta pesquisa poderá contribuir de maneira substancial para suprir a presente lacuna. Surgindo benefícios tanto para o Programa de Pós-Graduação em Computação Aplicada (PPCA) da Universidade de Brasília – UNB, quanto para a SGD/MGI.

Para a SGD a pesquisa trará uma série de benefícios sob várias perspectivas:

- Numa perspectiva de compliance contribuirá para adequação dos 254 órgãos do SISP às exigências normativas da LGPD e da PNSI, dentre outras legislações e orientações jurisprudenciais dos órgãos de controle interno e externo.

- Numa perspectiva de padronização contribuirá para uniformização dos procedimentos relativos à privacidade e segurança da informação relativos aos processos de trabalho, qualificação de pessoas e adoção de tecnologias, nos 254 órgãos do SISP.

- Numa perspectiva institucional contribuirá para o aumento da maturidade e resiliência, em termos de privacidade e segurança da informação, com estabelecimento de padrões mínimos aceitáveis, nos 254 órgãos do SISP.

- Numa perspectiva de gestão de riscos contribuirá para minimizar possíveis danos ligados aos aspectos reputacionais, financeiros e ou materiais decorrentes de incidentes de segurança ocorridos na gestão dos dados pessoais dos cidadãos, bem como nos aspectos ligados à privacidade e segurança da informação das plataformas, soluções e ou sistemas governamentais.

- Numa perspectiva de equidade, transparência e *accountability* contribuirá para o aumento da governança, transparência, confiança da sociedade e dos cidadãos, quanto à coleta, armazenamento, processamento e descartes dos dados pessoais custodiados pelo Estado brasileiro, em suas plataformas governamentais.

1.4 Objetivo Geral

Propor um Programa de Privacidade e Segurança da Informação (PPSI) que contribua nas temáticas de privacidade e segurança da informação para o aumento da maturidade e resiliência dos 254 órgãos do SISP provedores de serviços do Governo Digital do Brasil.

1.5 Objetivos Específicos

Buscando alcançar o objetivo geral proposto, os seguintes objetivos específicos foram estabelecidos:

- Consolidar os principais marcos legais nacionais e internacionais relacionados à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.
- Levantar e analisar trabalhos relacionados às temáticas de privacidade e segurança da informação, identificando abordagens relevantes que possam subsidiar a construção do programa proposto.
- Identificar as principais disciplinas teóricas sobre privacidade e segurança da informação que fundamentem a construção de um programa unificado de privacidade e segurança da informação.
- Mapear arquiteturas, frameworks e modelos relacionados à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, com base em referências nacionais e internacionais.
- Desenvolver um modelo de maturidade institucional em privacidade e segurança da informação, que permita avaliar e acompanhar o grau de evolução dos órgãos públicos.
- Propor um projeto piloto com os órgãos do SISP, visando à validação das premissas e da aplicabilidade do Programa de Privacidade e Segurança da Informação (PPSI).

1.6 Estrutura do Trabalho

O presente trabalho está estruturado nos seguintes capítulos:

- O Capítulo 2 define o procedimento metodológico adotado na presente pesquisa, adotando-se a Teoria do Enfoque Meta-Analítico Consolidado (TEMAC) como base para construção dos Capítulos 3 e 4. Seguido da estratégia de aplicar um estudo de caso confirmatório como base para proposta de validação do Programa de Privacidade e Segurança da Informação (PPSI).
- O Capítulo 3 discute os principais trabalhos relacionados ao objeto da pesquisa, ou seja, são identificadas as principais arquiteturas, frameworks, modelos, disciplinas e resultados discutidos pelos autores nas temáticas de privacidade e segurança da informação que darão suporte apara o desenvolvimento da presente pesquisa.
- O Capítulo 4 constrói a fundamentação teórica da pesquisa baseadas em conceitos, arquiteturas, frameworks, modelos, abordagens e tecnologias utilizados como suporte para desenvolvimento da pesquisa nas temáticas de privacidade e segurança da informação.
- O Capítulo 5 apresenta o Programa de Privacidade e Segurança da Informação (PPSI) suportado por uma metodologia formada pela consolidação dos estudos desenvolvidos nos capítulos 1, 2, 3 e 4 da presente pesquisa.
- O Capítulo 6 apresenta o modelo de maturidade do Programa de Privacidade e Segurança da Informação (PPSI) que subsidiou o estudo de caso confirmatório junto aos órgãos integrantes do SISP.
- O Capítulo 7 aplica o estudo de caso confirmatório realizado para avaliar a implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP).
- O Capítulo 8 discute os resultados do estudo de caso confirmatório do Programa de Privacidade e Segurança da Informação (PPSI) junto aos órgãos integrantes do SISP.

Capítulo 2

Procedimento Metodológico

Na visão de Wazlawick [10], o método de pesquisa é composto por um conjunto de etapas necessárias para demonstrar como os objetivos do trabalho serão alcançados ao longo da pesquisa. Assim, o presente estudo buscou adotar duas estratégias para o alcance dos objetivos da pesquisa:

- Primeiro, aplicando a Teoria do Enfoque Meta-Analítico Consolidado (TEMAC) para o levantamento dos principais trabalhos relacionados ao objeto de pesquisa e posterior construção do referencial teórico do estudo.
- Segundo, conduzindo um estudo de caso confirmatório, com implementação do Programa de Privacidade e Segurança da Informação (PPSI), junto a subconjunto de organizações do Sistema Integrado de Administração de Recursos de Tecnologia da Informação (SISP) do governo federal, objetivando a confirmação das premissas trazidas pelo PPSI.

2.1 Teoria do Enfoque Meta-Analítico Consolidado - TEMAC

Atualmente, diante do alto volume de informações geradas, da grande variedade de fontes de pesquisas, da velocidade de produção e de sua da qualidade, podemos afirmar que estamos diante de um cenário bastante promissor para o processo de pesquisa científica, com potencial para a busca de soluções para os mais diversos problemas das organizações. Sendo essencial assegurar que toda pesquisa garanta a relevância do tema estudado, a validade, confiabilidade e qualidade das informações, bem como apresente os trabalhos mais relevantes já produzidos sobre a temática objeto do trabalho.

Neste cenário, é essencial que o pesquisador lance mão de métodos para estruturação do trabalho de identificação, coleta e análise dos trabalhos científicos disponíveis.

Dessa forma, a revisão do estado da arte utilizou como referência a Teoria do Enfoque Meta-Analítico Consolidada (TEMAC). O referido método destaca a importância da identificação das principais discussões científicas sobre um determinado tema, identificando sua relevância, qualidade, quantidade e a direção das pesquisas para obtenção de uma base de dados qualificada para a realização da pesquisa. O método é descrito de forma sumarizada nos itens subsequentes, bem como são apresentados os resultados da aplicação do referido método no contexto das temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética. [11]

2.1.1 Descrição do método

De acordo com Mariano e Rocha [11], o TEMAC está dividido em três etapas, a saber:

- **Preparação da pesquisa (múltiplas bases de dados).**
- **Apresentação e interrelação dos dados.**
- **Detalhamento, modelo integrador e validação por evidências.**

2.1.2 Preparação da Pesquisa

Na fase de preparação das pesquisas buscamos abordar quatro questões centrais sugeridas pelo método como a definição das palavras-chaves ligadas ao tema do estudo, o espaço temporal da pesquisa, as bases de dados que serão utilizadas, bem como as áreas de conhecimento que serão consideradas.

a) Bases de dados utilizadas

As plataformas *Web of Science (WoS)* [8] e *SCOPUS* [9] foram utilizadas como referências para a presente pesquisa, em função da reconhecida qualidade das informações contidas nas bases, extensa cobertura temporal das publicações, grande variedade de títulos indexados, bem como a existência de plataformas próprias com extensa quantidade de ferramentas que facilitam a identificação, análise, extração e apresentação das informações.

b) Espaço temporal da pesquisa

As pesquisas nas bases *WoS* e *SCOPUS* adotaram estratégias complementares quanto ao horizonte temporal, na primeira base buscou-se utilizar o maior tempo possível disponível na referida base de tempo, entre 1945 e 2022, objetivando compreender o surgimento, evolução e consolidação do tema. De forma complementar, buscou-se utilizar a seguranda

base para refinamento das pesquisas, utilizando-se o espaço temporal de 5 anos (2018 a 2022), conforme sugerido por Mariano e Rocha [11].

c) Termos de pesquisa

No contexto da construção de programas, modelos, metodologias e ou frameworks nas temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, buscou-se identificar as palavras-chave da pesquisa utilizando-se cinco publicações referencias, de organismos internacionais, do campo da privacidade e da segurança da informação: *Center for Internet Security (CIS)* [12], *National Institute of Standards and Technology (NIST)* [13], *General Data Protection Regulation (GDPR)* [14], *DAMA INTERNACIONAL* [15] e ABNT NBR ISO/IEC 27001:2022 [16]. Resultando nas seguintes palavras-chave:

Tabela 2.1: Termos de Pesquisa: PPSI

Privacy	**Information Security**	**Cybersecurity**	**Programme**
Privacy	Information Security	Cybersecurity	Programme
Data Privacy	ISO/IEC 27001:2022	Cyber Threat	Architecture
Data Protection	ISMS	Cyber Space	Framework
Data Management	System	Cyber Intelligence	Model
Data Governance	Management	Cyber Defense	Governance
Data Quality	Risk	Cyber Crimes	Technology
Data Security	Controls	Cyber Resiliency	People
Data Interoperability	Performance	Cyber Maturity	Maturity
Personal Data Protection	Responsibilities	Cyber Programme	Methodology

Na sequência do trabalho, foram identificados os principais artigos compatíveis com o foco dessa pesquisa, realizando diversas combinações dos termos de pesquisa acima, resultado nas palavras-chave utilizadas como motor de busca nas plataformas *WoS e SCOPUS*. Considerando a similaridades dos resultados encontrados nas pesquisas em ambas as bases, os 422 artigos encontrados na base *SCOPUS*, foram incorporados a uma ferramenta da plataforma denominada de lista marcada, permitindo a extração de informações sobre os autores, anos das publicações, tipos de documentos, áreas do conhecimento, bem como publicações por países, dentre outras.

Pesquisa realizada em 14 de fevereiro de 2023 com os seguintes resultados:

d) Preparação dos dados para análise

Considerando a pesquisa inicial nas bases *WoS e SCOPUS*, a delimitação temporal, as áreas do conhecimento e tendo em perspectiva o tema central da dissertação no campo da privacidade, proteção de dados pessoais, segurança cibernética e segurança da informação,

Pesquisas	Palavras-chave	Resultados WoS	Total	Resultados Scopus	Total
1	*("Personal Data Protection" OR "Data Protection" OR "Data Privacy") AND (Frame*)*	43	43	55	55
2	*("Personal Data Protection" OR "Data Protection" OR "Data Privacy") AND (Model*)*	46	89	50	105
3	*("Personal Data Protection" OR "Data Protection" OR "Data Privacy") AND (Programme*)*	1	90	1	106
4	*("Information Security" OR "ISO/IEC 27001" OR "ISMS") AND (Frame*)*	104	194	77	183
5	*("Information Security" OR "ISO/IEC 27001" OR "ISMS") AND (Model*)*	186	380	50	233
6	*("Information Security" OR "ISO/IEC 27001" OR "ISMS") AND (Programme*)*	4	384	5	238
7	*("Cybersecurity" OR "Cyber Resiliency" OR "Cyber Maturity") AND (Frame*)*	97	481	100	338
8	*("Cybersecurity" OR "Cyber Resiliency" OR "Cyber Maturity") AND (Model*)*	108	589	50	388
9	*("Cybersecurity" OR "Cyber Resiliency" OR "Cyber Maturity") AND (Programme *)*	1	590	6	394
10	*("Personal Data Protection" AND "Information Security")*	2	592	2	396
11	*("Cybersecurity" AND "Information Security")*	15	607	23	419
12	*("Personal Data Protection" AND "Cybersecurity")*	2	609	3	422

Figura 2.1: Artigos Pré-Selecionados
Fonte: Própria

buscou-se aplicar filtros a base de dados pré-selecionada com objetivo de incluir referências bibliográficas como fontes de pesquisa, bem adotar critérios para a exclusão de algumas bibliografias não alinhadas com o tema central da pesquisa. Critérios operacionalizados pela leitura dos resumos das publicações, leitura completa de um conjunto específico de artigos, bem como o uso de ferramentas de análises das plataformas *WoS e SCOPUS*. Resultando nos seguintes ajustes:

d.1) Espaço temporal da pesquisa

Na figura 2.3 apresenta-se o refinamento dos resultados da base de dados das pesquisas individuais consolidadas, buscamos restringir o período temporal da pesquisa para os anos de 2018 a 2022. Resultando em 402 registros, distribuídos da seguinte forma:

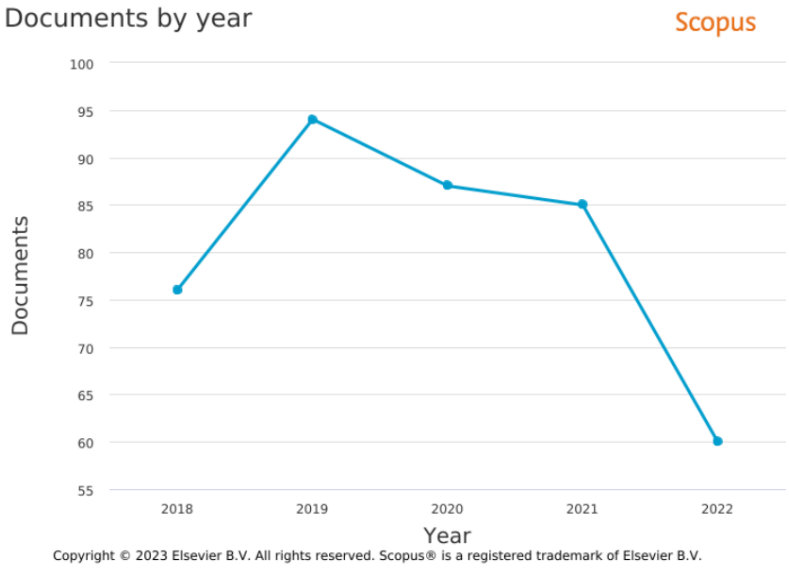

Figura 2.2: Evolução Temporal
Fonte: SCOPUS [9]

d.2 Áreas do conhecimento

No processo de definição das áreas de interesse da pesquisa buscamos nos concentrar nas áreas da Ciência da Computação e Engenharia, com publicações classificadas de forma concomitante nas áreas de Matemática, Ciências da Decisão, Ciências Sociais, Negócios, dentre outras. Decisão relevante considerando as etapas subsequentes do trabalho que primará pela qualidade das publicações que alicerçarão as discussões sobre os trabalhos relacionados e construção do referencial teórico.

Restando 401 registros, distribuídos na figura 2.4 nas seguintes áreas do conhecimento:

d.3 Tipos de documentos

Na sequência do trabalho optamos por considerar entre categorias elegíveis para integrar as futuras referências bibliográficas da pesquisa os estudos classificados como artigos e artigos de conferência, deixando de fora da pesquisa os capítulos de livros, revisões sistemáticas e notas em função da coerência das publicações com o escopo da pesquisa. Resultando em total de 368 publicações apresentadas na Figura 2.5.

d.4 Linguagem dos documentos

Por fim, buscamos manter na base de dados que guiará a presente pesquisa os trabalhos produzidos em língua inglesa, considerando a ampla aceitação da referida língua na

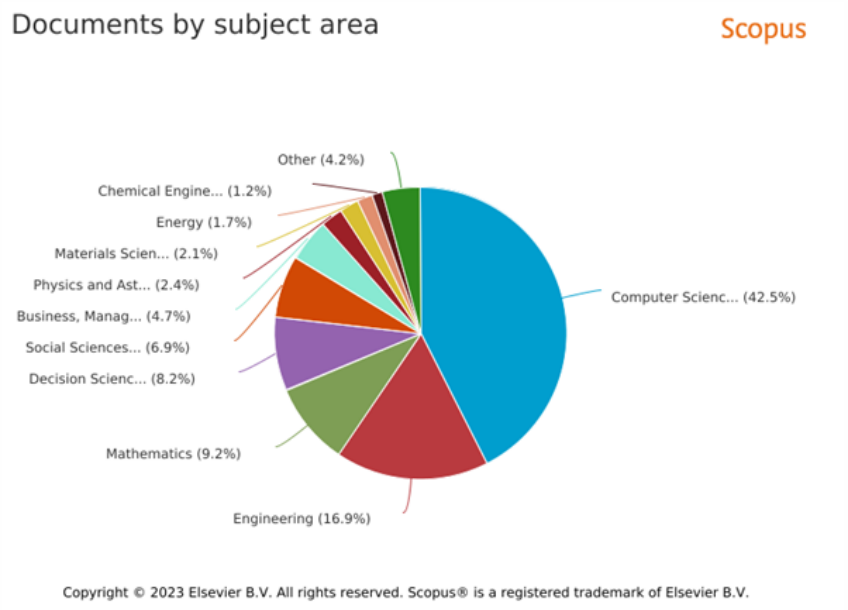

Figura 2.3: Áreas do Conhecimento
Fonte: SCOPUS [9]

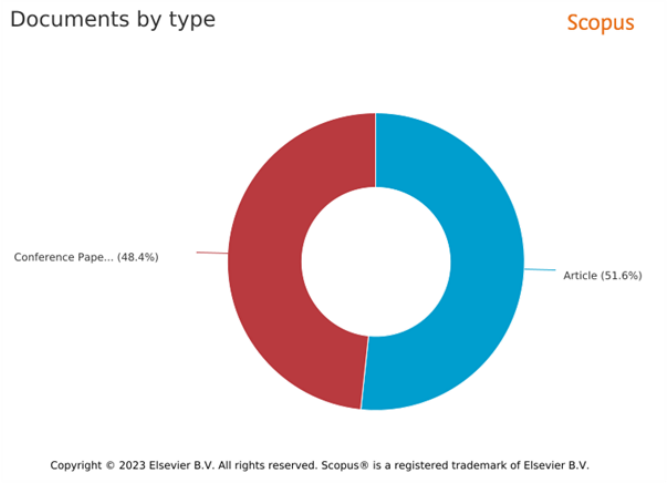

Figura 2.4: Tipos de Documentos
Fonte: SCOPUS [9]

comunidade acadêmica internacional. Consolidando-se em uma base de dados com 362 registros que constituirá as futuras referências bibliográficas da pesquisa.

2.1.3 Apresentação dos dados e inter-relações

Na etapa de análise das inter-relações dos dados, utilizou-se o software de mapeamento de redes VOSviewer[17], o referido programa é largamente empregado em pesquisas aca-

dêmicas, apresentando como fatores positivos sua gratuidade, precisão e facilidade de utilização.

a) Palavras-chave

Considerando a associação de palavras-chaves utilizadas nas pesquisas, é possível identificar a ocorrência de termos que aparecem juntos em clusters, facilitando a identificação de diferentes linhas de pesquisas.

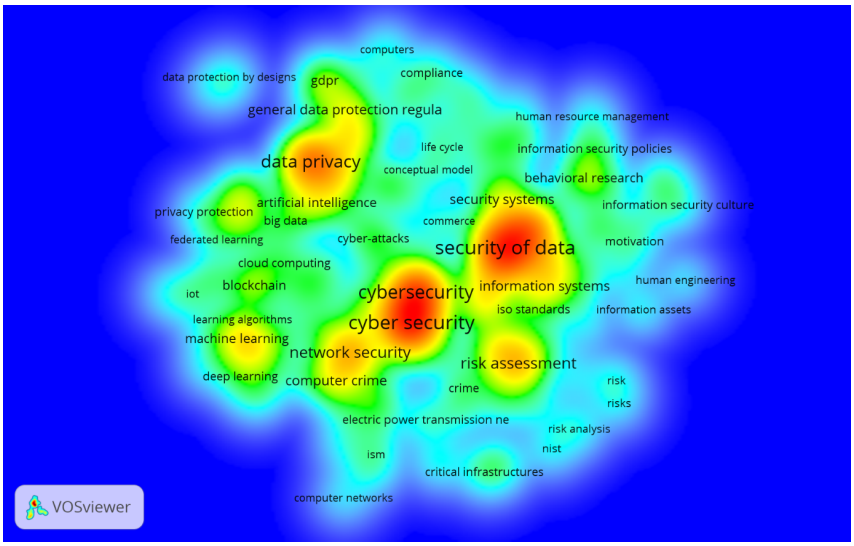

Figura 2.5: Palavras-Chave
Fonte: VOSviewer [17]

Numa análise preliminar do mapa de calor, verifica-se a ocorrência de um conjunto de clusters predominantemente concentrados nos termos *"Security of Data"*, *"Cybersecurity* ou *Cyber Security"* e *"Data Privacy"*. Porém, aprofundando-se a análise no mapa de calor encontramos outras possíveis linhas de pesquisa que podem ser úteis na construção dos elementos constitutivos da presente dissertação, a saber:

Cluster 1 (124 itens): Destaque para as abordagens sobre *Big Data*, *Cloud Computing*, *Internet of Things (IoT)*, *Deep Learning*, *Machine Learning*, *Data Mining*,*Network Securit* voltadas para o contexto da privacidade, proteção de dados e segurança da informação.

Cluster 2 (21 itens): Ênfase para os temas como *Conceptual Frameworks, Human Resource Management, Personnel, Motivation, Policies, Culture, Risks*, no contexto da segurança da informação, segurança de sistemas e segurança de dados.

Cluster 3 (18 itens): Significativo destaque para os temas de *Frameworks, Awareness, Assessment, Education Computing, Higher Education, Industrial Research* no contexto de ataques cibernéticos, redes de computadores e segurança cibernética.

Cluster 4 (17 itens): Forte concentração dos temas como *Artificial Intelligence, Compliance, Compliance Control, Conceptual Model, Laws and Legislation, GDPR, Legal Frameworks*, nos campos da privacidade, privacidade de dados pessoais e proteção de dados pessoais.

Cluster 5 (15 itens): Denota a importância da *Digital Transformation, Industrial Management, Information Management, Information Systems, Information Use, Governance, ISO 27001:2022*, no contexto da Segurança da Informação.

Cluster 6 (11 itens): Aponta os aspectos como *Budget Control, Cost, Cost Beneficit Analysis, Investments, Design, Methodology, Approach, Personnel Training*, no contexto do gerenciamento de riscos de privacidade e segurança da informação no âmbito do processo decisório dos gestores.

Cluster 7 (10 itens): Surge a discussão sobre a proteção de *Critical Infrastructures, Application Programs, Vulnerability Assessments*, no contexto da adoção de *frameworks* e modelos de maturidade em segurança cibernética, inclusive trazendo referências internacionais sobre o tema como o *Nacional Institute of Standards and Technology (NIST).*

b) Evolução do tema ano a ano

A Figura 2.6 demostra uma curva acentuada de crescimento das publicações nas áreas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética a partir do ano de 2017 com um pico no ano de 2019, tendência fortemente explicada pela publicação da GDPR no ano de 2016, com efeitos legais a partir de maio de 2018 para toda União Europeia. Fator que além de alavancar as discussões sobre as temáticas de privacidade e proteção de dados pessoais, intensificou os debates sobre segurança de dados, segurança da informação e segurança cibernética.

Cabendo ainda destacar na Figura 2.6 uma lenta queda no número de publicações nos anos subsequentes a 2019, com o menor número de publicações ocorrendo no ano de 2022. Fenômeno explicado em parte pelo arrefecimento das discussões em torno no início da vigência da GDPR na Europa, além de uma questão já apontada na pesquisa, ou seja, o fato das temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética serem tratadas de forma isolada na literatura especializada, com poucos trabalhos preocupando-se com uma integração efetiva das discussões sobre privacidade e segurança da informação.

c) Número de citações

Já em relação ao número de citações, há forte tendência de crescimento ao longo dos anos, como apontado na Figura 2.7. Característica que reforça o interesse crescente pelas temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança

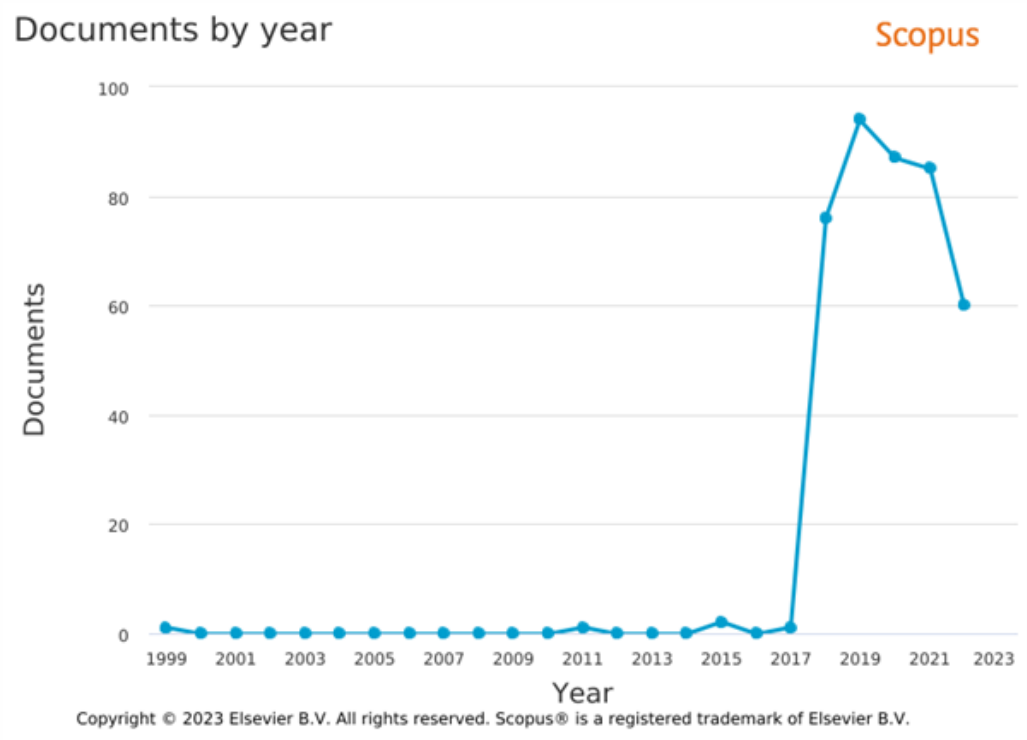

Figura 2.6: Evolução do Tema Ano-a-Ano
Fonte: SCOPUS [9]

cibernética, tratados como temáticas independentes, nos alertando, novamente, para escassez de publicações de qualidade que abordem as temáticas previamente citadas de forma integrada, complementar e sinérgica. Além, claro, de apontar para a qualidade dos 362 artigos previamente selecionados para presente pesquisa.

d) Principais autores

Buscando trazer visibilidade sobre os autores que mais publicaram nas áreas de privacidade, proteção de dados, segurança da informação e segurança cibernética na presente pesquisa, destaca-se na Figura 2.8 um seleto conjunto de 15 autores que tiveram de 2 a 6 publicações identificadas na base de dados tratada, que contou com um universo total de 158 autores.

e) Autores mais citados

A Figura 2.9 apresenta os autores mais citados no conjunto dos 362 trabalhos selecionados para a pesquisa, com destaque para ocorrência de 13 clusters que dominam os cenários das pesquisas nas temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética. Sendo importante destacar os trabalhos Govender S.G, Loock M., e Kritzingger.E (Cluster 1), com a publicação de 4 trabalhos nas áreas

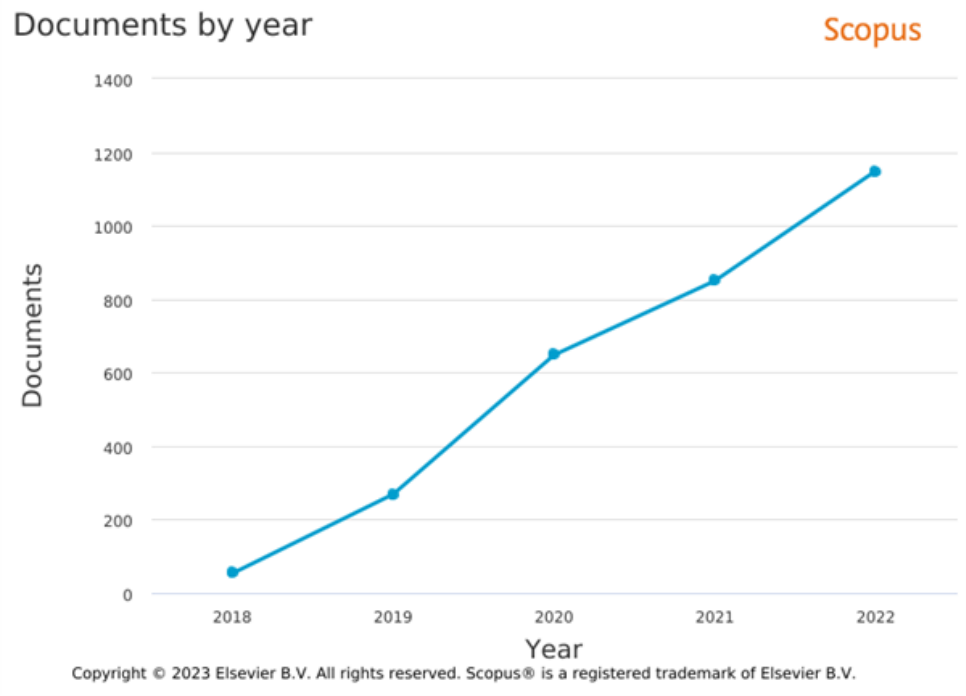

Figura 2.7: Número de Citações
Fonte: SCOPUS [9]

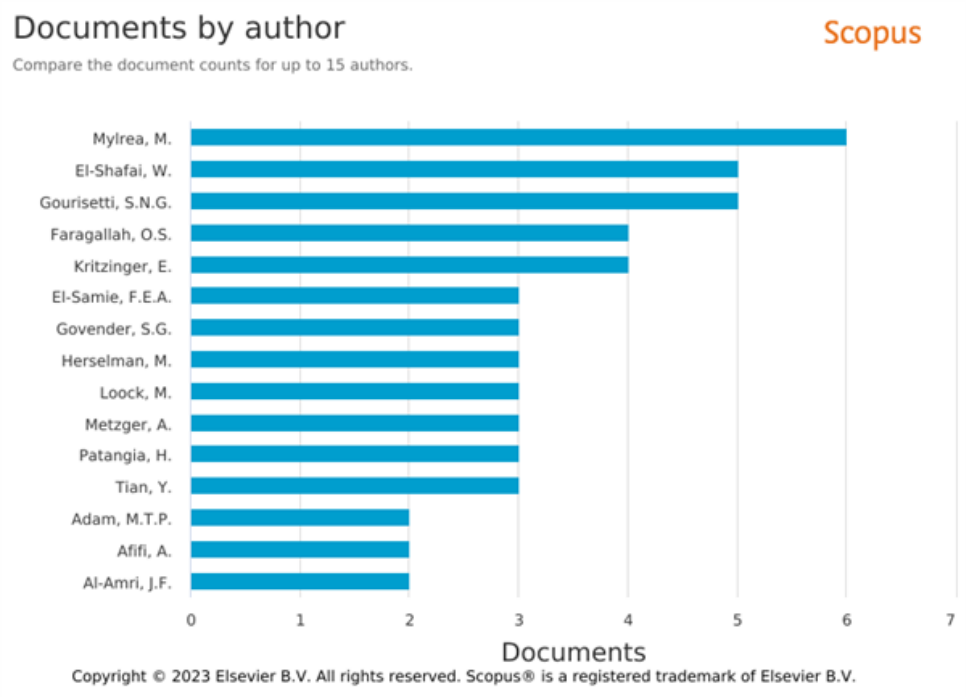

Figura 2.8: Autores mais Ativos
Fonte: SCOPUS [9]

de proposição de frameworks e ferramentas nas áreas de segurança da informação, riscos

em segurança da informação e proteção de dados, bem como os trabalhos de Mylrea M., Patangia H. e Gourisetti S.N.G (Cluster 2), focados na construção de frameworks dentro das várias disciplinas da área do conhecimento de segurança cibernética.

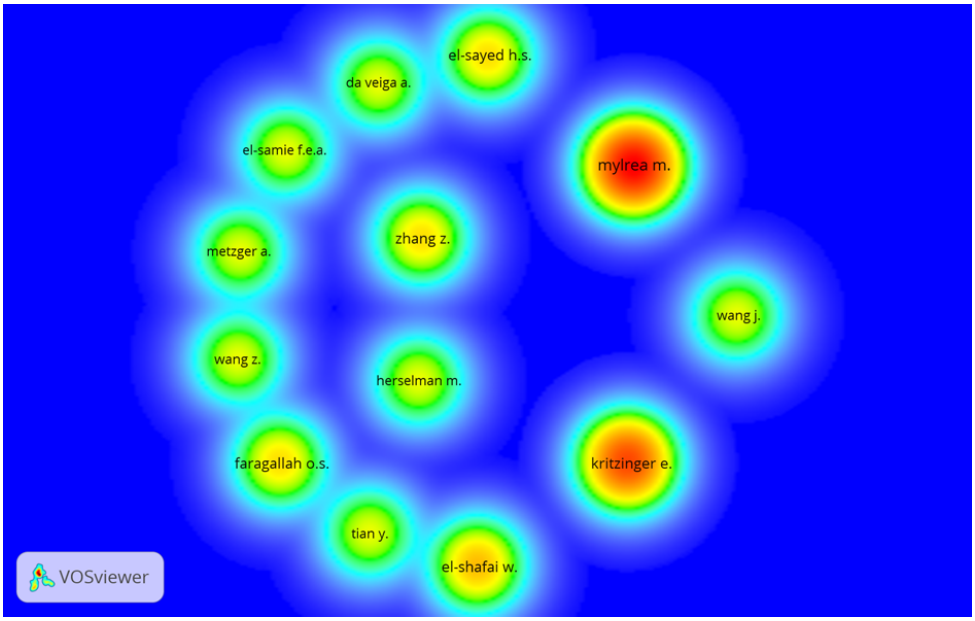

Figura 2.9: Autores mais Citados
Fonte: VOSVIEWER [17]

f) Países (Produção e Citação)

Buscou-se segmentar a análise da produção científica por países, dentro de campo de estudo da pesquisa, em duas vertentes, uma primeira focada nos países que mais publicaram sobre as temáticas nos últimos 5 anos, e uma segunda linha de trabalho destacando os trabalhos mais citados por países. Deixando em perspectiva o Brasil frente a ambos os cenários, considerando as possíveis contribuições do presente trabalho para produção científica nacional.

Quando analisa-se a a Figura 2.10 verifica-se uma supremacia nas publicações de países como Estados Unidos (65 publicações), Índia (35 publicações), China (27 publicações), Reino Unido (26 publicações) e África do Sul (23 publicações), além de outros países com considerável produção científica sobre o tema. Destacando-se o fato de o Brasil aparecer no ranking com apenas 5 publicações, majoritariamente voltadas para proposição de frameworks voltados para segurança da informação ou proteção de dados pessoais, com uma abordagem isolada dos temas, minimizando as relações de interdependência que existem entre as temáticas de privacidade e segurança cibernética.

Partindo para uma análise da Figura 2.11 identificamos um domínio em relação às citações de trabalhos científicos produzidos pelos países como China (637 citações), Estados

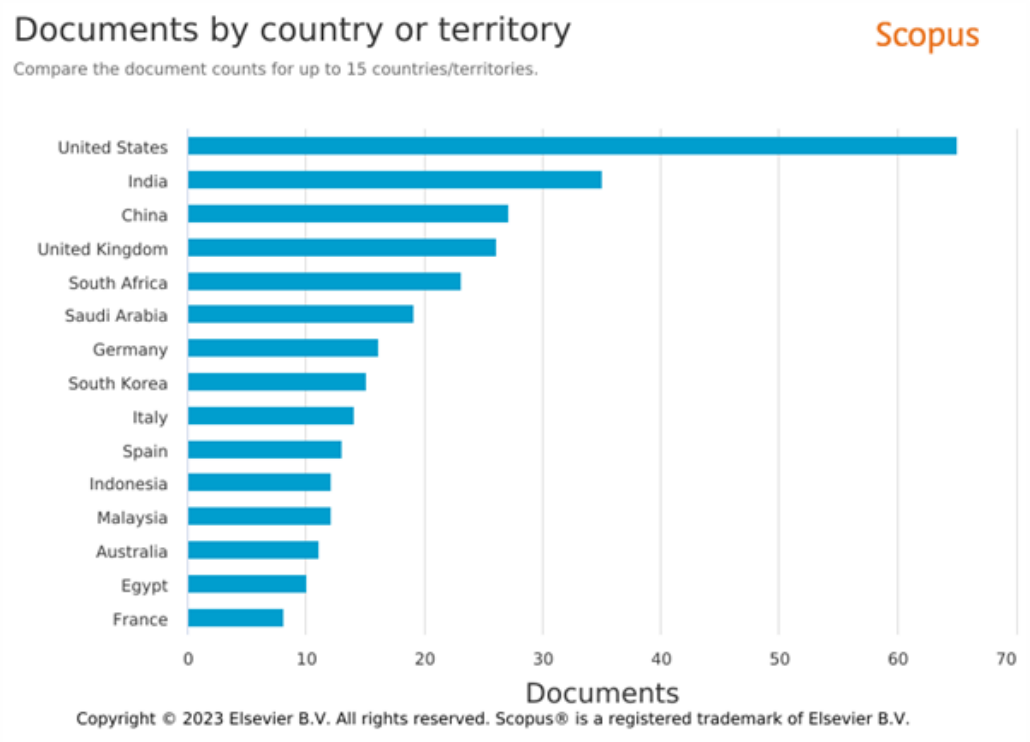

Figura 2.10: Produção Científica
Fonte: SCOPUS [9]

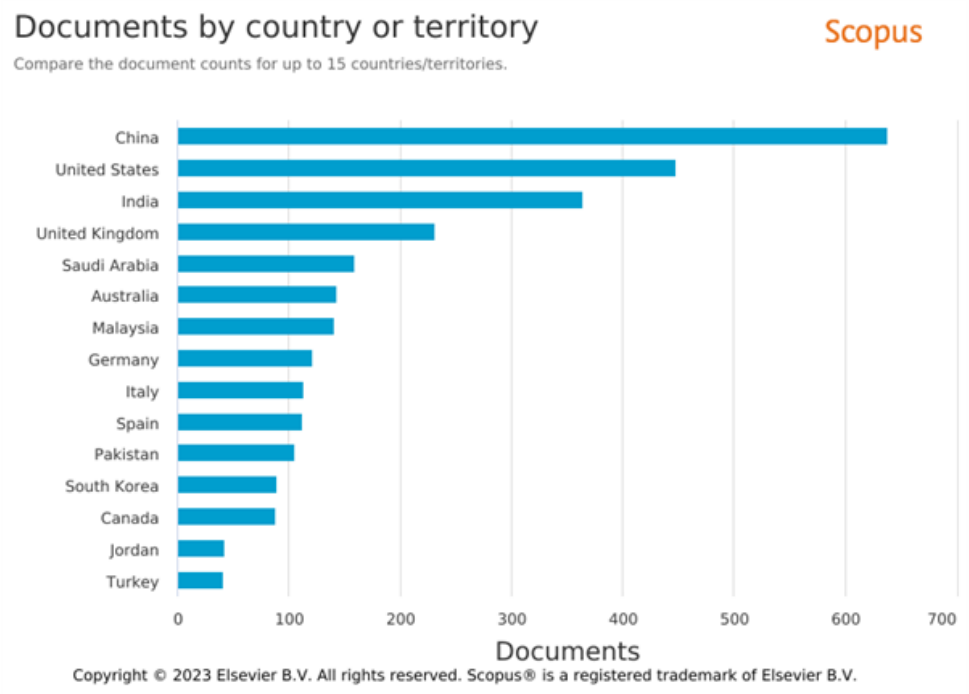

Figura 2.11: Citações
Fonte: SCOPUS [9]

Unidos (447 citações), Índia (363 citações), Reino Unido (230 citações) e Arábia Saudita (158 citações) denotando o volume e a qualidade da produção científica dos referidos países, porém, o Brasil aparece com apenas 57 citações, o que representa aproximadamente 2 porcento do total das 3134 citações.

g) Artigos mais citados

Na tabela 2.2 apresenta-se a relação dos 20 estudos mais citados na base de dados preparada para pesquisa. Com destaque para os trabalhos dos autores Moody G.D., Siponen M., Pahnila S (229 citações) e Liang G., Weller S.R., Luo F., Zhao J., Dong Z.Y (214 citações) e Sohal A.S., Sandhu R., Sood S.K., Chang V. (143 citações). Conjunto de autores que concentram quase vinte porcento do total de citações de toda base de dados preparada, ou seja, são responsáveis por 586 citações de um total de 3134 citações dos 362 documentos selecionados.

Tabela 2.2: Relação dos 20 Artigos + Citados

Artigos	Autores	Ano	Citações
Toward a unified model of information security policy compliance.	[18]	2018	229
Distributed Blockchain-Based Data Protection....Attacks.	[19]	2019	214
A cybersecurity framework to identify....environments.	[20]	2018	143
Exploring barriers of m-commerce adoption in SMEs....ISM.	[21]	2019	83
An AI-Enabled Three-Party Game Framework for....of IoT.	[22]	2019	72
Mimic defense: A designed-in cybersecurity defense framework.	[23]	2018	63
IIoT Cybersecurity Risk Modeling for SCADA Systems.	[24]	2018	59
Information security model of blockchain based....environment.	[25]	2019	55
Cybersecurity risk analysis model using fault tree....theory.	[26]	2018	53
An ontology-based cybersecurity framework for the....things.	[27]	2018	52
Motivation and opportunity-based model to....in organizations.	[28]	2019	51
A comprehensive model of information security....makers.	[29]	2020	48
Cybersecurity and information security – what goes where?.	[30]	2018	46
A framework for estimating information security....CURF	[31]	2019	41
Evaluating the explanatory power of....in higher education.	[32]	2019	39
The new EU cybersecurity framework:....Protection Regulation.	[33]	2019	38
Federated Learning and Differential Privacy:....data privacy	[34]	2020	37
Deterrence and prevention-based model....in organizations	[35]	2019	36
Developing cybersecurity education and awareness....(SMEs).	[22]	2019	33
Real options models for proactive....decision making.	[36]	2018	33

2.1.4 Detalhamento, modelo integrador e validação por evidências

A etapa final do TEMAC é composta pelas análises das principais contribuições e abordagens encontradas na base de dados tratada, através do Co-citation e Coupling. Na visão de Mariano e Rocha [11], o recurso de Cocitação *(Co-citation)* é utilizado para verificação de trabalhos que geralmente são citados em conjunto, podendo apontar semelhanças entre os estudos. Já o Acoplamento Bibliográfico *(Coupling)* permite mapear as principais frontes de pesquisas, ou seja, aqueles estudos que não poderia faltar em sua pesquisa.

a) *Co-citation*

O mapa de calor das cocitações ***(co-citation)*** na figura 2.12 aponta para as abordagens da pesquisa mais utilizadas, destacando-se um conjunto de quatro clusters compostos por um conjunto de vários núcleos, cenário que reforça o caráter abrangente da presente pesquisa com foco inicial nas áreas de privacidade, privacidade de dados, proteção de dados pessoais, segurança da informação e segurança cibernética.

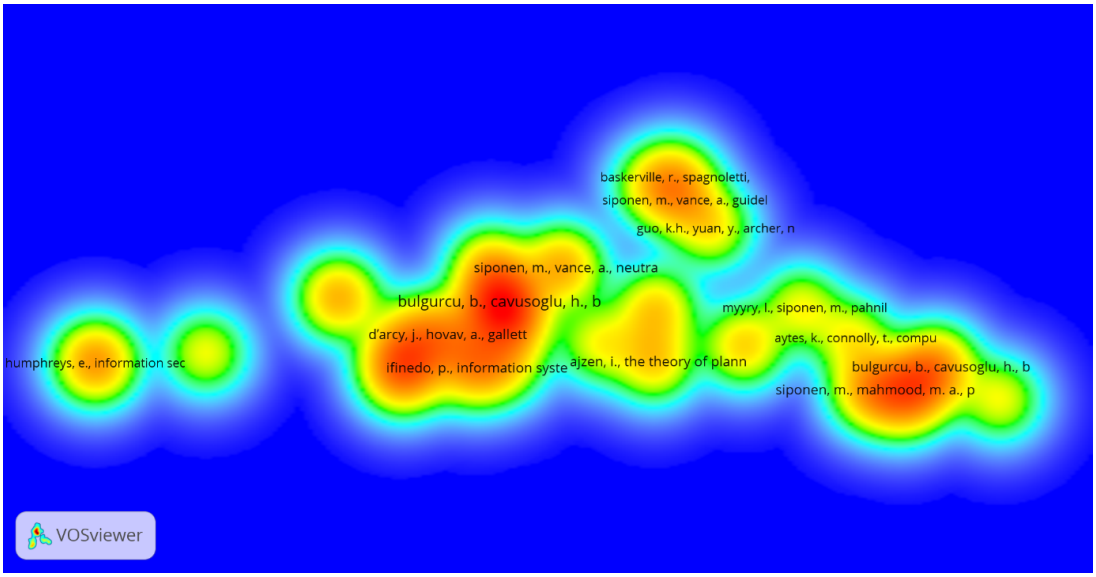

Figura 2.12: Cocitações
Fonte: VOSVIEWER [17]

O primeiro cluster representado pelos trabalhos de Bulgurcu, B., Cavusoglu, H., Benbasat, I.[37], D'Arcy, J., Hovav, A., Galletta, D.F. [38], Ifinedo, P. [39] e Puhakainen, P., Siponen, M. [40], concentram-se na temática da segurança da informação (SI) sob o prisma da potencialização das políticas de segurança da informação nas organizações por meio de programas de conscientização, capacitação, treinamento junto aos colaborado-

res. Explora-se os fatores humanos, como motivação, influência social e cognição, como elementos centrais para o sucesso da implementação das políticas de SI nas organizações.

Já o segundo cluster formado pelas contribuições dos trabalhos de Siponen, M., Mahmood, M., Pahnila, S. [41], Herath, T., Rao, H.R. [42], Siponen, M.T., Vance, A. [43], complementa a abordagem do primeiro cluster, aprofundando-se nas discussões sobre o papel dos colaboradores na implementação das políticas de SI, afirmando categoricamente que a adoção de práticas e políticas de segurança da informação é afetada por fatores organizacionais, ambientais e comportamentais. Seguindo para proposição de frameworks para implementação de políticas de SI alicerçados nas teorias de motivação de proteção, teorias da dissuasão, teoria da neutralização e comportamento organizacional.

O terceiro cluster composto pelos estudos de Baskerville, R., Spagnoletti, P., Kim, J. [44], Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E. [45], Siponen, M., Vance, A. [46], buscam trazer um aspecto prático para a temática de segurança da informação (SI) com estudos voltados para estratégias de SI que empregam princípios e práticas fundamentados nos paradigmas de prevenção e respostas aos incidentes de segurança. Discutindo de forma pragmática como usuários finais considerados "o elo mais fraco" no gerenciamento de SI, frequentemente, de forma consciente, se envolvem em certos usos inseguros de SI violando as políticas de segurança da informação sem intenções maliciosas. Por fim, provocam sobre o rigor e a relevância das pesquisas no campo de SI, sugerindo 5 diretrizes destinadas a aumentar a relevância da pesquisa de campo, usando exemplos de casos na área de segurança da informação (SI).

O quarto cluster integrado pelas pesquisas de Humphreys, E. [47], Siponen, M., Willison, R. [48], Von Solms, R., van Niekerk, J. [49], destacam a importância da adoção de frameworks e ou padrões internacionais na área de segurança da informação (SI), como exemplos das seminais normas BS7799, ISO/IEC 17799:2000, GASPP-GAISP e SSE-CMM, focados em pessoas, processos e tecnologia. Indicando que tais padrões buscam endereçar questões ligadas à compliance, governança e gestão de riscos nas organizações. Porém, já destacam o caráter genérico ou universal do escopo das referidas normas, que na visão dos autores seria um limitador para sua aplicação, uma vez que há grande diferença entre as organizações, bem quanto aos seus requisitos de segurança. Por fim, lançam as bases para as discussões sobre as diferenças entre segurança da informação e segurança cibernética.

b) *Coupling*

Já o mapa de calor do acoplamento bibliográfico ***(coupling)*** na figura 2.13 aponta os principais fronts da pesquisa, apresentando abordagens em crescimento, consolidação ou fortalecimento. Destacando-se um conjunto de dezenove clusters compostos por um con-

junto de vários núcleos, ou seja, trata-se de novas frentes de pesquisas que emergem das fronteiras entre as temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, onde buscamos destacar aquelas mais promissoras e aderentes ao foco da pesquisa.

O *cluster* principal apresenta um conjunto trabalhos voltados para construção de frameworks nas áreas de privacidade e proteção de dados pessoais, destacando-se os trabalhos de Baloyi, N., Kotzé, P., Cantiello, P. [50], Mastroianni, M., Rak, M. [51], Pedroza, G., Muntes-Mulero, V., Martin, Y.S., Mockly, G. [52], Torre, D., Alferez, M., Soltana, G., Sabetzadeh, M., Briand, L. [53]. Além de uma segunda vertente de pesquisa voltada para proposição de frameworks de segurança da informação e segurança cibernética com foco em gestão de riscos, maturidade, conscientização da força de trabalho, dentre outros aspectos explorados. Sobressaindo-se os trabalhos de Arbanas, K., Spremic, M., Zajdela Hrustek, N. [54], Giuca, O., Popescu, T.M., Popescu, A.M., Prostean, G., Popescu, D.E. [55]; Proença, D., Borbinha, J. [56].

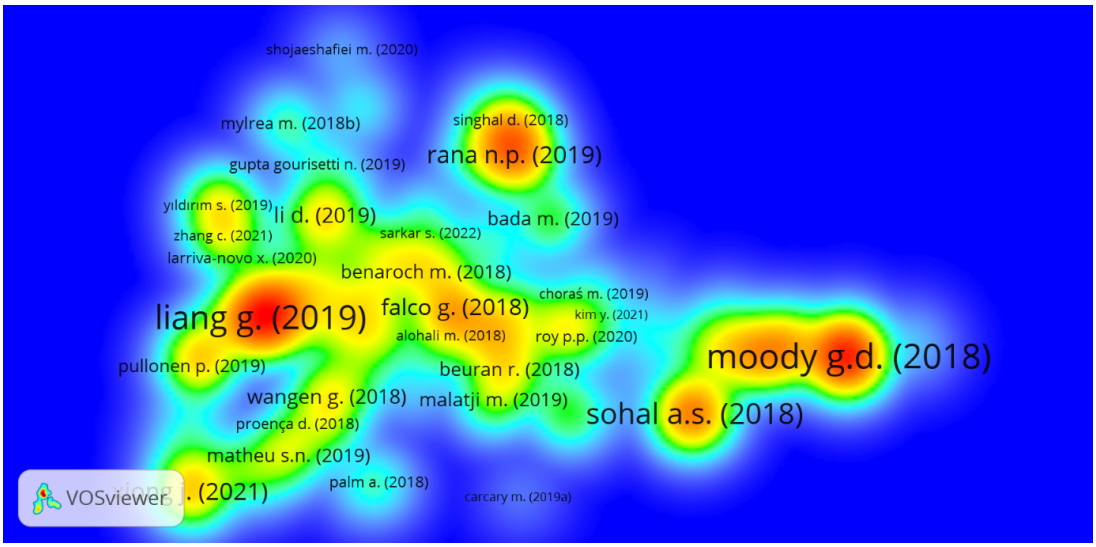

Figura 2.13: Coupling
Fonte: VOSVIEWER [17]

Na busca por estudos alinhados ao objeto da pesquisa foram identificamos alguns trabalhos que sinalizam o surgimento de pesquisas incipientes na interseção entre as temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, como os trabalhos dos autores Serrado, J., Pereira, R.F., Mira da Silva, M., Scalabrin Bianchi, I., no artigo: *Information security frameworks for assisting GDPR compliance in banking industry (2020)* [57], seguidos pelos autores Angelini, M., Ciccotelli, C., Franchina, L., Marchetti-Spaccamela, A., Querzoni, L. no estudo:*Italian National Framework for Cybersecurity and Data Protection (2020)* [58], complementados por Thomas, L., Gondal, I., Oseni, T., (Sally) Firmin, S., na publicação:*A framework for data privacy*

and security accountability in data breach communications (2022) [59], especializado pelos autores Verginadis, Y., Michalas, A., Gouvas, P., Schiefer, G., Hübsch, G., Paraskakis, I., no trabalho: *Paasword: a holistic data privacy and security by design framework for cloud services (2017)* [60], reforçados pela abordagem de Andraško, J., Mesarčík, M., Hamuľák, O., no estudo: *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework (2021)* [61] e alinhado com a visão de Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J., no estudo: *A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM) (2018)* [62].

2.2 Metodologia da Pesquisa (Estudo de Caso)

Complementando a abordagem teórica estruturada a partir da aplicação da Teoria do Enfoque Meta-Analítico Consolidado (TEMAC), esta seção descreve a condução do estudo de caso confirmatório adotado como estratégia metodológica para validar empiricamente a proposta do Programa de Privacidade e Segurança da Informação (PPSI). A utilização do estudo de caso permitiu analisar a implementação do modelo no contexto real dos órgãos do SISP, possibilitando a coleta de evidências práticas sobre sua aplicabilidade, seus desafios e seus resultados. Tal abordagem foi fundamental para assegurar a coerência entre o referencial teórico desenvolvido e a sua efetiva operacionalização no ambiente governamental.

Segundo Wazlawick [10]: O termo pesquisa pode referir-se a diversas atividades humanas, que vão desde a realização de pesquisas eleitorais até a pesquisa científica que buscam aumentar o conhecimento humano sobre como o mundo funciona ou poderia funcionar. Dessa forma, o presente estudo tipificado como uma pesquisa científica pode ser classificado quanto à sua natureza, aos objetivos e aos procedimentos técnicos.

Quanto à natureza da pesquisa, ela pode ser classificada em primária, secundária e terciária. As pesquisas primárias buscam apresentar conhecimentos novos a partir de observações e teorias construídas para explicá-las. Já as pesquisas secundárias ou bibliográficas buscam obter informações de trabalhos já publicados. Podendo tratar-se de mapeamento sistemático da literatura ou a revisão sistemática da literatura. Por fim, temos a categoria de pesquisas terciárias, que se constitui de uma revisão sistemática sobre revisões sistemáticas.

Quanto aos objetivos, as pesquisas podem ser classificadas em exploratórias, descritivas, explicativas ou de designer. A pesquisa exploratória é aquela em que o pesquisador não tem uma hipótese ou objetivo claro em mente. Podendo ser considerado um estágio inicial de um processo mais longo de pesquisa. A pesquisa descritiva é aquela que busca

descrever ou categorizar dados de uma realidade. A pesquisa explicativa é considerada a mais robusta. Pois, além de analisar os dados observados, busca suas causas e explicações. Por fim, temos a pesquisa de design ou de projeto que busca projetar como as coisas poderiam ser, ou seja, uma visão prospectiva do futuro .

Quanto aos procedimentos técnicos, as pesquisas podem ser categorizadas em bibliográfica, documental, experimental, de levantamento, pesquisa-ação, etnográfica ou estudo de caso. Cabendo destacar que por vezes são aplicadas técnicas mistas, por exemplo, o uso de pesquisas bibliográficas em conjunto com outros tipos de pesquisas. A pesquisa bibliográfica caracteriza-se pelo estudo de artigos, teses, livros e outras publicações geralmente disponibilizadas de forma sistematizada por editoras. Já a pesquisa documental consiste em análises de documentos ou dados que não foram sistematizadas. A pesquisa experimental caracteriza-se pela manipulação da realidade pelo pesquisador. Já a pesquisa de levantamento é realizada com a aplicação de questionários a um grupo de pessoas para identificarmos sua opinião sobre determinado tema. A pesquisa-ação, como o nome sugere, o pesquisador envolve-se com os pesquisados, participando ativamente dos trabalhos de pesquisa, buscando determinado resultado. A pesquisa etnográfica, o estudioso mergulha em determinado grupo social para entender seus comportamentos. Por fim, temos o estudo de caso, técnica onde o pesquisador irá estudar em profundidade uma realidade, podendo ser exploratório ou confirmatório.

De forma sintética, a presente pesquisa classifica-se, quanto à natureza, como secundária, quanto aos objetivos, como exploratória, e, quanto aos procedimentos técnicos, adota uma abordagem mista, combinando pesquisa bibliográfica com um estudo de caso confirmatório. Com a estrutura metodológica delineada nos capítulos 1 e 2, avançou-se para os capítulos 3 e 4, que se dedicaram, respectivamente, à análise dos trabalhos relacionados e à construção do referencial teórico da pesquisa.

Capítulo 3

Trabalhos Relacionados

No Capítulo 2, aplicou-se o método TEMAC às bases de dados original e consolidada, oriundas das plataformas *WoS* e *SCOPUS*, com o objetivo de identificar os artigos mais citados, as principais abordagens teóricas por meio da análise de cocitações *(co-citation)* e as frentes emergentes de pesquisa, mapeadas a partir da análise de acoplamento bibliográfico *(coupling)*. Adicionalmente, foram selecionados os artigos com maior aderência ao objetivo central da pesquisa. Como resultado, foi possível identificar um conjunto de 33 artigos com elevado potencial para contribuir com a proposição do Programa de Privacidade e Segurança da Informação (PPSI), fundamentado nas disciplinas de governança, metodologia, maturidade, tecnologia e pessoas, com foco nos órgãos integrantes do SISP.

3.1 Abordagens contemporâneas sobre privacidade e segurança da informação

Uma análise detalhada dos 33 artigos selecionados aponta para um conjunto de trabalhos envolvendo as temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética. Destaca-se que esses temas são frequentemente abordados de forma especializada e segmentada, o que reforça os resultados iniciais da pesquisa, os quais evidenciam uma lacuna na literatura quanto à proposição de programas integrados, complementares e sinérgicos nas áreas de privacidade e segurança da informação.

Além disso, foi possível identificar um conjunto de disciplinas recorrentes citadas em várias publicações do universo avaliado, o que sugere que tais disciplinas constituem fatores críticos de sucesso para o desenho e a implementação de programas nessas temáticas. Essas disciplinas concentram ações materializadas por meio de programas, projetos e processos, com destaque para governança, maturidade, metodologia, tecnologia e pessoas –

Tabela 3.1: Trabalhos Relacionados ao Projeto de Pesquisa: PPSI

Estudo/Autor	Programa/Disciplina	Ano	Fonte
Humphreys, E [47]	Governança	2008	*Co-citation*
Herath, T [42]	Pessoas	2009	*Co-citation*
Siponen, M [48]	Metodologia	2009	*Co-citation*
Puhakainen, P [40]	Pessoas	2010	*Co-citation*
Bulgurcu, B [37]	Pessoas	2010	*Co-citation*
Von Solms, R [49]	Tecnologia	2013	*Co-citation*
Baskerville, R [44]	Tecnologia	2014	*Co-citation*
Siponen, M [46]	Pessoas	2014	*Co-citation*
Glantz, C. [63]	Maturidade	2016	Objetivos
Verginadis, Y. [60]	Tecnologia	2017	*Coupling*
Sabillon, R. [62]	Tecnologia	2017	*Coupling*
Lidster, W. W. [64]	Metodologia	2018	Objetivos
Alsmadi, I [65]	Metodologia	2018	Objetivos
Moody G.D. [18]	Governança	2018	+Citados
Hu H. [23]	Tecnologia	2018	+Citados
Safa N.S. [28]	Pessoas	2018	+Citados
Von Solms B. [30]	Governança	2018	+Citados
Wangen G. [31]	Maturidade	2018	+Citados
Proença, D. [56]	Maturidade	2018	*Coupling*
Markopoulou D. [33]	Metodologia	2018	+Citados
Safa N.S. [35]	Pessoas	2019	+Citados
Bada M. [66]	Pessoas	2019	+Citados
Serrado, J. [57]	Metodologia	2020	*Coupling*
Angelini, M. [58]	Metodologia	2020	*Coupling*
Diesch R. [29]	Metodologia	2019	+Citados
Cantiello, P. [51]	Metodologia	2020	*Coupling*
Pedroza, G. [52]	Metodologia	2020	*Coupling*
Torre, D. [53]	Metodologia	2020	*Coupling*
Giuca, O. [55]	Metodologia	2020	*Coupling*
Andraško, J. [61]	Metodologia	2020	*Coupling*
Muncinelli, G. [67]	Metodologia	2020	Objetivos
Hajny, J. [68]	Metodologia	2020	Objetivos
Thomas, L. [59]	Metodologia	2020	*Coupling*

aspectos que se revelaram preditores relevantes de sucesso em programas de privacidade e segurança da informação.

A categorização apresentada na Tabela 3.1 está fundamentada nessas cinco disciplinas estruturantes já consolidadas na literatura sobre programas de privacidade e segurança da informação: Governança, Metodologia, Maturidade, Tecnologia e Pessoas. Essa classificação emergiu com consistência a partir da análise aprofundada dos 33 artigos selecionados, que revelaram a recorrência dessas disciplinas como pilares centrais na organização de

projetos, processos e ações voltados à privacidade e à segurança da informação. Dessa forma, a adoção dessas cinco categorias reflete tanto uma síntese teórica robusta quanto uma aderência prática aos modelos mais utilizados internacionalmente no desenho e na avaliação de programas integrados de privacidade e segurança da informação.

a) Disciplina: Governança

O primeiro grupo de autores discutem aspectos ligados à governança como variável preditora de sucesso na implementação de programas de privacidade e segurança da informação, com olhar especial para os subtemas de compliance, auditoria, comitês, normas, políticas e padrões. Destacando-se os estudos de Von Solms B., von Solms R. [30], que apontam para a necessidade de estabelecimento das estruturas de governança da segurança da informação e governança de cibersegurança em termos otimizados, simples, claros e na linguagem do negócio, de modo a esclarecer para os conselhos de administração e as diretorias executivas suas responsabilidades a respeito da das temáticas de segurança da informação e segurança cibernética na organização. Movimento acompanhado pelos autores Herath, T., Rao, H.R. [42] que provocam sobre a importância do estabelecimento de políticas de segurança da informação para garantir a segurança dos recursos de informação, porém alertando no trabalho sobre a efetividade de tais políticas uma vez que são afetadas por fatores organizacionais, ambientais e comportamentais.

Argumentos reforçados por Moody G.D., Siponen M., Pahnila S. [18], que propõem um modelo unificado de conformidade com a política de segurança da informação (UMISPC). Discussões que apontam para análise sobre a efetividade das estruturas de governança de comitês e políticas de segurança da informação que precisam ser acompanhados de perto por abordagens contemporâneas de auditorias de segurança da informação e segurança cibernética. Tema especializado para discussões sobre ameaças cibernéticas, riscos cibernéticos e ataques cibernéticos que evoluem em um cenário cibernético extremamente volátil, como apontado nos estudos de Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J. [62]. Visões reforçadas pelos autores que Markopoulou D., Papakonstantinou V., de Hert P. [33], que trazem as discussões sobre a Diretiva NIS, o papel da ENISA e o Regulamento Geral de Proteção de Dados (GDPR) no contexto do estabelecimento, dentre outros aspectos, das estruturas de governança nos países da União Europeia (EU), particularmente, no que diz respeito às suas obrigações de conformidade, bem como às obrigações dos Estados-Membros no que diz respeito às suas respectivas estratégias nacionais e cooperação a nível da UE.

b) Disciplina: Metodologia

O segundo grupo de autores discutem aspectos ligados à metodologia como variável central para o estabelecimento de padrões e ou referenciais para avaliação do sucesso na implementação de programas de privacidade e segurança da informação. Destacando-se os subtemas de arquiteturas, frameworks, modelos, avaliação, maturidade, compliance, dentre outros. Cabendo registro sobre o estudo de Humphreys, E. [47], que aponta para os trabalhos seminais da norma BS 7799, com foco no gerenciamento de segurança da informação relacionada a pessoas, processos e informações. Sendo considerada o embrião das atuais normas de segurança da informação que foram sendo transformadas em padrões internacionais publicados pela ISO/IEC. Valendo citar que esses padrões estão sendo usados por centenas de milhares de organizações em todo o mundo. Razão pela qual o autor busca explorar o que as referidas normas têm a oferecer às organizações, seus benefícios e desafios para implantação. Linha reforçada pelos autores Siponen, M., Willison, R. [48] que apontam que as primeiras normas na área de segurança da informação, como as seminais BS 7799, BS ISO/IEC 17799:2000, GASPP/GAISP e SSE-CMM, que eram genéricas ou universais em escopo, e por consequência, elas não conseguiam diferenciar as organizações que possuíam requisitos de segurança da informação específicos.

Já os autores Proença, D., Borbinha, J. [56] apontam para as conhecidas ISO/IEC 27001:2013 traçando um paralelo entre os desafios para o estabelecimento nas organizações de um Sistema de Gestão de Segurança da Informação (SGSI) e a proposição de um modelo de maturidade para o planejamento, implementação, monitoramento e melhoria de SGSI baseado na ISO/IEC 27001:2013. Na toada da proposição de frameworks nas áreas de segurança da informação e segurança cibernética, temos as visões dos autores Serrado, J., Pereira, R.F., Mira da Silva, M., Scalabrin Bianchi, I. [57] que buscam conectar os temas de segurança da informação com as temáticas da privacidade e proteção de dados pessoais, em especial, apontando os frameworks de segurança da informação como um possível vetor para implementação do General Data Protection Regulation (GPDR). Preocupações apontadas pelos autores Pedroza, G., Muntes-Mulero, V., Martin, Y.S., Mockly, G. [52], que discutem a implementação da privacidade e proteção de dados por design, trazendo as discussões sobre o desenvolvimento de sistemas centrado em dados com diversos atores envolvidos como cidadãos, indústria, reguladores, num contexto em que as políticas de utilização de dados estão longe de serem consensuais.

Já os autores Muncinelli, G., De Lima, E.P., Deschamps, F., Da Costa, S.E.G., Cestari, J.M.A.P [67], apresentam uma discussão bastante interessante sobre o modelo de capacidades, ou seja, o conjunto de recursos que uma organização necessita para comprimir sua missão institucional, correlacionando a temática com as implicações trazidas pela legislação que envolve a proteção dos dados pessoais no contexto da transformação digital

das organizações públicas e privadas.Cabendo destacando o caráter transdisciplinar do estudo que entende que o processo de transformação digital integra os aspectos jurídicos, tecnológicos, riscos, análise de negócios, boas práticas e padrões de gestão de tecnologia da informação e compliance digital. Desviando-se para a temática da segurança cibernética, os autores Hu H., Wu J., Wang Z., Cheng G [23], apresentam uma abordagem muito interessante sobre framework de defesa simulada. Destacando-se as vulnerabilidades nos sistemas cibernéticos como as principais causas de problemas no ambiente cibernético, seguidos pelo fato dos sistemas cibernéticos atuais serem estáticos, previsíveis e monoculturais, o que permite aos adversários planejar e lançar ataques de forma eficaz, além do fato das técnicas de defesa existentes não conseguirem detectar e eliminar ataques que empregam vulnerabilidades desconhecidas. Concluindo que o referido framework pode aumentar significativamente as dificuldades para os invasores, além aumentar a segurança dos sistemas cibernéticos.

c) Disciplina: Maturidade

O terceiro grupo de autores discutem aspectos ligados à maturidade como variável essencial para apontar a evolução, amadurecimento e sucesso na implementação de programas de privacidade e segurança da informação. Destacam-se os subtemas de gestão de riscos, modelos de maturidade, níveis de maturidade, *key performance metrics* (KPM) e *key performance indicators* (KPI), dentre outros. Tendo os autores Wangen G., Hallstensen C., Snekkenes E. [31], apresentando uma importante discussão sobre métodos de avaliação de riscos de segurança da informação, deixando patente a diversidade de abordagens e métodos para avaliação de riscos existente nas várias indústrias, destacando-se o método Core Unified Risk Framework (CURF), cujo escopo é comparar os vários métodos quanto à sua abrangência quando foca-se em avaliações de ativos, ameaças, vulnerabilidades e proteções, muitas vezes com medidas de probabilidade e consequência. Visão de gestão de riscos reforçada por Proença, D., Borbinha, J. [56], que apresentam um modelo de maturidade para o planejamento, implementação, monitoramento e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na ISO/IEC 27001. Tendo tal modelo como objetivo central fornecer às organizações uma ferramenta para obter os níveis atuais de maturidade do SGSI. E posteriormente, com os resultados em mãos, estabelecerem um plano de melhoria que guiará as organizações a atingirem o seu nível de maturidade desejado.

Argumentos alinhados com os estudos de Diesch R., Pfaff M., Krcmar H. [29], que desenvolveram um modelo de fatores de sucesso de gerenciamento (MSF), que identificou fatores que influenciam a segurança da informação que foram categorizados em 12 áreas. Os pesquisadores apontam que existem indicadores-chave de segurança, que afetam dire-

tamente o status de segurança de uma organização, ao passo, outros indicadores afetam indiretamente, cabendo aos gestores estar cientes dos MSFs diretos e indiretos para otimizarem suas decisões. Por fim, cabe uma interessante discussão trazida por Giuca, O., Popescu, T.M., Popescu, A.M., Prostean, G., Popescu, D.E., [55] que buscam conectar as temáticas de maturidade, programas de segurança cibernética e frameworks de gerenciamento de riscos de segurança cibernética. Na visão dos autores, está claro a necessidade aumentar a maturidade de seus recursos de segurança cibernética para acompanhar as ameaças cibernéticas em constante evolução e a rápida digitalização institucional, além de reconhecerem a importância da criação e do fortalecimento de seus programas de segurança cibernética para proteger os processos críticos de negócios, por meio da prevenção, detecção e resposta a ataques cibernéticos.

d) Disciplina: Tecnologia

O quarto grupo de autores discutem aspectos ligados à tecnologia como disciplina indutora, por meio de ferramentas, tecnologias disruptivas e processos de trabalho vinculados, do sucesso na implementação de programas de privacidade e segurança da informação. Destacando-se os subtemas de *Artificial Intelligence (AI), Cloud, Security Information and Event Management (SIEM)*, dentre outros. Registrando-se o trabalho dos autores Verginadis, Y., Michalas, A., Gouvas, P., Schiefer, G., Hübsch, G., Paraskakis, I. [60], que discutem os benefícios econômicos, operacionais e tecnológicos da adoção pelas organizações de estratégias de *Cloud*, tendo como narrativa central a questão da exposição a novas ameaças de segurança cibernética que as empresas passam a enfrentar com a adoção da referida tecnologia. Propondo o framework *PaaSword* baseado em um modelo de segurança sensível ao contexto, em conjunto com um mecanismo de aplicação de políticas necessárias, juntamente com uma distribuição física, criptografia e consulta a programas intermediários. Tratando-se de uma clara discussão sobre os dois lados de uma mesma moeda, a importância da adoção de tecnologias emergentes nas organizações, ao tempo que surgem novos desafios a serem enfrentados nas perspectivas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.

Na mesma direção temos as discussões trazidas pelos autores Andraško, J., Mesarčík, M., Hamuľák, O, [61] que debatem as interseções regulatórias entre *Artificial Intelligence (AI)*, proteção de dados pessoais e segurança cibernética. Apresentando um rico glossário de termos na área de *Artificial Intelligence (AI)*, em conexão com as temáticas de privacidade, proteção de dados pessoais e segurança cibernética, extraídos de documentos estratégicos sobre o tema no âmbito da União Europeia (UE). Visões reforçadas pelo autor Schreider, Tari. [69] que apresenta entre os pilares de um programa de cibersegurança a variável tecnologia, chegando a destacar dezenas de tecnologias utilizadas na área de

segurança cibernética como *Application Security Testing (AST), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Run-time Application Security Protection (RASP), Web Application Firewall (WAF), Authentication, Cloud security, Container security, Data Loss Prevention (DLP), Digital forensics, Distributed Denial of Service (DDoS) Mitigation, Deception technology, Domain Name Services (DNS) Attack Security, Encryption, Endpoint Protection Platform (EPP), Firewalls (FW), Identity and Access Management (IDAM), Internet of Things (IoT) Security, Intrusion Protection Systems (IPS), Network Access Control (NAC), Privileged Account Management (PAM), Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Threat Intelligence Platform (TIP), User and Entity Behavior Analysis (UEBA), Virtualization security, Vulnerability management, Web filtering, Whitelisting*, dentre outras tecnologias disponíveis.

e) Disciplina: Pessoas

Por fim, o quinto grupo de autores discutem aspectos ligados a pessoas como variável central no sucesso da implementação de programas de privacidade e segurança da informação. Destacam-se os subtemas de educação, capacitação, treinamento, programas de conscientização, dentre outros. Os autores Herath, T., Rao, H.R. [42] expõem em seu trabalho um fato conhecido na temática de segurança da informação, qual seja, que organizações estabelecem políticas de segurança da informação para garantir a segurança dos recursos de informação, no entanto, se os colaboradores e usuários finais dos sistemas de informações organizacionais não estiverem interessados ou não estiverem dispostos a seguir as políticas de segurança, esses esforços serão em vão. A tão discutida questão sobre o elemento humano como o "elo fraco" na corrente da segurança da informação. Destacando-se em seu trabalho que a eficiência, eficácia e efetividade da adoção de práticas e políticas de segurança da informação é afetada por fatores organizacionais, ambientais e comportamentais.

Aspectos confirmados pelo trabalho dos autores Puhakainen, P., Siponen, M. [40], que destacam que a não conformidade dos colaboradores com as políticas de segurança da informação (PSI) é uma preocupação fundamental para todas as empresas. Enfatizando que das múltiplas abordagens sobre conformidade em relação às PSI, o treinamento mostra-se como o mais utilizado, porém, poucos são os estudos existentes sobre treinamento que utilizam a teoria para explicar quais princípios de aprendizado afetam a conformidade do usuário ou oferecem evidências empíricas de sua eficácia prática. Argumentos reforçados pelos autores Bulgurcu, B., Cavusoglu, H., Benbasat, I. [37], que afirmam que muitas organizações reconhecem que colaboradores, muitas vezes considerados o elo mais fraco

da segurança da informação, também podem ser grandes ativos no esforço de reduzir os riscos relacionados à segurança da informação. Sugerindo que a atitude de um colaborador é influenciada pelo benefício da conformidade, custo da conformidade e custo da não conformidade, que são crenças sobre a avaliação geral das consequências da conformidade ou não conformidade.

Discussões seguidas pelos autores Siponen, M., Vance, A. [41] que apresentam a discussão sobre o rigor técnico e relevância prática de pesquisas no campo da segurança da informação. Destacando que apesar da importância do rigor técnico nas pesquisas, é preponderante reforçar o aspecto prático da pesquisa, apontando que as pesquisas atuais necessitam de relevância contextual e estão fora de contato com a prática. Na mesma linha os autores Alsmadi, I., Zarour, M. [65], destacam o relevante papel da tecnologia da informação no processo de transformação digital nos sistemas sociais, educacionais, econômicos e militares. Destacando-se que tal digitalização dos sistemas trás implícito os desafios ligados a ameaças cibernéticas no ciberespaço. Dessa forma, a busca constante pela manutenção da confiabilidade, disponibilidade e integridade de nossos sistemas de informação nunca foi tão exacerbada. Surgindo, assim espaço para ações educacionais para o elemento chave na cadeia da segurança da informação, ou seja, as pessoas. Propondo um framework baseado no *National Initiative for Cybersecurity Education 's (NICE)*, com destaque para os *KSAs (Knowledge, Skills, and Ability).*

Visão complementada pelos autores Safa N.S., Maple C., Watson T., Von Solms R. [28] que argumentam que a tecnologia da informação trouxe muitas vantagens para as organizações, mas a segurança da informação ainda é uma grande preocupação para as organizações que dependem dessa tecnologia. Trazendo uma importante discussão sobre a figura dos usuários da tecnologia da informação, que por dolo ou negligência, são uma fonte potencial de riscos aos ativos da organização. Destacando dois aspectos centrais ao explorar a questão das ameaças internas *(insiders)*, que são a motivação e a oportunidade. Na mesma linha os autores Safa N.S., Maple C., Furnell S., Azad M.A., Perera C., Dabbagh M., Sookhak M, [35], apresentam uma nova estrutura conceitual para mitigar o risco de *insiders* usando abordagens de dissuasão e prevenção. Assim, a certeza e a severidade das sanções percebidas influenciam fortemente as atitudes dos indivíduos e os impedem de má conduta, bem como os aspectos de aumentar o esforço, o risco e reduzir a recompensa (benefícios do crime) influenciam fortemente as atitudes dos colaboradores para prevenir o mau comportamento.

Já os autores Bada M., Nurse J.R.C. [66], reforçam como componente essencial da estratégia de segurança cibernética de uma organização as temáticas de educação e conscientização relativas a ameaças cibernéticas, proteção de dados e serviços corporativos. Propondo um modelo de alto nível para educação e conscientização sobre segurança ci-

bernética voltado para pequenas e médias empresas (PMEs). Discussões complementadas pelos os autores Von Solms, R., van Niekerk, J. [30] apresentam uma visão sobre os conceitos de segurança da informação e segurança cibernética que por vezes, de forma equivocada, são tidos como conceitos intercambiáveis. Argumentando que a segurança cibernética vai além dos limites da segurança da informação tradicional para incluir não apenas a proteção dos recursos de informação, mas também de outros ativos, incluindo a própria pessoa. Trazendo importantes discussões sobre o papel dos seres humanos na segurança cibernética, ora figurando com alvos potenciais de ataques cibernéticos ou mesmo participando de modo direto ou indireto de ataques cibernéticos.

Por fim, na linha de proposição de programas sistematizados nas áreas de privacidade e segurança da infromação, os autores Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., De Nicola, R. [68], afirmam de forma categórica que a educação e o treinamento em segurança cibernética são pré-requisitos essenciais para alcançar um ambiente digital seguro e favorável à privacidade. Constatando-se a falta de guias, recomendações, ferramentas práticas e bons exemplos que possam ajudar as instituições a projetar programas adequados de segurança cibernética. Destacando-se a falta um método abrangente para identificar as habilidades necessárias para as funções de segurança cibernética oferecidas no mercado de trabalho. Propondo na sequência o framework de habilidades em segurança cibernética SPARTA que fornece o elo perdido entre as funções de trabalho e os conhecimentos necessários, além de demostrar como desenvolver um currículo que reflita os requisitos do mercado de trabalho.

3.2 Determinação do enfoque teórico da pesquisa

Diante da análise dos 33 artigos com potencial de contribuição para o objeto desta pesquisa — a construção de um Programa de Privacidade e Segurança da Informação (PPSI) — foi possível identificar um conjunto de aspectos relevantes que fundamentam o referencial teórico proposto. Primeiramente, emergiram de forma recorrente um conjunto de cinco disciplinas essenciais que, em maior ou menor grau, estiveram presentes em todos os estudos analisados nas temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética. Essas disciplinas — governança, metodologia, maturidade, tecnologia e pessoas — se configuram como pilares fundamentais na formulação de programas, frameworks e modelos nessas áreas.

Em segundo lugar, constatou-se uma lacuna importante na literatura especializada: não foram identificados estudos que propusessem um programa de privacidade e segurança da informação construído de forma unificada, integrando de maneira sinérgica essas cinco disciplinas estruturantes. Essa ausência reforça a relevância, a atualidade e a originalidade

da presente pesquisa, que busca justamente preencher esse vazio ao propor um modelo integrado, complementar e convergente entre os domínios da privacidade e da segurança da informação, com foco na entrega de valor público e no fortalecimento institucional das organizações do governo digital.

Nesse contexto, a Tabela 3.1 apresenta os 33 artigos selecionados, classificados conforme a disciplina predominante em sua abordagem. A categorização adotada tem como base as cinco disciplinas estruturantes identificadas na literatura — governança, metodologia, maturidade, tecnologia e pessoas — que, conforme demonstrado, emergem como fatores críticos de sucesso na formulação de programas integrados de privacidade e segurança da informação. Essa sistematização contribui para consolidar a fundamentação teórica da pesquisa e orientar as etapas subsequentes de construção e avaliação do PPSI.

Capítulo 4

Fundamentação Teórica

O presente capítulo tem como objetivo apresentar a fundamentação teórica que sustenta a proposição do Programa de Privacidade e Segurança da Informação (PPSI). A construção desse arcabouço teórico inicia-se pela análise dos principais marcos normativos que tornam mandatória a implementação de programas de privacidade e segurança da informação no âmbito da administração pública federal. Em seguida, são discutidas arquiteturas, frameworks e modelos de referência que oferecem subsídios para a estruturação de iniciativas nessas áreas. A seção também é alicerçada em fundamentos conceituais vinculados às disciplinas de governança, metodologia, maturidade, tecnologia e pessoas, eixos centrais da proposta do PPSI. Por fim, são apresentadas possíveis estratégias para a implementação de programas organizacionais e destacados habilitadores críticos ao sucesso de iniciativas voltadas à promoção da privacidade e da segurança da informação.

4.1 Privacidade e Proteção de Dados Pessoais (GDPR, LGPD)

Inicialmente é relevante apresentar os principais marcos legais ligados à privacidade e proteção de dados no contexto mundial e nacional. Dando grande destaque para a referência europeia no contexto da privacidade e proteção de dados pessoais com uma breve apresentação da estrutura da *General Data Protection Regulation* (GDPR), bem como apresentando as principais características do marco legal brasileiro com a Lei Geral de Proteção de Dados Pessoais (LGPD), ambos os marcos legais sinalizando para necessidade de construção de programas sistematizados de privacidade e proteção de dados pessoais.

4.1.1 GDPR

A General Data Protection Regulation (GDPR) é considerada uma legislação complexa uma vez que apresenta de forma introdutória uma sequência de 173 considerandos sobre o contexto geral da Lei, seguido por 99 artigos divididos em 11 capítulos. Sendo relevante destacar que a referida norma se aplica principalmente às organizações estabelecidas na União Europeia (EU), porém, cabendo em algumas hipóteses, sua aplicação estender-se para outras organizações estabelecidas fora da UE.[70]

a) GDPR / Objetivos:

a) O presente regulamento estabelece regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e regras relativas à livre circulação de dados pessoais. b) O presente regulamento protege os direitos e liberdades fundamentais das pessoas físicas e, em particular, o seu direito à proteção dos dados pessoais. c) A livre circulação de dados pessoais na União Europeia não pode ser restringida nem proibida por motivos relacionados com a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais.

b) GDPR / Definições:

Dessa forma, considerando os objetivos da pesquisa, cabe de forma sumarizada a apresentação de algumas definições ligados à GDPR no contexto de construção de um Programa de Privacidade e Segurança da Informação (PPSI) [70]: a) Dados pessoais: *Qualquer informação relativa a uma pessoa física identificada ou identificável (titular dos dados). Uma pessoa natural identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos do físico, fisiológico, identidade genética, mental, econômica, cultural ou social dessa pessoa física.* b)Tratamento: *Significa qualquer operação ou conjunto de operações que é realizado em dados pessoais ou em conjuntos de dados pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.* c) Controlador: *A pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outros, determina as finalidades e os meios de tratamento dos dados pessoais; se as finalidades e os meios desse tratamento forem determinados pelo União ou do Estado-Membro, o responsável pelo tratamento ou os critérios específicos para a sua nomeação devem estar previstos por normas legais da União ou do Estado-Membro.*

e) Consentimento: *Significa qualquer indicação dada livremente, específica, informada e inequívoca da vontade do titular dos dados pela qual ele ou ela, por uma declaração ou por uma ação afirmativa clara, significa consentimento para o processamento de dados pessoais que lhe digam respeito.* f) Violação de dados pessoais: *Significa uma violação de segurança que conduz à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou processados de outra forma*, dentre outros.

c) GDPR / Segurança no tratamento:

Tendo em conta as técnicas mais avançadas, os custos de execução e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como a probabilidade e gravidade diferentes do risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante tomam as medidas técnicas e organizativas adequadas para assegurar um nível de proteção adequado ao risco. Essas medidas incluem, se for caso, o seguinte: a) A pseudonimização e a cifragem dos dados pessoais. b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços relacionados com o tratamento numa base contínua. c) A capacidade de restabelecer rapidamente a disponibilidade e o acesso aos dados pessoais em caso de incidente físico ou técnico. d) Um procedimento para rever, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizativas destinadas a garantir a segurança do tratamento.

Na avaliação do nível de proteção adequado, devem ser tidos especialmente em conta os riscos associados ao tratamento, em especial devido à destruição, perda, alteração ou divulgação ou acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

4.1.2 LGPD

A Lei Geral de Proteção de Dados (LGPD) conta com um total de 65 artigos divididos em 10 Capítulos e Seções, sendo relevante discutirmos alguns comandos do instrumento jurídico que guardam estreita relação com os objetivos da presente pesquisa, como as principais definições previstas no Art. 5º, os princípios plasmados no Art. 6º, os direitos do titular dos dados pessoais descritos no Art. 18º, as regras aplicáveis ao tratamento de dados pessoais pelo poder público, discutidos nos importantes Art. 23 ao Art. 32, as discussões sobre segurança e boas práticas estampados nos Art. 46 ao Art. 51 e por fim, o Art. 52 que apresenta as discussões sobre as sanções administrativas que podem ser impostas pela Autoridade Nacional de Proteção de Dados (ANPD). [71]

a) LGPD / Objetivos:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

b) LGPD / Destinatários:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a) A operação de tratamento seja realizada no território nacional. b) A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional. c) Os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

c) LGPD / Definições:

Dessa forma, considerando os objetivos da pesquisa, cabe de forma sumarizada a apresentação das principais definições ligados à LGPD no contexto de construção de um Programa de Privacidade e Segurança da Informação (PPSI) [71]: a) Dados pessoais: *Informação relacionada à pessoa natural identificada ou identificável.* b) Dado pessoal sensível: *Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.* c) Titular: *Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.* d) Controlador: *Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.* e) Operador: *Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.* f) Encarregado: *Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).* g) Tratamento: *Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.* h) Consentimento: *Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.*, dentre outros.

d) LGPD / Princípios:

Buscando a formação de um quadro geral sobre a LGPD é relevante a compreensão dos princípios previstos no Art. 6º da Lei Geral de Proteção de Dados (LGDP) no contexto de construção de um Programa de Privacidade e Segurança da Informação (PPSI): a) *Finalidade.* b) *Adequação.* c) *Limitação.* d) *Livre Acesso.* e) *Qualidade.* f) *Transparência.* g) *Segurança.* h) *Prevenção.* i) *Não discriminação.* e j) *Responsabilização e prestação de contas.*

e) LGPD / Direitos dos titulares:

Seguindo na construção de uma quadro geral da pesquisa é essencial a compreensão dos direitos dos titulares previstos no Art. 18º da Lei Geral de Proteção de Dados (LGDP) no contexto de construção de um Programa de Privacidade e Segurança da Informação (PPSI): a) *Confirmação da existência de tratamento.* b) *Acesso aos dados.* c) *Correção de dados incompletos, inexatos ou desatualizados.* d) *Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.* e) *Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.* f) *Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei.* g) *Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dado.* h) *Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.* i) *Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.*

f) LGPD / Tratamento de Dados pelo Poder Público:

Dado que a presente pesquisa busca a construção de um Programa de Privacidade e Segurança da Informação (PPSI) voltado para os mais de 250 órgãos integrantes SISP do governo federal, é essencial o conhecimento sobre as principais diretrizes da LGPD voltados para o tratamento de dados pessoais pelo poder público.

Conforme previsto no Artº 23 da LGPD, o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: a) *Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre*

a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos. b) *Seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.*

Seguido pelo Artº 25 da LGPD, que informa que os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Reforçado pelo Artº 26 da LGPD, que aponta que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

Conectado com a previsão do Artº 27 da LGPD, que prevê que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada à autoridade nacional e dependerá de consentimento do titular, exceto: a) nas hipóteses de dispensa de consentimento previstas nesta Lei. b) nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei. e c) nas exceções constantes do § 1º do art. 26 desta Lei.

Complementado por alerta tipificado no Artº 29 da LGPD, que prevê que a autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Repisado por competências previstas nos Artº 31 e Artº 32 da LGPD, que apontam que quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação. Bem como solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

g) LGPD / Segurança e Sigilo de Dados:

Sendo essencial para condução da presente pesquisa o conhecimento dos referidos comandos previstos na seção que trata da segurança e do sigilo de dados na jornada para proposição de um programa de privacidade e segurança da informação (PPSI).

Conforme previsto no Artº 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de

acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Comando plasmado no Artº 47 da LGPD, que prevê que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Reforçado pelo robusto Artº 48 da LGPD, que aponta que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Detalhando em seu § 1º, que a comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: a) A descrição da natureza dos dados pessoais afetados. b) As informações sobre os titulares envolvidos. c) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial. d) Os riscos relacionados ao incidente. e) Os motivos da demora, no caso de a comunicação não ter sido imediata. f) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Reforçado no § 2º, que prevê que a autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: a) Ampla divulgação do fato em meios de comunicação. e b) Medidas para reverter ou mitigar os efeitos do incidente.

Finalizando no § 3º, que aponta que no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Discussões finalizadas no Artº 49 da LGPD, que determinada que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

h) LGPD / Das Boas Práticas e da Governança:

Seção que aponta para necessidade de desenho de programa de governança em privacidade, muito em linha com as aspirações da presente pesquisa que propõe a construção de um Programa de Privacidade e Segurança da Informação (PPSI).

Discussões iniciadas no Artº 50 da LGPD, que prevê que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos,

incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Valendo destacar os requisitos de um programa de governança em privacidade, que no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta. c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados. d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade. e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular. f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos. g) conte com planos de resposta a incidentes e remediação. h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

i) LGPD / Sanções Administrativas:

Por fim, o central Artº 52 da LGPD, prevê que os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: a) advertência, com indicação de prazo para adoção de medidas corretivas. b) multa simples, de até 2 (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R50.000.000,00 (cinquenta milhões de reais) por infração.c) multa diária, observado o limite total a que se refere o inciso II. d) publicização da infração após devidamente apurada e confirmada a sua ocorrência. e) bloqueio dos dados pessoais a que se refere a infração até a sua regularização. f) eliminação dos dados pessoais a que se refere a infração. g) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador. h) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador. e i) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

4.2 Segurança da Informação e Segurança Cibernética (PNSI, PNCiber)

De forma preliminar, é importante apresentar os principais marcos legais ligados à segurança da informação e segurança cibernética no contexto nacional. Dando grande destaque para a Política Nacional de Segurança da Informação (PNSI)[72], prevista no Decreto nº 9.637, de 26 de Dezembro de 2018 e a Política Nacional de Cibersegurança (PNCiber)[73], aprovada pelo Decreto nº 11.856, de 26 de Dezembro de 2023.

Cabendo breves conceituações sobre os termos segurança da informação e segurança cibernética, que segundo a Portaria GSI/PR Nº 93, de 18 de outubro de 2021 [74], que aprova o glossário de segurança da informação, possui significados diferentes: a) Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. b) Segurança cibernética: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

4.2.1 PNSI

O basilar Decreto nº 9.637, de 26 de Dezembro de 2018, está estruturado em sete capítulos contando com disposições gerais, princípios, objetivos, instrumentos, comitê gestor de segurança da informação, competências e disposições finais. Cabendo destacar alguns pontos relevantes do referido decreto que poderão contribuir para proposição do PPSI.

a) PNSI / Escopo:

Art. 1º Fica instituída a Política Nacional de Segurança da Informação (PNSI), no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional.

b) PNSI / Abrangência:

Art. 2º Para os fins do disposto neste Decreto, a segurança da informação abrange: a) a segurança cibernética. b) a defesa cibernética. c) a segurança física e a proteção de dados organizacionais. d) as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

c) PNSI / Princípios:

Art. 3º São princípios da PNSI: a) soberania nacional. b) respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação. c) visão abrangente e sistêmica da segurança da informação. d) responsabilidade do País na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação. e) intercâmbio científico e tecnológico relacionado à segurança da informação entre os órgãos e as entidades da administração pública federal. f) preservação do acervo histórico nacional. g) educação como alicerce fundamental para o fomento da cultura em segurança da informação. h) orientação à gestão de riscos e à gestão da segurança da informação, dentre outros.

d) PNSI / Objetivos:

Art. 4º São objetivos da PNSI: a) contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais. b) fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação. c) aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação. d) fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação. e) fortalecer a cultura da segurança da informação na sociedade. f) orientar ações relacionadas: I) segurança dos dados custodiados por entidades públicas. II) segurança da informação das infraestruturas críticas. III) proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica. IV) tratamento das informações com restrição de acesso. g) contribuir para a preservação da memória cultural brasileira.

e) PNSI / Instrumentos:

Art. 5º São instrumentos da PNSI: a) A Estratégia Nacional de Segurança da Informação. e b) Os planos nacionais.

Desafios alcançados nas organizações públicas pela implementação de um conjunto de estruturas de governança listadas no decreto:

f) PNSI / Governança:

Art. 8º Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República nas atividades relacionadas à segurança da informação.

Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete: a) implementar a PNSI. b) elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República. c) designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade. d) instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI, dentre outros.

Valendo um destaque para a composição e as atribuições do Comitê de Segurança da Informação das organizações do SISP:

§ 1º Art. 15. O comitê de segurança da informação interno de que trata o inciso IV do caput será composto por: a) o gestor da segurança da informação do órgão ou da entidade, que o coordenará. b) um representante da Secretaria-Executiva ou da unidade equivalente do órgão ou da entidade. c) um representante de cada unidade finalística do órgão ou da entidade. d) o titular da unidade de tecnologia da informação e comunicação do órgão ou da entidade.

§ 3º O comitê de segurança da informação interno dos órgãos e das entidades da administração pública federal tem as seguintes atribuições: a) assessorar na implementação das ações de segurança da informação. b) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação. c) propor alterações na política de segurança da informação interna. d) propor normas internas relativas à segurança da informação.

Por fim, cabe destacar o importante Art. 17, que aponta que compete à alta administração dos órgãos e das entidades da administração pública federal a governança da segurança da informação, e especialmente: a) monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação. d) planejar a execução de programas, de projetos e de processos relativos à segurança da informação. e) estabelecer diretrizes para o processo de gestão de riscos de segurança da informação. g) implementar controles internos fundamentados na gestão de riscos da segurança da informação, dentre outros.

4.2.2 PNCiber

O Decreto nº 11.856/2023, institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança com a finalidade de orientar a atividade de segurança cibernética no País. Destacando-se seus princípios, objetivos, instrumentos e a constituição e composição do Comitê Nacional de Cibersegurança (CNCiber). [73]

PNCiber / Princípios:

O referido decreto apresenta como princípios: I - a soberania nacional e a priorização dos interesses nacionais; II - a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; III - a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade; IV - a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; V - a educação e o desenvolvimento tecnológico em segurança cibernética; VI - a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética; e VII - a cooperação técnica internacional na área de segurança cibernética.

PNCiber / Objetivos:

Na sequência, o referido normativo apresenta os 11 objetivos que contribuirão para o alcance da finalidade da Política Nacional de Cibersegurança: I - promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; II - garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; III - fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos; IV - contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço; V - estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos; VI - incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; VII - desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade; VIII - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; IX - incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre: a) a União, os Estados, o Distrito Federal e os Municípios; b) os Poderes Executivo, Legislativo e Judiciário; c) o setor privado; e d) a sociedade em geral; X - desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais; e XI - implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética.

PNCiber / Instrumentos:

Contando com dois instrumentos na busca do alcance de seus princípios e objetivos: I) a Estratégia Nacional de Cibersegurança; e II - o Plano Nacional de Cibersegurança.

PNCiber / CNCiber:

Sendo instituído o Comitê Nacional de Cibersegurança - CNCiber, no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, com a finalidade de acompanhar a implementação e a evolução da PNCiber. Tendo como competências: I - propor atualizações para a PNCiber, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança; II - avaliar e propor medidas para incremento da segurança cibernética no País; III - formular propostas para o aperfeiçoamento da prevenção, da detecção, da análise e da resposta a incidentes cibernéticos; IV - propor medidas para o desenvolvimento da educação em segurança cibernética; V - promover a interlocução com os entes federativos e a sociedade em matéria de segurança cibernética; VI - propor estratégias de colaboração para o desenvolvimento da cooperação técnica internacional em segurança cibernética; e VII - manifestar-se, por solicitação do Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, sobre assuntos relacionados à segurança cibernética.

4.3 Frameworks em Privacidade e Proteção de Dados Pessoais

Uma vez apresentados os conceitos basilares sobre privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, por meio de marcos legais como *GDPR*, LGPD, PNSI e E-Ciber, voltados para os órgãos integrantes do SISP, vale uma discussão sobre os possíveis frameworks adotados nas áreas de privacidade e proteção de dados pessoais que poderão contribuir com subsídios para composição de um futuro framework de privacidade e segurança da informação a ser desenvolvido no âmbito do Programa de Privacidade e Segurança da Informação (PPSI).

Os controles e medidas de privacidade e proteção de dados pessoais apresentados foram selecionados por destacarem-se como as principais referências internacionais disponíveis sobre o tema. Cabendo destaque para as normas brasileiras publicadas pela Associação Brasileira de Normas Técnicas (ABNT): ABNT NBR ISO/IEC relativas à privacidade, proteção de dados pessoais, além das publicações do *National Institute of Standards and Technology* (NIST) relativas ao seu framework de privacidade e proteção de dados pessoais.

4.3.1 ISO/IEC e ABNT/NBR

A *International Organization for Standardization / International Electrotechnical Commission* (ISO/IEC) é uma organização internacional não governamental independente composta por membros de normalização de vários países. A referida instituição congrega

especialistas de todo mundo para compartilhar conhecimentos e desenvolver normas internacionais voluntárias, baseadas em consenso e relevantes para o mercado mundial, que apoiam a inovação e soluções para os desafios globais. Por outro lado, a Associação Brasileira de Normas Técnicas (ABNT), como representante da ISO/IEC no Brasil, por meio das Normas Brasileiras de Referência (NBR), apresenta um conjunto de normas e diretrizes de caráter técnico que tem como função padronizar processos nacionais e internacionais para a elaboração de produtos e prestação de serviços no Brasil.

Dentro os diversos documentos publicados pela ISO/IEC e ABNT NBR, vale destacarmos um conjunto de normas referenciais utilizadas no presente trabalho como subsídios para construção de controles e medidas ligados às temáticas de privacidade e proteção de dados pessoais: ABNT NBR ISO/IEC 29100:2020, ABNT NBR ISO/IEC 27018:2014, ABNT NBR ISO/IEC 29151:2017, ABNT NBR ISO/IEC 29134:2017, ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 29184:2021.

a) ABNT/NBR - ISO/IEC: 29100:2020

A seminal norma internacional apresenta uma estrutura de alto nível para a proteção de dados pessoais em sistemas de TI e Tecnologia da Informação e Comunicação (TIC). É de natureza geral e coloca os aspectos organizacionais, técnicos e processuais em uma estrutura geral de privacidade [75].

Destaca-se a seção 5 da referida norma que apresenta os princípios de privacidade desenvolvidos por vários países e organizações internacionais. Sendo relevante pontuar a importância da observância dos referidos princípios no projeto, desenvolvimento e implementação de políticas e controles de privacidade no âmbito das organizações. Discutindo-se os 11 princípios de privacidade amplamente aceitos na comunidade internacional: a) Consentimento e escolha. b) Legitimidade e especificação de objeto. c) Limitação de coleta. d) Minimização de dados. e) Uso, retenção e limitação da divulgação. f) Precisão e qualidade g) Abertura, transparência e notificação. h) Participação individual e acesso. i) Responsabilização. j) Segurança da informação. l) Compliance com a privacidade.

b) ABNT/NBR - ISO/IEC: 27018:2021

Já a ABNT NBR ISO/IEC 27018:2021 (Código de prática para proteção de dados pessoais (DP) em núvens públicas que atuam como operadores de DP) foca nos aspectos de privacidade em serviços de computação em nuvem providos pela indústria. A referida norma apresenta-se como forma de uma extensão das consolidadas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022 voltada para o contexto de processamento de dados pessoais em nuvem, além de uma extensão de controles voltados

especificamente para a proteção de dados pessoais em nuvem, baseados na ABNT NBR ISO/IEC 29100:2020.

Destaca-se que a intenção da ABNT NBR ISO/IEC 27018:2021, quando utilizada em conjunto com os objetivos de controle de segurança da informação descritos na ABNT NBR ISO/IEC 27002:2022, é criar um conjunto comum de categorias e controles de segurança que possam ser implementados por um provedor de serviços de computação em nuvem pública que atua como um operador de DP [76].

c) ABNT/NBR - ISO/IEC: 29151:2020

A relevante norma ABNT NBR ISO/IEC 29151:2020 fornece o código de prática para proteção de dados pessoais para atender aos requisitos identificados na gestão de riscos de segurança da informação (ABNT NBR ISO/IEC 27005) e avaliação de impacto de privacidade (ABNT NBR ISO/IEC 29134) [77].

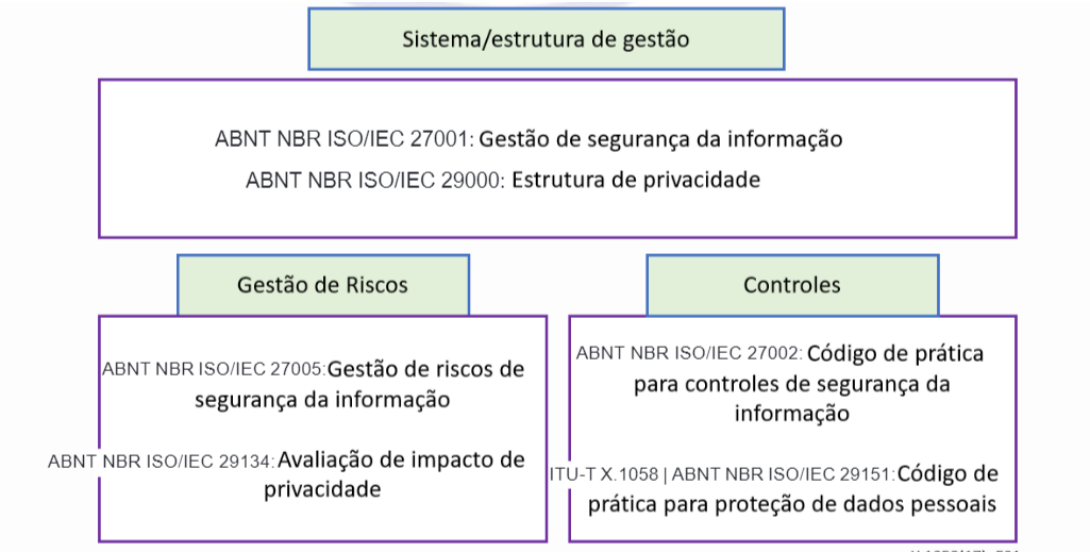

Figura 4.1: Relação da ABNT NBR ISO/IEC 29151:2020 / Família de Normas ISO/IEC
Fonte: ABNT [77]

d) ABNT/NBR - ISO/IEC: 29134:2020

A presente norma trata da importante temática da Avaliação de Impacto de Privacidade (PIA), considerando pela ABNT NBR ISO/IEC 29134:2020, *"como um instrumento para avaliar os potenciais impactos na privacidade de um processo, sistema de informação, programa, módulo de software, dispositivo ou outra iniciativa que trate de dados pessoais (DP), e em consulta às partes interessadas, para tomar ações necessárias para tratar risco à privacidade"* [78].

Destacando-se brevemente alguns benefícios da realização de um PIA: a) Identificar impactos de privacidade, riscos de privacidade e responsabilidades. b) Fornecer entradas para a concepção de proteção da privacidade (*Privacy by Design*) c) Analisar criticamente os riscos de privacidade de um novo sistema de informações e avaliar seu impacto e probabilidade. d) Fornecer a base para a provisão de informações de privacidade aos titulares de DP em qualquer ação recomendada de mitigação dos riscos para os titulares de DP. e) Manter atualizações ou *upgrades* posteriores com funcionalidade adicional suscetível a impactar os DP que sejam manipulados. f) Compartilhar e mitigar riscos de privacidade com partes interessadas, ou fornecer evidências relacionadas à compliance.

e) ABNT/NBR - ISO/IEC: 27701:2019

A ABNT NBR ISO/IEC 27701:2019 busca especificar os requisitos e orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão da ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022 para gerenciamento de privacidade no contexto da organização [79].

O presente padrão traz os requisitos relacionados ao SGIP e fornece orientações para que os controladores e operadores de dados pessoais possam aperfeiçoar o programa de governança sobre os dados pessoais sob suas responsabilidades. A ABNT NBR ISO/IEC 27701:2019 é aplicável a todos os tipos e tamanhos de organizações, incluindo instituições públicas e privadas, entidades governamentais e organizações sem fins lucrativos.

Destacando-se a importante correlação entre as temáticas de privacidade e segurança da informação demonstrada na Tabela 4.1 [79].

Tabela 4.1: Mapeamento da Extensão de Segurança da Informação/Privacidade

ABNT NBR ISO/IEC 27001:2022	**ABNT NBR ISO/IEC 27701:2019**
Segurança da Informação (SI)	Segurança da Informação e Privacidade (SIP)
Política de SI	Política de SIP
Gestão SI	Gestão de SIP
Sistema de Gestão de SI (SGSI)	Sistema de Gestão de PI (SGPI)
Objetivos de SI	Objetivos de SIP
Desempenho de SI	Desempenho de SIP
Requisitos de SI	Requisitos de SIP
Riscos de SI	Riscos de SIP
Avaliação de Riscos de SI	Avaliação de Riscos de SIP
Tratamento de Riscos de SI	Tratamento de Riscos de SIP

4.3.2 NIST PF 1.1

Uma segunda fonte de informações que poderá contribuir de maneira substancial para a proposição de Programa de Privacidade e Segurança da Informação (PPSI) para os órgãos integrantes do SISP é o *NIST Privacy Framework* [80].

O NIST Privacy Framework é destinado a ajudar as organizações a identificar e gerenciar o risco de privacidade para criar produtos e serviços inovadores, protegendo a privacidade dos indivíduos. Esse Framework conceitua a Estrutura Básica de Privacidade e aborda um conjunto de funções de privacidade de dados pessoais, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica.

A Estrutura Básica do Framework de Privacidade consiste em cinco funções simultâneas e contínuas: Identificar-P, Governar-P, Controlar-P, Comunicar-P, Proteger-P. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de privacidade de uma organização.

4.3.3 CIS PRIVACY

Uma terceira fonte de informações que poderá contribuir de maneira substancial para a proposição de Programa de Privacidade e Segurança da Informação (PPSI) para os órgãos integrantes do SISP é o *CIS Privacy.*

Segundo o CIS: *"O Guia de Privacidade dos Controles CIS fornece as melhores práticas e orientações para implementar os Controles Críticos de Segurança CIS (Controles CIS), considerando os impactos de privacidade na força de trabalho, clientes e organizações terceirizadas, como contratados. O Guia de Privacidade apóia os objetivos dos Controles CIS, alinhando os princípios de privacidade e destacando possíveis preocupações de privacidade que podem surgir ao usar os Controles CIS."* [81],

O documento é destinado aos profissionais de tecnologia da informação que são familiarizados com o CIS Controls, bem como profissionais das áreas de privacidade e jurídica das organizações. Trata-se da construção de uma ponte entre a visão de profissionais de tecnologia da informação que precisam entender como os aspectos de privacidade impactam a implementação dos controles de segurança do CIS, bem como os profissionais da área legal precisam ter um melhor entendimento sobre como as modernas tecnologias podem impactar a privacidade.

4.4 Frameworks em Segurança da Informação e Segurança Cibernética

Como já discutido, uma vez apresentados os conceitos basilares sobre privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, por meio de marcos legais como GDPR, LGPD, PNSI e E-Ciber, voltados para os órgãos integrantes do SISP, vale uma discussão sobre os possíveis frameworks adotados nas áreas de segurança da informação e segurança cibernética que poderão contribuir com subsídios para composição de um futuro framework de privacidade e segurança da informação a ser desenvolvido no âmbito do Programa de Privacidade e Segurança da Informação (PPSI). Cabendo destaque para as normas brasileiras publicadas pela Associação Brasileira de Normas Técnicas (ABNT): ABNT NBR ISO/IEC relativas à segurança da informação, segurança cibernética, além das referenciais publicações do *Center for Internet Security* (CIS) e *National Institute of Standards and Technology* (NIST).

4.4.1 ISO/IEC e ABNT/NBR

Dentro os diversos documentos publicados pela ISO/IEC e ABNT NBR, vale destacarmos um conjunto de normas referenciais utilizadas no presente trabalho como subsídios para construção de controles e medidas ligados às temáticas de segurança da informação e segurança cibernética que poderão contribuir para proposição de um programa de privacidade e segurança da informação (PPSI): ABNT/NBR-ISO/IEC 27001:2022, ABNT/NBR-ISO/IEC 27002:2022, ABNT/NBR-ISO/IEC 27003:2020, ABNT/NBR-ISO/IEC 27004:2017, ABNT/NBR-ISO/IEC 27005:2019, ABNT/NBR-ISO/IEC 27007:2021, ABNT/NBR-ISO/IEC 27014:2021 e ABNT/NBR-ISO/IEC 27032:2015.

a) ABNT/NBR - ISO/IEC: 27001:2022

A basilar Norma ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos – trata das temáticas objeto da presente pesquisa, ou seja, os temas de segurança da informação, segurança cibernética e proteção à privacidade. Buscando especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação (SGSI) dentro do contexto da organização.

A adoção de um SGSI é uma decisão estratégica para uma organização.O estabelecimento e a implementação de um SGSI de uma organização são influenciados pelas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem

Normas ABNT NBR	Foco da Norma
ABNT NBR ISO/IEC 27001:2022	Segurança da Informação, segurança cibernética e proteção à privacidade – Sistema de gestão da segurança da informação – Requisitos.
ABNT NBR ISO/IEC 27002:2022	Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de Segurança da Informação.
ABNT NBR ISO/IEC 27003:2020	Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão da segurança da informação – Orientações.
ABNT NBR ISO/IEC 27004:2017	Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão da segurança da informação – Monitoramento, Medição, Análise e Avaliação.
ABNT NBR ISO/IEC 27005:2019	Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação.
ABNT NBR ISO/IEC 27007:2021	Segurança da Informação, segurança cibernética e proteção à privacidade – Diretrizes para auditoria de sistemas de gestão da segurança da informação.
ABNT NBR ISO/IEC 27014:2021	Segurança da Informação, segurança cibernética e proteção à privacidade – Governança da Segurança da Informação.
ABNT NBR ISO/IEC 27032:2015	Tecnologia da Informação – Técnicas de Segurança – Diretrizes para segurança cibernética.

Figura 4.2: Normas ABNT NBR /Segurança da Informação e Segurança Cibernética
Fonte: Própria

ao longo do tempo. O SGSI preserva a confiabilidade, integridade e disponibilidade da informação pela aplicação de um processo de gestão de riscos, e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados [82].

b) ABNT/NBR - ISO/IEC: 27002:2022

Já a robusta Norma ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – foca nos Controles de Segurança da Informação.

A Norma ABNT NBR ISO/IEC 27002:2022 apresenta 8 seções tratando: a) escopo b) referências normativas c) termos e definições d) estrutura deste documento e) controles organizacionais f) controles de pessoas g) controle físicos h) controles tecnológicos.

Cabendo destacar a "lógica de funcionamento" da Norma ABNT NBR ISO/IEC 27002:2022, detalhada na seção 4 da presente publicação [83]:

Por exemplo, cada controle da presente norma foi associado a cinco atributos com valores correspondentes, da seguinte forma: a) Tipo de controle: Preventivo, Detectivo e Corretivo. b) Propriedades de segurança da informação: Confidencialidade, Integridade e Disponibilidade. c) Conceitos de segurança cibernética: Identificar, Proteger, Detectar, Responder e Recuperar. d) Capacidades operacionais: Governança, Gestão de Ativos,

Proteção da Informação, Segurança em Recursos humanos, Segurança Física, Segurança de Sistemas e Redes, Segurança de Aplicações, Configuração Segura, Gestão de Identidade e Acesso, Gestão de Ameaças e Vulnerabilidades, Continuidade, Segurança do Relacionamento na Cadeia de Suprimentos, Legal e Compliance, Gestão de Eventos de Segurança da Informação e Garantia de Segurança da Informação. e) Domínios de segurança: Governança e Ecossistema ("Governança do Sistema de Segurança da Informação e Gestão de Riscos" e Gestão de Segurança Cibernética do Ecossistema"), Proteção ("Arquitetura de Segurança da Informação de TI", "Administração da Segurança de TI" e "Segurança Física e Ambiental"), Defesa ("Detectar" e "Gestão de Incidente de Segurança Computacional" e Resiliência ("Operações de Continuidade" e "Gestão de Crises").

4.4.2 CIS, CIS 8.1 e NIST CSF 2.0

a) *Center for Internet Security: CIS*

O *Center for Internet Security (CIS)* é uma organização internacional sem fins lucrativos formada por indivíduos e instituições voluntários, responsáveis pelo *CIS Critical Security Controls v8*, melhores práticas reconhecidas globalmente para proteger sistemas e dados de TI. Dessa forma, liderados pela CIS, os Controles CIS evoluíram com apoio da comunidade que: a) compartilham percepções sobre ataques e invasores, identificam as causas básicas e as traduzem em classes de ação defensiva. b) criam e compartilham ferramentas, ajudas de trabalho e histórias de adoção e solução de problemas. c) mapeiam os controles CIS com estruturas regulatórias e de compliance, a fim de garantir o alinhamento e trazer prioridade e foco. d) identificam problemas e barreiras comuns (como avaliação inicial e roteiros de implementação), e as resolvem como uma comunidade.

b) *CIS Controls V8.1*

Os Controles CIS refletem o conhecimento combinado de especialistas de todas as partes do ecossistema (empresas, governos, indivíduos), com todas as funções (times de respostas e analistas de ameaças, tecnólogos, operadores e defensores de tecnologia da informação (TI), pesquisadores de vulnerabilidades, fabricantes de ferramentas, provedores de soluções, usuários, formuladores de políticas, auditores, etc.) e em muitos setores (governo, poder, defesa, finanças, transporte, academia, consultoria, segurança, TI, etc.), que se uniram para criar, adotar e apoiar os Controles CIS Os Controles do CIS objetivam: a) Simplificar a sua abordagem de proteção contra ameaças. b) cumprir com os padrões da indústria / governos. c) atingir a essencial *Cyber Hygiene*. d) transformar informação em ação. e) cumprir a Lei [84].

c) *CIS Controls V8.1* : Ecossistema

O *CIS Critical Security Controls v8* é formado por 18 controles críticos de segurança cibernética integrados por um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura de rede por meio de controles que aplicam as melhores práticas para mitigar os mais comuns tipos de ataques cibernéticos. Os controles do CIS v8 utilizam como estratégia de implementação a lógica de camadas, passando por 3 grupos de implementação: Grupo de Implementação 1 - IG1 (56 medidas), Grupo de Implementação 2 - IG2 (74 medidas) e por fim, grupo de implementação 3 - IG3 (23 medidas), dependendo do estágio de maturidade da organização. Valendo um destaque para um forte ecossistema que ferramentas que apoiam a implementação dos Controles do CIS, CIS RAM (Gestão de Riscos), CIS BENCHMARKS (Produtos/Vendors) e CIS SecureSuite (Comunidade/Capacitações), dentre outras [84].

c) *NIST Cybersecurity Framework (CSF2.0)*

Por fim, cabe uma discussão sobre o seminal *NIST CSF* que segue para sua versão 2.0. O NIST Cybersecurity Framework (CSF) fornece orientação às organizações para entender, gerenciar, reduzir e comunicar melhor os riscos de segurança cibernética. É um fundamento e recurso essencial utilizado por todos os setores ao redor do mundo. O CSF foi adotado voluntariamente e em políticas e mandatos governamentais em todos os níveis ao redor do mundo, refletindo sua natureza duradoura e flexível para transcender riscos, setores, tecnologias e fronteiras nacionais. [85]

O CSF pode ser definido como uma abordagem baseada em riscos que visa auxiliar o gerenciamento do risco de segurança cibernética e é composto por três partes fundamentais: a estrutura básica, os níveis de implementação e as avaliação da estrutura. A estrutura básica focada no conjunto de atividades de segurança cibernética, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica. Os níveis de implementação descrevem o grau em que as práticas de gerenciamento do risco de segurança cibernética de determinada organização evidenciam as características definidas no framework. Por fim, a avaliação da estrutura é caracterizada como sendo a harmonização de padrões, diretrizes e práticas à estrutura básica em um cenário de implementação específico [86].

4.5 Programas de Privacidade e Segurança da Informação (EC-Council e ISACA)

No presente tópico buscou-se apresentar alguns programas referenciais nas temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança da informação como forma sinalizar possíveis abordagens durante a fase de proposição de um programa de privacidade e segurança da informação para os órgãos integrantes do SISP.

4.5.1 CCISO: EC-Council

O primeiro referencial apresentado é proveniente do Conselho Internacional de Consultores de Comércio Eletrônico, conhecido como EC-Council, foi fundado em 2003 para oferecer educação em segurança e programas de certificação. Tendo dentre suas principais certificações a Certified Chief Information Security Officer (CCISO), desenvolvida para servir como um programa de certificação para executivos de segurança da informação.

Na visão da referida organização um programa em segurança da informação deverá abordar os seguintes tópicos dentro de sua metodologia: Etapa 1) Governança e Gestão de Riscos: o tópico concentra-se em como garantir que o programa de segurança da informação está alinhado com as necessidades da organização. Cobrindo os temas de governança da segurança da informação, fundamentos da segurança da informação, descrição de um programa típico de segurança da informação, além da descrições de leis e estruturas relevantes para a segurança da informação. Etapa 2) Controles de Segurança da Informação, Conformidade e Gestão de Auditoria: descreve-se como uma organização estabelece e implementa controles de segurança, estruturas de controle e o ciclo de vida do controle. Trazendo ampla cobertura de processos e conceitos de auditoria de segurança da informação. Etapa 3: Gerenciamento e Operações do Programa de Segurança: discutise abordagens de gerenciamento de programas, projetos e processos, bem como gestão de recursos e orçamento. Destacando-se que programas de segurança da informação são compostos por projetos com ciclos de vida determinados, bem como processos com fluxos de trabalho contínuos na organização. Etapa 4: Competências Essenciais de Segurança da Informação: o tópico descreve um conjunto de competências: técnicas, gestão e processos que precisam ser desenvolvidas pelos times de segurança da informação para busca de eficiência, eficácia e efetiva do programa na organização. Etapa 5: Planejamento Estratégico, Finanças, Compras e Gestão de Fornecedores: discute-se como as organizações usam o planejamento estratégico para estabelecer metas e definir planos para alcançá-las. Cobre tópicos como contabilidade, finanças e compras e gestão de fornecedores [87].

4.5.2 CISM: ISACA

O segundo referencial apresentado vem da ISACA. Como líder globalmente reconhecida em segurança da informação (SI) e tecnologia da informação (TI) há mais de 50 anos, a ISACA é uma organização profissional comprometida com o avanço da confiança digital, capacitando profissionais de SI/TI para aumentar suas habilidades e conhecimentos em auditoria, segurança cibernética, tecnologia emergente e muito mais. Tendo dentre suas principais certificações a Certified Information Security Manager (CISM), desenvolvida em 2002 para servir como um programa de certificação para executivos de segurança da informação.

Na visão da referida organização um programa em segurança da informação deverá abordar os seguintes tópicos dentro de sua metodologia: Etapa 1) Governança de Segurança da Informação: tópico que aborda a governança corporativa e estratégia de segurança da informação. Cobrindo a importância do programa de segurança da informação está alinhado com as necessidades do negócio da organização. Etapa 2) Gestão de Riscos de Segurança da Informação: ponto que trata da avaliação de riscos de segurança da informação e resposta a Riscos de Segurança da Informação. Cobrindo a importância do levantamento dos riscos da organização e deseno da estratégia de respostas aos respectivos riscos. Etapa 3: Arquitetura do Programa de Segurança da Informação: tópico que aborda duas fases distindas composta pelo desenvolvimento do programa de segurança da informação e gerenciamento do programa de segurança da informação. Etapa 4: Gerenciamento de Incidentes: tópico que foca prontidão no gerenciamento de incidentes e operações de gerenciamento de incidentes. Temáticas fundamentais para alcance dos objetivos de eficiência, eficácia e efetividade de um programa de segurança da informação [88].

4.5.3 Programa de Cibersegurança: Visão Genérica

Terceiro referencial apresentado vem dos estudos da obra: Construindo um Programa de Cibersegurança Efetivo de Tari Schreider. O trabalho robusto que apresenta uma visão agnóstica sobre a proposição de um programa de cibersegurança para organizações de variados tamanhos, setores e níveis de maturidade.

Na visão do referido autor um programa em segurança da informação deverá abordar os seguintes tópicos dentro de sua metodologia: Etapa 1) Crie o Guia de Design de Programa: o tópico foca na criação de guia que reunirá todos os elementos para o desenho de seu programa de cibersegurança. Conterá a arquitetura, modelos, frameworks, princípios, práticas e seu plano de programa. Etapa 2) Defina a Estrutura do Programa: trata-se da construção organizacional dos domínios do seu programa de cibersegurança (Escritório

do CISO, Engenharia de Segurança, Operação de Segurança, Inteligência de Ameaças Cibernéticas, Respostas a Ameaças Cibernéticas, Segurança Física e Operações de Recuperação de Desastres). Conterá a estrutura de segurança cibernética declarada em seu guia de design (CIS, ISO, NIST, etc.) que influenciará o design geral do programa. Etapa 3) Identificar as Tecnologias do Programa: o tópico discute as tecnologias utilizadas para dar apoio aos domínios da estrutura do programa. Saber quais tecnologias selecionar é impulsionado principalmente pelos requisitos de tratamento de risco de seu programa de segurança cibernética. Etapa 4) Crie o Programa de Treinamento em Cibersegurança: discute-se a a importância da primeira linha de defesa ser a consciência de segurança e a cultura de segurança de sua organização. Sugerindo-se que programa busque um equilíbrio entre educação e testes, onde os usuários desenvolvem a memória muscular necessária para servir como firewalls humanos, interrompendo as ameaças antes que elas tenham a chance de se estabelecer na organização. Etapa 5) Amadureça o Programa de Cibersegurança: tópico onde discute-se o estabelecimento de um modelo de maturidade para o programa, seguido da necessidade de customização, uma vez que as organizações possuem seus própios perfis de risco, restrições de negócio e apetite de investimento. Além de reforçar a ideia de segurança na medida certa, uma vez nem todos os aspectos de um programa de segurança cibernética precisam ter o mesmo nível de maturidade [69].

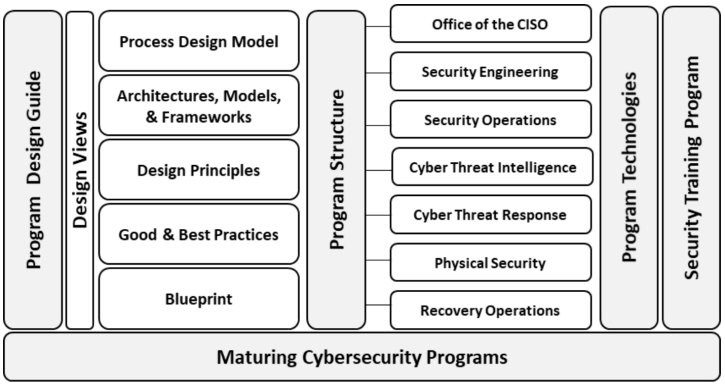

Figura 4.3: Arquitetura de Referência de Design de Programa
Fonte: Tari Schreider [69]

Os capítulos anteriores estabeleceram a base conceitual para a construção do Programa de Privacidade e Segurança da Informação (PPSI). O Capítulo 3 apresentou os principais trabalhos relacionados, enquanto o Capítulo 4 consolidou os fundamentos teóricos que sustentam a proposta. Com esse arcabouço, o Capítulo 5 introduz o PPSI, com diretrizes e estratégias práticas. O objetivo é assegurar que sua metodologia contribua efetivamente para elevar a maturidade e a resiliência das organizações integrantes do SISP.

Capítulo 5

Proposta do Programa de Privacidade e Segurança da Informação (PPSI)

Partindo-se da definição do problema, construção da justificativa, estabelecimento do objetivo geral e objetivos específicos da pesquisa, alicerçado em um procedimento metodológico composto pelas teorias do enfoque meta analítico consolidado (TEMAC) e a respectiva metodologia de pesquisa, seguido pela identificação dos principais trabalhos relacionados ao objeto da pesquisa, chega-se a fundamentação teórica apontando para as principais teorias, estratégias, programas, frameworks e disciplinas ligadas ao campo da privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética. Por fim, foi elaborada a proposta de um Programa de Privacidade e Segurança da Informação (PPSI), voltado para os 254 órgãos integrantes do SISP.

5.1 PPSI: O Programa

O programa de privacidade e segurança da informação (PPSI), instituído por meio da Portaria SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023, caracteriza-se como um conjunto de projetos e processos distribuídos nas disciplinas de governança, maturidade, metodologia, pessoas e tecnologia objetivando elevar a maturidade e a resiliência dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do governo federal.[89]

5.2 PPSI: Processo de Construção

Para garantir a implementação eficaz do PPSI, é essencial adotar um processo estruturado que traduza os conceitos teóricos em ações concretas. Com base nos trabalhos relacionados e na fundamentação teórica da pesquisa, foi selecionado o modelo ADDIOI, reconhecido por seu caráter incremental e contínuo. A seguir, detalham-se suas seis etapas: a) Align (Alinhamento), b) Design (Projeto), c) Develop (Desenvolvimento), d) Implement (Implementação), e) Operate (Operação) e f) Improve (Melhoria). Esse modelo proporciona às organizações e gestores uma visão abrangente do ciclo de planejamento, organização, implementação, operação, manutenção, monitoramento e avaliação do PPSI, possibilitando sua operacionalização dentro de uma lógica de aprimoramento cíclico, contínuo e incremental.[90]

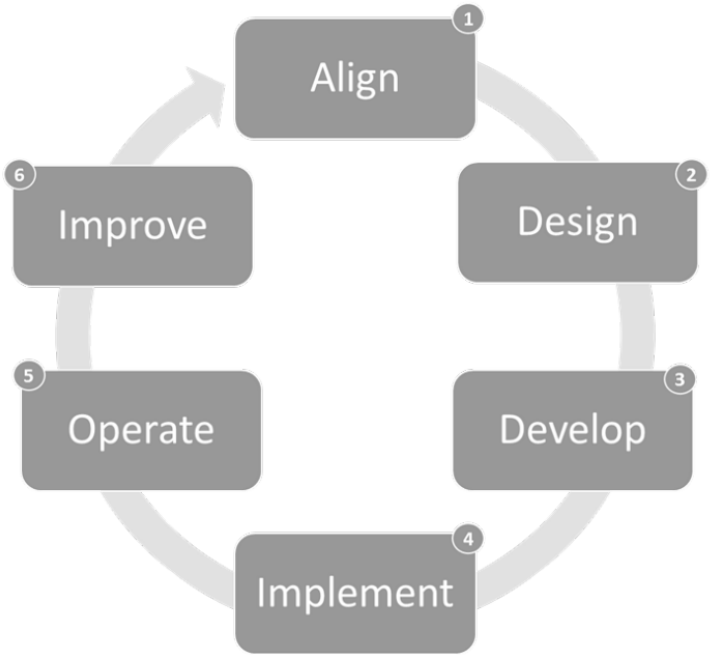

Figura 5.1: Modelo ADDIOI
Fonte: Tari Schreider [69]

O processo de construção do PPSI foi composto por 6 etapas:

- **Etapa 1**: Alinhamento (Definição dos direcionadores internos e externos).
- **Etapa 2**: Projeto (Definição da arquitetura, frameworks, modelos e disciplinas).
- **Etapa 3**: Desenvolvimento (Definição de projetos pilotos, configurações e ajustes).
- **Etapa 4**: Implementação (Definição de métodos, recursos e cronogramas).

- **Etapa 5**: Operação (Definição do modelo de gerenciamento e sustentação).
- **Etapa 6**: Melhoria (Definição do modelo maturidade, monitoramento e avaliação).

5.2.1 Etapa 1: Alinhamento

Na etapa de Align (Alinhamento), buscou-se mapear os principais direcionadores internos e externos às organizações, com o objetivo de customizar, para o contexto do SISP, o conjunto de ações do PPSI. Os direcionadores internos concentram-se na identificação de: a) elementos estratégicos da organização, como missão, visão de futuro, valores, objetivos e metas. b) modelos de governança corporativa, governança de segurança da informação e gestão de riscos. c) aspectos da cultura organizacional e o perfil profissional predominante. Já os direcionadores externos têm como foco a identificação de: a) perfil de risco em privacidade da organização. b) perfil de risco cibernético. c) regulamentações setoriais aplicáveis. d) tecnologias emergentes no setor. e e) dinâmica do mercado de trabalho, entre outros. Os resultados desse mapeamento devem atuar como drivers para a customização das ações do PPSI durante a etapa de Design (Projeto), assegurando sua aderência às realidades organizacionais.

5.2.2 Etapa 2: Projeto

Na etapa de Design (Projeto), foram estruturadas as bases do Programa de Privacidade e Segurança da Informação, alinhadas às necessidades específicas das organizações — considerando tanto os direcionadores internos quanto os externos. Nesse processo de concepção do programa, foram abordados os seguintes aspectos: a) definição da arquitetura, frameworks, modelos e disciplinas a serem adotados. b) Definição de projetos-piloto, configurações e ajustes necessários. c) Definição de métodos, recursos e cronogramas. d) Definição do modelo de gerenciamento e sustentação. e) Definição do modelo de maturidade, monitoramento e avaliação. A customização do programa é essencial para que organizações com características únicas — como missão, visão, objetivos estratégicos, porte, perfil dos colaboradores e diferentes níveis de maturidade e resiliência — possam alcançar os níveis adequados de desenvolvimento no contexto do PPSI. Os resultados dessa etapa devem ser amplamente discutidos, validados e aprovados pela alta administração das organizações integrantes do SISP.

5.2.3 Etapa 3: Desenvolvimento

Durante a etapa de Develop (Desenvolvimento), a organização e seus gestores realizaram um conjunto de configurações, avaliações e ajustes na arquitetura, frameworks, mode-

los, processos e projetos relacionados às disciplinas basilares do programa. Buscaram movimentos ágeis de planejamento, organização, implementação, operação, manutenção, monitoramento e avaliação dos resultados preliminares do projeto. Sugeriram ciclos curtos, de 90 a 120 dias, para a implantação de processos e a execução de projetos-piloto, seguidos de avaliações e, eventualmente, do pivoteamento de processos e iniciativas. Esses resultados facilitaram o desenvolvimento e a customização dos serviços de privacidade e segurança da informação no contexto da organização. Tratou-se de uma etapa voltada ao refinamento das decisões previamente aprovadas na fase de projeto.

5.2.4 Etapa 4: Implementação

Na etapa de Implement (Implementação), a organização partiu para a implantação dos processos e projetos vinculados a cada disciplina básica previamente selecionada do PPSI (governança, maturidade, metodologia, tecnologia e pessoas). Foi o momento de definição do método de implementação do programa, com atenção especial à alocação de recursos, à gestão de cronogramas e à condução rigorosa da gestão de riscos do projeto. A etapa também contou com o suporte dos habilitadores de sucesso do programa, visando maior eficiência, eficácia e efetividade. A implantação dos projetos, dos processos, o treinamento dos colaboradores e a implementação dos habilitadores de sucesso constituíram as atividades principais dessa fase.

5.2.5 Etapa 5: Operação

Durante a etapa de Operate (Operação), foi realizado o gerenciamento efetivo e a execução das atividades diárias previstas nos controles e medidas de privacidade e segurança da informação, previamente definidos na arquitetura, nos frameworks, nos modelos e nas disciplinas do programa. Tratou-se da gestão de ferramentas tecnológicas voltadas à privacidade e à segurança da informação, do monitoramento de ameaças internas e externas, da implementação de processos de resposta a incidentes, da elaboração de planos de continuidade de negócio e recuperação de desastres, bem como da condução das atividades de inteligência de ameaças cibernéticas, entre outros processos. A sustentabilidade do programa constituiu o foco principal dessa etapa.

5.2.6 Etapa 6: Melhoria

Dada a abordagem cíclica do modelo, na fase de Improve (Melhoria) buscou-se o aprimoramento constante do PPSI. Nessa etapa, foram estabelecidas as principais métricas de desempenho, e avaliações regulares foram utilizadas para definir a linha de base do programa. Além disso, um modelo de maturidade foi aplicado para orientar as melhorias

contínuas do programa. Os resultados obtidos durante a fase de melhoria alimentaram todas as demais fases da metodologia de construção do PPSI. A melhoria cíclica, contínua e incremental constituiu a principal atividade dessa etapa.

5.3 PPSI: Modelo Proposto

Considerando-se as seis etapas de construção do PPSI, propôs-se um modelo baseado no conceito de linhas de defesa, estruturado em cinco frentes de atuação, com enfoque na articulação simultânea das temáticas de governança, maturidade, metodologia, pessoas e tecnologia. O objetivo foi apoiar a implementação das iniciativas do PPSI no âmbito dos órgãos e entidades integrantes do SISP, assegurando coerência entre as frentes e promovendo a integração dos esforços institucionais nas diferentes dimensões do programa.

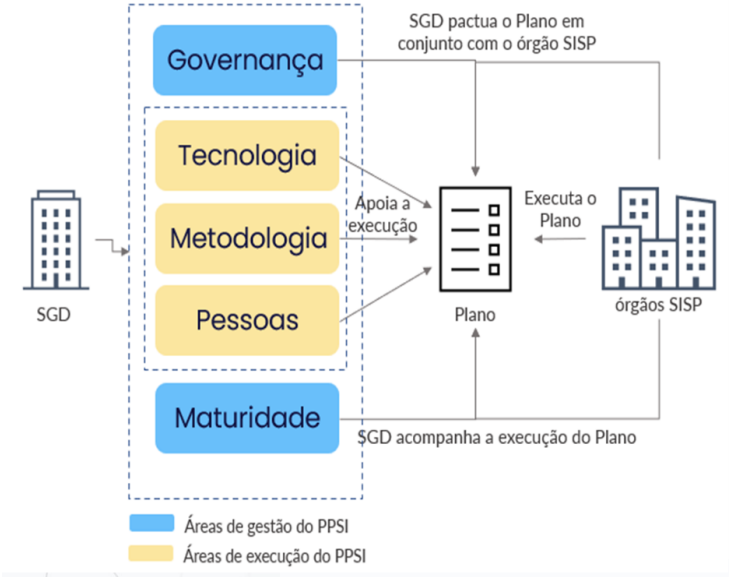

Figura 5.2: Modelo PPSI
Fonte: Cartilha PPSI [91]

5.4 PPSI: Linhas de Defesa

O Programa de Privacidade e Segurança da Informação (PPSI) tem como objetivo elevar a maturidade e a resiliência, em termos de privacidade e segurança da informação, dos órgãos integrantes do SISP. É sustentado por um conjunto de valores centrais como maturidade, resiliência, efetividade, colaboração e inteligência e por uma estratégia focada no planejamento, implementação e monitoramento de projetos e processos estruturados. Nesse sentido, as linhas de defesa do PPSI se configuram como pilares fundamentais para a

sua operacionalização, organizando as iniciativas em cinco frentes temáticas: governança, metodologia, maturidade, tecnologia e pessoas. Cada uma dessas frentes desempenha um papel essencial no sucesso do programa e serão apresentada a seguir.

5.4.1 Governança

A linha de defesa voltada à governança é responsável por avaliar, direcionar e monitorar as ações do PPSI. Assegurando a entrega de benefícios, a otimização dos recursos e o engajamento das partes interessadas. Como vertente de gestão, atua na prospecção de projetos inovadores e na gestão de projetos transversais necessários para garantir a operação do PPSI. Adicionalmente, promove parcerias com órgãos e entidades públicas, entidades privadas e organismos internacionais para desenvolver e dar sustentação às iniciativas relacionadas às temáticas privacidade e segurança da informação. Dedicando-se a produção de normas para formalização do programa, prospecção de modelos de gestão de riscos, construção da estrutura de governança do programa e incubadora de projetos para parcerias no Brasil e no mundo.

5.4.2 Metodologia

A dimensão de metodologia é responsável por definir e manter a estrutura de controles de privacidade e segurança da informação. Bem como promover as boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos relacionados à temática de Privacidade e Segurança da Informação. Focando em consultorias técnicas, atendimento aos participantes do programa, análise de normativos, atualização e produção de guias e modelos. Cabendo destacar o framework de privacidade e segurança da informação do PPSI e os mais de 30 guias e ou modelos que dão suporte à implementação do framework do PPSI.

5.4.3 Maturidade

A componente de maturidade é responsável por diagnosticar o grau de implementação dos controles de Privacidade e Segurança da Informação pelos órgãos e entidades pertencentes ao SISP. Sensibiliza de forma contínua a Estrutura de Governança do PPSI e acompanha a implementação de controles conforme Plano de Trabalho pactuado entre asorganizações do SISP e a Secretaria de Governo Digital (SGD/MGI). Trazendo em seu portifólio de serviços o Programa de Apoio ao Diagnóstico do PPSI, Programa de apoio à evolução do grau de maturidade do PPSI, Gestão das Comunidades Regionalizadas de Privacidade e Segurança da Informação, além do acompanhamento dos indicadores de Privacidade (IPriv) e de Segurança (ISeg).

5.4.4 Tecnologia

A frente de tecnologia é responsável pela coordenação coordenar o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br), identificar e disseminar informações sobre vulnerabilidades e apoiar na prevenção, tratamento e resposta a incidentes cibernéticos. Tendo em seu portófio de serviços: apoio na prevenção, tratamento e resposta a incidentes cibernéticos, comunicação e colaboração com outras ETIRs, Apoio na criação de ETIRs dos órgãos SISP, inteligência de ameaças, publicação de alertas e recomendações, monitoração de padrões maliciosos no tráfego externo da rede, execução de testes de intrusão em ativos de informação, análise não-invasiva e contínua de vulnerabilidades, testes estáticos e dinâmicos de segurança em aplicações e análise de vulnerabilidades sob demanda.

5.4.5 Pessoas

Por fim, a linha de defesa de pessoas é responsável por promover a cultura de Privacidade e Segurança da Informação, estabelecer e coordenar o Centro de Excelência em Privacidade e Segurança da Informação (CEPS.Gov.br) fomentando ações de engajamento que visam promover a mudança cultural em todos os níveis da estrutura organizacional dos órgãos e entidades, por meio de sensibilização, conscientização e capacitação visando o adequado uso do recursos de tecnologia da informação na execução dos processos de trabalho referente à temática de Privacidade e Segurança da Informação. Destacando-se projetos como a Pós-Gradução em Privacidade e Segurança da Informação, Projetos de Residência Tecnológica, Trilhas de Aprendizagem em Ambiente Virtual e Fomento a Palestras sobre a temática.

5.5 PPSI: Eixos Estruturantes

Além das linhas de defesa que sustentam a implementação do PPSI, o programa se apoia em um conjunto de eixos estruturantes que conferem robustez e articulação sistêmica às suas iniciativas. Esses eixos operam como catalisadores das ações desenvolvidas nas frentes de governança, metodologia, maturidade, tecnologia e pessoas, proporcionando recursos, estruturas e competências indispensáveis à consolidação do programa nos órgãos do SISP. Cada eixo estruturante foi concebido para fortalecer a capacidade institucional da Secretaria de Governo Digital (SGD/MGI) e das 254 organizações integrantes do sistema, promovendo sinergia, padronização e suporte técnico-operacional. A seguir, são apresentados os principais eixos estruturantes que viabilizam e ampliam o impacto do PPSI no governo digital brasileiro.

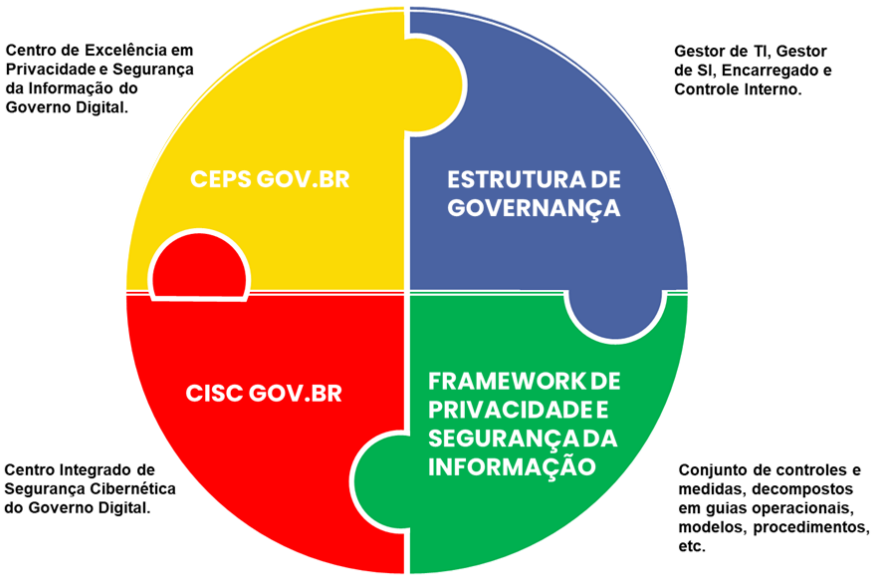

Figura 5.3: Eixos Estruturantes do PPSI
Fonte: Cartilha PPSI [91]

5.5.1 Estrutura de Governança

O eixo trata da estrutura de governança do PPSI em cada órgão e entidade da administração pública federal direta, autárquica e fundacional. A referida estrutura formada pelo Gestor TIC, Gestor de SI, Encarregado e Controle Interno são responsaveis juntamente com a alta direção pela implementação do programa nas organizações com suporte da Secretaria de Governo Digital (SGD/MGI). Destacando-se os seguintes papéis:

a) Gestor de TIC

Responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de TIC.

b) Gestor de SI

Responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação.

c) Encarregado pela Proteção de Dados Pessoais

Atua como canal de comunicação entre instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

d) Controle Interno

Atua no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha da defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

5.5.2 Framework do PPSI

O Framework de privacidade e segurança da informação é composto por um conjunto de controles, metodologias e ferramentas de apoio que tem como base: LGPD, PNCiber, PNSI, CIS Controls (v8.1), Normas ISO/IEC e ANBT, Estrutura do Privacy Framework (NIST), Normativos da ANPD e GSI, além de recomendações efetuadas pelos órgãos federais de controle interno e externo. Sendo etapas da implementação do framework: Autoavaliação, Análise de lacunas, Planejamento e Implementação.

Figura 5.4: Framework de Priv e SI
Fonte: Cartilha PPSI [91]

5.5.3 CISC.GOV.BR

O Centro Integrado de Segurança Cibernética do Governo Digital (CISC.GOV.BR) é caracterizado como uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (Etir) e atua a nível de coordenação operacional, ofertando uma série de serviços para o seu público-alvo, formado pelos órgãos do SISP. (art. 13 da Portaria SGD/MGI nº 852, de 28 de março de 2023). A missão do CISC Gov.br é promover a coordenação das ações de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do SISP. Focado na entrega de serviços apoio em diversas ações de resposta a incidentes cibernéticos nos órgãos e entidades, elaboração e publicação de alertas e recomendações, produção de inteligência para detecção eficaz de ameaças cibernéticas, testes estáticos e dinâmicos de segurança de aplicações, comunicação e colaboração com outras equipes de prevenção, tratamento e resposta a incidentes cibernéticos, monitoramento de padrões maliciosos no tráfego externo de rede e execuçãosob demanda de testes de intrusão e análise de vulnerabilidades em ativos de informação.

5.5.4 CEPS.GOV.BR

O Centro de Excelência em Privacidade e Segurança da Informação (CEPS.GOV.BR) tem como missão promover a cultura de privacidade e segurança da informação nos órgãos e entidades. (art. 19 da Portaria SGD/MGI nº 852 de 28 de março de 2023). Dentre os objetivos do Centro de Excelência, pode-se citar: Promover parcerias com órgãos e entidades públicas, instituições privadas e organismos internacionais, nos termos da legislação, apoiar os órgãos e entidades para a efetiva implementação da estrutura de controles de privacidade e segurança da informação por meio de ações conjuntas e colaborativas, disseminar conhecimentos sobre as boas práticas nas temáticas de privacidade e segurança da informação, Promover ações de sensibilização, conscientização e capacitação dos recursos humanos em temas relacionados à privacidade e à segurança da informação e promover a criação de fóruns especializados para prospectar oportunidades e trocas de experiências e informações.

5.5.5 Relação entre as Linhas de Defesa e Eixos do PPSI

A estruturação do PPSI foi concebida para explorarmos as sinergias entre suas linhas de defesa e os seus eixos estruturantes. Dessa forma, o objetivo de aumento de maturidade e resiliência das organizações do SISP poderá ser alcançado pelas organizações por meio de um processo contínuo de planejamento, execução, verificação e ações corretivas (PDCA) de ciclos de implementação dos controle de privacidade e segurança da informação previstos no framework de privacidade e segurança da informação. Abordagens previstas na

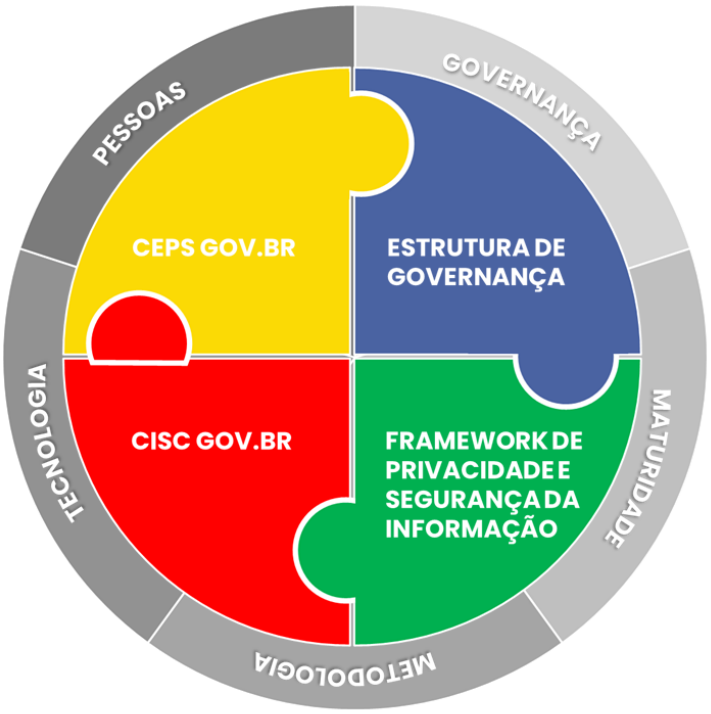

Figura 5.5: Linhas de Defesa e Eixos do PPSI
Fonte: Cartilha PPSI [91]

Portaria SGD/MGI nº 852 de 28 de março de 2023, que prevê um processo contínuo de implementação de controles e medidas de privacidade e segurança da informação para um período de sete ciclos com duração semestral, entre julho de 2023 e dezembro de 2026. Momentos de avaliarmos o aumento da maturidade e resiliência das organizações do SISP por meio dos indicadores de base (iBase), privacidade (iPriv) e indicador de segurança da informação (iSeg).

Ao longo deste capítulo, foi apresentada a proposta do Programa de Privacidade e Segurança da Informação (PPSI), um modelo estruturado para apoiar os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) na implementação de práticas mais robustas de privacidade e segurança da informação. A formulação do PPSI contemplou as linhas de defesa de governança, metodologia, tecnologia, pessoas e, especialmente, maturidade, um fator determinante para a evolução da privacidade e segurança cibernética nas organizações públicas.

Contudo, durante o processo de qualificação da pesquisa, foi identificado um importante desafio: a ampla abrangência do objetivo de pesquisa, que propunha a estruturação completa de um programa de privacidade e segurança da informação. A partir das discussões com os integrantes da banca, concluiu-se que um recorte mais específico seria necessário para aprofundar a análise e garantir uma contribuição mais aplicável, relevante

e concreto. Razão pela qual, a disciplina de maturidade emergiu como o eixo central para a continuidade dos estudos.

Com base nessa diretriz, o Capítulo 6 é dedicado ao desenvolvimento de um modelo de avaliação de maturidade, essencial para compreender a evolução da implementação do PPSI nos órgãos do SISP. Essa abordagem permitirá uma análise estruturada do nível de conformidade e da capacidade das organizações em adotar e sustentar práticas efetivas de privacidade e segurança da informação ao longo dos ciclos do programa. Além disso, o modelo proposto será um instrumento fundamental para medir impactos, identificar lacunas e direcionar ações estratégicas futuras.

Dessa forma, a transição do Capítulo 5 para o Capítulo 6 representa o aprofundamento técnico da proposta do PPSI, ao introduzir o modelo de avaliação de maturidade como instrumento estruturante para mensuração da aderência, evolução e efetividade dos controles implementados. A partir da definição de métricas e indicadores específicos, busca-se garantir a escalabilidade do programa, permitindo diagnósticos precisos, monitoramento contínuo e suporte à tomada de decisão estratégica no contexto da privacidade e segurança da informação no setor público.

Capítulo 6

Modelo de Avaliação de Maturidade

6.1 Introdução

A implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) exige não apenas um conjunto estruturado de diretrizes e processos, mas também um mecanismo eficaz para medir seu progresso e impacto ao longo do tempo. Nesse contexto, a avaliação da maturidade organizacional torna-se um elemento essencial para garantir que os controles estabelecidos sejam aplicados de forma consistente, permitindo que os órgãos avancem de maneira progressiva e estruturada.

Para atender a essa necessidade, este capítulo apresenta o Modelo de Avaliação de Maturidade, uma abordagem metodológica desenvolvida para mensurar o nível de adoção, evolução e consolidação das práticas de privacidade e segurança da informação dentro das instituições públicas federais. O modelo está fundamentado em quatro eixos principais, que sustentam a estrutura do PPSI:

6.1.1 Definição dos Controles:

Conjunto de medidas organizacionais e técnicas estruturadas para garantir privacidade e segurança da informação. Inclui requisitos mínimos, boas práticas e conformidade com normativos como a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Segurança da Informação (PNSI) e a Política Nacional de Segurança Cibernética (PNCiber).

6.1.2 Níveis de Maturidade:

O Modelo de Avaliação de Maturidade do PPSI classifica os órgãos em cinco níveis progressivos, do Inicial (implementação mínima) ao Otimizado (governança plenamente integrada). A evolução ocorre conforme os controles de , estruturação básica, privacidade

e segurança da informação são adotados de maneira estruturada, passando pelos estágios Inicial (adoção parcial), Intermediário (implementação consistente, mas com lacunas) e Aprimorado (monitoramento contínuo e melhoria ativa). Essa estrutura permite um acompanhamento preciso da maturidade organizacional, orientando ajustes estratégicos ao longo dos ciclos do PPSI.

6.1.3 Ciclos de Implementação:

Adoção progressiva dos controles ao longo dos sete ciclos semestrais do PPSI, permitindo que as organizações avancem de maneira estruturada e gradual na aplicação das medidas de privacidade e segurança da informação.

6.1.4 Avaliação por Indicadores:

Monitoramento contínuo da evolução organizacional com base em três indicadores estratégicos:

- a) iBase – Indicador de Estruturação Básica de Governança em Privacidade e Segurança da Informação.
- b) iPriv – Indicador de Maturidade em Privacidade, medindo a conformidade com as práticas de proteção de dados pessoais.
- c) iSeg – Indicador de Segurança da Informação, avaliando a adoção de controles de proteção cibernética.

A aplicação do modelo de maturidade segue uma abordagem estruturada, incorporando avaliações periódicas, auditorias e métricas quantitativas para garantir um acompanhamento efetivo da evolução organizacional. Os dados coletados ao longo dos ciclos semestrais permitem a identificação de gaps, boas práticas e áreas de aprimoramento, possibilitando ajustes estratégicos na implementação do PPSI.

6.2 Fundamentos do Modelo de Maturidade

A implementação de um modelo estruturado para avaliar a maturidade organizacional é fundamental para garantir a evolução contínua das práticas de privacidade e segurança da informação no âmbito do Programa de Privacidade e Segurança da Informação (PPSI). Para que os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) possam acompanhar de forma progressiva a adoção dos controles estabelecidos,

é necessário um método padronizado de mensuração, alinhado a referências normativas nacionais e internacionais.

O Modelo de Avaliação de Maturidade do PPSI foi desenvolvido para suprir essa necessidade, permitindo que cada organização compreenda seu nível atual de conformidade e defina estratégias de aprimoramento com base em uma abordagem estruturada. Essa metodologia garante que os órgãos públicos avancem na implementação das melhores práticas de segurança e privacidade, reduzindo riscos, fortalecendo a governança e assegurando a proteção de dados pessoais e institucionais.

Este modelo é sustentado por diretrizes reconhecidas globalmente e adaptadas à realidade do setor público federal brasileiro, garantindo conformidade regulatória e alinhamento estratégico com as políticas nacionais de segurança cibernética e proteção de dados.

6.2.1 Objetivos e Justificativa

O Modelo de Avaliação de Maturidade do PPSI tem como principal objetivo mensurar e acompanhar a evolução da implementação das diretrizes de privacidade e segurança da informação nos órgãos do SISP. Entre os principais benefícios proporcionados pelo modelo, destacam-se:

a) Monitoramento contínuo da evolução organizacional, permitindo ajustes estratégicos baseados em evidências.

b) Fortalecimento da governança em privacidade e segurança da informação, garantindo que as práticas sejam institucionalizadas e aprimoradas ao longo do tempo.

c) Aprimoramento da resiliência organizacional, reduzindo vulnerabilidades e aumentando a capacidade de resposta a incidentes de segurança e conformidade regulatória.

d) Criaço de um referencial padronizado, permitindo comparaços e benchmarking entre os órgos do SISP.

Com essa abordagem, o modelo possibilita a adaptação contínua das organizações às novas exigências regulatórias e às melhores práticas internacionais, contribuindo para um ecossistema mais seguro e confiável dentro do governo digital brasileiro.

6.2.2 Referências Metodológicas e Normativas

O modelo é baseado em metodologias amplamente reconhecidas no campo da privacidade e segurança da informação. Para garantir sua robustez e aplicabilidade, ele incorpora princípios e frameworks consolidados, tais como:

a) NIST Cybersecurity Framework (NIST CSF) – Estrutura amplamente utilizada para a implementação de boas práticas de segurança cibernética, com ênfase em identificação, proteção, detecção, resposta e recuperação.

b) CIS Controls – Conjunto de controles de segurança cibernética desenvolvidos pelo Center for Internet Security (CIS), com foco na mitigação de ameaças e melhoria da postura de segurança organizacional.

c) ISO/IEC 27001 e ISO/IEC 27701 – Normas internacionais que estabelecem requisitos para a gestão da segurança da informação e da privacidade, fornecendo um referencial para a conformidade regulatória e a governança de dados.

Além das diretrizes internacionais, o modelo também está alinhado às normativas nacionais que regem a privacidade e a segurança da informação no setor público, incluindo:

a) Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) – Marco regulatório que estabelece diretrizes para o tratamento de dados pessoais no Brasil.

b) Política Nacional de Segurança da Informação (PNSI – Decreto nº 9.637/2018) – Diretriz governamental que define princípios e estratégias para a segurança da informação no país.

c) Política Nacional de Cibersegurança (PNCiber – Decreto nº 11.856/2023) – Política Nacional de Cibersegurança voltada para o fortalecimento da resiliência cibernética e proteção das infraestruturas críticas.

d) Portaria SGD/MGI nº 852/2023 – Regulamentação específica para os órgãos do SISP, estabelecendo diretrizes e requisitos mínimos para a implementação do PPSI.

e) Framework de Privacidade e Segurança da Informação do PPSI.

6.2.3 Etapas da Implementação do Modelo

A materização da implementação, operação e melhoria contínua do PPSI é viabilizada por meio de sua metodologia prevista no Art. 9º, da PORTARIA SGD/MGI Nº 852/2023 que aponta como etapas para a implementação do Framework de Privacidade e Segurança da Informação: Autoavaliação, Análise de lacunas, Planejamento e Implementação das medidas.

A adoção desse modelo de maturidade permite que os órgãos do SISP avaliem seu nível de conformidade, identifiquem lacunas e definam planos de ação para aprimoramento contínuo. Dessa forma, o governo federal avança na construção de um ambiente digital mais seguro, resiliente e alinhado às melhores práticas globais de segurança e privacidade.

6.3 Estrutura do Modelo de Maturidade

O Modelo de Avaliação de Maturidade do PPSI foi desenvolvido para fornecer um referencial estruturado que permita aos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) compreender sua posição atual em relação à privacidade e à segurança da informação e planejar sua evolução de forma progressiva.

Figura 6.1: Framework de Priv e SI
Fonte: Cartilha PPSI [91]

A estrutura do modelo está baseada em quatro eixos principais que orientam sua aplicação:

a) Definição dos Controles: Conjunto de diretrizes organizacionais e técnicas que estabelecem requisitos mínimos para garantir privacidade e segurança da informação nos órgãos do SISP.

b) Níveis de Maturidade: Classificação dos órgãos conforme sua adoção e aprimoramento dos controles de privacidade e segurança da informação.

c) Ciclos de Implementação: Processo estruturado para a evolução contínua dos órgãos ao longo dos ciclos semestrais do PPSI.

d) Avaliação por Indicadores: Mecanismos que permitem mensurar a evolução da maturidade organizacional nas disciplinas do PPSI.

6.3.1 Definição dos Controles

O Framework de Privacidade e Segurança da Informação é resultado de extensa pesquisa de abordagens e modelos para implementação de controles e medidas que visam a assegurar a privacidade, a proteção de dados pessoais e a segurança da informação. [92].

O Framework de Privacidade e Segurança da Informação do PPSI, formado um conjunto de 32 Controles e 310 Medidas, apresenta 3 grandes categorias de controles:

a) Estruturação Básica: Estruturação da governança institucional, incluindo políticas organizacionais, designação de responsáveis (Gestor de TIC, Encarregado de Dados, Gestor de Segurança da Informação) e criação de processos internos para assegurar a conformidade com a legislação vigente.

b) Controles de Segurança Cibernética: Proteção dos ativos digitais, detecção e resposta a ameaças, mitigação de riscos e implementação de mecanismos de defesa para fortalecer a resiliência organizacional.

c) Controles de Privacidade: Diretrizes para a proteção de dados pessoais, alinhadas à Lei Geral de Proteção de Dados (LGPD), visando a minimização de riscos, governança da privacidade e medidas de mitigação de impactos à confidencialidade e integridade dos dados tratados pelos órgãos públicos.

A. Os Controles de Estruturação Básica: Controle 0

Os controles de estruturação básica de gestão em privacidade e segurança da informação visam atender às ações de conformidade mínima estabelecidas por regulamentos. O papel da alta administração é essencial para prover os meios e recursos necessários para o estabelecimento dessa categoria de controles dentro do órgão ou entidade.Essa estrutura é composta pelo Controle 0 (Zero) e um conjunto de 7 medidas essenciais, descritas a seguir:

- O órgão nomeou um Gestor de Tecnologia da Informação e Comunicação (TIC)?
- O órgão nomeou um Gestor de Segurança da Informação (CISO)?
- O órgão nomeou um Responsável pela Unidade de Controle Interno?
- O órgão instituiu um Comitê de Segurança da Informação?
- O órgão instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR)?
- O órgão elaborou uma Política de Segurança da Informação (POSIN)?
- O órgão nomeou um Encarregado pelo Tratamento de Dados Pessoais (DPO)?

Essas medidas garantem a estruturação mínima necessária para que os órgãos possam avançar na implementação dos demais controles de segurança e privacidade.

B. Os Controles de Segurança Cibernética: Controles 1 a 18

Os controles de segurança cibernética são baseados no CIS Controls v8, visando mitigar riscos cibernéticos por meio de medidas prioritárias e práticas recomendadas. Os principais controles incluem:

- **Controle 1**: Inventário e Controle de Ativos Institucionais: Identificar e gerenciar dispositivos conectados.
- **Controle 2**: Inventário e Controle de Ativos de Software: Identificar e monitorar aplicações.
- **Controle 3**: Proteção de Dados: Garantir que dados sensíveis sejam protegidos contra acessos não autorizados.
- **Controle 4**: Configuração Segura de Ativos e Software: Implementar padrões de configuração segura.
- **Controle 5**: Gestão de Contas: Gerenciar contas e credenciais de usuários.
- **Controle 6**: Gestão do Controle de Acesso: Implementar regras de acesso baseadas em privilégios mínimos.
- **Controle 7**: Gestão Contínua de Vulnerabilidades: Identificar e corrigir vulnerabilidades.
- **Controle 8**: Gestão de Registros de Auditoria: Monitorar atividades e registros.
- **Controle 9**: Proteções de E-mail e Navegador Web: Garantir segurança contra ataques via e-mails e navegadores.
- **Controle 10**: Defesas Contra Malware: Implementar medidas contra códigos maliciosos.
- **Controle 11**: Recuperação de Dados: Assegurar backups e planos de recuperação.
- **Controle 12**: Gestão da Infraestrutura de Rede: Proteger a arquitetura de rede.
- **Controle 13**: Monitoramento e Defesa da Rede: Identificar e responder a ataques na rede.
- **Controle 14**: Conscientização e Treinamento de Segurança: Promover a educação de usuários.

- **Controle 15**: Gestão de Provedores de Serviços: Monitorar fornecedores e parceiros.
- **Controle 16**: Segurança de Aplicações: Proteger sistemas desenvolvidos ou adquiridos.
- **Controle 17**: Gestão de Resposta a Incidentes: Estabelecer processos para lidar com incidentes.
- **Controle 18**: Testes de Invasão: Simular ataques para validar controles de segurança.

C. Os Controles de Privacidade: Controles 19 a 32

Os controles de privacidade estão alinhados a normas como ISO/IEC 29100, 27701 e a LGPD, garantindo conformidade com a proteção de dados pessoais. Os principais controles incluem:

- **Controle 19**: Inventário e Mapeamento: Identificar fluxos e dados tratados pela organização.
- **Controle 20**: Finalidade e Hipóteses Legais: Estabelecer a legalidade no tratamento de dados.
- **Controle 21**: Governança: Criar uma estrutura de governança para proteção de dados.
- **Controle 22**: Políticas, Processos e Procedimentos: Formalizar diretrizes para tratamento de dados.
- **Controle 23**: Conscientização e Treinamento: Treinar colaboradores sobre privacidade.
- **Controle 24**: Minimização de Dados: Coletar e processar apenas dados necessários.
- **Controle 25**: Gestão do Tratamento: Monitorar atividades de tratamento de dados.
- **Controle 26**: Acesso e Qualidade: Garantir que os titulares tenham acesso e controle sobre seus dados.
- **Controle 27**: Compartilhamento e Transferência: Estabelecer regras para transferir dados a terceiros.

- **Controle 28**: Supervisão em Terceiros: Monitorar fornecedores e parceiros quanto à conformidade com privacidade.
- **Controle 29**: Abertura, Transparência e Notificação: Comunicar de forma clara como os dados são tratados.
- **Controle 30**: Avaliação de Impacto, Monitoramento e Auditoria: Realizar avaliações periódicas de impacto à privacidade.
- **Controle 31**: Segurança Aplicada à Privacidade: Integrar segurança e privacidade nas operações.

Por fim, cabe destacar que os controles e medidas mencionados nesta seção estão disponíveis para consulta no Framework de Privacidade e Segurança da Informação, bem como na planilha oficial de autodiagnóstico. Optou-se por não transcrevê-los integralmente nesta dissertação devido à expressiva quantidade de itens, o que poderia comprometer a objetividade do texto e sobrecarregar seus anexos. Ambos os materiais estão acessíveis no portal da Secretaria de Governo Digital. [92, 93]

6.3.2 Níveis de Maturidade

O Modelo de Avaliação de Maturidade do PPSI classifica os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) conforme seu nível de adoção e aprimoramento dos controles de privacidade e segurança da informação. O modelo propõe cinco níveis de maturidade para avaliar a evolução da implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do SISP. Cada nível representa um estágio de evolução, desde uma implementação mínima até a maturidade plena.

iMC	Nível de Maturidade
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Figura 6.2: Indicador e Nível de Maturidade
Fonte: Cartilha PPSI [91]

Os níveis de maturidade são definidos da seguinte forma:

a) Nível 1 – Inicial (Implementação mínima ou inexistente) - Descrição: Órgão sem estrutura formalizada de privacidade e segurança da informação. Adoção de práticas é pontual e desorganizada. Características: a) Não há políticas ou diretrizes formais de privacidade e segurança; b) Ausência de responsáveis designados (exemplo: Encarregado de Dados ou Gestor de Segurança da Informação); c) Baixa conscientização sobre segurança e privacidade; e d) Risco elevado de incidentes de segurança sem capacidade de resposta estruturada.

b) Nível 2 – Básico (Controles aplicados parcialmente, com grandes lacunas) - Descrição: Órgão inicia esforços para estruturar um programa de segurança e privacidade, mas de forma reativa e sem integração organizacional. Características: a) Políticas e diretrizes básicas estabelecidas, mas sem aplicabilidade ampla; b) Encarregado de Dados e Gestor de Segurança podem ter sido designados, mas sem atuação efetiva; c) Implementação parcial de controles mínimos de segurança (exemplo: senhas fortes, backups básicos); d) Treinamentos de conscientização ocorrem de forma esporádica; e e) Monitoramento de segurança e resposta a incidentes limitados.

c) Nível 3 – Intermediário (Adoção regular dos controles, mas ainda há riscos) - Descrição: O órgão tem uma governança mais estruturada, adota políticas e processos, mas ainda enfrenta desafios na implementação plena. Características: a) Governança parcialmente estruturada, com diretrizes e papéis formalizados; b) Controles de segurança cibernética e privacidade implementados, mas com lacunas em auditoria e melhoria contínua; c) Indicadores básicos de maturidade (iBase, iPriv, iSeg) começam a ser monitorados; d) Plano de resposta a incidentes definido, mas com baixa eficiência operacional; e e) Programas de conscientização e treinamento mais frequentes.

d) Nível 4 – Em aprimoramento (Práticas bem estabelecidas, com melhoria contínua) - Descrição: O órgão adota um programa consolidado, com processos bem definidos e cultura organizacional voltada à segurança e privacidade. Características: a) Privacidade e Segurança fazem parte da governança estratégica do órgão; b) Indicadores de maturidade são monitorados e usados para ajustes contínuos; c) Automação parcial de controles (exemplo: gestão de acessos, detecção de ameaças); d) Gestão de fornecedores e contratos inclui requisitos de privacidade e segurança; e e) Simulações de resposta a incidentes realizadas periodicamente.

e) Nível 5 – Aprimorado (Maturidade plena, segurança e privacidade integradas à estratégia organizacional) - Descrição: O órgão atinge um nível de excelência, onde segurança e privacidade são elementos fundamentais da estratégia e da operação organizacional. Características: a) Privacidade e segurança são integradas ao ciclo de vida dos processos e sistemas; b) Monitoramento contínuo e análise preditiva de riscos; c) Uso de inteligência artificial e automação para detecção e resposta a ameaças; d) Auditorias frequentes e

alinhamento com padrões internacionais (NIST, ISO, CIS); e e) Governança aprimorada com participação ativa da alta administração.

A definição desses níveis permite uma avaliação objetiva do progresso de cada órgão, facilitando a priorização de esforços e investimentos para alcançar maior maturidade em segurança e privacidade.

6.3.3 Ciclos de Implementação

Os sete ciclos do PPSI estruturam um processo de evolução contínua, permitindo que os órgãos do SISP alcancem níveis avançados de maturidade em privacidade e segurança da informação. O modelo assegura que o PPSI não apenas estabeleça diretrizes robustas, mas também forneça um mecanismo dinâmico de adaptação às novas ameaças e regulamentações. A implementação progressiva fortalece as capacidades institucionais, reduz vulnerabilidades críticas e aprimora a governança cibernética dos órgãos públicos, garantindo maior resiliência contra ameaças cibernéticas e conformidade regulatória. Eles seguem um modelo semestral, alinhado à Portaria SGD/MGI nº 852/2023, permitindo uma adoção gradual dos controles de segurança e privacidade.

A. Estrutura dos Ciclos Semestrais

Os ciclos semestrais foram criados para garantir que os órgãos possam:

a) Planejar e implementar os controles de forma estruturada;

b) Evoluir a maturidade organizacional em privacidade e segurança de maneira contínua;

c) Reduzir riscos institucionais associados à proteção de dados e segurança da informação;

d) Garantir conformidade com normativos como LGPD, PNSI e PNCiber.

e) Cada ciclo é estruturado com fases progressivas que orientam a implementação e evolução dos controles.

B. Etapas dos Ciclos de Implementação

Os sete ciclos do PPSI estruturam a evolução dos órgãos do SISP, desde a implementação inicial até a governança avançada, garantindo maturidade, resiliência e adaptação contínua, conforme descritos abaixo.

a) 1º Ciclo (2º Semestre de 2023) – Implementação Inicial. No primeiro ciclo, a implementação concentrou-se em controles e medidas críticas de baixa ou média complexidade, permitindo que os órgãos iniciassem a adequação ao programa sem necessidade de contratação adicional. Essa fase foi essencial para estabelecer a estrutura básica do PPSI

e definir os primeiros níveis de maturidade organizacional. Além disso, criou as bases para a mensuração de progresso, permitindo que os órgãos identificassem seus principais desafios e oportunidades de aprimoramento.

b) 2º Ciclo (1º Semestre de 2024) – Expansão das Medidas Críticas - Com a evolução do programa, o segundo ciclo ampliou a implementação de controles de médio e alto esforço, exigindo maior envolvimento das organizações. Essa etapa focou em medidas que demandaram mais planejamento e execução, mas ainda sem necessidade de contratações, garantindo uma expansão estruturada da capacidade organizacional em privacidade e segurança da informação. Os indicadores começaram a ser monitorados mais de perto, permitindo ajustes estratégicos na implementação do programa.

c) 3º Ciclo (2º Semestre de 2024) – Controles Dependentes de Contratação - A partir do terceiro ciclo, a complexidade da implementação aumentou com a introdução de controles que poderiam exigir contratações estratégicas, como aquisição de ferramentas de segurança da informação, serviços especializados e infraestrutura tecnológica avançada. A avaliação da capacidade dos órgãos foi um fator fundamental para garantir que os investimentos fossem planejados corretamente, alinhando as necessidades institucionais com o orçamento disponível. Esse ciclo também marcou o início da integração de novas práticas para o fortalecimento dos frameworks de segurança e privacidade.

d) 4º Ciclo (1º Semestre de 2025) – Integração e Automação - O quarto ciclo focou na evolução e automação dos controles implementados nos ciclos anteriores. As organizações começaram a adotar soluções mais integradas para otimizar processos e reduzir a carga operacional das equipes de segurança e privacidade. Além disso, houve aprimoramento na resposta a incidentes e no monitoramento contínuo de riscos, garantindo um maior alinhamento entre tecnologia e governança organizacional. Essa fase foi crucial para consolidar práticas maduras e iniciar a transição para um modelo mais automatizado.

e) 5º Ciclo (2º Semestre de 2025) – Consolidação e Governança Avançada - Com os controles fundamentais implementados, o quinto ciclo priorizou o fortalecimento da governança e gestão de riscos. As organizações avançaram na adoção de indicadores estratégicos, como iPriv, iSeg e iBase, permitindo uma análise mais precisa da maturidade organizacional e da eficácia das políticas implementadas. A inteligência de segurança passou a ser um pilar central, garantindo uma abordagem mais proativa e baseada em dados para a gestão de riscos cibernéticos.

f) 6º Ciclo (1º Semestre de 2026) – Especialização Técnica e Segurança Avançada - No sexto ciclo, o PPSI atingiu um nível de especialização elevado, focando na adoção de controles altamente técnicos e no fortalecimento da capacidade operacional das equipes de segurança e privacidade. A necessidade de profissionais qualificados tornou-se ainda mais evidente, uma vez que os processos implementados passaram a exigir conhecimento

avançado em segurança cibernética, proteção de dados e inteligência artificial aplicada à segurança. Além disso, houve um alinhamento mais rigoroso com frameworks internacionais e normativas regulatórias, garantindo conformidade plena com padrões globais.

g) 7º Ciclo (2º Semestre de 2026) – Retrospectiva e Planejamento Futuro - Encerrando o modelo de implementação, o sétimo ciclo foi dedicado à revisão crítica e avaliação dos impactos das fases anteriores. Com base nas consultas aos órgãos participantes, foram identificados novos desafios e oportunidades de aprimoramento para as fases futuras do programa. Esse ciclo focou na preparação do PPSI 2.0, estabelecendo novas diretrizes estratégicas e metodologias aprimoradas para consolidar uma cultura de privacidade e segurança da informação no governo digital.

Em síntese, os sete ciclos do PPSI representam uma jornada estruturada de amadurecimento institucional, que vai desde a implementação inicial até a consolidação de práticas avançadas de governança, automação e segurança cibernética. Essa abordagem em fases progressivas permite que os órgãos do SISP evoluam de forma coordenada, adaptando-se às exigências regulatórias, às ameaças emergentes e às necessidades específicas de cada estágio. O modelo cíclico garante não apenas a continuidade e o monitoramento da evolução, mas também a incorporação de lições aprendidas e a preparação para futuras versões do programa, como o PPSI 2.0.

6.3.4 Avaliação por Indicadores

A avaliação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) é realizada por meio de indicadores estruturados que permitem mensurar a evolução da maturidade organizacional em governança, privacidade e segurança da informação.

A. Indicadores de Maturidade do PPSI

Os seguintes indicadores foram desenvolvidos para acompanhar a implementação do PPSI e apoiar o aprimoramento contínuo das práticas adotadas:

Os seguintes indicadores foram desenvolvidos para acompanhar a implementação do PPSI e apoiar o aprimoramento contínuo das práticas adotadas:

a) iBase (Indicador de Estruturação Básica de Governança em Privacidade e Segurança da Informação) - Avalia a existência e a formalização de políticas, processos e estruturas de governança para privacidade e segurança da informação nos órgãos do SISP.

b) iPriv (Indicador de Maturidade em Privacidade) - Mede o grau de conformidade dos órgãos do SISP com a Lei Geral de Proteção de Dados (LGPD), analisando a implementação de processos de tratamento, proteção e governança de dados pessoais.

c) iSeg (Indicador de Segurança da Informação) - Avalia a adoção e a efetividade dos controles de segurança cibernética implementados, com base em frameworks reconhecidos, como NIST CSF, CIS Controls e ISO/IEC 27001 e 27002.

B. Métodos de Coleta e Avaliação

A mensuração dos indicadores do PPSI é realizada por meio de diferentes métodos, garantindo um diagnóstico preciso e fundamentado:

a) Autoavaliação Institucional - Os órgãos do SISP realizam uma avaliação interna da sua maturidade, reportando seu nível de conformidade e implementação dos controles exigidos.

b) Auditorias e Avaliações Externas - Validação das informações fornecidas pelas autoavaliações por meio de inspeções técnicas, auditorias e verificações conduzidas por especialistas.

c) Análise Documental e Métricas Quantitativas - Monitoramento de relatórios de conformidade, análise de incidentes de segurança e privacidade, e avaliação de métricas operacionais relacionadas à implementação do PPSI.

C. Estratégias de Ajuste e Melhoria

Os dados obtidos a partir da avaliação dos indicadores são fundamentais para a evolução do PPSI. Algumas estratégias adotadas incluem:

a) Utilização dos Indicadores para Ajustes no PPSI - Os resultados da avaliação orientam a definição de ações corretivas e preventivas, possibilitando um ajuste contínuo na implementação do programa.

b) Customização do Modelo para Diferentes Perfis de Órgãos - Considerando as diferenças entre os órgãos do SISP (exemplo: ministérios, autarquias, universidades federais), os indicadores permitem adaptações específicas, garantindo um modelo flexível e aplicável a diferentes realidades organizacionais.

c) Monitoramento Contínuo e Ciclos de Aprimoramento - Os dados coletados são analisados periodicamente, permitindo ajustes estratégicos nos ciclos do PPSI e contribuindo para o aprimoramento contínuo da maturidade em privacidade e segurança da informação nos órgãos do governo digital.

6.3.5 Indicadores de Maturidade: iBase, iPriv e iSeg

Como já citado na Seção 6.3.4, com o objetivo de possibilitar análises comparativas entre instituições, ciclos e categorias temáticas, foram definidos três indicadores consolidados de maturidade: iBase, iPriv e iSeg. Esses indicadores sintetizam o desempenho das

organizações a partir da estruturação e implementação dos controles do PPSI, de forma a apoiar o monitoramento da evolução institucional.

a) iBase (Indicador de Estrutura Mínima de Governança): Componente: Controle 0, Estrutura Inicial de Governança.

Fórmula: iBase = iMCo.

b) iPriv (Indicador de Maturidade em Privacidade): Componentes: Controles 1 a 13, além do Controle 0 com peso 4.

Fórmula: iPriv = [(iMCo×4)+ (13/i=1 iMCi)] / 17

c) iSeg (Indicador de Maturidade em Segurança da Informação): Componentes: Controles 14 a 31, além do Controle 0 com peso 4.

Fórmula: iSeg = [(iMCo×4)+ (31/i=14 iMCi)] / 22

6.4 Reflexões sobre a Construção do Modelo

A construção do Modelo de Avaliação de Maturidade do PPSI demandou um processo estruturado e fundamentado em princípios metodológicos consolidados, alinhando referências normativas, frameworks de privacidade e segurança, e a realidade institucional dos órgãos do SISP. Esse modelo foi concebido para servir como uma ferramenta de diagnóstico e acompanhamento da evolução da maturidade organizacional, garantindo uma aplicação progressiva e adaptável ao longo dos ciclos de implementação do PPSI.

A seguir, discutimos os principais aspectos considerados na construção do modelo, divididos em quatro eixos principais: (i) fundamentos e diretrizes, (ii) estrutura e componentes, (iii) desafios na modelagem e (iv) ajustes metodológicos para sua implementação.

6.4.1 Fundamentos e Diretrizes

A elaboração do modelo partiu da necessidade de medir e acompanhar o avanço da implementação do PPSI, garantindo padronização na avaliação e comparabilidade entre órgãos. Para isso, foram considerados os seguintes elementos:

a) Adoção de frameworks e normas reconhecidas: O modelo foi desenvolvido com base em diretrizes da ISO/IEC 27001, ISO/IEC 27701, NIST CSF, CIS Controls, LGPD, PNSI e PNCiber, garantindo aderência às melhores práticas internacionais.

b) Estratégia baseada em ciclos de implementação: Optou-se por uma abordagem gradual e estruturada em ciclos semestrais, permitindo que os órgãos evoluíssem progressivamente nos níveis de maturidade.

c) Indicadores estratégicos de avaliação: Foram definidos três indicadores principais para medir a maturidade organizacional: iBase – Indicador de estruturação básica em segurança e privacidade, iPriv – Indicador de conformidade com a LGPD e gestão de

privacidade e iSeg – Indicador de implementação de controles de segurança da informação e cibernética.

Essa abordagem garantiu que o modelo não fosse apenas um mecanismo de auditoria, mas sim um instrumento de gestão contínua de privacidade e segurança da informação nos órgãos do SISP.

6.4.2 Estrutura e Componentes do Modelo

A modelagem seguiu uma estrutura baseada em níveis de maturidade, garantindo uma avaliação escalonada do progresso dos órgãos. Para isso, foram definidos: Cinco níveis de maturidade, variando de Inicial (Nível 1) a Otimizado (Nível 5), conforme a adoção progressiva dos controles do PPSI. Três domínios principais de avaliação: Governança, Segurança Cibernética e Privacidade. 32 controles e 310 medidas de segurança e privacidade, divididos entre controles básicos, controles avançados e práticas estratégicas. Além disso, o modelo foi concebido para ser aplicado de forma flexível, permitindo ajustes conforme as especificidades de cada órgão, garantindo escalabilidade para diferentes níveis de maturidade organizacional.

6.4.3 Desafios na Modelagem

A fase de construção do modelo enfrentou desafios metodológicos e conceituais que exigiram adaptações para garantir sua aplicabilidade prática. Entre os principais desafios identificados, destacam-se:

a) Harmonização entre padrões normativos: A necessidade de alinhar diferentes frameworks e regulamentações exigiu um esforço adicional para garantir coesão entre os critérios de avaliação.

b) Definição de métricas quantitativas e qualitativas: A quantificação da maturidade foi um ponto crítico, exigindo um equilíbrio entre medições objetivas e análises qualitativas para garantir uma avaliação precisa do progresso organizacional.

c) Adaptação à realidade dos órgãos do SISP: O modelo precisava ser aplicável a órgãos com diferentes níveis de maturidade, exigindo flexibilidade na adoção dos controles sem comprometer a comparabilidade entre instituições.

Para mitigar esses desafios, foram realizadas validações preliminares e ajustes metodológicos, preparando o modelo para sua futura aplicação nos ciclos do PPSI.

6.4.4 Ajustes Metodológicos para Implementação

Com base na fase de modelagem, foram definidos ajustes metodológicos estratégicos para garantir uma implementação mais eficiente nos órgãos do SISP:

a) Definição de um roadmap de implementação: Foram estruturados ciclos semestrais, permitindo uma adoção gradual do modelo, evitando sobrecarga e facilitando o ajuste das organizações ao novo framework.

b) Criação de guias e materiais de apoio: Foram desenvolvidos documentos explicativos para padronizar a aplicação do modelo, incluindo guias operacionais e exemplos práticos.

c) Capacitação das equipes responsáveis: Para facilitar a adoção, foram previstas ações de treinamento e suporte técnico, garantindo que as equipes dos órgãos compreendam os critérios de avaliação e aplicação do modelo.

6.5 Considerações Finais

A construção do Modelo de Avaliação de Maturidade do PPSI representa um avanço metodológico significativo para a governança da segurança e privacidade no Governo Digital do Brasil. Esse modelo foi concebido para oferecer uma abordagem estruturada, escalável e adaptável, permitindo que os órgãos do SISP evoluam de forma progressiva na adoção de boas práticas.

A preparação para a aplicação do modelo envolveu ajustes metodológicos, estruturação de indicadores estratégicos e planejamento dos ciclos de implementação. Essa etapa foi essencial para garantir que o modelo não apenas avaliasse a maturidade das instituições, mas também servisse como um guia para a evolução contínua da segurança e privacidade.

Os próximos passos incluem a aplicação do modelo nos ciclos de implementação do PPSI, o que será detalhado nos capítulos seguintes:

No Capítulo 7 – Estudo de Caso Confirmatório, será descrito o processo de aplicação do modelo aos órgãos do SISP, abordando a metodologia de implementação e os desafios operacionais.

No Capítulo 8 – Discussão dos Resultados, será realizada uma análise crítica da aplicação do modelo, destacando tendências observadas, fatores de sucesso e ajustes necessários para aprimorar futuras iterações do PPSI. Com isso, a pesquisa avança para a fase prática, validando a aplicabilidade do modelo e seu impacto na governança de privacidade e segurança da informação no Governo Digital do Brasil.

Capítulo 7

Estudo de Caso Confirmatório

7.1 Introdução

O estudo de caso confirmatório é uma abordagem metodológica utilizada para validar empiricamente a eficácia e aplicabilidade de um modelo previamente desenvolvido. No contexto desta pesquisa, ele se torna fundamental para comprovar a implementação e os impactos do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP).[10]

A adoção do estudo de caso confirmatório neste trabalho tem como objetivo avaliar a evolução da maturidade em privacidade e segurança da informação das organizações participantes, verificando se os controles, diretrizes e processos estabelecidos no PPSI foram eficazes para fortalecer a governança e a resiliência cibernética no Governo Digital.

Dessa forma, este capítulo apresenta a aplicação prática do modelo de maturidade do PPSI ao longo de três ciclos semestrais de implementação, fornecendo uma análise estruturada sobre os avanços obtidos e os desafios enfrentados. Além disso, ele estabelece a conexão entre a teoria e a prática, demonstrando como as diretrizes formuladas nos capítulos anteriores foram implementadas no ambiente real das organizações do SISP.

Por fim, os resultados deste estudo de caso irão embasar a análise quantitativa e qualitativa dos impactos do PPSI, que serão detalhados no Capítulo 8 – Discussão dos Resultados.

7.2 Escopo do Estudo de Caso

O escopo do estudo de caso confirmatório abrange a aplicação do Programa de Privacidade e Segurança da Informação (PPSI) nos 254 órgãos que compõem o Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP). Esses órgãos

representam um universo diverso, incluindo ministérios, agências reguladoras, autarquias, fundações, universidades e institutos, sendo responsáveis por serviços digitais essenciais para milhões de cidadãos brasileiros.

A escolha do SISP como objeto do estudo de caso se justifica por três fatores principais:

a) Abrangência e impacto estratégico: O SISP reúne as principais entidades responsáveis pela governança da tecnologia da informação no Governo Federal, sendo um ambiente ideal para avaliar a maturidade e evolução da privacidade e da segurança da informação.

b) Conformidade regulatória e necessidade de padronização: A implementação do PPSI se alinha diretamente às exigências da Portaria SGD/MGI nº 852/2023, que estabelece diretrizes para elevar a resiliência e maturidade das organizações governamentais em privacidade e segurança da informação.

c) Disponibilidade de dados e possibilidade de acompanhamento longitudinal: O estudo de caso foi estruturado para permitir uma análise em três ciclos de implementação, possibilitando a mensuração da evolução ao longo do tempo e a identificação de padrões que possam guiar futuras melhorias no PPSI.

7.2.1 Papel da Secretaria de Governo Digital (SGD/MGI)

A Secretaria de Governo Digital (SGD/MGI) desempenha um papel fundamental na liderança e coordenação do PPSI junto aos 254 órgãos que compõem o SISP, orientando a adoção das diretrizes, promovendo capacitação e monitorando a evolução da implementação do programa em cada instituição. Essa atuação centraliza a governança da privacidade e segurança da informação no Governo Digital brasileiro, garantindo a harmonização das iniciativas e a adoção progressiva das melhores práticas nos diferentes órgãos e entidades federais. Suas principais funções incluem:

a) Definição de diretrizes e metodologias para a implementação dos controles de segurança e privacidade.

b) Apoio técnico e normativo aos órgãos participantes, por meio da disponibilização de guias, ferramentas e treinamentos.

c) Monitoramento da evolução dos indicadores de maturidade e avaliação periódica dos resultados obtidos a partir do autodiagnóstico dos órgãos do SISP.

d) Articulação institucional para fomentar a adoção das melhores práticas e garantir alinhamento estratégico entre os diversos setores do Governo Digital.

O modelo de governança fortalece a aplicação do PPSI e possibilita a construção de um ambiente digital mais seguro e resiliente, alinhado às melhores práticas nacionais e internacionais.

7.3 Aplicação do Modelo de Avaliação de Maturidade

A aplicação do Modelo de Avaliação de Maturidade do PPSI no estudo de caso confirmatório teve como objetivo mensurar o nível de adoção e efetividade das práticas de privacidade e segurança da informação nos órgãos do Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP). Esse modelo permitiu um diagnóstico estruturado, possibilitando a identificação de avanços, desafios e oportunidades de aprimoramento ao longo dos três ciclos de implementação.

A metodologia utilizada seguiu um processo baseado em autodiagnóstico institucional, auditorias amostrais e indicadores quantitativos e qualitativos. A avaliação foi conduzida por meio de três principais componentes:

7.3.1 Instrumento de Autodiagnóstico

a) Aplicação de um questionário estruturado para que os órgãos avaliassem seu nível de conformidade em relação aos controles estabelecidos pelo PPSI. b) Os resultados foram utilizados para medir a maturidade institucional e estabelecer planos de ação para evolução nos ciclos subsequentes.

7.3.2 Auditorias e Validação Externa

a) Realização de auditorias amostrais para verificar a consistência das respostas do autodiagnóstico e validar as evidências apresentadas. b) Utilização de metodologias baseadas em frameworks internacionais, como ISO/IEC 27001, ISO/IEC 27702, NIST CSF e CIS Controls.

7.3.3 Métricas e Indicadores de Maturidade

a) Aplicação dos indicadores estratégicos desenvolvidos no Capítulo 6 (iBase, iPriv e iSeg). b) Monitoramento contínuo dos indicadores para acompanhar a evolução da maturidade ao longo dos ciclos de implementação.

7.4 Processo de Coleta e Análise dos Dados

7.4.1 Coleta Inicial de Dados

a) Aplicação do autodiagnóstico junto aos órgãos do SISP no início de cada ciclo. b) Reuniões técnicas e capacitações para garantir o correto preenchimento dos formulários.

7.4.2 Análise e Correlação dos Resultados

a) Consolidação dos dados do autodiagnóstico e cruzamento com informações das auditorias externas. b) Identificação de tendências e desafios comuns entre os órgãos avaliados.

7.4.3 Geração de Relatórios e Feedbacks

a) Produção de relatórios de maturidade para cada órgão, destacando avanços, lacunas e recomendações de melhoria. b) Sessões de devolutiva para as organizações, com orientações para o planejamento das próximas ações.

7.5 Período de Tempo e Estrutura dos Ciclos de Implementação

A implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do SISP foi estruturada em três ciclos semestrais, totalizando um período de 18 meses. Essa abordagem foi planejada para permitir uma adoção progressiva dos controles de privacidade e segurança da informação, considerando as diferentes realidades e níveis de maturidade das instituições participantes.

Cada ciclo teve objetivos específicos, alinhados com as diretrizes estabelecidas no Modelo de Avaliação de Maturidade do PPSI. Essa estrutura possibilitou a identificação de avanços graduais e desafios ao longo do tempo, permitindo ajustes estratégicos conforme necessário.

7.5.1 Estruturação dos Ciclos do PPSI

A implementação do PPSI seguiu um planejamento estruturado em três ciclos principais:

Ciclo 1 – Implementação Inicial (2º Semestre de 2023)

Objetivo principal: Estabelecer a base da governança de privacidade e segurança da informação nos órgãos do SISP.

Principais ações:

a) Realização do autodiagnóstico inicial para mapear o nível de maturidade de cada órgão.

b) Adoção de controles básicos, incluindo políticas institucionais, nomeação de responsáveis e implementação de processos fundamentais.

c) Sensibilização e capacitação das equipes internas sobre as diretrizes do PPSI.

d) Definição de planos de ação para mitigar vulnerabilidades e estruturar processos internos.

Desafios encontrados:

a) Resistência inicial à adoção de novos processos.

b) Necessidade de alinhamento entre diferentes áreas organizacionais.

c) Reduzido quadro de pessoas para implementação da medidas preconizadas.

d) Limitações orçamentárias para implementação imediata de algumas medidas.

Ciclo 2 – Expansão das Medidas Críticas (1º Semestre de 2024)

Objetivo principal: Ampliar a adoção de controles críticos de segurança e privacidade, consolidando os avanços obtidos no primeiro ciclo.

Principais ações:

a) Implementação de controles avançados para a proteção de dados pessoais e segurança da informação.

b) Criação e disseminação de guias orientativos, padronizando a aplicação das medidas do PPSI.

c) Monitoramento dos indicadores iBase, iPriv e iSeg, avaliando o progresso das organizações.

d) Ajustes nos processos internos com base nos aprendizados do primeiro ciclo.

Desafios encontrados:

a) Variação na velocidade de adoção das medidas entre os órgãos.

b) Necessidade de aprimoramento da capacitação das equipes técnicas e administrativas.

c) Desafios na implementação de medidas mais estruturadas sem necessidade de grandes contratações.

Ciclo 3 – Controles Dependentes de Contratação (2º Semestre de 2024)

Objetivo principal: Implementar os controles que exigem investimentos financeiros e maior planejamento institucional.

Principais ações:

a) Aquisição de soluções tecnológicas para fortalecimento da segurança da informação.

b) Integração com frameworks internacionais (ISO/IEC 27001, NIST CSF, CIS Controls).

c) Fortalecimento da gestão de riscos e monitoramento contínuo dos indicadores.

d) Revisão dos processos de governança e ajustes para otimização dos resultados obtidos.

Desafios encontrados:

a) Dependência de processos licitatórios e de orçamento para aquisição de ferramentas.

b) Diferentes níveis de engajamento institucional, exigindo maior articulação da SGD/MGI.

c) daptação dos órgãos às diretrizes internacionais de privacidade e segurança da informação.

7.6 Considerações sobre a Estrutura dos Ciclos

A estruturação dos ciclos proporcionou um crescimento progressivo da maturidade dos órgãos, permitindo que a implementação do PPSI ocorresse de forma ordenada e sustentável. Essa abordagem favoreceu:

a) Adoção gradual de boas práticas, evitando sobrecarga operacional.

b) Identificação de desafios em tempo real, possibilitando ajustes estratégicos.

c) Engajamento contínuo das equipes, promovendo a cultura de segurança e privacidade dentro das instituições.

A transição entre os ciclos foi acompanhada de análises periódicas e relatórios de maturidade, garantindo uma visão clara da evolução do PPSI e preparando o terreno para a Discussão dos Resultados, que será explorada no Capítulo 8.

7.7 Vantagens do Método e Desafios Encontrados

A adoção do estudo de caso confirmatório para validar o Programa de Privacidade e Segurança da Informação (PPSI) trouxe benefícios significativos para a análise da evolução da maturidade dos órgãos do Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP). No entanto, a implementação do programa também apresentou desafios que exigiram ajustes estratégicos ao longo dos ciclos.

7.7.1 Vantagens do Método

A estruturação da implementação do PPSI em três ciclos semestrais, aliada à aplicação do Modelo de Avaliação de Maturidade, proporcionou uma abordagem sistemática e iterativa, trazendo os seguintes benefícios:

1) Avaliação Longitudinal da Maturidade:a) A mensuração da evolução ao longo dos ciclos permitiu compreender tendências e padrões de adoção dos controles de privacidade e segurança da informação. b) A comparação dos resultados entre ciclos ajudou a identificar pontos críticos de melhoria e a ajustar estratégias conforme necessário.

2) Engajamento Institucional e Cultura de Segurança: a) A realização do autodiagnóstico nos órgãos do SISP incentivou a autoconsciência sobre o nível de maturidade

em privacidade e segurança da informação. b) As capacitações promovidas ao longo do programa contribuíram para a construção de uma cultura organizacional mais forte em relação à proteção de dados e gestão de riscos cibernéticos.

3) Validação Empírica do Modelo de Avaliação: a) O estudo de caso possibilitou a testagem prática do Modelo de Avaliação de Maturidade do PPSI, verificando sua adequação às realidades institucionais dos órgãos do SISP. b) A análise dos indicadores estratégicos (iBase, iPriv e iSeg) demonstrou a eficácia do modelo na identificação de avanços e na priorização de ações para melhoria contínua.

4) Flexibilidade e Adaptação às Particularidades dos Órgãos: a) A metodologia adotada permitiu que cada órgão implementasse as diretrizes do PPSI conforme sua realidade e nível de maturidade. b) O modelo possibilitou ajustes personalizados, garantindo uma abordagem mais inclusiva e realista para os diferentes contextos institucionais.

5) Sustentabilidade e Continuidade da Implementação: a) A divisão em ciclos facilitou a integração progressiva das práticas de segurança e privacidade às operações institucionais. b) Os resultados obtidos serviram de base para o aprimoramento da governança de segurança da informação no longo prazo, consolidando um modelo sustentável.

7.7.2 Desafios Encontrados

Apesar das vantagens, a implementação do PPSI nos órgãos do SISP enfrentou desafios significativos, que demandaram ajustes estratégicos ao longo do processo.

1. Resistência Organizacional e Mudança Cultural: a) Alguns órgãos apresentaram resistência inicial na adoção das diretrizes do PPSI, seja por falta de priorização do tema, seja por desconhecimento dos benefícios da implementação. b) Foi necessário um trabalho contínuo de sensibilização e envolvimento da alta gestão para garantir o compromisso institucional com a privacidade e segurança da informação.

2. Disparidade de Maturidade Entre os Órgãos: a) O levantamento inicial revelou grande heterogeneidade no nível de maturidade das organizações participantes, tornando desafiador o estabelecimento de um ritmo uniforme de implementação. b) Para mitigar esse desafio, foram adotadas estratégias diferenciadas de suporte técnico e acompanhamento para os órgãos com menor nível de maturidade.

3. Limitações Orçamentárias e Infraestruturais: A implementação de algumas medidas do PPSI exigiu investimentos em tecnologias de segurança da informação, o que representou um obstáculo para órgãos com restrições orçamentárias. b) Como alternativa, foram priorizadas ações que não dependiam exclusivamente de recursos financeiros, como melhoria na governança, capacitações e revisão de processos internos.

4. Desafios na Contratação de Soluções Tecnológicas: a) A dependência de processos licitatórios para aquisição de ferramentas e serviços especializados em segurança da in-

formação impactou o ritmo da implementação em alguns órgãos. b) Em resposta a essa questão, foram criadas diretrizes para otimizar os processos de contratação, promovendo maior alinhamento com as necessidades do PPSI.

5 Necessidade de Maior Integração Entre Equipes Técnicas e Administrativas: a) Em alguns órgãos, a implementação do PPSI ficou restrita às áreas técnicas de segurança da informação, sem o devido envolvimento das áreas de privacidade e de governança. b) Para resolver essa lacuna, foram promovidas ações de capacitação direcionadas para lideranças e tomadores de decisão, garantindo uma abordagem mais holística.

7.8 Conclusões

A implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema Integrado de Administração dos Recursos de Tecnologia da Informação (SISP) revelou avanços significativos, ao mesmo tempo em que expôs desafios e oportunidades de melhoria. O estudo de caso confirmatório demonstrou a importância de uma abordagem estruturada para a elevação da maturidade em segurança e privacidade, garantindo maior resiliência das instituições governamentais diante das crescentes ameaças cibernéticas.

Os ciclos de implementação do PPSI permitiram uma análise aprofundada sobre a adoção das diretrizes e controles estabelecidos. Os resultados evidenciaram padrões que serão explorados de forma detalhada no próximo capítulo, incluindo:

1. Análise quantitativa dos dados coletados: Avaliação dos indicadores estratégicos de maturidade (iBase, iPriv e iSeg) e sua evolução ao longo dos ciclos.

2. Interpretação qualitativa dos resultados: Identificação de padrões e tendências observadas no autodiagnóstico das instituições participantes.

3. Comparação entre os ciclos: Evolução da implementação ao longo do tempo e os principais fatores que influenciaram o sucesso ou os desafios do programa.

4. Impacto da metodologia adotada: Reflexão sobre a eficácia do modelo de avaliação e das estratégias de implementação do PPSI.

5. Considerações para futuras edições do programa: Sugestões de aprimoramento com base nas evidências coletadas durante o estudo de caso.

Dessa forma, o Capítulo 8 aprofundou a análise dos dados coletados, consolidou os principais achados da pesquisa e forneceu subsídios relevantes para a evolução contínua do Programa de Privacidade e Segurança da Informação (PPSI). A leitura crítica dos resultados permitiu não apenas validar a aplicabilidade do modelo proposto, como também fundamentar recomendações estratégicas voltadas ao fortalecimento da governança, da proteção de dados pessoais e da segurança da informação nas organizações do SISP.

Capítulo 8

Discussão dos Resultados da Pesquisa

8.1 Introdução

A implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) buscou fortalecer a maturidade organizacional nas temáticas de privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética. Para avaliar a evolução desse processo, foi conduzido um estudo de caso confirmatório, detalhado no Capítulo 7, que permitiu medir os impactos do programa nos órgãos participantes ao longo de três ciclos de implementação, gerando evidências concretas sobre o grau de maturidade alcançado e sobre a efetividade do modelo como instrumento de gestão estratégica da privacidade e segurança da informação.

Neste capítulo, são discutidos os principais achados da pesquisa, com base na análise dos dados coletados por meio do autodiagnóstico institucional, auditorias amostrais e indicadores estratégicos (iBase, iPriv e iSeg). A abordagem adotada permite uma interpretação estruturada dos resultados, combinando análises quantitativas e qualitativas para compreender os desafios, avanços e oportunidades de aprimoramento do PPSI no contexto do governo digital brasileiro. [92].

A estrutura da discussão segue a lógica do CRISP-DM (Cross-Industry Standard Process for Data Mining), uma metodologia amplamente utilizada para modelagem e análise de dados. Essa escolha se justifica pela capacidade do modelo de oferecer um ciclo estruturado e iterativo de entendimento do problema, preparação dos dados e avaliação de resultados. No contexto da administração pública, essa abordagem contribui para que os resultados da pesquisa possam ser replicados por outras organizações interessadas em estruturar programas semelhantes. [94]

O capítulo está organizado da seguinte forma:

- A Seção 8.2 detalha o processo de coleta e tratamento dos dados.
- A Seção 8.3 apresenta a análise quantitativa.
- A Seção 8.4 complementa com uma análise qualitativa.
- A Seção 8.5 reflete sobre a implementação do PPSI.
- A Seção 8.6 discute recomendações futuras.
- A Seção 8.7 apresenta as considerações finais.

Com isso, este capítulo se propõe a apresentar evidências que contribuam não apenas para a validação do modelo proposto, mas também para seu contínuo aperfeiçoamento e expansão no Governo Digital.

8.2 Coleta e Tratamento dos Dados

A análise dos resultados do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) baseia-se em um conjunto estruturado de dados coletados ao longo dos ciclos de implementação do programa. Esses dados foram obtidos por meio de três principais fontes: autodiagnósticos institucionais, auditorias amostrais e indicadores quantitativos de maturidade.

O processo de coleta e tratamento dos dados seguiu as diretrizes do CRISP-DM (Cross-Industry Standard Process for Data Mining), permitindo uma abordagem estruturada e replicável na organização das informações.[94] O modelo foi aplicado nas seguintes fases:

8.2.1 Fontes de Dados

A pesquisa utilizou múltiplas fontes para garantir uma visão abrangente e precisa sobre a implementação do PPSI. Os dados foram coletados a partir de:

a) Autodiagnóstico Institucional: Aplicação de questionários estruturados para que os órgãos do SISP avaliassem seu nível de conformidade com os controles estabelecidos pelo PPSI. O autodiagnóstico foi conduzido em cada ciclo semestral e forneceu dados primários sobre a percepção e adoção dos controles de privacidade e segurança da informação. [95]

(b) Auditorias Amostrais: Para validar as informações fornecidas no autodiagnóstico, foram realizadas auditorias em uma amostra representativa dos órgãos participantes. Esse processo incluiu inspeções documentais, entrevistas com responsáveis pelos

programas institucionais de privacidade e segurança, além da verificação de evidências de implementação.[96]

(c) Indicadores de Maturidade: Três indicadores estratégicos foram utilizados para medir a evolução dos órgãos ao longo dos ciclos: iBase (Indicador de Estruturação Básica): Avalia a implementação das estruturas mínimas de governança. iPriv (Indicador de Maturidade em Privacidade): Mede a conformidade dos órgãos com a Lei Geral de Proteção de Dados (LGPD) e boas práticas de proteção de dados pessoais. e iSeg (Indicador de Segurança da Informação): Analisa a adoção dos controles de segurança cibernética conforme frameworks como CIS Controls, NIST CSF e ISO/IEC 27001 e 27002. [92]

Essas três fontes forneceram uma base sólida para a análise dos resultados, permitindo a triangulação das informações e a identificação de padrões de implementação do PPSI nos órgãos públicos federais.

8.2.2 Processamento e Tratamento dos Dados

Após a coleta, os dados passaram por um processo de normalização, padronização e validação, garantindo que as análises fossem consistentes e comparáveis entre os diferentes ciclos de implementação. O tratamento seguiu três etapas principais:

a) Limpeza e Normalização: Os dados coletados foram revisados para remover inconsistências, duplicidades e valores atípicos. Além disso, os questionários preenchidos incorretamente ou com respostas incompletas foram descartados ou corrigidos com base em auditorias.

(b) Categorização e Consolidação: Para facilitar a análise, os dados foram organizados em categorias de maturidade, permitindo a comparação entre órgãos e a avaliação de tendências ao longo dos ciclos. Essa categorização seguiu os cinco níveis de maturidade definidos no modelo PPSI: Inicial, Básico, Intermediário, Avançado e Otimizado.

(c) Aplicação de Indicadores: Os resultados normalizados foram utilizados para calcular os indicadores iBase, iPriv e iSeg, fornecendo uma visão quantitativa da evolução da maturidade dos órgãos do SISP.

8.2.3 Estruturação dos Dados para Análise

Após o tratamento e organização dos dados, a estruturação seguiu um processo que facilitou a análise e garantiu a clareza nas interpretações. A análise foi dividida em três dimensões principais, que forneceram uma visão clara da evolução dos órgãos do SISP no cumprimento do PPSI:

1. Evolução dos Indicadores de Maturidade: Objetivo: Avaliar como os órgãos avançaram ao longo dos ciclos do PPSI em relação à privacidade e segurança da informação. Método: A comparação de iBase, iPriv, e iSeg nos três ciclos (inicial, intermediário e avançado) permitiu identificar progressos, melhorias contínuas e áreas que requerem mais atenção.

2. Correlação entre Implementação dos Controles e Níveis de Maturidade: Objetivo: Entender como os diferentes controles impactaram a evolução dos níveis de maturidade nos órgãos. Método: Foi analisado como a implementação de controles de governança, privacidade e segurança afetam os indicadores iBase, iPriv, e iSeg. A análise cruzada desses dados permitiu entender quais controles tiveram maior impacto na melhoria da maturidade.

3. Identificação de Desafios e Barreiras: Objetivo: Detectar obstáculos enfrentados pelos órgãos durante a implementação do PPSI. Método: A análise qualitativa dos dados do autodiagnóstico e das auditorias amostrais, em conjunto com os indicadores quantitativos, destacou dificuldades recorrentes, como falta de recursos, resistência cultural ou desafios técnicos.

Com essas três dimensões de análise, foi possível identificar padrões de avanço, entender os fatores críticos que contribuíram para o sucesso ou dificuldades na implementação, e fornecer uma base sólida para a análise quantitativa e qualitativa dos resultados.

8.3 Análise Quantitativa

Após a coleta e o tratamento dos dados, a análise quantitativa tem como objetivo mensurar o progresso da maturidade organizacional em relação à privacidade e segurança da informação nos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Para tanto, utilizamos três indicadores estratégicos: iBase, iPriv e iSeg, que permitem medir a evolução da governança, conformidade com a Lei Geral de Proteção de Dados (LGPD) e a adoção dos controles de segurança cibernética.

8.3.1 Visão Geral dos Dados Consolidados

Antes de iniciarmos a análise quantitativa detalhada, é fundamental apresentar uma visão geral dos dados consolidados que servirão de base para as avaliações dos indicadores de maturidade no Programa de Privacidade e Segurança da Informação (PPSI). Esses dados foram organizados na Planilha Master, que contém informações coletadas durante os três ciclos do programa (Ciclo 1, Ciclo 2 e Ciclo 3).

A referida planilha reúne dados de diversos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e está estruturada para permitir uma análise

comparativa ao longo dos ciclos de implementação do PPSI. A seguir, são apresentadas algumas informações essenciais sobre a organização dos dados.

A. Estrutura da Planilha Master

A planilha contém as seguintes variáveis-chave:

1. Órgãos e Categorias: Cada linha da planilha corresponde a um órgão do SISP, com a categoria (ex: Agência, Especiais) e o nome do órgão (ex: ABIN, AEB, AGU). Além disso, é especificada a região geográfica de cada órgão (ex: Centro-Oeste, Sudeste), permitindo uma análise por região.

2. Indicadores de Maturidade: São apresentados três indicadores principais para cada órgão: iBase, iSeg e iPriv.

3. Ciclos de Implementação: Cada ciclo do PPSI é representado por um conjunto de dados: Ciclo 1 (Implementação Inicial), Ciclo 2 (Expansão das Medidas Críticas) e Ciclo 3 (Controles Dependentes de Contratação).

4. Semestre e Ano: Para cada ciclo, os dados estão segmentados por ano e semestre, com o intuito de capturar as mudanças ao longo do tempo e possibilitar uma análise mais detalhada.

B. Estatísticas Gerais

Com base na planilha consolidada, algumas estatísticas gerais podem ser extraídas para oferecer uma visão preliminar do conjunto de dados:

1) Número de Órgãos Participantes: A planilha apresenta um total de 254 órgãos do SISP, com o total de 249 (98,03 Porcento) participantes efetivos em pelo menos 1 dos 3 ciclos objeto da pesquisa, conforme apresentado na figura 8.1.

2) Distribuição por Ciclos: A planilha apresenta dados de um período de 18 meses (3 ciclos completos), conforme apresentado na figura 8.2.

- Ciclo 1 (Implementação Inicial): 229 órgãos (90,16 Porcento)
- Ciclo 2 (Expansão das Medidas Críticas): 198 órgãos (77,95 Porcento)
- Ciclo 3 (Controles Dependentes de Contratação): 237 órgãos (93,31 Porcento)

3. Dados Gerais de Média, Desvio Padrão, Valores Máximo e Mínimo por Ciclos, conforme tabela 8.1:

Essas estatísticas fornecem uma visão inicial da evolução dos indicadores de maturidade e permitem identificar tendências gerais antes de entrar nas análises mais detalhadas.

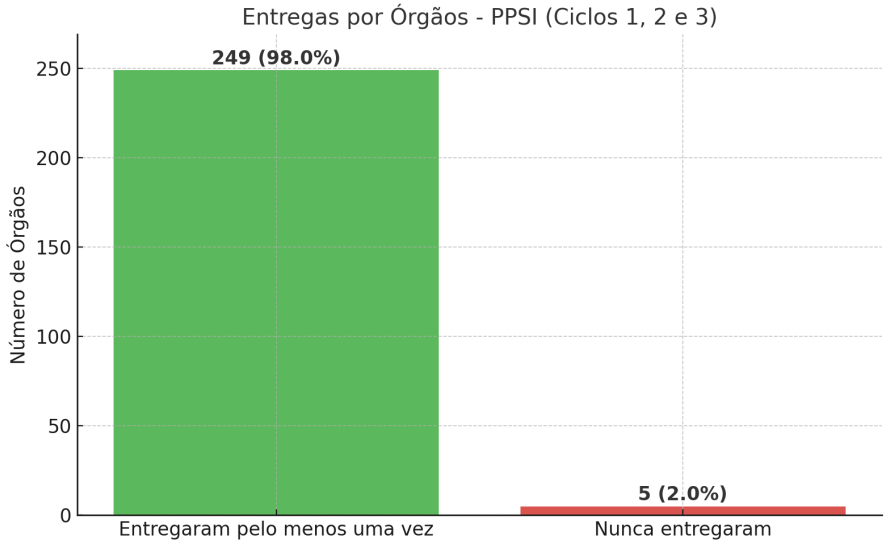

Figura 8.1: Percentual Participação no PPSI
Fonte: Autor

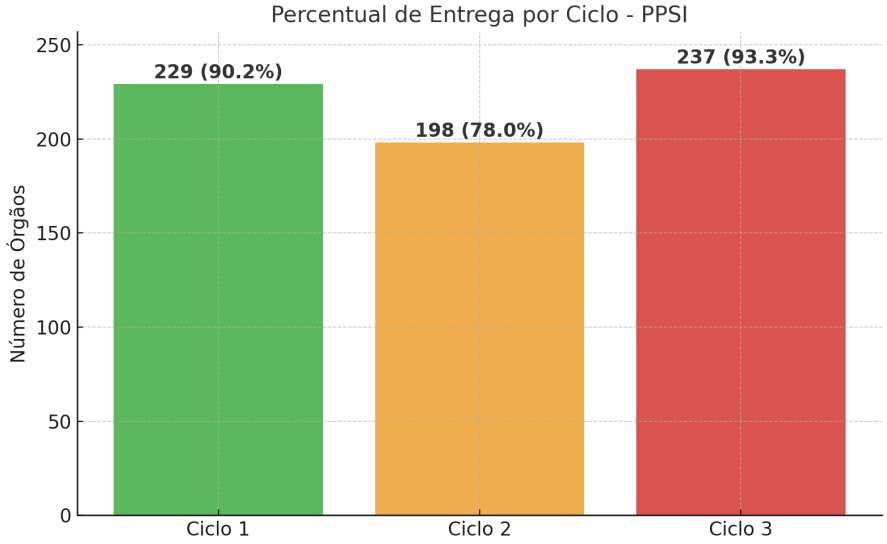

Figura 8.2: Percentual Participação no PPSI
Fonte: Autor

8.3.2 Cálculo dos Indicadores

O processo de cálculo dos indicadores foi realizado por meio de uma metodologia quantitativa que combina a autoavaliação institucional e auditorias amostrais, com base nas metodologias de governança, privacidade e segurança adotadas. A seguir, detalhamos como cada indicador foi calculado:

1. iBase (Indicador de Estruturação Básica de Governança em Privacidade e Segurança da Informação): Objetivo: Avaliar a existência de políticas e estruturas mínimas

Tabela 8.1: Estatísticas Descritivas dos Indicadores do PPSI por Ciclo

Indicador	**Ciclo 1 (2023/1**	**Ciclo 2 (2024/1)**	**Ciclo 3 (2024/2)**
iBase (Governança)	Média: 0,57	Média: 0,55	Média: 0,67
iBase (Governança)	Mín: 0,00	Mín: 0,00	Mín: 0,00
iBase (Governança)	Máx: 1,00	Máx: 1,00	Máx: 1,00
iBase (Governança)	DP: 0,31	DP: 0,37	DP: 0,30
iPriv (Privacidade)	Média: 0,31	Média: 0,30	Média: 0,36
iPriv (Privacidade)	Mín: 0,00	Mín: 0,00	Mín: 0,00
iPriv (Privacidade)	Máx: 0,88	Máx: 0,87	Máx: 0,90
iPriv (Privacidade)	DP: 0,22	DP: 0,24	DP: 0,22
iSeg (Segurança)	Média: 0,34	Média: 0,33	Média: 0,41
iSeg (Segurança)	Mín: 0,00	Mín: 0,00	Mín: 0,00
iSeg (Segurança)	Máx: 0,89	Máx: 0,89	Máx: 0,89
iSeg (Segurança)	DP: 0,22	DP: 0,24	DP: 0,21

de governança em privacidade e segurança da informação. Método de Cálculo: Foi calculado com base na implementação de controles fundamentais, como a designação de responsáveis por privacidade e segurança da informação, criação de comitês internos e a formalização de políticas de privacidade e segurança. dentre outros. O indicador recebeu uma pontuação de 0 a 1, sendo 0 para ausência de estruturação e 1 para uma governança completamente formalizada e em operação.

2. iPriv (Indicador de Maturidade em Privacidade): Objetivo: Medir a conformidade dos órgãos do SISP com as práticas de proteção de dados pessoais, em especial com a LGPD. Método de Cálculo: Calculado a partir da adesão a práticas e controles relacionados à proteção de dados pessoais, incluindo a implementação de políticas de consentimento, o tratamento de dados pessoais sensíveis, a capacidade de resposta a incidentes de privacidade, dentre outros. A pontuação também variou de 0 a 1, onde 0 indica não conformidade e 1 corresponde à conformidade total com os requisitos da LGPD.

3. iSeg (Indicador de Segurança da Informação): Objetivo: Avaliar a adoção e a eficácia dos controles de segurança da informação, baseando-se em frameworks como ISO/IEC 27001 e 27002, CIS Controls e NIST CSF. Método de Cálculo: Esse indicador foi calculado com base na implementação dos controles de segurança cibernética, como a gestão de riscos de segurança, a proteção contra malware, a segurança em redes e sistemas, e a implementação de respostas a incidentes, dentre outros. A pontuação também variou de 0 a 1, onde 0 indica não conformidade e 1 corresponde à conformidade total com os requisitos da segurança.

8.3.3 Comparação de Ciclos

Com os valores dos indicadores calculados, foi possível comparar a evolução ao longo dos três ciclos do PPSI:

Ciclo 1 (Implementação Inicial): Fase em que os órgãos começaram a adotar controles básicos de governança e segurança. Esperava-se uma pontuação mais baixa, com foco em iniciar a formalização dos controles e processos.

Ciclo 2 (Expansão das Medidas Críticas): Durante este ciclo, a implementação dos controles foi ampliada, e os órgãos buscaram melhorar a efetividade dos processos de segurança e privacidade.

Ciclo 3 (Controles Dependentes de Contratação): Nesse ciclo, os órgãos implementaram controles mais avançados, com base em tecnologias externas, ferramentas de segurança, e auditorias mais robustas.

8.3.4 Gráficos e Visualizações

A seguir, são apresentados gráficos que ilustram a evolução dos indicadores do PPSI ao longo dos três ciclos:

Gráfico 1: Evolução Média do Indicador iBase por Ciclos

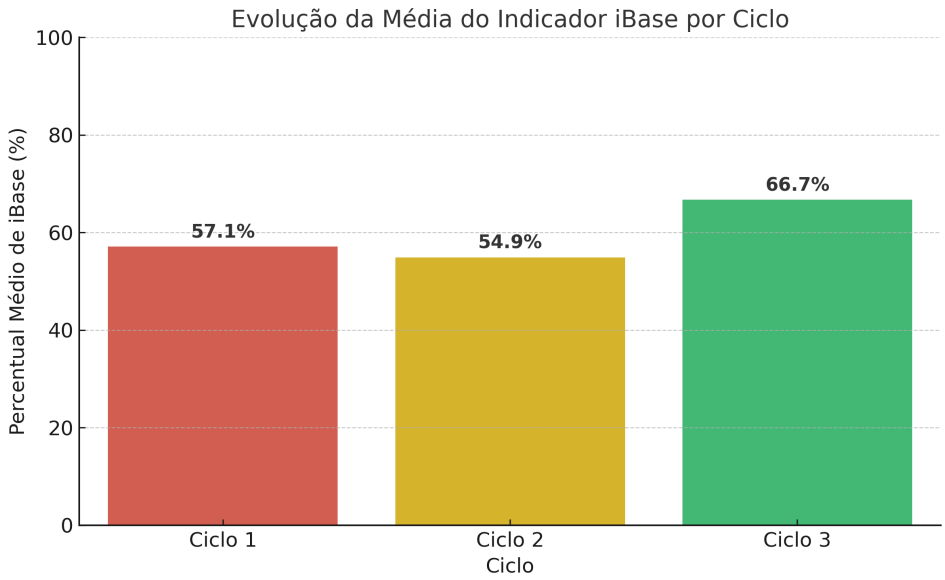

Figura 8.3: Evolução Média do Indicador iBase por Ciclos
Fonte: Autor

A Figura 8.3 mostra que o indicador iBase apresentou evolução positiva ao longo dos três ciclos de implementação, refletindo a consolidação da estrutura mínima de go-

vernança. Depois de uma leve queda entre o Ciclo 1 (57,1) e o Ciclo 2 (54,9), houve uma recuperação consistente no Ciclo 3, que alcançou 66,7. Esse avanço indica que os órgãos estão fortalecendo suas estruturas de governança em privacidade e segurança da informação, com mais clareza sobre papéis, responsabilidades e processos.

Gráfico 2: Evolução Média do Indicador iPriv por Ciclos

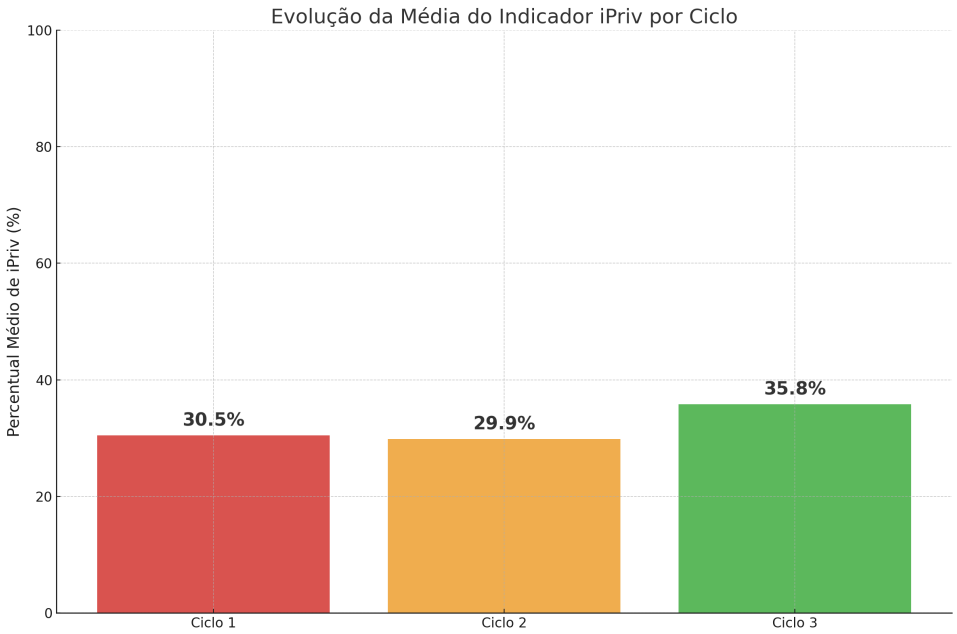

Figura 8.4: Evolução Média do Indicador iPriv por Ciclos
Fonte: Autor

Conforme mostra a Figura 8.4, o indicador iPriv, que avalia a maturidade em privacidade e proteção de dados, apresentou uma leve queda do Ciclo 1 (30,5) para o Ciclo 2 (29,9). Já no Ciclo 3, houve uma recuperação relevante, com a média subindo para 35,8. Essa evolução sugere que, após um período de estabilidade, os órgãos começaram a avançar de forma mais consistente na implementação de práticas relacionadas à privacidade.

Gráfico 3: Evolução Média do Indicador iSeg por Ciclos

Já Figura 8.5, que apresenta o indicador iSeg, que mede a maturidade em segurança da informação, evidencia uma queda entre o Ciclo 1 (34,1) e o Ciclo 2 (33,3). Já no Ciclo 3, houve um avanço expressivo, com a média subindo para 41,2. Esse salto indica que, após um período de estagnação, os órgãos voltaram a investir com mais força em medidas de segurança da informação.

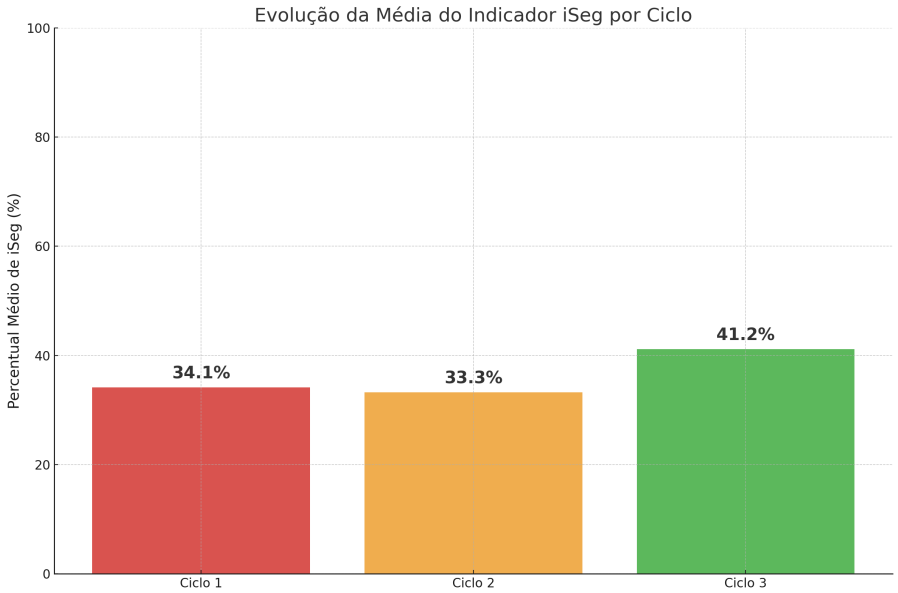

Figura 8.5: Evolução Média do Indicador iSeg por Ciclos
Fonte: Autor

Gráfico 4: Evolução Média dos Níveis de Maturidade por Ciclos

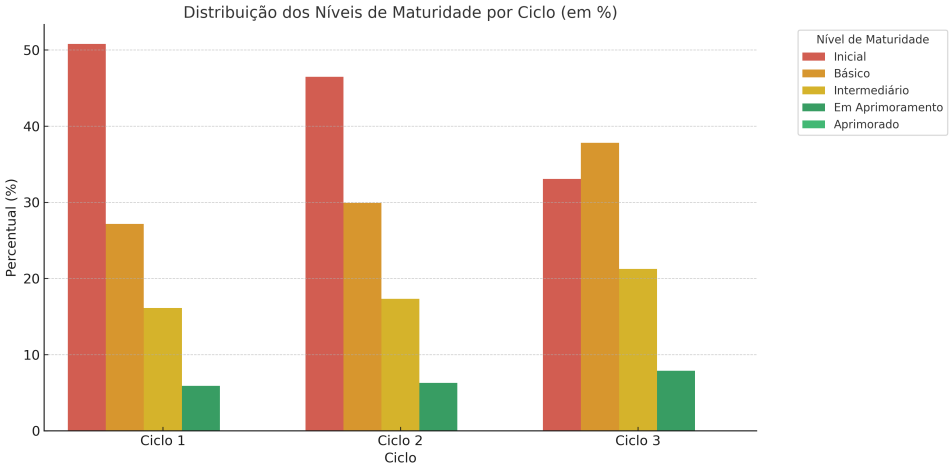

Figura 8.6: Evolução Média dos Níveis de Maturidade
Fonte: Autor

A distribuição dos níveis de maturidade ao longo dos ciclos mostra uma tendência clara de avanço. O percentual de órgãos no nível Inicial caiu de 51 no Ciclo 1 para 33 no Ciclo 3, indicando uma redução significativa da baixa maturidade. Ao mesmo tempo, houve crescimento nos níveis Básico e Intermediário, especialmente no Ciclo 3, refletindo o esforço das instituições em estruturar suas práticas. O nível Em Aprimoramento tam-

bém avançou discretamente, sugerindo que uma parcela dos órgãos começa a atingir um patamar mais robusto de governança em privacidade e segurança da informação.

Gráfico 5: Média dos Indicadores por Categorias

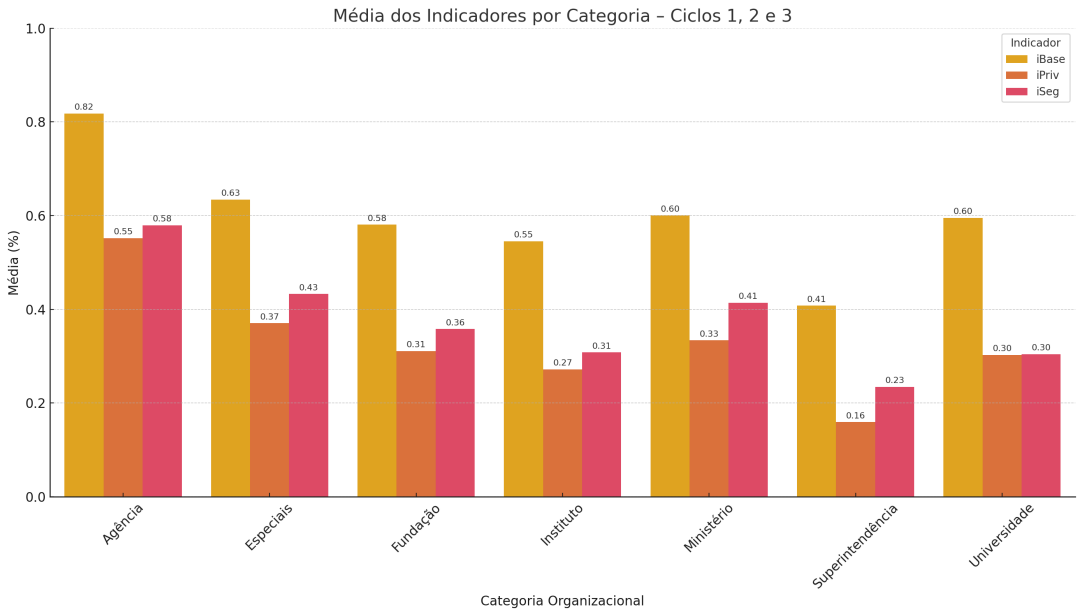

Figura 8.7: Média dos Indicadores por Categorias
Fonte: Autor

Agências lideram com folga em todos os indicadores. Apresentam média de 84,1 em governança (iBase), 60,3 em segurança (iSeg) e 57,3 em privacidade (iPriv). Esses resultados refletem estruturas mais robustas, melhor alinhamento estratégico e capacidade institucional para implementar as diretrizes do PPSI com consistência e continuidade.

A categoria Especiais, formada por órgãos com perfis variados, ocupa a segunda posição, com 72,7 em governança, 50,4 em segurança e 41,8 em privacidade. Apesar da heterogeneidade, o grupo demonstra avanços sólidos, especialmente nos aspectos organizacionais e técnicos, ainda que com diferenças relevantes entre os órgãos.

Os Ministérios mostram evolução importante, alcançando 69,4 em governança, 48,8 em segurança e 38,9 em privacidade. Embora ainda haja espaço para crescimento, especialmente na proteção de dados pessoais, os resultados indicam maturidade crescente e maior institucionalização das práticas de segurança e privacidade.

Com 65,6 em governança, 41,6 em segurança e 35,9 em privacidade, as Fundações apresentam desempenho intermediário. A estruturação em governança é razoável, mas ainda há desafios técnicos e operacionais para alcançar níveis mais altos de maturidade nos demais indicadores.

As Universidades registram 64,3 em governança, 34,0 em segurança e 32,9 em privacidade. Apesar das limitações estruturais e operacionais, observa-se um esforço contínuo dessas instituições para incorporar os princípios do PPSI, principalmente por meio da melhoria em governança.

Por fim, os Institutos apresentam os menores níveis de maturidade entre as categorias analisadas: 61,7 em governança, 34,5 em segurança e 30,2 em privacidade. Os resultados indicam uma adoção inicial das práticas do programa, com necessidade de reforço institucional e apoio mais direcionado para avançar.

8.3.5 Correlação entre Controles e Níveis de Maturidade

A correlação entre os controles implementados pelos órgãos do SISP e os níveis de maturidade observados ao longo dos ciclos revela insights valiosos sobre a efetividade do PPSI. A partir da análise evolutiva dos controles nos três ciclos de implementação, foi possível identificar padrões de progresso, estagnação e variações no ritmo de adoção entre os diferentes tipos de controles. Com base nos dados consolidados, foram elaborados três gráficos distintos que evidenciam a evolução percentual dos controles entre os ciclos 1 e 2, entre os ciclos 2 e 3, e de forma acumulada entre os ciclos 1 e 3.

As Figuras 8.8 a 8.11 permitem uma leitura comparativa da trajetória de maturidade dos controles, destacando avanços consistentes e pontos que exigem atenção adicional. As análises gráficas que se seguem aprofundam essas interpretações, buscando compreender os fatores que explicam as diferentes curvas de crescimento e sua relação com a natureza dos controles (governança, tecnologia, metodologia, pessoas ou maturidade).

Gráfico 1: Evolução entre os Ciclos 1 e 2

Como mostra a Figura 8.8, a evolução dos controles entre o Ciclo 1 e o Ciclo 2 revela um momento crucial de estruturação inicial do PPSI, no qual os órgãos concentraram esforços nos controles considerados mais acessíveis e de rápida implementação. Os maiores avanços percentuais nesse intervalo ocorreram, em sua maioria, em controles relacionados à conscientização e treinamento de usuários, gestão de ativos, controle de acesso e inventário de dispositivos. Esses resultados indicam que as primeiras ações priorizaram a base organizacional e a cultura de segurança, componentes fundamentais para viabilizar estágios posteriores mais técnicos e especializados.

A evolução significativa desses controles pode ser atribuída à sua menor dependência de recursos externos, como contratações ou aquisições tecnológicas, e maior capacidade de execução direta pelas equipes internas. Por outro lado, controles com menor avanço nesse intervalo inicial apontam para barreiras institucionais ou estruturais, como a ausência de

Figura 8.8: Evolução dos Controles C1-C2
Fonte: Autor

processos formalizados ou dificuldades de integração com outras áreas do órgão. Assim, o primeiro salto de maturidade foi fortemente impulsionado por ações de governança, educação e metodologias organizacionais.

Gráfico 2: Evolução entre os Ciclos 2 e 3

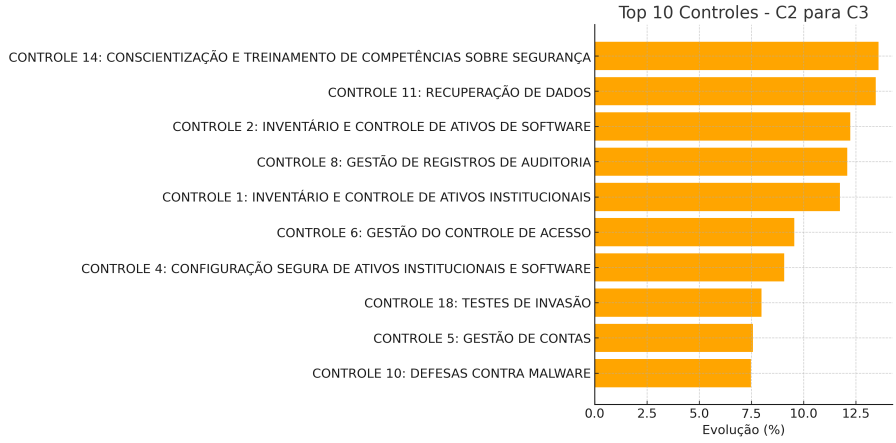

Figura 8.9: Evolução dos Controles C2-C3
Fonte: Autor

A Figura 8.9 mostra que a evolução entre os Ciclos 2 e 3 marca um estágio mais avançado do processo de maturidade, no qual os órgãos do SISP passaram a consolidar práticas anteriormente iniciadas e a investir em controles mais técnicos e complexos. Diferentemente do ciclo anterior, onde predominavam ações estruturantes e de fácil internalização, este ciclo evidencia o amadurecimento organizacional, refletido no avanço de controles

como testes de invasão, segurança de endpoints, proteção contra malware e gestão de vulnerabilidades.

A presença desses controles no topo da evolução percentual sugere maior capacidade técnica dos órgãos, bem como possíveis avanços em processos de contratação e aquisição de soluções especializadas. Nota-se também uma continuidade nos esforços de capacitação, com o controle de conscientização e treinamento de usuários mantendo crescimento expressivo. Essa combinação de esforços técnicos e de cultura organizacional aponta para uma transição relevante entre um estágio inicial de estruturação e um estágio intermediário mais robusto, com ganhos consistentes em resiliência cibernética.

Gráfico 3: Evolução entre os Ciclos 1 e 3

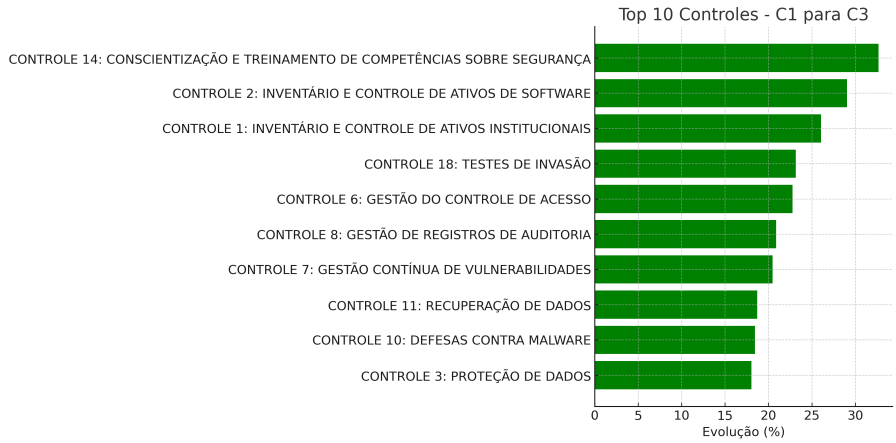

Figura 8.10: Evolução dos Controles C1-C3
Fonte: Autor

A Figura 8.10 fornece uma visão longitudinal da evolução dos controles entre os Ciclos 1 e 3 das instituições ao longo do tempo, evidenciando os controles que mais contribuíram para o aumento da maturidade em privacidade e segurança da informação no âmbito do PPSI. O destaque absoluto recai sobre o Controle 14 – Conscientização e Treinamento de Usuários, que lidera o ranking de crescimento percentual com um avanço superior a 30. Esse resultado confirma a eficácia das estratégias de sensibilização e capacitação promovidas em escala federal, reforçando a importância do fator humano como base para o fortalecimento da cultura de segurança.

Em seguida, aparecem controles ligados à gestão de ativos, controle de acessos, testes de invasão e inventário de dispositivos, sinalizando que tanto os fundamentos organizacionais quanto aspectos técnicos avançaram de forma consistente ao longo dos ciclos. Essa trajetória cumulativa evidencia que o modelo do PPSI, baseado em ciclos semestrais pro-

gressivos, tem sido eficaz para promover um amadurecimento sustentável dos controles, respeitando o tempo institucional necessário para mudanças estruturais e tecnológicas.

Gráfico 4: Controles de Menor Evolução

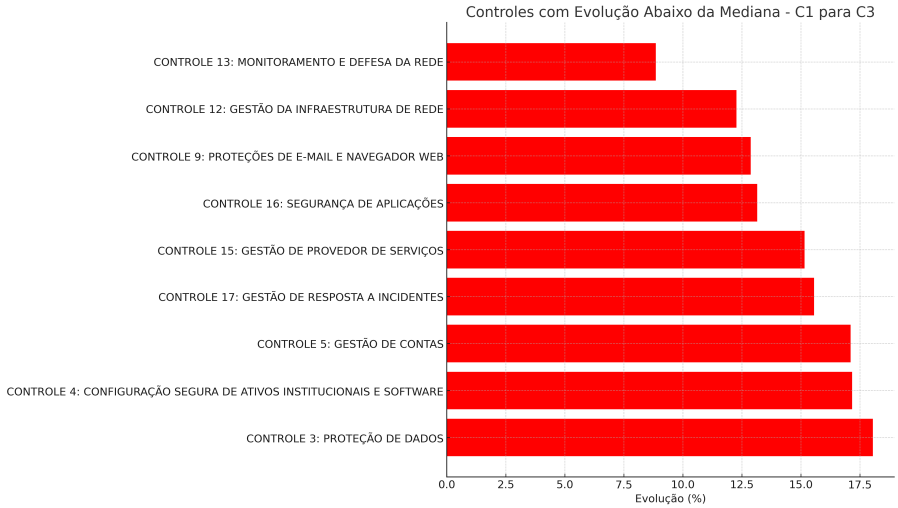

Figura 8.11: Controles Abaixo da Mediana - C1-C3
Fonte: Autor

A Figura 8.11 apresenta os controles com evolução percentual abaixo da mediana, destacando desafios persistentes na adoção de certas medidas — proteção de dados, configuração segura de ativos institucionais e software, gestão de contas, gestão de resposta a incidentes, gestão de provedor de serviços, segurança de aplicações, proteções de e-mail e navegador web, gestão da infraestrutura de rede e monitoramento e defesa da rede — reforça a existência de desafios estruturais, operacionais e técnicos enfrentados por diversos órgãos públicos.

Esses controles, em sua maioria, envolvem processos mais complexos, que exigem automação, integração entre equipes de TI e segurança, aquisições tecnológicas e respostas coordenadas a eventos de segurança. A baixa evolução dessas práticas sinaliza a necessidade de intervenções estratégicas por parte da gestão central do PPSI, como apoio à contratação compartilhada, fornecimento de soluções referência, reforço na capacitação especializada e ações orientadas por riscos. Ao mesmo tempo, a visualização desses dados em formato gráfico permite destacar com clareza os pontos de maior fragilidade institucional, fornecendo subsídios para priorizações mais assertivas nos ciclos subsequentes do programa.

8.4 Análise Qualitativa

Além dos resultados quantitativos apresentados na seção anterior, a análise qualitativa dos dados coletados permitiu uma compreensão mais profunda dos fatores que influenciaram a implementação e a evolução do PPSI nos órgãos do SISP. Enquanto os indicadores forneceram uma visão estruturada da maturidade em privacidade e segurança da informação, os relatos, observações diretas, feedbacks institucionais e padrões comportamentais identificados ao longo dos ciclos revelaram aspectos cruciais não capturados apenas por números. Essa dimensão qualitativa foi essencial para identificar barreiras, destacar boas práticas e compreender as percepções institucionais sobre o modelo proposto.

8.4.1 Desafios Enfrentados na Implementação

1. Falta de equipe dedicada: Muitos órgãos relataram escassez de profissionais alocados exclusivamente para privacidade e segurança, o que compromete a continuidade das ações. 2. Baixa prioridade institucional: A ausência de apoio direto da alta gestão foi um entrave recorrente à adoção plena do PPSI. 3. Dependência de contratação de soluções: A implementação de controles mais avançados esbarrou em limitações orçamentárias e na morosidade dos processos de contratação. 4. Desconhecimento sobre frameworks: Parte significativa das equipes técnicas demonstrou dificuldade em compreender e aplicar referências como NIST, CIS Controls e ISO/IEC. 5. Fragmentação das responsabilidades: Em alguns órgãos, as ações de privacidade e segurança estavam dispersas entre áreas diferentes, sem integração ou governança definida.

8.4.2 Padrões Observados entre os Órgãos

1. Evolução rápida em estruturas já organizadas: Órgãos com comitês, políticas e responsáveis nomeados evoluíram mais rapidamente. 2. Baixa maturidade em privacidade (iPriv): Mesmo órgãos com razoável estrutura em segurança da informação apresentaram deficiências em privacidade. 3. Consolidação dos controles básicos (iBase): A maioria dos órgãos demonstrou maior facilidade na implementação de controles de estruturação básica. 4. Dificuldade com controles dependentes de contratação (Ciclo 3): Soluções de DLP, SIEM ou anonimização, por exemplo, foram pouco implementadas. 5. Participação ativa em ciclos correlacionada à maturidade: Órgãos que participaram dos ciclos iniciais apresentaram níveis superiores nos indicadores.

8.4.3 Boas Práticas Identificadas

1. Criação de Comitês de Privacidade e Segurança: Órgãos que institucionalizaram a governança conseguiram maior adesão interna ao programa. 2. Adoção de trilhas de capacitação estruturadas: Alguns órgãos desenvolveram ou adaptaram trilhas de aprendizado específicas sobre o PPSI. 3. Integração com auditorias internas: A validação dos controles foi inserida nos planos de auditoria em algumas instituições, reforçando o caráter de governança. 4. Uso de indicadores para reporte à alta gestão: Métricas como iBase, iPriv e iSeg foram utilizadas para sensibilizar diretores e conselhos superiores. 5. Compartilhamento de soluções entre órgãos: Iniciativas como guias, modelos de documentos e cronogramas foram compartilhadas entre instituições via CEPS.GOV.BR.

8.4.4 Percepções sobre o PPSI

1. Programa reconhecido como referência confiável: A proposta do PPSI foi amplamente percebida como uma base sólida e alinhada às normativas nacionais e internacionais, o que facilitou sua aceitação institucional. 2. Valorização dos indicadores estratégicos: Os indicadores iBase, iPriv e iSeg foram considerados ferramentas objetivas e úteis para acompanhar a evolução e justificar decisões de investimento e priorização. 3. Demanda por adaptações setoriais: Algumas instituições sinalizaram a necessidade de versões específicas do programa para contextos como universidades, agências reguladoras ou empresas estatais. 4. Importância do suporte técnico da coordenação nacional: O apoio oferecido pela Secretaria de Governo Digital (SGD/MGI), por meio de oficinas, reuniões e canais de esclarecimento, foi destacado como fator decisivo para o engajamento e continuidade das ações. 5. Percepção de transformação institucional: Diversos órgãos relataram que a adoção do programa contribuiu para mudanças estruturais e culturais, fortalecendo a governança em privacidade e segurança da informação.

8.5 Reflexões sobre a Implementação do PPSI

A implementação do Programa de Privacidade e Segurança da Informação (PPSI) ao longo dos ciclos monitorados revelou aprendizados relevantes, tanto do ponto de vista técnico quanto organizacional. A seguir, são apresentadas reflexões estruturadas a partir da comparação entre os resultados esperados e os obtidos, considerando os diferentes níveis de maturidade institucional, o engajamento das equipes e a efetividade das estratégias adotadas.

8.5.1 Convergência entre teoria e prática

1. O programa mostrou-se aplicável em diferentes realidades institucionais, validando os fundamentos teóricos adotados na sua concepção (NIST, ISO, LGPD etc.). 2. A estrutura baseada em ciclos semestrais foi eficaz para promover avanços graduais, respeitando as limitações de tempo e recursos dos órgãos. 3. O uso de indicadores objetivos permitiu alinhar expectativas entre equipes técnicas e decisores estratégicos. 4. As linhas de defesa e os eixos estruturantes funcionaram como guias claros para orientar ações prioritárias. 5. A proposta de autoavaliação institucional, combinada com validação externa, aumentou a credibilidade dos resultados.

8.5.2 Benefícios da Aplicação do Modelo

1. Mensuração objetiva da evolução da maturidade organizacional ao longo dos ciclos de implementação. 2. Identificação de padrões e desafios transversais, permitindo um ajuste mais preciso das políticas e diretrizes do PPSI. 3. Criação de uma cultura de governança baseada em dados, proporcionando maior embasamento para tomada de decisões estratégicas. 4. Engajamento das equipes institucionais, promovendo conscientização e capacitação contínua dos profissionais envolvidos. 5. Integração efetiva entre as dimensões de privacidade e segurança da informação, evidenciando os ganhos obtidos com uma abordagem unificada, complementar e sinérgica.

8.5.3 Aprendizados organizacionais

1. A ausência de uma governança mínima impacta fortemente a capacidade de implementação de controles, mesmo os mais básicos. 2. Órgãos com liderança engajada avançaram mais rapidamente, demonstrando a importância do patrocínio institucional. 3. A criação de espaços de troca (como CEPS.GOV.BR) fortaleceu a colaboração interinstitucional. 4. A aplicação prática evidenciou a necessidade de uma linguagem mais acessível em algumas etapas do programa. 5. O envolvimento das unidades de controle interno e controle externo aumentou a legitimidade da proposta dentro das instituições.

8.5.4 Desafios identificados

1. Houve dificuldade em integrar plenamente os controles de privacidade nos ciclos iniciais, especialmente em órgãos sem DPOs designados. 2. Alguns órgãos interpretaram os ciclos como um checklist, sem internalização real da cultura de segurança e privacidade. 3. A dependência de contratações externas gerou atrasos em ciclos intermediários (especialmente Ciclo 3). 4. Em alguns casos, os indicadores foram preenchidos de forma otimista,

exigindo maior esforço de validação técnica. 5. A integração com outros programas de governo (como normas GSI, ANPD, auditorias do TCU, auditorias da CGU e metas da Estratégia de Governo Digital) ainda carece de maior articulação.

8.5.5 Potencial estratégico do programa

1. O PPSI se consolidou como uma ferramenta indutora de maturidade em governança de privacidade e segurança da informação. 2. Tem potencial para orientar políticas públicas, planejamentos estratégicos institucionais e decisões de investimento em TIC. 3. Pode ser adaptado como referência para estados e municípios, bem como para os poderes legislativo e judiciário. 4. Atua como instrumento de prestação de contas e transparência em temas sensíveis ao cidadão. 5. Contribui diretamente para o fortalecimento da confiança no Governo Digital brasileiro.

8.6 Caminhos Futuros e Recomendações

A experiência com a implementação do Programa de Privacidade e Segurança da Informação (PPSI) nos órgãos do SISP revelou não apenas os avanços conquistados, mas também oportunidades relevantes de aprimoramento e expansão. A seguir, são apresentadas recomendações práticas e estratégicas para fortalecer o programa e ampliar seus impactos no ecossistema do Governo Digital brasileiro.

8.6.1 Fortalecimento da Sustentação Institucional (Governança)

1. Incluir o PPSI no planejamento estratégico institucional dos órgãos como ação contínua e transversal. 2. Estabelecer normativos complementares que tornem obrigatória a estrutura mínima de governança em privacidade e segurança da informação. 3. Integrar os ciclos do PPSI às auditorias internas e externas, criando um ciclo virtuoso de melhoria contínua. 4. Consolidar o apoio político e técnico do MGI, assegurando continuidade mesmo com mudanças administrativas. 5. Incentivar a formalização de comitês de privacidade e segurança, com participação de áreas de negócio diversas.

8.6.2 Consolidação do Framework PPSI (Metodologia)

1. Consolidar a metodologia de implementação e avaliação do PPSI como um processo contínuo e iterativo, baseado em ciclos semestrais, articulado com o modelo de maturidade proposto e com foco em melhoria progressiva. 2.Atualizar periodicamente o framework de privacidade e segurança da informação utilizado como referência no PPSI, com base nos

aprendizados dos ciclos e nas normas internacionais (ISO/IEC 27001, 27701, NIST CSF, Privacy Framework, CIS Controls). 3. Desenvolver guias operacionais simplificados para facilitar a internalização do modelo por órgãos com menor maturidade. 4. Integrar os eixos do framework (governança, segurança cibernética e privacidade) às rotinas institucionais de planejamento, risco e auditoria. 5. Promover ações de benchmark com outros países e organismos internacionais para aprimorar a metodologia e o framework de referência.

8.6.3 Melhoria Contínua do Modelo de Avaliação (Maturidade)

1. Aprimorar os critérios de avaliação dos indicadores (iBase, iPriv, iSeg) com base nas evidências coletadas nos ciclos anteriores. 2. Incluir novos indicadores relacionados à gestão de riscos de privacidade e segurança da informação. 3. Estabelecer métricas de qualidade da informação declarada nos instrumentos de autoavaliação. 4. Desenvolver mecanismos de feedback automatizado, com relatórios personalizados por órgão. 5. Promover rodadas periódicas de validação cruzada entre os órgãos, estimulando o engajamento colaborativo.

8.6.4 Fortalecimento do CISC.GOV.BR (Tecnologia)

1. Ampliar a atuação do CISC.GOV.BR como centro coordenador, promovendo articulação nacional com os órgãos do SISP em eventos críticos. 2. Desenvolver planos de resposta a incidentes customizados para o setor público, com roteiros práticos e integração com o PPSI. 3. Instituir exercícios regulares de simulação de incidentes cibernéticos, integrando os órgãos federais em ações coordenadas. 4. Automatizar o fluxo de comunicação de incidentes, criando interfaces seguras entre os órgãos e o CISC para alertas, notificações e atualizações em tempo real. . Integrar a resposta a incidentes ao processo de avaliação de maturidade, reconhecendo a existência de planos testados e equipes treinadas como critérios de avanço nos ciclos do PPSI.

8.6.5 Expansão das Ações do CEPS.GOV.BR (Pessoas)

1. Ofertar trilhas formativas específicas para cada ciclo, alinhadas ao nível de maturidade dos órgãos. 2. Ampliar a capacitação de lideranças e gestores públicos, para que compreendam e patrocinem o PPSI. 3. Fomentar a produção de conteúdos de apoio (vídeos, FAQs, modelos de documentos) para facilitar a implementação. 4. Investir no desenvolvimento de ferramentas digitais integradas ao CEPS, para automação da coleta e análise de indicadores. 5. Criar grupos técnicos temáticos regionais, com apoio mútuo e compartilhamento de boas práticas.

8.6.6 Integração de Tecnologias Emergentes ao PPSI (Nova Torre)

1. Mapear e acompanhar tendências tecnológicas com impacto direto em privacidade e segurança, incluindo inteligência artificial, big data, computação em nuvem, computação quântica, Internet das Coisas (IoT), biometria e blockchain. 2. Atualizar os controles do PPSI para contemplar requisitos de privacidade, segurança e ética no uso dessas tecnologias, com ênfase em riscos de processamento em ambientes distribuídos e hiperconectados. 3. Incluir critérios de avaliação de maturidade tecnológica nos indicadores (iBase, iPriv, iSeg), com foco em automação, monitoramento contínuo e resposta inteligente. 4. Estimular a adoção de ferramentas de análise comportamental (UEBA), gestão de identidades baseada em risco, e resposta automatizada a incidentes de segurança e privacidade. 5. Avaliar o impacto regulatório e técnico da adoção dessas tecnologias, com foco em mitigação de riscos emergentes, resiliência organizacional e conformidade com a LGPD e normas internacionais.

8.6.7 Ampliação do Escopo de Aplicação do PPSI (Nova Torre)

1. Expandir o PPSI para estados e municípios, com adaptações simplificadas e apoio técnico da União. 2. Incluir empresas estatais (SERPRO e DATAPREV), ampliando o alcance da governança digital. 3. Oferecer versão compacta para órgãos de pequeno porte, respeitando suas capacidades técnicas. 4. Alinhar o PPSI com programas internacionais de privacidade e segurança da informação, ampliando a reputação institucional. 5. Articular parcerias com instituições privadas, acadêmicas e organismos multilaterais, para apoio técnico e difusão do modelo.

8.7 Considerações Finais

A análise dos dados coletados ao longo dos ciclos do PPSI demonstrou avanços significativos na estruturação e consolidação de práticas em privacidade e segurança da informação entre os órgãos do SISP. A aplicação do modelo de maturidade permitiu não apenas mensurar o progresso obtido, mas também identificar desafios persistentes e oportunidades estratégicas de aprimoramento.

As evidências coletadas reforçam a relevância da abordagem metodológica adotada, bem como a aplicabilidade prática do framework proposto, especialmente no contexto da transformação digital do Governo Federal. Diante da complexidade e da dinamicidade dos riscos emergentes, torna-se imprescindível um olhar mais amplo e propositivo sobre os próximos passos.

A consolidação dos dados confirma que o objetivo geral da pesquisa foi plenamente alcançado, ao propor e aplicar um modelo de avaliação de maturidade em privacidade e segurança da informação no contexto do Governo Digital Brasileiro, com foco na elevação da maturidade e da resiliência de 254 órgãos públicos federais vinculados ao SISP.

Os objetivos específicos também foram atingidos de forma consistente, conforme descrito a seguir:

1. Foram consolidados os principais marcos legais nacionais e internacionais relacionados à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, com destaque para a LGPD, o GDPR, a Política Nacional de Segurança da Informação e os marcos estratégicos do Plano Nacional de Cibersegurança, conforme apresentado no Capítulo 4.

2. Foram levantados e analisados diversos trabalhos relacionados às temáticas de privacidade e segurança da informação, permitindo identificar abordagens teóricas e práticas relevantes que subsidiaram a formulação do modelo proposto. Essa análise, detalhada no Capítulo 3, revelou ainda a inexistência de propostas integradas com foco simultâneo em privacidade e segurança.

3. Foram identificadas, a partir da literatura especializada, cinco disciplinas teóricas fundamentais — governança, metodologia, maturidade, tecnologia e pessoas — que sustentaram a estrutura conceitual do programa unificado de privacidade e segurança da informação apresentado no Capítulo 5.

4. Foram mapeadas arquiteturas, frameworks e modelos de referência nacionais e internacionais, como ISO/IEC, NIST, CIS Controls e a LGPD, que orientaram a formulação da matriz de controles e medidas aplicada no modelo, conforme descrito nos Capítulos 5 e 6.

5. Foi desenvolvido um modelo de maturidade institucional em privacidade e segurança da informação, composto por ciclos de implementação, 32 controles e 310 medidas, além de indicadores consolidados (iBase, iPriv, iSeg), capazes de avaliar e acompanhar a evolução dos órgãos públicos ao longo do tempo (Capítulo 6).

6. Por fim, foi implementado um projeto piloto ampliado, com a participação das 254 organizações do SISP, permitindo validar a aplicabilidade, a escalabilidade e os benefícios estratégicos do modelo proposto, conforme evidenciado nos Capítulos 7 e 8.

Dessa forma, a pesquisa apresenta contribuições teóricas, metodológicas e práticas para o fortalecimento da governança em privacidade e segurança da informação no setor público, alinhadas aos desafios contemporâneos do Governo Digital.

Referências

[1] Vial, Gregory: *Understanding digital transformation: A review and a research agenda*. The journal of strategic information systems, 28(2):118–144, 2019. 1

[2] Demirkan, Haluk, James C Spohrer e Jeffrey J Welser: *Digital innovation and strategic transformation*. It Professional, 18(6):14–18, 2016. 1

[3] `https://www.gov.br/governodigital/pt-br/sisp/secretaria-de-governo-digital-sgd`. 1

[4] `https://www.worldbank.org/en/programs/govtech/gtmi`. 1

[5] `https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf`. 2

[6] `https://www.gov.br/governodigital/pt-br`. 2

[7] `https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11437.htm`. 2

[8] `https://www-webofscience.ez54.periodicos.capes.gov.br/wos/woscc/basic-search`. 4, 8

[9] `https://www-scopus.ez54.periodicos.capes.gov.br/search/form.uri?display=basic`. 4, 8, 11, 12, 15, 16, 18

[10] Wazlawick, Raul Sidnei: *Metodologia de pesquisa para ciência da computação*, volume 3. Elsevier, 2020. 7, 23, 88

[11] Mariano, Ari Melo e Maíra Santos Rocha: *Revisão da literatura: apresentação de uma abordagem integradora*. Em *AEDEM International Conference*, volume 18, páginas 427–442, 2017. 8, 9, 20

[12] `https://www.cisecurity.org/`. 9

[13] `https://www.nist.gov/`. 9

[14] `https://eur-lex.europa.eu/eli/reg/2016/679/oj`. 9

[15] `https://www.dama.org/cpages/body-of-knowledge`. 9

[16] 2023. `https://www.iso.org/standard/27001`. 9

[17] https://www.vosviewer.com/. 12, 13, 17, 20, 22

[18] Moody, Gregory D, Mikko Siponen e Seppo Pahnila: *Toward a unified model of information security policy compliance*. MIS quarterly, 42(1), 2018. 19, 26, 27

[19] Liang, Gaoqi, Steven R Weller, Fengji Luo, Junhua Zhao e Zhao Yang Dong: *Distributed blockchain-based data protection framework for modern power systems against cyber attacks*. IEEE Transactions on Smart Grid, 10(3):3162–3173, 2018. 19

[20] Sohal, Amandeep Singh, Rajinder Sandhu, Sandeep K Sood e Victor Chang: *A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments*. Computers & Security, 74:340–354, 2018. 19

[21] Rana, Nripendra P, Daniel J Barnard, Abdullah MA Baabdullah, Daniel Rees e Sian Roderick: *Exploring barriers of m-commerce adoption in smes in the uk: Developing a framework using ism*. International Journal of Information Management, 44:141–153, 2019. 19

[22] Xiong, Jinbo, Mingfeng Zhao, Md Zakirul Alam Bhuiyan, Lei Chen e Youliang Tian: *An ai-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of iot*. IEEE Transactions on Industrial Informatics, 17(2):922–933, 2019. 19

[23] Hu, Hongchao, Jiangxing Wu, Zhenpeng Wang e Guozhen Cheng: *Mimic defense: a designed-in cybersecurity defense framework*. IET Information Security, 12(3):226–237, 2018. 19, 26, 29

[24] Falco, Gregory, Carlos Caldera e Howard Shrobe: *Iiot cybersecurity risk modeling for scada systems*. IEEE Internet of Things Journal, 5(6):4486–4495, 2018. 19

[25] Li, Daming, Zhiming Cai, Lianbing Deng, Xiang Yao e Harry Haoxiang Wang: *Information security model of block chain based on intrusion sensing in the iot environment*. Cluster computing, 22:451–468, 2019. 19

[26] Gusmão, Ana Paula Henriques de, Maisa Mendonça Silva, Thiago Poleto, Lúcio Camara e Silva e Ana Paula Cabral Seixas Costa: *Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory*. International Journal of Information Management, 43:248–260, 2018. 19

[27] Mozzaquatro, Bruno Augusti, Carlos Agostinho, Diogo Goncalves, João Martins e Ricardo Jardim-Goncalves: *An ontology-based cybersecurity framework for the internet of things*. Sensors, 18(9):3053, 2018. 19

[28] Safa, Nader Sohrabi, Carsten Maple, Tim Watson e Rossouw Von Solms: *Motivation and opportunity based model to reduce information security insider threats in organisations*. Journal of information security and applications, 40:247–257, 2018. 19, 26, 32

[29] Diesch, Rainer, Matthias Pfaff e Helmut Krcmar: *A comprehensive model of information security factors for decision-makers*. Computers & Security, 92:101747, 2020. 19, 26, 29

[30] Von Solms, Basie e Rossouw Von Solms: *Cybersecurity and information security–what goes where?* Information & Computer Security, 26(1):2–9, 2018. 19, 26, 27, 33

[31] Wangen, Gaute, Christoffer Hallstensen e Einar Snekkenes: *A framework for estimating information security risk assessment method completeness: Core unified risk framework, curf.* International Journal of Information Security, 17:681–699, 2018. 19, 26, 29

[32] Rajab, Majed e Ali Eydgahi: *Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education.* Computers & Security, 80:211–223, 2019. 19

[33] Markopoulou, Dimitra, Vagelis Papakonstantinou e Paul De Hert: *The new eu cybersecurity framework: The nis directive, enisa's role and the general data protection regulation.* Computer Law & Security Review, 35(6):105336, 2019. 19, 26, 27

[34] Rodríguez-Barroso, Nuria, Goran Stipcich, Daniel Jiménez-López, José Antonio Ruiz-Millán, Eugenio Martínez-Cámara, Gerardo González-Seco, M Victoria Luzón, Miguel Angel Veganzones e Francisco Herrera: *Federated learning and differential privacy: Software tools analysis, the sherpa. ai fl framework and methodological guidelines for preserving data privacy.* Information Fusion, 64:270–292, 2020. 19

[35] Safa, Nader Sohrabi, Carsten Maple, Steve Furnell, Muhammad Ajmal Azad, Charith Perera, Mohammad Dabbagh e Mehdi Sookhak: *Deterrence and prevention-based model to mitigate information security insider threats in organisations.* Future Generation Computer Systems, 97:587–597, 2019. 19, 26, 32

[36] Benaroch, Michel: *Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making.* Information Systems Research, 29(2):315–340, 2018. 19

[37] Bulgurcu, Burcu, Hasan Cavusoglu e Izak Benbasat: *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness.* MIS quarterly, páginas 523–548, 2010. 20, 26, 31

[38] D'Arcy, John, Anat Hovav e Dennis Galletta: *User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach.* Information systems research, 20(1):79–98, 2009. 20

[39] Ifinedo, Princely: *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.* Information & Management, 51(1):69–79, 2014. 20

[40] Puhakainen, Petri e Mikko Siponen: *Improving employees' compliance through information systems security training: an action research study.* MIS quarterly, páginas 757–778, 2010. 20, 26, 31

[41] Siponen, Mikko, M Adam Mahmood e Seppo Pahnila: *Employees' adherence to information security policies: An exploratory field study.* Information & management, 51(2):217–224, 2014. 21, 32

[42] Herath, Tejaswini e H Raghav Rao: *Protection motivation and deterrence: a framework for security policy compliance in organisations*. European Journal of information systems, 18:106–125, 2009. 21, 26, 27, 31

[43] Siponen, Mikko e Anthony Vance: *Neutralization: New insights into the problem of employee information systems security policy violations*. MIS quarterly, páginas 487–502, 2010. 21

[44] Baskerville, Richard, Paolo Spagnoletti e Jongwoo Kim: *Incident-centered information security: Managing a strategic balance between prevention and response*. Information & management, 51(1):138–151, 2014. 21, 26

[45] Guo, Ken H, Yufei Yuan, Norman P Archer e Catherine E Connelly: *Understanding nonmalicious security violations in the workplace: A composite behavior model*. Journal of management information systems, 28(2):203–236, 2011. 21

[46] Siponen, Mikko e Anthony Vance: *Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations*. European Journal of Information Systems, 23(3):289–305, 2014. 21, 26

[47] Humphreys, Edward: *Information security management standards: Compliance, governance and risk management*. information security technical report, 13(4):247–255, 2008. 21, 26, 28

[48] Siponen, Mikko e Robert Willison: *Information security management standards: Problems and solutions*. Information & management, 46(5):267–270, 2009. 21, 26, 28

[49] Von Solms, Rossouw e Johan Van Niekerk: *From information security to cyber security*. computers & security, 38:97–102, 2013. 21, 26

[50] Baloyi, Ntsako e Paula Kotzé: *A data privacy model based on internet of things and cyber-physical systems reference architectures*. Em *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, páginas 258–268, 2018. 22

[51] Cantiello, Pasquale, Michele Mastroianni e Massimiliano Rak: *A conceptual model for the general data protection regulation*. Em *Computational Science and Its Applications–ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part VIII 21*, páginas 60–77. Springer, 2021. 22, 26

[52] Pedroza, Gabriel, Victor Muntes-Mulero, Yod Samuel Martin e Guillaume Mockly: *A model-based approach to realize privacy and data protection by design*. Em *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, páginas 332–339. IEEE, 2021. 22, 26, 28

[53] Torre, Damiano, Mauricio Alferez, Ghanem Soltana, Mehrdad Sabetzadeh e Lionel Briand: *Modeling data protection and privacy: application and experience with gdpr*. Software and Systems Modeling, 20:2071–2087, 2021. 22, 26

[54] Arbanas, Krunoslav, Mario Spremic e Nikolina Zajdela Hrustek: *Holistic framework for evaluating and improving information security culture.* Aslib Journal of Information Management, 73(5):699–719, 2021. 22

[55] Giuca, Olivia, Traian Mihai Popescu, Alina Madalina Popescu, Gabriela Prostean e Daniela Elena Popescu: *A survey of cybersecurity risk management frameworks.* Em *Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8*, páginas 240–272. Springer, 2021. 22, 26, 30

[56] Proença, Diogo e José Borbinha: *Information security management systems-a maturity model based on iso/iec 27001.* Em *Business Information Systems: 21st International Conference, BIS 2018, Berlin, Germany, July 18-20, 2018, Proceedings 21*, páginas 102–114. Springer, 2018. 22, 26, 28, 29

[57] Serrado, João, Ruben Filipe Pereira, Miguel Mira da Silva e Isaías Scalabrin Bianchi: *Information security frameworks for assisting gdpr compliance in banking industry.* Digital Policy, Regulation and Governance, 22(3):227–244, 2020. 22, 26, 28

[58] Angelini, Marco, Claudio Ciccotelli, Luisa Franchina, Alberto Marchetti-Spaccamela e Leonardo Querzoni: *Italian national framework for cybersecurity and data protection.* Em *Privacy Technologies and Policy: 8th Annual Privacy Forum, APF 2020, Lisbon, Portugal, October 22–23, 2020, Proceedings 8*, páginas 127–142. Springer, 2020. 22, 26

[59] Thomas, Louise, Iqbal Gondal, Taiwo Oseni e Selena Sally Firmin: *A framework for data privacy and security accountability in data breach communications.* Computers & Security, 116:102657, 2022. 23, 26

[60] Verginadis, Yiannis, Antonis Michalas, Panagiotis Gouvas, Gunther Schiefer, Gerald Hübsch e Iraklis Paraskakis: *Paasword: A holistic data privacy and security by design framework for cloud services.* Journal of Grid Computing, 15:219–234, 2017. 23, 26, 30

[61] Andraško, Jozef, Matúš Mesarčík e Ondrej Hamul'ák: *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the eu legal framework.* AI & SOCIETY, páginas 1–14, 2021. 23, 26, 30

[62] Sabillon, Regner, Jordi Serra-Ruiz, Victor Cavaller e Jeimy Cano: *A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (csam).* Em *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, páginas 253–259. IEEE, 2017. 23, 26, 27

[63] Glantz, Clifford, Sriram Somasundaram, Michael Mylrea, Ron Underhill e Andrew Nicholls: *Evaluating the maturity of cybersecurity programs for building control systems.* US Department of Energy Office of Scientific and Technical Information, 2016. 26

[64] LIdster, William W: *Factors that influence selection of frameworks for information security program management: A correlational study*. Tese de Doutoramento, Capella University, 2018. 26

[65] Alsmadi, Izzat e Mohammad Zarour: *Cybersecurity programs in saudi arabia: issues and recommendations*. Em *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, páginas 1–5. IEEE, 2018. 26, 32

[66] Bada, M e JRC Nurse: *Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes). information and computer security, 27 (3), 393–410*, 2019. 26, 32

[67] Muncinelli, Gianfranco, Edson Pinheiro de Lima, José Marcello AP Cestari, Fernando Deschamps e Sergio E Gouvea da Costa: *Developing a conceptual model for process capability in the brazilian data protection regulation context*. Journal of Industrial Integration and Management, 6(04):407–427, 2021. 26, 28

[68] Hajny, Jan, Sara Ricci, Edmundas Piesarskas, Olivier Levillain, Letterio Galletta e Rocco De Nicola: *Framework, tools and good practices for cybersecurity curricula*. IEEE Access, 9:94723–94747, 2021. 26, 33

[69] Schreider, Tari: *Building an effective cybersecurity program*. Rothstein Publishing, 2019. 30, 58, 60

[70] `https://gdpr-info.eu/`. 36

[71] `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`. 37, 38

[72] `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm`. 43

[73] Nacional, Imprensa. `https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm`. 43, 45

[74] Nacional, Imprensa: *Imprensa nacional*. `https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370`. 43

[75] 29100:2020, ABNT/NBR: *Target normas: Pesquisa por [29100] em nbr/nm*. `https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/29100`. 48

[76] 27018:2021, ABNT/NBR: *Target normas: Pesquisa por [27018] em nbr/nm*. `https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/27018`. 49

[77] 29151:2020, ABNT/NBR: *Target normas: Pesquisa por [29151] em nbr/nm*. `https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/29151`. 49

[78] 29134:2020, ABNT/NBR: *Target normas: Pesquisa por [29134] em nbr/nm.* https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/29134. 49

[79] 27701:2019, ABNT/NBR: *Target normas: Pesquisa por [27701] em nbr/nm.* https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/27701. 50

[80] Lefkovitz, Naomi e Katie Boeckl: *Portuguese translation of the NIST privacy framework version 1.0*. 2021. 51

[81] https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide. 51

[82] 27001:2022, ABNT/NBR: *Target normas: Pesquisa por [27001] em nbr/nm.* https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/27001. 53

[83] 27002:2022, ABNT/NBR: *Target normas: Pesquisa por [27002] em nbr/nm.* https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/27002. 53

[84] https://www.cisecurity.org/controls. 54, 55

[85] Reviewers, Note to: *Nist cybersecurity framework 2.0 concept paper: Potential significant updates to the cybersecurity framework.* https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf. 55

[86] Stine, Kevin e Matthew Barrett: *Portuguese translation of the framework for improving critical infrastructure cybersecurity version 1.1 (cybersecurity framework).* 2021. 55

[87] https://www.eccouncil.org/. 56

[88] https://www.isaca.org/. 57

[89] https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. 59

[90] Maymi, Fernando e Shon Harris: *Cissp all-in-one exam guide.* McGraw Hill Professional, 2021. 60

[91] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/cartilha_ppsi.pdf. 63, 66, 67, 69, 75, 79

[92] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. 75, 79, 96, 98

[93] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos. 79

[94] https://www.ibm.com/docs/pt-br/spss-modeler/18.5.0?topic=dm-crisp-help-overview. 96, 97

[95] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos. 97

[96] https://portal.tcu.gov.br/imprensa/noticias/organizacoes-publicas-de-tecnologia-d 98