Arcabouço normativo de cibersegurança na Administração Pública Federal do Brasil: uma revisão sistemática de escopo

1st Walter Lopes Neto
Departamento de Engenharia Elétrica
Universidade de Brasília
Natal, Brazil
walter.lopes@ifrn.edu.br

2nd Rafael Rabelo Nunes
Departamento de Engenharia Elétrica
Universidade de Brasília
Natal, Brazil
rafaelrabelo@unb.br

***Resumo*—Este artigo examina o arcabouço normativo de Segurança da Informação (SI) e cibersegurança na Administração Pública Federal (APF) brasileira. O objetivo é identificar os principais atores institucionais, suas relações, os principais normativos, bem como o alinhamento das regulamentações nacionais com as referências internacionais. Para alcançar este objetivo uma revisão de escopo foi conduzida seguindo as diretrizes do PRISMA-ScR, mapeando decretos, instruções normativas, portarias, diretrizes oficiais e relatórios de auditoria. Como resultado desta revisão, 36 documentos foram identificados, sendo 34 atos normativos e 2 relatórios de auditoria do Tribunal de Contas da União (TCU). Os resultados mostram que, embora a APF tenha uma ampla base normativa, faltam mecanismos para mensurar desempenho e eficácia. Além disso, foi identificado alinhamento conceitual com os padrões internacionais, contudo, há fragmentação institucional e ausência de indicadores e metas explícitos. Recomenda-se a incorporação de métricas de desempenho, o desenvolvimento de uma estrutura unificada de monitoramento e o fortalecimento de mecanismos de coordenação e responsabilização para aumentar a maturidade da segurança cibernética na APF.**

***Index Terms*—Cibsersegurança, Governança, Administração Pública Federal, Programa de Privacidade e Segurança da Informação (PPSI).**

I. Introdução

A multiplicidade de atores, normativos e instrumentos de controle relacionados à Segurança da Informação (SI) e cibersegurança na Administração Pública Federal (APF) gera complexidade institucional [1], a qual dificulta a aplicação eficiente, eficaz e efetiva dessas políticas, sobretudo diante de recursos humanos, técnicos e orçamentários limitados. Segundo o TCU, as principais causas para a não implementação dos controles de segurança são a falta de recursos ou investimento, a carência de pessoal e a ausência de capacitação adequada [2]. Esse cenário confirma que a fragmentação regulatória compromete a coordenação e amplia vulnerabilidades sistêmicas na governança da cibersegurança [3]. No Brasil, a cibersegurança é organizada de forma setorizada, de acordo com os critérios de cada órgão público, em cada um dos Poderes do Estado.

No âmbito do Poder Executivo Federal, por exemplo, um recente marco regulatório é o Decreto n° 12.572/2025, que implementa a nova Política Nacional de Segurança da Informação (PNSI) [4] no âmbito da APF. A PNSI é um instrumento que estabelece princípios, diretrizes estratégicas e objetivos para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações no país. Dentre os principais objetivos da PNSI destacam-se reestruturar a PNSI anterior para priorizar a gestão de riscos e a criação de uma rede colaborativa abrangente, incorpora normativos do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e define de forma mais clara as responsabilidades institucionais na Administração Pública Federal [5].

Com a evolução do arcabouço normativo nos últimos anos, o Brasil passou a contar com diversos instrumentos de governança de SI e cibersegurança no setor público federal, tais como a Política Nacional de Segurança da Informação – PNSI (Decreto nº 12.572/2025 [4]), a Estratégia Nacional de Segurança Cibernética (E-Ciber), Decreto nº 12.573/2025 [6] e, mais recentemente, a Política Nacional de Cibersegurança (PNCiber), Decreto nº 11.856/2023. Além disso, normas complementares emanadas de órgãos centrais (como instruções normativas do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e portarias do Ministério da Gestão e da Inovação (MGI) estabelecem requisitos e procedimentos específicos para a implementação de controles de segurança nos órgãos federais. Esse conjunto normativo constitui de arcabouço normativo federal de cibersegurança, cujo entendimento integral é essencial para avaliar a governança e a efetividade da segurança cibernética no setor público.

A partir deste contexto destacam-se as seguintes questões de pesquisa:

- Questão de Pesquisa 1: Quem são os principais atores institucionais responsáveis pela formulação, implementação e fiscalização das políticas de Segurança da Informação e Cibersegurança na APF?

- Questão de Pesquisa 2: Quais são as relações institucionais e normativos estabelecidas entre esses atores, e como elas configuram um arranjo de governança em cibersegurança na APF?
- Questão de Pesquisa 3: Quais são os principais normativos federais vigentes sobre Segurança da Informação e Cibersegurança, e de que forma eles se alinham (ou não) a padrões e referências internacionais?

Para responder a essas questões, realizou-se uma revisão sistemática de escopo mapeando as políticas, normas e mecanismos de governança de cibersegurança na APF. Nas seções a seguir, descrevem-se os procedimentos metodológicos adotados e, posteriormente, apresentam-se os achados estruturados conforme os objetivos da revisão.

II. Método

Esta revisão seguiu as diretrizes do **PRISMA-ScR** (Preferred Reporting Items for Systematic reviews and Meta-Analyses – Scoping Review extension). A pergunta norteadora considerou os elementos PICO adaptados ao contexto de políticas públicas:

- **População (P)**: Normativos, políticas e documentos oficiais sobre segurança da informação e cibersegurança no âmbito da Administração Pública Federal do Brasil, bem como estudos e relatórios avaliando tais normativos.
- **Intervenção (I)**: Implementação de políticas/normas de cibersegurança e mecanismos de governança associados, tais como comitês, planos estratégicos, programas de conformidade) na APF.
- **Comparação (C)**: Comparação entre diferentes normativos da APF e destes em relação a frameworks internacionais de referência (ISO 27032, NIST CSF etc.).
- **Outcomes (O)**: Identificação dos principais atores institucionais responsáveis pela formulação, implementação e fiscalização das políticas de SI e cibersegurança na APF, bem como dos principais normativos.

Esta revisão não foi previamente registrada em repositório de revisões sistemáticas, como o PROSPERO, nem possui protocolo previamente publicado.

A análise seguiu o fluxograma PRISMA (Figura 1). Para esta análise, bases governamentais e acadêmicas foram consultadas, com critérios de inclusão e exclusão definidos.

III. Fontes de dados e estratégia de busca

Foram consultadas múltiplas fontes de informação, abrangendo tanto repositórios governamentais quanto bases acadêmicas. No âmbito governamental, a pesquisa incluiu: (i) o Portal Gov.br, com destaque para os repositórios da Presidência da República e da Imprensa Nacional, a fim de identificar decretos e portarias; (ii) as publicações do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), contendo normas complementares e instruções normativas de segurança; (iii) o portal do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP/MGI), com diretrizes técnicas específicas; e (iv) relatórios e auditorias de órgãos de controle, notadamente o Tribunal de Contas da União (TCU) e a Controladoria-Geral da União (CGU).

Paralelamente, foi conduzida a busca em literatura acadêmica e técnica por meio das bases Google Scholar, SciELO e Scopus. O objetivo foi identificar estudos que analisassem a política de cibersegurança brasileira ou apresentassem dados complementares, tais como levantamentos de maturidade, avaliações de implementação e comparações com padrões internacionais.

- Critérios de Inclusão: (i) Documentos normativos federais brasileiros relevantes publicados nos últimos 15 anos (por exemplo, decretos presidenciais, instruções normativas, portarias ministeriais) que estabelecessem diretrizes de segurança da informação/cibernética; (ii) Relatórios oficiais de avaliação ou auditoria da governança de TI/Segurança na APF; (iii) Artigos científicos ou técnicos que avaliassem aspectos de governança de cibersegurança na administração pública brasileira, especialmente quanto a desempenho ou alinhamento com boas práticas; (iv) Documentos internacionais de referência citados no contexto brasileiro (como *frameworks* e ISO/NIST) para efeito comparativo. (v) Foram também incluídos programas e normativos setoriais relevantes, como o Programa de Privacidade e Segurança da Informação (PPSI), instituído pelo MGI/SGD, por seu papel transversal de apoio à implementação da LGPD e de diretrizes de segurança da informação na APF. Assim, foram considerados documentos até agosto de 2025.
- Critérios de Exclusão: Documentos focados exclusivamente em segurança de informação de setores fora da esfera federal (estadual, municipal ou setor privado); normas obsoletas integralmente revogadas por versões mais novas; notícias ou matérias de mídia que não agregassem dado factual comprovável; publicações acadêmicas fora do escopo (por exemplo, estudos puramente técnicos sobre criptografia ou *malware* sem relação com políticas públicas).

As estratégias de busca utilizadas em cada fonte estão sintetizadas na Tabela I, que apresenta os termos de busca aplicadas em bases acadêmicas (Google Scholar, SciELO e Scopus) e institucionais (Portal Gov.br, site do GSI/PR, repositórios do TCU e da CGU). Os resultados variaram de acordo com a natureza de cada fonte consultada. As bases acadêmicas retornaram majoritariamente literatura secundária, incluindo estudos analíticos sobre a Administração Pública Federal e segurança cibernética, em consonância com os termos empregados. Entretanto, decretos, leis, instruções normativas e relatórios de controle raramente se encontram indexados nessas bases. Por essa razão, a busca foi complementada por fontes institucionais, as quais permitiram identificar normativos primários atualizados e documentos oficiais essenciais para a análise.

Tabela I
Estratégia de Busca Detalhada

Fonte	Termos de busca utilizados
Google Scholar	(“segurança cibernética” or ”cibersegurança”AND ((“administração pública federal” or ”apf”) OR (”brasil”OR ”brasileira”))
Scopus	((”Cybersecurity”AND ”Brazil”AND ”Public Administration”)
Portal Gov.br	Pesquisa livre por termos: “cibersegurança”, “segurança da informação”, “Política Nacional”, “E-Ciber”, “PNCiber”.
GSI/PR	Navegação manual e consulta de repositórios de instruções normativas (INs).
TCU e CGU	Relatórios, auditorias e instruções normativas relacionados à segurança cibernética na APF.

A. Seleção dos estudos

Foram identificados 294 registros em bases governamentais e acadêmicas, além de 18 registros adicionais obtidos por meio de rastreamento de referências e páginas institucionais específicas. Após a remoção de 74 duplicatas, 238 registros seguiram para a triagem inicial por título e resumo, etapa em que 178 foram excluídos por não atenderem aos critérios de elegibilidade. Restaram 60 documentos para leitura em texto completo. Desses, 24 foram excluídos (22 por falta de aderência ao escopo e 2 por indisponibilidade de acesso), resultando em um corpus final de 36 documentos - sendo 34 normativos (leis, decretos, instruções normativas, portarias e resoluções) e 2 relatórios oficiais do TCU. Todos os documentos incluídos foram submetidos à síntese qualitativa.

A triagem consistiu inicialmente na leitura de títulos e sumários para eliminar registros fora do tema. Em seguida, realizou-se a leitura integral dos documentos remanescentes, definindo-se a inclusão com base nos critérios estabelecidos. Divergências foram solucionadas por consenso entre o autor principal e o orientador, não havendo necessidade de arbitragem externa. Os 34 normativos selecionados estão listados na Tabela IX.

O processo de seleção documental é representado pelo fluxograma PRISMA-ScR (Figura 1), que detalha quantitativamente as etapas de identificação, triagem, elegibilidade e inclusão. Adicionalmente, a Tabela X apresenta o *checklist* PRISMA, conforme as diretrizes metodológicas adotadas.

B. Matriz de Extração de Dados (Data charting process)

Esses dados foram então tabulados e agrupados para permitir uma análise comparativa entre categorias de documentos. Em particular, categorizaram-se os normativos em grupos temáticos (detalhados na seção de Resultados) de modo a identificar sobreposições, complementaridades e lacunas em cada grupo.

Para cada documento selecionado, elaborou-se uma matriz contendo as seguintes variáveis:

- **Tipo de documento**: Política, estratégia, norma técnica, relatório, estudo acadêmico ou framework internacional.

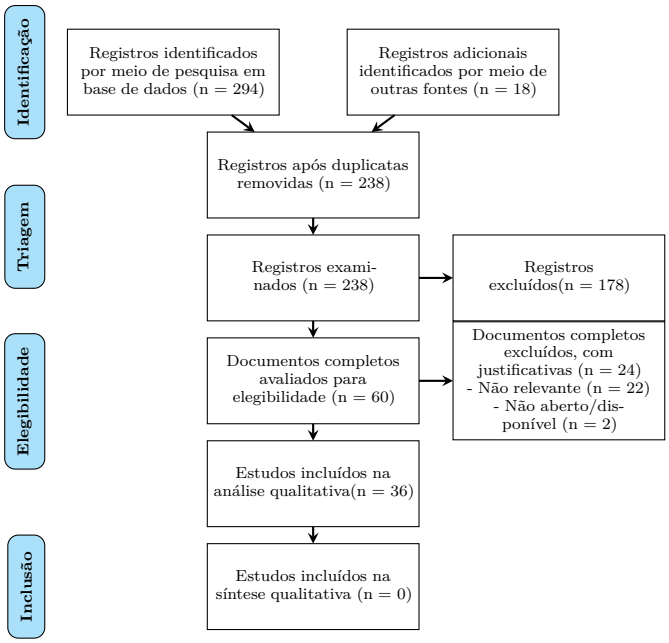

Figura 1. Fluxograma PRISMA-ScR do processo de seleção documental.

- **Órgão responsável**: Instituição emissora do documento.
- **Ano de publicação**.
- **Escopo e resumo do conteúdo**.
- **Observações relevantes**: Informações adicionais, como alinhamento a padrões internacionais, existência de mecanismos de monitoramento, ou lacunas apontadas por auditorias.

Os dados foram tabulados e agrupados para análise comparativa entre as categorias de documentos.

C. Extração e análise dos dados

A extração dos dados dos documentos incluídos foi conduzida com base na matriz de extração de dados descrita previamente, de forma a assegurar uniformidade na coleta das principais informações relativas a cada fonte. A análise consistiu em uma síntese qualitativa descritiva, com os documentos agrupados por categorias similares como descrito na Tabela IX, tais como Camada estratégica com a formulação, coordenação, normatização, Camada de controle, com a fiscalização, auditoria e integridade, Camada operacional, com a implementação, resposta e apoio e Reguladores de temas específicos, com as exigências específicas de ciber. Em seguida, os documentos foram comparados, buscando identificar:

- Convergências e divergências (ex.: diferentes documentos cobrindo o mesmo assunto ou lacunas não cobertas por nenhum normativo);
- Elementos de alinhamento a padrões internacionais (ex.: menção a frameworks como NIST CSF, ISO 27001/27032, controles CIS, etc., nos textos normativos);

- Mecanismos de implementação e monitoramento previstos (ex.: existência de comitês, exigência de planos, previsão de métricas ou relatórios de acompanhamento);
- Lacunas apontadas por avaliações (ex.: achados de auditorias do TCU ou estudos indicando baixa aplicação prática de determinada norma).

Os resultados foram apresentados de forma predominantemente descritiva, acompanhados de tabelas de síntese para cada grupo de documentos.

O processo de triagem foi conduzido pelo autor principal e validado pelo orientador, que revisou as etapas metodológicas e participou da discussão de eventuais dúvidas de inclusão/exclusão.

IV. Resultados

Os achados objetivos desta revisão são apresentados a seguir, organizados em subseções de acordo com os focos de investigação. Inicialmente, procede-se à caracterização geral dos documentos incluídos, considerando seu tipo, período de publicação e órgãos emissores. Em seguida, são detalhados os principais normativos identificados, agrupados em categorias temáticas e acompanhados de tabelas de síntese. Na sequência, apresentam-se os principais atores institucionais envolvidos na governança de segurança da informação e cibersegurança na Administração Pública Federal, bem como as características observadas nos arranjos estabelecidos entre esses atores. Por fim, propõe-se uma taxonomia que integra os diferentes níveis e funções de cada componente do arcabouço identificado.

A. Caracterização geral dos documentos incluídos

O conteúdo final desta revisão consistiu em 36 documentos, sendo 34 normativos federais e 2 relatórios de controle, conforme mencionado. Esses documentos abrangem o período aproximado de 2011 a 2025, concentrando-se especialmente a partir de 2015, quando se intensificam as iniciativas nacionais em cibersegurança. Todos os documentos são vigentes ou relevantes até a data de corte (agosto/2025).

Em termos de tipos de normativos incluídos, tem-se: leis federais (por exemplo, a Lei nº 13.709/2018 (LGPD), entre outras), decretos presidenciais (que instituíram políticas e estratégias nacionais, e estruturas como redes e comitês), instruções normativas (principalmente do GSI/PR e da CGU, estabelecendo regras operacionais e de governança), portarias ministeriais (sobretudo do extinto Ministério do Planejamento e atual Ministério da Gestão e da Inovação em Serviços Públicos - MGI, relativas ao Sistema de Administração dos Recursos de Tecnologia da Informação - SISP e programas de segurança).

Quanto à origem institucional dos documentos: a maioria (cerca de 70%) foi emanada do Poder Executivo Federal (Presidência da República, GSI/PR, Ministérios); outros são provenientes de órgãos de controle (TCU, CGU) e entidades autônomas ou de outros poderes (como a Autoridade Nacional de Proteção de Dados (ANPD), o Conselho Monetário Nacional/Banco Central no setor financeiro. Observou-se, portanto, que a governança de cibersegurança na esfera pública federal envolve diversos atores normatizadores, refletindo a transversalidade do tema e convergindo com análises que defendem uma governança multissetorial como condição para enfrentar a complexidade do tema [3].

Em relação ao escopo de conteúdo, os documentos variam entre diretrizes estratégicas de alto nível, por exemplo, a PNSI e a PNCiber estabelecendo princípios e objetivos nacionais até normas técnicas específicas, por exemplo, instruções normativas detalhando requisitos de segurança em computação em nuvem ou uso de mídias sociais em órgãos públicos. Há também documentos de governança de TI/governança de dados (como a Lei nº 14.129/2021 -Lei de Governo Digital, e normas de compartilhamento de dados) que, embora não tratem exclusivamente de cibersegurança, foram incluídos por possuírem interfaces importantes com a segurança da informação, com exemplo da proteção de dados, autenticação digital, transparência. A Estratégia de Governo Digital [7] buscou integrar segurança, transparência e transformação digital. Neste contexto, o Decreto nº 9.854/2019 regulamentou o compartilhamento de dados entre órgãos e entidades [8].

Não foram incluídas nesta contagem final publicações acadêmicas puras; entretanto, utilizou-se literatura acadêmica selecionada para embasar a discussão, mesmo que tais estudos não componham o rol de documentos incluídos.

B. Principais normativos identificados

Os principais normativos federais vigentes em matéria de SI e cibersegurança na APF foram organizados em categorias temáticas, conforme resumido nas Tabelas IV a

A seguir, cada conjunto será brevemente descrito:

1) Políticas e estratégias nacionais de segurança (estratégicas): Incluem a Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 12.572/2025 [4] e que estabeleceu diretrizes gerais e estruturas de governança de SI no governo federal; a Estratégia Nacional de Segurança Cibernética (E-Ciber), Decreto nº 12.573/2025 [6] e que delineou objetivos e iniciativas para elevar a maturidade em cibersegurança no período 2020–2023; a recém-criada Política Nacional de Cibersegurança (PNCiber), Decreto nº 11.856/2023 [9], que definiu princípios e objetivos nacionais de segurança cibernética e criou o Comitê Nacional de Cibersegurança (CNCiber); e o Decreto nº 10.748/2021, que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos integrando as equipes de tratamento de incidentes (ETIR) dos órgãos da APF. Esses instrumentos formam o arcabouço estratégico de mais alto nível, conforme Tabela IX para resumo desses decretos.

2) Normas operacionais de SI emanadas do GSI/PR: Compõem um conjunto de Instruções Normativas (IN) voltadas à implantação prática da política de segurança nos órgãos. Destacam-se a IN GSI/PR nº 1/2020 [10], que

estabelece a estrutura de gestão de segurança da informação nos órgãos, incluindo a obrigatoriedade de criação de Comitês de SI, do Gestor de Segurança da Informação, da equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) e planos de segurança. Destaca-se também a IN GSI/PR nº 3/2021, que dispõe sobre processos de SI, abrangendo gestão de riscos de SI, tratamento de incidentes, mapeamento de ativos de informação, gestão de continuidade de negócios em SI, gestão de mudanças nos aspectos de SI e avaliação de conformidade de SI. A IN GSI/PR nº 5/2021 [11], que define requisitos mínimos de segurança para uso de computação em nuvem na APF e a IN GSI/PR nº 6/2021 [12], que traz diretrizes para uso seguro de mídias sociais pelos órgãos públicos. Essas normas detalham controles e procedimentos técnicos, funcionando como complementos obrigatórios às políticas estratégicas, conforme representado na Tabela III para uma visão geral.

3) Diretrizes de governança digital, dados e informação: Abrangem normativos base que, embora não focados exclusivamente em segurança cibernética, estabelecem estruturas de gestão da informação e tecnologia no governo, com impactos na segurança. Neste grupo foram incluídos, por exemplo, a Lei nº 14.129/2021 (Lei de Governo Digital), que impulsiona a transformação digital e a prestação digital de serviços públicos, trazendo implicitamente preocupações de segurança na infraestrutura; a Lei nº 12.527/2011. A Lei de Acesso à Informação estabeleceu o princípio da transparência como fundamento da gestão pública [13] e seus decretos regulamentadores (Decreto nº 7.724/2012 e Decreto nº 7.845/2012), que tratam de transparência e classificação da informação (áreas que tangenciam confidencialidade e necessidade de proteção de dados sigilosos), a Medida Provisória nº 2.200-2/2001, que instituiu a ICP-Brasil (infraestrutura de chaves públicas), base para certificados digitais, que foi regulamentada em 2001 [14]. A Lei nº 14.063/2020, sobre assinaturas eletrônicas no âmbito público; e o Decreto nº 10.046/2019, que estabeleceu regras para compartilhamento de dados entre órgãos públicos com salvaguardas de segurança. Estes normativos, sumarizados na Tabela IV, compõem o pano de fundo legal que interage com a política de segurança, por exemplo, definindo requisitos de autenticidade e integração de cadastros, que implicam requisitos de segurança da informação).

4) Proteção de dados pessoais (LGPD e normas da ANPD): Esse conjunto normativo abrange dispositivos relacionados à Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD) [15], a qual estabeleceu novos paradigmas regulatórios para o tratamento de dados pessoais no Brasil. Embora possua escopo mais amplo que a Administração Pública Federal, a LGPD impacta diretamente a gestão e o tratamento de dados nos órgãos públicos. Integram esse grupo também os diplomas legais que instituíram e estruturaram a Autoridade Nacional de Proteção de Dados (ANPD), tais como a Lei nº 13.853/2019 — que alterou a LGPD para transformar a ANPD em órgão da administração pública federal direta, inicialmente vinculado à Presidência da República — e a Lei nº 14.460/2022, que conferiu à ANPD natureza de autarquia de caráter especial. Além disso, destacam-se as Resoluções do Conselho Diretor da ANPD, que compõem normativos complementares de relevância prática: a Resolução CD/ANPD nº 1/2021, que disciplina o regulamento de fiscalização e o processo administrativo sancionador; a Resolução CD/ANPD nº 2/2022, voltada aos agentes de tratamento de pequeno porte; e a Resolução CD/ANPD nº 4/2023, que estabelece critérios de dosimetria e aplicação de sanções. A Tabela VII consolida esses instrumentos, evidenciando a base legal da proteção de dados pessoais no setor público e sua governança regulatória exercida pela ANPD.

5) Normas do SISP e contratação de TIC: A gestão de tecnologia da informação na APF é coordenada pelo Sistema de Administração dos Recursos de TI (SISP), atualmente sob responsabilidade do MGI/Secretaria de Governo Digital. A estrutura do SISP foi consolidada por meio do decreto nº 1.048, de 21 de janeiro de 1994 [16]. Nesse contexto, destacam-se a Portaria SGD/MGI nº 852/2023, que instituiu o Programa de Privacidade e Segurança da Informação (PPSI) [17] no âmbito da APF, sendo um programa guarda-chuva para iniciativas de melhoria de maturidade, resiliência e efetividade em privacidade/segurança; e a Portaria SGD/MGI nº 4.339/2023, que regulamenta o autodiagnóstico de governança de TIC dos órgãos e o índice de governança de TIC (iGOVSISP), instrumento que avalia a maturidade em diversas dimensões, incluindo aspectos de segurança da informação. Além dessas portarias, incluem-se as normas de contratação de bens e serviços de TI que incorporam requisitos de segurança, em especial a IN SGD/ME nº 94/2022 estabelece o processo de contratações de TIC (revogando/atualizando o arcabouço anterior, como a IN 1/2019) e a IN SEGES 73/2020 permanece aplicável apenas como regra geral de pesquisa de preços. Por fim, integra esse grupo o Decreto nº 7.579/2011 (alterado posteriormente) que organiza o próprio SISP e define papéis – embora o decreto do SISP seja anterior a muitas políticas de segurança, ele estrutura a governança de TI na qual as iniciativas de segurança se inserem. Todos esses documentos estão listados na Tabela VIII, enfatizando como requisitos de segurança estão integrados à gestão de TIC e às obrigações de órgãos e fornecedores.

O Programa de Privacidade e Segurança da Informação (PPSI), desenvolvido pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI) por meio da Secretaria de Governo Digital (SGD), foi identificado como um instrumento que operacionaliza diretrizes de segurança da informação e privacidade no âmbito dos órgãos integrantes do SISP. Diferentemente dos decretos presidenciais (PNSI, E-Ciber e PNCiber), o PPSI atua como plano de implementação para órgãos integrantes do SISP, fomentando ações práticas de conformidade e integração à LGPD e mapeando práticas do NIST CSF e ISO 29100/27701 sob a LGPD [18].

6) Normas de controle, auditoria e gestão de riscos: Abrangem dispositivos oriundos do TCU e da CGU que, embora não estabeleçam políticas de segurança em si, influenciam a implementação e avaliação dessas políticas. Incluem-se também normativos da CGU como a IN Conjunta MP/CGU nº 01/2016 (sobre gestão de riscos e controles internos na APF) e a IN CGU nº 03/2017 (Normas de Auditoria Interna Governamental, com orientações para planos anuais de auditoria (PAINT), que podem abranger segurança da informação), além do Referencial Técnico da Atividade de Auditoria Interna Governamental instituído pela Portaria CGU nº 1.089/2018. Esses instrumento, listados na Tabela VII, estabelecem exigências de gestão de riscos, auditoria e controle que indiretamente incluem a temática de segurança da informação, e são importantes pois cobram resultados das políticas. Ademais, relatórios do TCU incluídos na revisão, especificamente o Levantamento de Segurança Cibernética de 2021 e a Estratégia de Fiscalização em Segurança Cibernética de 2022, fornecem recomendações e destacam áreas críticas que demandam aprimoramento.

7) Regulações setoriais específicas: Por fim, foram identificados normativos voltados a setores críticos que complementam o arcabouço geral. Por exemplo, no setor de telecomunicações, a Resolução Anatel nº 740/2020 [19]estabeleceu regras específicas de cibersegurança para provedores de serviços de telecomunicações. No setor financeiro, a Resolução do Conselho Monetário Nacional (CMN) - CMN nº 4.893/2021 e a Resolução do Banco Central do BRasil (BCB) nº 85/2021 [20] instituíram política de segurança cibernética e requisitos de contratação de serviços de processamento e armazenamento em nuvem para instituições financeiras. Na regulação financeira, destacam-se as normas do CMN e do Banco Central que tratam de requisitos de resiliência cibernética. Embora tais normas setoriais não sejam de cumprimento direto por órgãos da administração direta, elas integram a estratégia nacional de cibersegurança ao elevar o patamar de segurança em infraestruturas críticas sob regulação federal. A Tabela VIII elenca esses exemplos, que demonstram a preocupação com segurança também em domínios regulados específicos telecomunicações e financeiro, complementando as políticas amplas da APF.

As Tabelas IV a IX, sintetizam cada normativo mencionado, indicando sua classificação (tipo de instrumento), órgão responsável principal, e uma nota de escopo/observações relevantes. Essas tabelas servem como referência consolidada do arcabouço normativo identificado.

Siglas: PR=Presidência; CN=Congresso Nacional; GSI/PR=Gabinete de Segurança Institucional; CNCiber=Comitê Nacional de Cibersegurança; MGI/SGD=Ministério da Gestão e Inovação/Secretaria de Governo Digital; ANPD=Autoridade Nacional de Proteção de Dados; TCU=Tribunal de Contas da União; CGU=Controladoria-Geral da União; SISP=Sistema de Administração dos Recursos de TI.

Tabela II
Estratégias/Políticas nacionais de SI e Ciber na APF

Normativo	**Classificação**	**Responsável**	**Âmbito/Observações**
Decreto n 12.572/2025 [4] (PNSI)	Política/Decreto (SI)	PR; coord.: GSI/PR	Estrutura de governança de SI; diretrizes gerais.
Decreto nº 12.573/2025 (E-Ciber)	Estratégia nacional (ciber)	PR; coord.: GSI/PR	Objetivos 2020–2023 para elevar maturidade.
Decreto nº 11.856/2023 (PNCiber)	Política nacional (ciber)	PR; coord.: GSI/PR; cria CNCiber	Princípios/objetivos; governança nacional.
Decreto nº 10.748/2021 (Rede de Incidentes)	Decreto organizacional	PR; coord.: GSI/PR	Integra ETIRs da APF; cooperação na resposta.

Tabela III
Normas operacionais de SI (GSI/PR)

Normativo	**Classificação**	**Responsável**	**Âmbito/Observações**
IN GSI/PR nº 1/2020	IN (governança de SI)	GSI/PR	Comitê, papéis, planos, classificação.
IN GSI/PR nº 3/2021	IN (processos de SI)	GSI/PR	Riscos, incidentes, continuidade, awareness.
IN GSI/PR nº 5/2021	IN (nuvem)	GSI/PR	Requisitos mínimos para cloud na APF.
IN GSI/PR nº 6/2021	IN (mídias sociais)	GSI/PR	Diretrizes para uso institucional.

C. Atores institucionais e arranjos identificados

Um dos objetivos desta revisão consistiu em identificar os principais atores institucionais envolvidos na governança da segurança da informação e da cibersegurança no âmbito federal, bem como compreender como se estruturam os arranjos de governança entre eles (Questões de Pesquisa 1 e 2). A Tabela IX sintetiza os atores mapeados, agrupando-os em camadas de atuação, e explicita seus papéis institucionais e os principais dispositivos normativos que fundamentam suas atribuições, bem como apresenta os principais atores institucionais identificados nesta pesquisa, destacando suas responsabilidades na formulação, implementação e fiscalização das políticas de segurança da informação e de cibersegurança na Administração Pública Federal.

D. Camada estratégica

Assim, na camada estratégica e de normatização, destacam-se:

1) Presidência da República (PR): A PR constitui a instância máxima responsável pela formulação e edição de políticas

Tabela IV
Governança digital, dados e informação (leis/decretos-base)

Normativo	Classificação	Responsável	Âmbito/Observações
Lei nº 14.129/2021 (Governo Digital)	Lei (gov. digital)	CN/PR; coord.: MGI/SGD	Digitalização e prestação de serviços.
Lei nº 12.527/2011 (LAI)	Lei (transparência)	CN/PR	Acesso à informação; interfaces com SI.
Dec. nº 7.724/2012 (Reg. LAI Exec.)	Decreto regl.	PR	Procedimentos de atendimento à LAI.
Dec. nº 7.845/2012 (Info. classificadas)	Decreto regl.	PR; coord.: GSI/PR	Salvaguarda/tratamento de informação classificada.
MP nº 2.200-2/2001 (ICP-Brasil)	MP (assinaturas)	PR/ITI	Infraestrutura de chaves públicas.
Lei nº 14.063/2020 (Assinaturas eletrônicas)	Lei (identidade/assinatura)	CN/PR	Uso de assinaturas no poder público.
Dec. nº 10.046/2019 (Compart. de dados)	Decreto (dados)	PR; coord.: MGI	Regras e salvaguardas de compartilhamento.

Tabela V
Proteção de dados pessoais (ANPD)

Normativo	Classificação	Responsável	Âmbito/Observações
Lei nº 13.709/2018 (LGPD)	Lei (proteção de dados)	CN/PR; reg.: ANPD	Regras de tratamento; sanções.
Lei nº 13.853/2019 (Cria ANPD)	Lei (estrutura)	CN/PR	Institui a ANPD.
Dec. nº 10.474/2020 (Estrutura da ANPD)	Decreto organizacional	PR; ANPD	Competências internas.
Lei nº 14.460/2022 (ANPD autarquia)	Lei (natureza)	CN/PR; ANPD	Autarquia de natureza especial.
Res. CD/ANPD nº 2/2022 (Fiscalização/PAS)	Resolução	ANPD	Regras de fiscalização e PAS.
Res. CD/ANPD nº 4/2023 (Dosimetria)	Resolução	ANPD	Critérios de sanção administrativa.

nacionais por meio de decretos presidenciais. No campo da segurança cibernética e da informação, dela emanaram os principais instrumentos normativos de alcance nacional, incluindo a Política Nacional de Segurança da Informação (PNSI), a Estratégia Nacional de Segurança Cibernética (E-Ciber), a Política Nacional de Cibersegurança (PNCiber) e o decreto que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC). Dessa forma, a PR exerce papel central na institucionalização e formalização de políticas públicas nessa área.

No âmbito da Presidência, o Gabinete de Segurança Institucional da PR (GSI/PR) desempenha a função de formulação de diretrizes de segurança da informação e da cibersegurança no Poder Executivo Federal. Esse órgão é responsável por editar normas complementares — como as Instruções Normativas específicas de segurança — e por presidir instâncias colegiadas de governança, a exemplo do Comitê Gestor de Segurança da Informação, assegurando a articulação normativa e a tradução das diretrizes estratégicas em orientações operacionais para os demais órgãos.

2) Comitê Nacional de Cibersegurança (CNCiber): criado pelo Decreto nº 11.856/2023 (PNCiber) como instância interministerial e multissetorial para coordenar a implementação da política nacional de cibersegurança. O CNCiber inclui representantes de diversos setores do governo e possivelmente da sociedade, visando integrar esforços, representando um avanço na governança, formalizando um fórum de alto nível para coordenação intersetorial em cibersegurança.

3) Ministério da Gestão e Inovação/Secretaria de Governo Digital (MGI/SGD): como órgão central do SISP, tem entre suas atribuições a governança de TIC no Executivo. Isso inclui emitir políticas, programas, estratégias e manuais, tais como o Programa PPSI e iGOVSISP, bem como promover a transformação digital segura. O MGI/SGD, portanto, atua na governança de TI e dados, sendo um ator-chave na implementação de controles de segurança nos sistemas governamentais.

4) Autoridade Nacional de Proteção de Dados (ANPD): A criação da Autoridade Nacional de Proteção de Dados (ANPD) [22] fortaleceu a governança regulatória do setor. Embora a ANPD tenha atuação transversal (setor público e privado), é relevante na APF por regular e fiscalizar o cumprimento da LGPD nos órgãos públicos federais. A ANPD emite normas (resoluções) e pode sancionar órgãos em caso de infrações à LGPD. Portanto, figura como ator regulador específico para a dimensão de proteção de dados pessoais, complementando a política de segurança da informação. A ANPD publicou resoluções normativas que detalham sanções, dosimetria e guias orientativos.

E. Na camada de controle e fiscalização, os principais atores são

1) Tribunal de Contas da União (TCU): O Tribunal de Contas da União (TCU) tem desempenhado papel central na avaliação da governança de tecnologia da informação e da segurança da informação no setor público, produzindo auditorias relevantes que influenciam diretamente a formulação e a revisão de políticas. Entre os principais trabalhos, destacam-se o Levantamento de Governança e Gestão em TI (iGG 2022) e o Acórdão nº 1338/2022-Plenário, que evidenciaram deficiências estruturais significativas e induziram ações corretivas no âmbito da Administração Pública Federal [23], [24]. Em auditorias subsequentes, o TCU também identificou falhas críticas de configuração em milhares de domínios governamentais, revelando, por exemplo, que 84% dos domínios avaliados apresentavam risco elevado de ataque e que apenas 8% implementavam integralmente mecanismos de proteção contra *phishing*. Tais achados reforçam o papel indutor do Tribunal na melhoria contínua das práticas de segurança cibernética. Mais recentemente, o Acórdão nº 523/2024 consolidou essa atuação ao recomendar o fortalecimento da gestão de riscos em segurança cibernética e da informação na Administração Pública Federal, com vistas a aprimorar controles, proteger dados e assegurar a conformidade regulatória no ambiente digital [2]. Assim, o TCU, na condição de órgão de controle externo, tem se consolidado como agente ativo na indução de avanços na governança de TI e na segurança cibernética no país. [25].

2) Controladoria-Geral da União (CGU): órgão de controle interno do Executivo, responsável por auditorias, inspeções e promoção da integridade. A CGU coeditou normas de gestão de riscos (IN conjunta 01/2016) e normas de auditoria interna (IN 03/2017), e por meio de suas auditorias avalia também aspectos

Tabela VI
SISP/MGI e contratações de TIC

Normativo	Classificação	Responsável	Âmbito/Observações
Portaria SGD/MGI nº 852/2023 (PPSI)	Portaria/Programa	MGI/SGD	Programa de Privacidade e SI (valores: maturidade, efetividade).
Portaria SGD/MGI nº 4.339/2023 (iGOVSISP)	Portaria	MGI/SGD	Autodiagnóstico e índice de maturidade (SISP).
IN SEGES/ME nº 73/2020 (Contratação TIC)	IN (contratações)	ME/SEGES (à época)	Requisitos de governança/segurança em TIC.
IN SEGES/ME nº 94/2022 (altera IN 73)	IN (contratações)	ME/SEGES	Ajustes; impactos em SI/ciber.
Decreto *(Decreto nº 7.579/2011 (Organiza o SISP)*	Decreto organizacional	PR; órgão central: MGI/SGD	Define SISP e responsabilidades.

Tabela VII
Controle e fiscalização (TCU/CGU)

Normativo	Classificação	Responsável	Âmbito/Observações
Rel. TCU – Levantamento Ciber (2021)	Relatório (diagnóstico)	TCU	Implementação de medidas básicas; indicadores.
Rel. TCU – Estratégia Fiscalização (2022)	Relatório (planejamento)	TCU	Recomendações e prioridades de fiscalização.
IN Conjunta MP/CGU nº 01/2016	IN (riscos/controles/governança)	MP (à época) / CGU	Diretrizes para gestão de riscos e controles.
IN CGU nº 03/2017 (NAIG/PEF)	IN (auditoria interna)	CGU	Normas de auditoria; PAINT/RAINT.
Portaria CGU nº 1.089/2018 (RT-AIG/PEF)	Portaria (referencial técnico)	CGU	Orienta planejamento, execução e reporte.

Tabela VIII
Regulação setorial (quando aplicável)

Normativo	Classificação	Responsável	Âmbito/Observações
Anatel – Res. nº 740/2020	Resolução (telecom)	Anatel	Requisitos de segurança cibernética em redes.
CMN/BCB – Res. CMN nº 4.893/2021; Res. BCB nº 85/2021	Resoluções (SFN)	CMN/BCB	Política de ciber; requisitos de nuvem no SFN.

de SI nos órgãos. A CGU produziu guias de integridade e governança aplicáveis ao setor público. Atua, portanto, garantindo que os órgãos desenvolvam controles internos e atendam às políticas, funcionando como mecanismo de *accountability*.

3) Outros órgãos reguladores setoriais: embora não listados na Tabela VIII por serem mais específicos, vale mencionar que agências reguladoras como a Anatel (telecom) e o Banco Central (no âmbito do CMN) no financeiro também atuam como *stakeholders* institucionais, ao exigirem padrões de segurança em suas respectivas esferas. Esses atores setoriais se conectam à governança geral por meio de iniciativas como o CNCiber, que prevê participação multissetorial.

O arranjo descrito revela que não há um único órgão responsável pela governança de cibersegurança no âmbito federal, mas sim uma governança compartilhada. A Presidência da República lidera estrategicamente no Executivo, o MGI integra aspectos de governança digital, a ANPD zela por dados pessoais, e o TCU/CGU monitoram e cobram resultados, enquanto cada órgão público é responsável por implementar localmente as diretrizes, normalmente através de seus Comitês de SI e Unidades de Segurança da Informação. Essa multiplicidade de atores, suas relações e competências são discutidas em detalhe na seção de Discussão.

F. Taxonomia normativa e institucional

As relações institucionais e normativos estabelecidas entre esses atores configuram um arranjo de governança em cibersegurança no âmbito da Administração Pública Federal. Para representar essas interações, foi elaborada uma proposta de taxonomia normativa e institucional. A partir dos documentos e atores mapeados, torna-se possível delinear uma estrutura em camadas do arcabouço de cibersegurança da APF, na qual os níveis normativos são diretamente associados aos níveis institucionais correspondentes.

1) Camada estratégica: composto pelas políticas e estratégias nacionais (PNSI, E-Ciber, PNCiber) editadas pela Presidência da República. Nesse nível define-se o enquadramento princípiosa nível macro, objetivos nacionais, e a criação de instâncias de coordenação, tais como o CNCiber. Os atores correspondentes são a PR, como editora das normas por meio dos seus órgãos e o GSI/PR como formulador técnico. Essas políticas têm abrangência em todo o Executivo Federal e, em alguns aspectos, sinalizam diretrizes ao país como um todo.

2) Camada tática: aqui situam-se as normas complementares e setoriais que operacionalizam as políticas. Inclui as IN do GSI (que padronizam estruturas e processos de SI nos órgãos), as portarias do MGI (que inserem segurança na governança de TI e programas específicos), as resoluções da ANPD (que regulam a proteção de dados), normas do SISP, e eventuais políticas setoriais (como as de Anatel, BCB etc. para setores críticos). Essas normas estabelecem de forma detalhada responsabilidades, procedimentos e controles a serem adotados. Os principais atores correspondem aos órgãos centrais emissores, como o GSI, o MGI, a ANPD, os Ministérios e as Agências Reguladoras, com cada órgão atuando no âmbito de suas respectivas competências. Esse nível normativo pode ser compreendido como a instância de tradução entre a dimensão estratégica e a operacional, assegurando que as diretrizes de alto nível sejam efetivamente desdobradas em requisitos práticos de implementação.

3) Camada Operacional e de Implementação: corresponde aos órgãos e entidades da APF enquanto implementadores das políticas e normas. Cada ministério, autarquia, fundação etc. deve

Tabela IX
Atores institucionais da governança de SI e Cibersegurança na APF e respectivos papéis

Ator institucional	Papel (síntese)	Principais bases legais / normativos
Camada estratégica — formulação, coordenação, normatização		
Presidência da República (PR)	Edição de políticas e decretos nacionais	Decr. 12.572/2025 (PNSI); Decr. 12.573/2025 (E-Ciber); Decr. 11.856/2023 (PNCiber); Decr. 10.748/2021 (Rede Federal de Incidentes) [21]
GSI/PR	Formulação de diretrizes de SI/ciber no Executivo; normas complementares	IN GSI 1/2020; 3/2021; 5/2021; 6/2021
CNCiber	Coordenação intersetorial da PNCiber	Decr. 11.856/2023
MGI / Secretaria de Governo Digital (órgão central do SISP)	Governança de TIC/digital; instrumentos de gestão	Decr. 7.579/2011 (SISP)[a]; Port. SGD/MGI 852/2023 (PPSI); Port. SGD/MGI 4.339/2023 (iGOVSISP)
ANPD	Regulação e fiscalização de proteção de dados	Lei 13.709/2018 (LGPD); Lei 14.460/2022; Decr. 10.474/2020; Res. CD/ANPD 2/2022; 4/2023
Camada de controle — fiscalização, auditoria e integridade		
TCU (controle externo)	Auditorias e diretrizes de desempenho	IN TCU 84/2020; Levantamento de Segurança Cibernética (2021); Estratégia de Fiscalização (2022)
CGU (controle interno do Executivo)	Auditoria interna gov., riscos e integridade	IN Conj. MP/CGU 01/2016; IN CGU 03/2017; Port. CGU 1.089/2018 (RT-AIG)
Camada operacional — implementação, resposta e apoio		
SISP — órgão central, órgãos setoriais (ministérios) e seccionais (autarquias/fundações)	Implementação de TIC/SI nos órgãos	Decr. 7.579/2011; Port. 4.339/2023
SERPRO; Dataprev	Operadores de TI e serviços críticos à APF	Leis de criação e contratos com a APF
CGI.br / NIC.br / CERT.br	Boas práticas e resposta a incidentes (cooperação)	Decr. 4.829/2003 (CGI.br)
MD / ComDCiber	Defesa cibernética e cooperação	Atos do MD; PNSI/PNCiber
MJSP / Polícia Federal	Investigação de crimes cibernéticos	Competências legais da PF
MCTI; MCOM; MRE	P&D, telecom e cooperação internacional	Atos setoriais; Marco Civil; Gov. Digital; tratados
Reguladores de temas específicos - exigências específicas de ciber		
Anatel	Requisitos de ciber em telecom	Res. Anatel 740/2020 (atual. 767/2024)
CMN / BCB	Requisitos prudenciais de ciber/nuvem no SFN	Res. CMN 4.893/2021; Res. BCB 85/2021
ITI (ICP-Brasil)	Infraestrutura de chaves públicas e assinaturas	MP 2.200-2/2001

Abreviações: PR: Presidência da República; GSI/PR: Gabinete de Segurança Institucional; MGI/SGD: Ministério da Gestão e Inovação/Secretaria de Governo Digital; SISP: Sistema de Administração dos Recursos de TI; ANPD: Autoridade Nacional de Proteção de Dados; TCU: Tribunal de Contas da União; CGU: Controladoria-Geral da União; MD: Ministério da Defesa; MJSP: Ministério da Justiça e Segurança Pública; MCTI: Ministério da Ciência, Tecnologia e Inovação; MCOM: Comunicações; MRE: Relações Exteriores; ITI: Instituto Nacional de Tecnologia da Informação.

instituir sua própria governança de segurança com comitê, planos e procedimentos, conforme as diretrizes superiores. Nesse nível, os atores são os próprios órgãos públicos, unidades de TI/Segurança, autoridades locais de SI e comitês internos. É onde as políticas se concretizam em ações tais como treinamentos, controles técnicos, gestão de incidentes local dentre outros. Neste caso, muitos órgãos editam normativos internos tais como portarias e manuais, para regulamentar a segurança em seu âmbito, alinhados aos normativos centrais.

4) Camada de Controle: é composto pelos mecanismos de verificação de conformidade e desempenho. Inclui as auditorias do TCU (controle externo) e da CGU (controle interno), além de monitoramentos que venham a ser realizados por comitês, por exemplo no caso de o CNCiber instituir monitoramentos periódicos. Os instrumentos normativos nesse nível são as resoluções, instruções e referenciais de auditoria citados, que exigem ou orientam avaliações periódicas. Os atores são TCU, CGU e também o CNCiber, que tem mandato para acompanhar a evolução da política e o CGSI/GSI (Comitê Gestor de SI do GSI, que acompanha a implementação da PNSI).

Em síntese, essa taxonomia, conforme ilustrada na Figura 2, evidencia quatro camadas: (1) Política Estratégica Nacional, (2) Normatização Tática/Operacional, (3) Implementação pelos Órgãos, e (4) Nível de Controle e Monitoramento. Idealmente, essas camadas formam um ciclo virtuoso no qual políticas orientam normas, normas guiam implementações e implementações são avaliadas por controles. Os resultados dessas avaliações realimentam ajustes de curso e melhorias nas políticas. Dentre os achados desta revisão, porém, foi possível identificar que esse ciclo ainda não está plenamente completo, conforme discutiremos a seguir, sobretudo no que tange à falta de realimentação por indicadores e à fragmentação entre atores.

G. Alinhamento dos normativos com os padrões internacionais

A seguir serão apresentados de que forma os principais normativos federais vigentes sobre Segurança da Informação e Cibersegurança se alinham a padrões e referências internacionais.

Dentre as principais lacunas identificadas nesta revisão, destacam-se:

- Ausência de indicadores claros em políticas estratégicas.
- Monitoramento baseado em auditorias externas (TCU), não previsto nos normativos.
- Ênfase em processos e conformidade, não em resultados.
- Governança fragmentada entre GSI/PR, MGI, CNCiber.

V. Discussão

Os documentos mapeados permitem a análise do estágio atual da governança de cibersegurança na APF. O Brasil estabeleceu uma arquitetura normativa abrangente e inspirada em padrões internacionais – por exemplo, a PNSI e a E-Ciber incorporam conceitos presentes em *frameworks* internacionais, como a necessidade de elevar

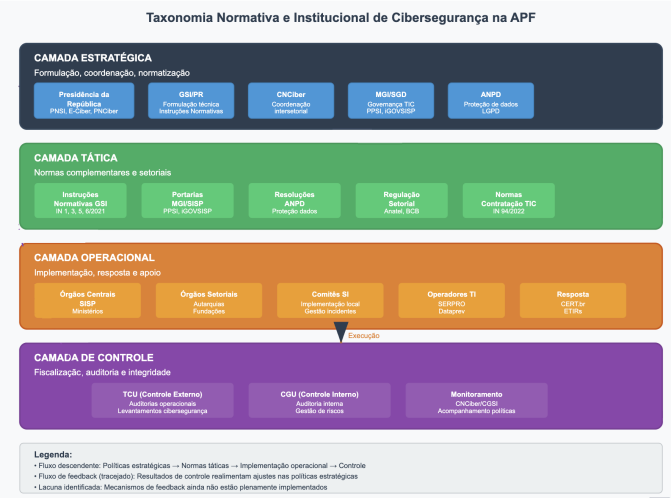

Figura 2. Taxonomia Normativa e Institucional de Cibersegurança na APF.

a maturidade em segurança e envolver múltiplos atores na governança. Na prática, porém, os achados sugerem desafios na tradução dessas diretrizes em melhorias tangíveis na postura de segurança dos órgãos públicos. A seguir, discutimos os principais aspectos emergentes, conectando as evidências encontradas às questões de pesquisa e à literatura.

A. *Complexidade e sobreposição institucional*

Dentre os achados, destaca-se a complexidade institucional e possível sobreposição de competências na governança de segurança cibernética na APF. A revisão revelou múltiplos órgãos centrais com papéis relevantes tais como o GSI/PR, MGI/SGD, ANPD, CGI.br (no caso de governança da internet), além dos órgãos de controle (TCU/CGU) e dos próprios órgãos setoriais. Essa multiplicidade sem uma coordenação integrada histórica levou a uma governança fragmentada [1]. Cada entidade tem enfoque em determinado um aspecto, tais como o GSI/PR nas normas de SI e ciber para o Executivo, o MGI nas práticas de governança de TI, a ANPD na proteção de dados e o TCU cobrando resultados.

Na literatura de políticas públicas e governança de TI, essa fragmentação é apontada como prejudicial à eficácia das iniciativas, pois ocorrem sobreposições normativas e lacunas de responsabilidade. Por exemplo, constatou-se na revisão que tanto o GSI/PR quanto a CGU editaram normas sobre gestão de riscos, cada qual com enfoques distintos, o que pode confundir os órgãos executores sobre qual seguir prioritariamente. Do mesmo modo, a existência de uma Política de Segurança da Informação (PNSI) separada de uma Política de Cibersegurança (PNCiber) pode gerar dúvidas sobre escopo, neste sentido o decreto da PNCiber/2023 [9] visa integrar esses aspectos.

Adicionalmente, lacunas de coordenação ficaram evidentes, até 2023, durante esta pesquisa, não foi identificado um comitê único que alinhasse as ações de GSI/PR, MGI, Defesa Cibernética (MD), setores regulados e demais interessados. A criação do CNCiber é uma resposta a isso, congregando membros de diversos setores do executivo e possivelmente outros poderes, com a missão de "propor medidas e acompanhar a evolução da segurança cibernética nacional". Essa iniciativa é alinhada às boas práticas internacionais de governança, uma vez que muitos países possuem estruturas similares de coordenação nacional.

Cabe ressaltar a distinção entre órgãos normatizadores e órgãos implementadores. As evidências sugerem que alguns órgãos centrais produzem normas, mas não possuem meios de forçar sua implementação uniforme. Por exemplo, o GSI/PR expedía as IN de segurança e aguardava que cada órgão cumprisse, porém não existia até recentemente um mecanismo sistemático de monitoramento central desse cumprimento, ficando tal verificação a cargo eventual de auditorias do TCU. Esse vácuo de monitoramento colaborou para que houvesse órgãos muito adiantados e outros muito atrasados em adoção de controles, sem que isso fosse evidente no nível central.

Em suma, a complexidade do arranjo institucional brasileiro é um fator de desafio. Por um lado, envolve múltiplos *stakeholders* o que é positivo para abrangência; por outro, dificulta a responsabilização e o acompanhamento coeso das políticas. A governança evoluiu com a CNCiber, mas persiste a necessidade de clarificar papéis para evitar redundâncias, tais como entre GSI/PR e MGI na emissão de diretrizes de SI e cibersegurança, e de fortalecer a atuação conjunta.

B. *Convergência com referenciais internacionais*

No que ser refere ao alinhamento dos normativos com padrões internacionais, como indicado na Questão de Pesquisa 3, os resultados indicam que o arcabouço normativo brasileiro incorporou diversos conceitos presentes em *frameworks* mundialmente aceitos, porém ainda não adotou plenamente mecanismos chave recomendados por esses referenciais. Dois marcos internacionais citados nesta revisão são o *NIST Cybersecurity Framework* (CSF) e a ISO/IEC 27032:2012 (Diretrizes para segurança cibernética) [26]: O NIST CSF (2014) define cinco funções: Identificar, Proteger, Detectar, Responder, Recuperar. Além disso, sugere que organizações avaliem periodicamente seu nível de maturidade (*tiers*) em cada função. Isso encoraja a definição de um perfil atual e desejado de segurança, com medição de progresso ao longo do tempo. Trata-se de um *framework* amplamente adotado nos EUA e referência em vários países.

A ISO 27032 enfatiza a coordenação multissetorial (governo, setor privado, sociedade) na gestão de riscos cibernéticos e recomenda adoção de boas práticas e monitoramento da implementação. Também destaca a importância de métricas para avaliar a capacidade de cibersegurança tanto em nível nacional quanto organizacional.

As políticas brasileiras demonstram convergência conceitual com esses padrões em alguns aspectos, dentre eles, destacam a necessidade de operacionalizar padrões internacionais com mecanismos práticos de avaliação e métricas contínuas [3].

A E-Ciber 2020 [6] explicitamente tinha como objetivo elevar o nível de maturidade em segurança cibernética na APF, o que está alinhado à ideia central do NIST CSF de melhoria contínua de maturidade. Também citava ações de capacitação, gestão de riscos, proteção de infraestruturas críticas, temas presentes internacionalmente. A PNSI/2018 e a PNCiber/2023 incorporaram princípios como cooperação, resiliência, gestão de riscos, também ecoando recomendações globais.

Contudo, falta operacionalizar certas práticas desses *frameworks*. Uma diferença marcante é a ausência de métricas e avaliação periódica institucionalizada nas políticas nacionais, enquanto tanto NIST CSF quanto ISO 27032 [**?**] pregam monitoramento contínuo. No NIST CSF [27], é inerente a medição de progresso via *tiers*, já no Brasil, a PNSI/E-Ciber não estabeleceram processo análogo. Países com programas nacionais de cibersegurança costumam definir *Key Performance Indicators(KPIs)* de cibersegurança, tais como, número de incidentes reportados, tempo médio de resposta, porcentagem de instituições com certo nível de maturidade frequentemente publicados em relatórios anuais. No caso brasileiro, somente recentemente o TCU começou a coletar alguns dados para composição de indicadores, via questionários de auditoria, e o MGI, através do iGOVSISP [28], introduziu avaliação anual de maturidade em TI.

Outro aspecto que aponta necessidade de alinhamento é a abordagem de gestão de riscos e resposta a incidentes. *Frameworks* internacionais enfatizam exercícios contínuos, compartilhamento de informações de ameaças e coordenação ampla. O Brasil avançou ao criar a Rede Federal de Gestão de Incidentes Cibernéticos (Decreto 10.748/2021), uma estrutura que se assemelha a redes de *Computer Security Incident Response Team (CSIRTs)* nacionais em outros países, visando cooperação na resposta a incidentes, convergindo com as recomendações ISO 27032 de coordenação.

Nota-se que alguns instrumentos internacionais foram usados em avaliações internas, embora não pelas políticas. O TCU baseou seu levantamento de 2021 em controles críticos do *CIS (Center for Internet Security)* e mapeou a implementação básica nos órgãos. Pesquisadores brasileiros também empregaram *frameworks*: o estudo de Bonifácio et al. (2020) [29] usou o NIST CSF combinado para avaliar a execução da PNSI, e Azambuj & Souza (2020) [30] propuseram modelo de maturidade inspirado na E-Ciber (objetivo de maturidade) e *frameworks* internacionais. Esses esforços mostram um potencial

de aproximação: há conhecimento disponível e adaptado à realidade nacional que poderia ser formalmente adotado nas políticas.

Adicionalmente, a atualização recente do *Cybersecurity Framework* para a versão NIST CSF 2.0 reforça a relevância das lacunas identificadas neste estudo. A introdução da função *Govern* como pilar estruturante do *framework* evidencia o reconhecimento, pela comunidade internacional, de que a governança, abrangendo a definição de estratégias, papéis, responsabilidades e mecanismos de medição de desempenho, constitui o alicerce de uma cibersegurança eficaz. Nesse contexto, a fragmentação institucional e a limitada utilização de indicadores-chave de desempenho (KPIs) na Administração Pública Federal configuram um ponto crítico de melhoria, distanciando o arcabouço nacional das melhores práticas globais [27].

Em resumo, o arcabouço normativo brasileiro cita e se inspira em referências internacionais, mas carece de implementar os mecanismos práticos que essas referências julgam cruciais, principalmente a cultura de métricas e melhoria contínua. A criação do CNCiber com mandato para acompanhar a evolução da segurança cibernética nacional é um passo que pode levar a maior alinhamento, uma vez que o acompanhamento estruturado de indicadores de desempenho é fundamental para aprimorar a cibersegurança.

C. Lacunas de efetividade normativa

Um dos achados da revisão foi a ausência de indicadores mensuráveis ou metas quantitativas nos normativos analisados. Essa ausência de indicadores confirma críticas que apontam a necessidade de mecanismos objetivos para consolidar a cibersegurança como eixo de soberania digital [3]. Essa pode ser considerada uma lacuna no arcabouço brasileiro atual, com implicações na eficácia e efetividade das políticas. Da mesma forma, as instruções normativas operacionais focam em procedimentos a implementar, porém não exigem que se meça os resultados desses procedimentos, como redução de incidentes e melhoria de tempos de resposta).

Essa ênfase em *compliance* de processos, ao invés de performance de resultados, indica uma mentalidade de implementação normativa mais burocrática do que orientada a desempenho. Os órgãos cumprem a norma, por exemplo, criam o comitê, publicam a política interna, mas muitas vezes não são cobrados sobre o quão efetivas são essas medidas, consequentemente, abre-se espaço para um fenômeno identificado, muitas vezes a política é formalmente implementada, mas não gera mudanças substanciais na realidade, pois não há acompanhamento estruturado.

Os principais dados quantitativos identificados para avaliar a efetividade vieram de fora dos normativos: as auditorias do TCU e pesquisas independentes. O Levantamento de Segurança Cibernética do TCU (2021) revelou, por exemplo, que 56% dos órgãos federais não possuíam gestão contínua de vulnerabilidades, e percentuais similares não adotavam outras práticas básicas. Isso indica que mesmo controles mínimos preconizados pelas normas não estavam implementados em larga medida, ou seja, as políticas não estavam sendo eficazes. Outro dado: 57,8% dos órgãos careciam de programas contínuos de treinamento em segurança, dado apresentado pelo TCU e citado em nossas recomendações. Esses números funcionam como indicadores de efetividade.

Em suma, identifica-se uma lacuna de efetividade normativa: as normas estabelecem o quê deve ser feito (estruturas, planos, controles), porém não asseguram como verificar se foi bem feito. Isso compromete tanto a eficácia (atingir os objetivos propostos) quanto a efetividade (ter impacto real) das políticas, pois sem metas claras não se pode aferir sucesso ou fracasso. Há movimentos emergentes para suprir essa lacuna, tais como a portaria do iGOVSISP introduz avaliação anual de maturidade de TI que inclui segurança, criando um comparativo anual entre órgãos. O CNCiber tem competência para acompanhar a evolução da cibersegurança nacional. O desafio agora é incorporar esses mecanismos de forma estruturada na gestão pública, passando de uma governança reativa para uma governança proativa baseada em evidências e indicadores contínuos.

Por fim, os relatórios de controle do TCU incluídos fornecem uma visão da implementação dessas políticas nos órgãos e, portanto, complementam os normativos ao evidenciar lacunas práticas. A baixa aderência aos controles recomendados é evidenciada pelos achados do TCU, que revelaram que apenas 2% dos domínios avaliados implementavam todos os controles de conexão segura (HTTPS) testados e que 81% não utilizavam a assinatura de domínio (DNSSEC), expondo os serviços a riscos significativos [2].

D. Papel dos órgãos de controle e regulação

Os órgãos de controle, em especial o TCU e, em certa medida, a CGU, emergem dos achados como atores cruciais para impulsionar a efetividade das políticas de cibersegurança. De certa forma, eles preencheram a lacuna deixada pelas normas quanto ao monitoramento de resultados. O TCU quantificou a implementação de controles e evidenciou lacunas. A CGU, por sua vez, tem papel de apoiar melhorias contínuas via suas orientações e auditorias. A existência de um referencial de gestão de riscos (IN conjunta 01/2016) e de manuais de auditoria interna fornecem método para órgãos avaliarem riscos de SI. Quanto aos órgãos reguladores setoriais (Anatel, Bacen), sua atuação complementa a dos órgãos centrais. Eles impõem requisitos de segurança nas empresas e entidades sob sua regulação, o que melhora a resiliência dos serviços críticos que, em última análise, impactam o setor público (por exemplo, telecomunicações seguras, instituições financeiras seguras). Do ponto de vista do arcabouço geral, porém, nota-se que essas iniciativas setoriais têm pouca integração formal com a estratégia central de APF. A conexão deverá se dar via CNCiber, onde assentos para setores críticos permitirão troca de informações. Antes disso, cada setor atuava isoladamente. Assim, o papel desses reguladores na governança ampla era limitado cuidavam de seu setor, mas não havia um esforço coordenado nacional de troca de boas práticas ou gerenciamento de riscos sistêmicos. É relevante destacar o papel da Autoridade Nacional de Proteção de Dados (ANPD), em funcionamento desde 2021, como órgão regulador responsável por fiscalizar a aplicação da Lei Geral de Proteção de Dados (LGPD), inclusive no âmbito da APF. Sua atuação tende a induzir avanços significativos na governança e na proteção de dados pessoais. Considerando-se a proteção de dados como um domínio específico da segurança da informação, a exigência de relatórios de impacto em órgãos públicos aproxima esse campo da agenda de segurança cibernética. Entretanto, a ANPD atua de forma paralela, o que suscita o desafio de evitar a fragmentação entre iniciativas de proteção de dados e políticas de cibersegurança. Nesse sentido, a participação da ANPD em arranjos de coordenação mais integrados, como aqueles potencialmente viabilizados pelo Comitê Nacional de Cibersegurança (CNCiber), pode contribuir para maior coerência e sinergia nas políticas públicas. Em suma, os órgãos de controle e regulação têm sido catalisadores de efetividade, tais como o TCU expondo falhas e cobrando ações. A continuação da participação ativa do TCU é uma garantia de que o tema não sairá da pauta, uma vez que o Tribunal vem incluindo cibersegurança como área de risco alto em suas estratégias de fiscalização recentes. Para a gestão pública, isso significa que há pressão externa por resultados, o que pode incentivar os gestores a adotarem métricas e prestar contas regularmente, mesmo que a legislação não explicitasse essa obrigação originalmente.

E. Integração setorial e riscos críticos

Por fim, merece discussão a integração entre o arcabouço geral da APF e as iniciativas setoriais, bem como a atenção a riscos críticos, infraestruturas críticas e serviços essenciais. A revisão identificou normativos específicos de setores tais como telecomunicações e financeiro, que estabelecem requisitos de cibersegurança para atores daqueles domínios. Essa setorização reflete a estrutura do Estado brasileiro, na qual órgãos reguladores independentes tratam de seus setores. Contudo, do ponto de vista de segurança nacional cibernética, ameaças muitas vezes atravessam setores e um incidente grave em infraestrutura crítica pode ter impacto em cascata no governo.

Outro aspecto de integração setorial é a padronização de requisitos, uma vez que, no Brasil, as exigências de cibersegurança variam conforme o setor. Por exemplo, bancos têm que seguir as resoluções do Conselho Monetário Nacional (CMN) e do Banco Central do Brasil, com disposições específicas de nuvem, dentre outras, enquanto órgãos públicos seguem as IN do GSI/PR e portarias do MGI, que podem não ser idênticas. Essa disparidade pode gerar níveis de segurança desiguais e pontos fracos exploráveis. Como possível solução, destaca-se a construção de um *framework* unificado adaptável a cada setor, mas com um núcleo comum de controles, facilitando inclusive que órgãos que atuam em múltiplos setores, tais como Ministério das Comunicações, que lida com telecomunicações e com sua própria estrutura, tenham uma orientação única. Em termos de riscos

críticos, nota-se que o arcabouço federal de segurança da informação tradicionalmente focou na proteção da informação classificada e nos sistemas governamentais internos. Contudo, a transformação digital e a interconexão entre serviços públicos e privados aumenta a relevância de parcerias intersetoriais para segurança. Por exemplo, ataques a fornecedores de TI governamentais podem afetar dezenas de órgãos; ataques a sistemas bancários podem afetar pagamentos de benefícios sociais, etc. A governança nacional precisa contemplar esses cenários, e normativos como a PNCiber apontam nessa direção ao incluir princípios de cooperação ampla.

Em conclusão, reforça-se que o arcabouço normativo federal em cibersegurança está inserido em um contexto maior que envolve setor privado, outras esferas de governo e sociedade. A integração setorial ainda é um desafio em andamento: reconhecido nas estratégias, iniciado por algumas ações (CNCiber, Rede de Incidentes), mas distante de uma maturidade ideal.

VI. Conclusão

A presente revisão de escopo permitiu mapear as principais políticas e normativos de cibersegurança na Administração Pública Federal brasileira, revelando um cenário em que as diretrizes existem e são abrangentes. Constatou-se que a Administração Pública Federal dispõe de um arcabouço normativo amplamente alinhado às boas práticas internacionais quanto à definição do que deve ser realizado. Todavia, observa-se a ausência de mecanismos que assegurem a avaliação da qualidade da execução e da efetividade dos resultados obtidos. As principais lacunas detectadas incluem:

- **Falta de indicadores e metas claras:** As políticas estratégicas ou instruções analisadas não definem indicadores-chave de desempenho (KPIs) relativos à segurança da informação/cibernética. Isso dificulta a avaliação da eficácia (cumprimento de objetivos) e a efetividade (impacto real em redução de danos) das iniciativas. Sem metas quantitativas ou marcos de sucesso, há risco de "cumprir a norma" sem saber se problemas foram resolvidos.
- **Ênfase em *compliance* em detrimento dos resultados** Os normativos analisados concentram-se predominantemente na exigência de estruturas organizacionais e na elaboração de planos formais, mas não estabelecem mecanismos de incentivo ou de responsabilização vinculados a resultados concretos. Não foram identificados dispositivos normativos que imponham aos órgãos a obrigação de alcançar níveis mínimos de maturidade em segurança ou de reduzir incidentes em proporções específicas. Tal configuração evidencia uma orientação ainda centrada na conformidade burocrática, em detrimento de uma abordagem de gestão orientada ao desempenho e à efetividade dos controles implementados.
- **Governança fragmentada:** A multiplicidade de atores sem uma clara integração de esforços pode levar a lacunas de responsabilidade.

A ausência de indicadores mensuráveis e de mecanismos estruturados de acompanhamento compromete a capacidade do governo em avaliar o real impacto das políticas existentes. As conclusões reforçam a necessidade de ações estratégicas para fortalecer a cibersegurança institucional na esfera pública federal.

Com base nos achados desta revisão, recomenda-se um conjunto de ações integradas para fortalecer a maturidade em SI e cibernética institucional da APF, descritas a seguir:

1) **Ajuste Normativo:** Revisar as principais políticas e normas complementares para incluir explicitamente a necessidade de indicadores de desempenho. Por exemplo, futuras estratégias nacionais podem vir acompanhadas de um plano de ação contendo metas quantificáveis para cada objetivo estratégico. Esses indicadores devem ser alinhados a padrões internacionais para viabilizar *benchmarking*. Ademais, sugere-se que novos normativos incorporem obrigações de reporte periódico de incidentes e de status de controles pelos órgãos, tais como exigir que cada órgão publique anualmente métricas de sua capacidade de segurança.
2) **Framework Unificado:** Desenvolver ou implementar um *framework* nacional de métricas de cibersegurança para a APF. Esse *framework* poderia inspirar-se no NIST CSF que definindo níveis de maturidade por domínios de capacidade e em metodologias acadêmicas já propostas para o contexto brasileiro. Com isso, seria possível aplicar índices padronizados de maturidade cibernética em todos os órgãos federais, aferido anualmente via autoavaliação validada por auditoria, similar ao iGOVSISP, porém focado especificamente em segurança da informação/cibernética. Os resultados então poderiam ser usados para alimentar painéis de acompanhamento governamental, evidenciando avanços e fragilidades de forma transparente e orientando decisões centralizadas. Esse *framework* unificado ajudaria a migrar de avaliações esporádicas (como o levantamento ad hoc do TCU) para um monitoramento contínuo institucionalizado.
3) **Fortalecimento da governança:** Dentre as ações possíveis estão a de colaborar com escolas de governo (ENAP, ESAF etc.) para ofertar formações em gestão de riscos, proteção de dados e resposta a incidentes, e demais temáticas relacionadas à cibersegurança, de modo contínuo. Adicionalmente, recomenda-se o apoio técnico diferenciado, oferecendo suporte adicional, como consultoria centralizada, soluções compartilhadas e sistemas de segurança gerenciados, a órgãos com menos recursos ou expertise. Isso melhora a equidade e eficiência, evitando duplicação de esforços e elevando o patamar mínimo de segurança de todos os órgãos. A implementação das recomendações apresentadas possibilita a transição de um modelo essencialmente reativo, caracterizado pela atuação apenas após a ocorrência de incidentes e caracterizado pelo atendimento formal a requisitos de conformidade, para uma abordagem proativa e orientada a resultados. Nesse novo paradigma, torna-se viável monitorar continuamente o nível de proteção cibernética dos órgãos da Administração Pública Federal e adotar medidas preventivas capazes de mitigar falhas antes que estas se concretizem em incidentes de segurança. Em síntese, é preciso complementar as ações relativas ao que é necessário fazer, definido em determinados normativos com o mecanismos de como avaliar se foi realizado e, se os critérios de qualidade foram atingidos, permitindo à APF um maior fortalecendo da resiliência institucional frente a ameaças digitais.
4) **Institucionalizar a cultura de melhoria contínua e Transparência:** Entende-se como recomendável aumentar a transparência dos resultados agregados de cibersegurança governamental, a exemplo de outros países que publicam relatórios anuais de cumprimento de controles e de incidentes em suas agências. Divulgar, de forma consolidada, sem expor vulnerabilidades individuais, o panorama de maturidade e ocorrências no setor público federal pode aumentar a *accountability* e permitir à sociedade e aos gestores acompanhar a evolução (ou eventual estagnação) na proteção dos serviços públicos digitais. Assim, implementar as recomendações poderá auxiliar no amadurecimento do modelo de governança de cibersegurança, hoje predominantemente reativo (atuando somente após incidentes ou constatações do controle) e de conformidade formal, para um modelo proativo e orientado a resultados. Neste caso, passa a ser possível verificar, a qualquer tempo, o nível de proteção cibernética dos órgãos federais e agir antes que as falhas se materializem em incidentes. A adoção dessas medidas poderá contribuir para que a APF possa migrar de um arcabouço normativo prescritivo para uma modelo de governança cibernética orientado à resultados, fortalecendo a resiliência institucional frente às crescentes ameaças digitais.

VII. Limitações da Revisão

Por tratar-se de uma revisão de escopo, o estudo privilegiou o levantamento abrangente de normas e evidências disponíveis, em detrimento de uma análise aprofundada de cada iniciativa local ou caso individual. Assim, esta revisão se limitou à esfera do poder executivo federal, não contemplando pormenorizadamente normas de outros poderes ou esferas, exceto quando influenciam o contexto geral. Pesquisas futuras podem complementar este trabalho com estudos de caso em órgãos específicos, verificando como implementaram as diretrizes e quais resultados obtiveram, bem como desenvolvendo modelos quantitativos para correlacionar a adoção de controles com a redução de incidentes na esfera governamental brasileira. Apesar dessas limitações, acredita-se que os achados aqui apresentados oferecem um panorama a servir de base para

aperfeiçoamentos na política pública de segurança cibernética, um campo cada vez mais crítico para a continuidade e a confiança nos serviços públicos em meio à era digital.
Como extensões e aprofundamentos desta pesquisa, sugerem-se os seguintes trabalhos futuros:

- **Estudos de caso em órgãos federais específicos:** Analisar a implementação real dos normativos mapeados em um conjunto de órgãos, por exemplo, um ministério, uma autarquia e uma universidade federal ou instituto federal, identificando facilitadores e barreiras que encontram na prática, e avaliando empiricamente se a adoção das políticas resultou em melhorias, tais como menor número de incidentes e melhor avaliação em auditorias.
- **Modelos quantitativos de avaliação de impacto:** Desenvolver e testar modelos que quantifiquem a relação entre adoção de controles de segurança e redução de incidentes ou perdas. Por exemplo, utilizar dados históricos (quando disponíveis) para verificar se órgãos que aderiram mais cedo às políticas tiveram menos incidentes significativos. Isso ajudaria a demonstrar concretamente o valor das políticas.
- **Frameworks de maturidade adaptados à APF:** Com base em *frameworks* internacionais, propor um modelo de maturidade em cibersegurança calibrado para a realidade institucional brasileira. Esse modelo poderia ter níveis e critérios ajustados ao tipo de órgão público federal, e ser implementado como piloto em algumas instituições antes de eventual adoção ampla.
- **Barreiras institucionais para adoção de indicadores:** Investigar, sob uma perspectiva de administração pública e gestão, quais são os obstáculos culturais, organizacionais ou políticos que dificultam a adoção de indicadores de desempenho no setor público, especialmente na área de TI/SI. Entender por que, apesar das recomendações, as instituições demoram a incorporar métricas, pode auxiliar no desenho de políticas de mudança.

Este conjunto de pesquisas futuras complementaria o panorama aqui traçado, contribuindo para uma melhor compreensão da implementação e para o desenho de melhorias sustentadas na governança de segurança da informação e de segurança cibernética governamental.

Referências

[1] "Levantamento de governança e gestão de segurança da informação e cibernética na administração pública federal," Brasília, DF, 2021.

[2] Tribunal de Contas da União, "Acórdão 523/2024 - plenário," Decisão oficial do Tribunal de Contas da União, 2024, documento mencionado no arquivo do TCU [64]. [Online]. Available: https://portal.tcu.gov.br/acordaos/523-2024.htm

[3] L. Belli, B. Franqueira, E. Bakonyi, L. Chen, N. Couto, S. Chang, N. Da Hora, and W. B. Gaspar, *Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 2023, edição eletrônica, Licença Creative Commons. [Online]. Available: https://www.researchgate.net/publication/371753843_Ciberseguranca_uma_visao_sistemica_rumo_a_uma_Proposta_de_Marco_Regulatorio_para_um_Brasil_digitalmente_soberano

[4] Presidência da República, "Decreto nº 12.572, de 4 de agosto de 2025," https://www.in.gov.br/en/web/dou/-/decreto-n-12.572-de-4-de-agosto-de-2025-646197612, 2025, Dispõe sobre normas de segurança da informação e cibersegurança no âmbito da Administração Pública Federal.

[5] "Política Nacional de Segurança da Informação (PNSI) — página institucional," Portal Gov.br, Gabinete de Segurança Institucional da Presidência da República (GSI/PR), acesso em: 17 ago. 2025. [Online]. Available: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/politica-nacional-de-seguranca-da-informacao

[6] Presidência da República Federativa do Brasil, "Decreto nº 12.573, de 4 de agosto de 2025: Institui a estratégia nacional de cibersegurança (e-ciber)," Diário Oficial da União, 2025, estabelece a segunda versão da Estratégia Nacional de Cibersegurança, com foco em governança, soberania digital, proteção de infraestruturas críticas e conscientização social. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm

[7] Ministério da Economia - Secretaria de Governo Digital, "A estratégia de governo digital," Governo Federal do Brasil, Brasília, DF, Tech. Rep., 2021, documento oficial disponível no portal Governo Digital. [Online]. Available: https://www.gov.br/governodigital/pt-br/estrategia-de-governo-digital

[8] Brasil - Presidência da República, "Lei nº 9.854, de 27 de novembro de 2019," Diário Oficial da União, Nov. 2019, dispõe sobre [inserir o tema específico da lei]. [Online]. Available: https://www.in.gov.br/en/web/dou/-/lei-n-9.854-de-27-de-novembro-de-2019-232042743

[9] Presidência da República (Brasil), "Decreto nº 11.856, de 26 de dezembro de 2023. institui a política nacional de cibersegurança e o comitê nacional de cibersegurança." 2023, brasília, DF.

[10] G. de Segurança Institucional da Presidência da República, "Instrução normativa gsi/pr nº 1, de 27 de maio de 2020," 2020, brasília, DF.

[11] ——, "Instrução normativa gsi/pr nº 5, de 30 de agosto de 2021: Requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e entidades da administração pública federal," Diário Oficial da União, 2021, dispõe sobre requisitos mínimos de segurança da informação para computação em nuvem na administração pública federal. [Online]. Available: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/computacao-em-nuvem/principais-normas

[12] Gabinete de Segurança Institucional da Presidência da República (GSI/PR), "Instrução normativa gsi/pr nº 6, de 2021," Instrução Normativa, junho 2021, disponível em: https://www.gov.br/secretariageral/pt-br/assuntos/legislacao/IN_GSI_PR_n6_2021.pdf. [Online]. Available: https://www.gov.br/secretariageral/pt-br/assuntos/legislacao/IN_GSI_PR_n6_2021.pdf

[13] "Lei nº 12.527, de 18 de novembro de 2011 — lei de acesso à informação," Diário Oficial da União, 2011, regulamenta o direito constitucional de acesso a informações públicas, estabelecendo o princípio da transparência na gestão pública. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

[14] Presidência da República Federativa do Brasil, "Medida provisória nº 2.200-2, de 24 de agosto de 2001: Institui a infraestrutura de chaves públicas brasileira (icp-brasil)," Diário Oficial da União, 2001, estabelece a ICP-Brasil como base para certificação digital e transações eletrônicas seguras no Brasil. [Online]. Available: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm

[15] "Lei nº 13.709, de 14 de agosto de 2018, lei geral de proteção de dados pessoais (lgpd)," Diário Oficial da União, 2018, institui a Lei Geral de Proteção de Dados Pessoais que regula o tratamento de dados pessoais no Brasil. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[16] Governo Federal do Brasil, "Sistema de administração dos recursos de informação e informática – sisp," Decreto nº 1.048, de 15 de março de 1994, 1994, estrutura consolidada em decretos e instruções que regem a governança de TIC desde 2001. [Online]. Available: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d1048impressao.htm

[17] Ministério da Gestão e da Inovação em Serviços Públicos (Brasil), "Programa de privacidade e segurança da informação (ppsi)," https://www.gov.br/gestao/pt-br/assuntos/governanca-de-dados/ppsi, 2023, secretaria de Governo Digital. Acesso em: 19 ago. 2025.

[18] M. A. F. de Sousa, D. C. da Silva, and H. D. Soares, "Prioritization strategy for measures in the brazilian security framework," *Journal not specified*, 2025, trabalho apresentado em 2025.

[19] A. N. de Telecomunicações (Anatel), "Resolução nº 740, de 21 de dezembro de 2020 — regulamento de segurança cibernética aplicada ao setor de telecomunicações," Diário Oficial da União, 2020, estabelece condutas, procedimentos e regras de cibersegurança para prestadoras de serviços de telecomunicações. [Online]. Available: https://www.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740

[20] B. C. do Brasil, "Resolução bcb nº 85, de 8 de abril de 2021 — política de segurança cibernética e requisitos para contratação de serviços de processamento e armazenamento de dados e computação em nuvem," Diário Oficial da União, 2021, estabelece regras de cibersegurança para instituições de pagamento autorizadas pelo Banco Central do Brasil. [Online]. Available: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o+BCB&numero=85

[21] Presidência da República (Brasil), "Decreto nº 10.748, de 16 de julho de 2021. institui a rede federal de gestão de incidentes cibernéticos." 2021, brasília, DF.

[22] Presidência da República, "Decreto nº 10.474, de 26 de agosto de 2020: Aprova a estrutura regimental da autoridade nacional de proteção de dados (anpd)," Diário Oficial da União, 2020, institui formalmente a ANPD como órgão de proteção de dados pessoais no Brasil conforme a LGPD. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10474.htm

[23] T. de Contas da União, "Relatório de auditoria operacional em governança de segurança da informação," TCU, Tech. Rep., 2022, acórdão n.º 1338/2022-Plenário. [Online]. Available: https://portal.tcu.gov.br

[24] ——, "Levantamento de governança e gestão em tecnologia da informação - igg 2022," TCU, Tech. Rep., 2022. [Online]. Available: https://portal.tcu.gov.br

[25] ——, "Relatório de auditoria operacional - protege-ti 2023: Segurança cibernética e da informação em serviços web, correio eletrônico e resolução de nomes," TCU, Brasília, Tech. Rep. TC 017.413/2023-0, 2023. [Online]. Available: https://portal.tcu.gov.br

[26] ISO/IEC, *ISO/IEC 27032:2023 — Cybersecurity Guidelines*, Std., 2023.

[27] N. I. of Standards and Technology, "Cybersecurity framework 2.0," National Institute of Standards and Technology (NIST), Gaithersburg, MD, Tech. Rep., 2024, cybersecurity Framework 2.0, NIST Cybersecurity White Paper. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29

[28] Ministério da Gestão e da Inovação em Serviços Públicos, "Portaria sgd/mgi nº 4.339, de 10 de agosto de 2023: Índice de maturidade em governança em tecnologia da informação do sisp (igovsisp)," Ministério da Gestão e da Inovação em Serviços Públicos, Brasília, DF, Tech. Rep., 2023, institui o índice iGOVSISP e regulamenta o autodiagnóstico de governança de TI dos órgãos do SISP. [Online]. Available: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/autodiagnostico-igovsisp

[29] A. Bonifácio *et al.*, "Proposta de avaliação da política nacional de segurança da informação por processo de análise hierárquica," *Perspectivas em Ciência da Informação*, vol. 27, no. 4, pp. 38–56, 2022.

[30] A. Azambuja and J. Neto, "Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal," *Revista do Serviço Público (RSP/ENAP)*, vol. 71, no. 3, pp. 660–712, 2020.

Apêndice A
PRISMA 2020 Checklist

A Tabela X apresenta o checklist PRISMA 2020 utilizado nesta revisão sistemática de escopo (Scoping Review), indicando como cada item foi atendido ao longo deste estudo.

Tabela X
PRISMA 2020 Checklist - Aplicação na Revisão

Section and Topic	Item	Checklist Item	Location where item is reported
TITLE			
Title	1	Identify the report as a systematic review.	Title
ABSTRACT			
Abstract	2	Structured abstract following PRISMA Abstract Checklist.	Abstract section
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	Introduction
Objectives	4	Provide explicit statement of objective(s) or question(s) the review addresses.	Introduction (final paragraph)
METHODS			
Eligibility Criteria	5	Specify inclusion and exclusion criteria and how studies were grouped.	Method (Eligibility Criteria subsection)
Information Sources	6	List all sources consulted and dates.	Method (Sources subsection)
Search Strategy	7	Present full search strategies including keywords and limits.	Method (Search Strategy subsection)
Selection Process	8	Describe selection process, reviewers involved, and criteria applied.	Method (Selection Process subsection)
Data Collection Process	9	Methods used to collect data from included documents.	Method (Data Extraction subsection)
Data Items	10a/10b	List and define outcomes and other variables sought.	Method (Data Extraction and PICO subsections)
Study Risk of Bias Assessment	11	Describe methods to assess risk of bias in included studies.	Not assessed (Scoping Review protocol)
Effect Measures	12	Specify effect measures used.	Not applicable (Scoping Review)
Synthesis Methods	13a-f	Methods for qualitative synthesis and presentation.	Method (Analysis subsection and Results)
Reporting Bias Assessment	14	Methods to assess risk of bias due to missing results.	Not assessed (Scoping Review)
Certainty Assessment	15	Methods to assess certainty in body of evidence.	Not assessed (Scoping Review)
RESULTS			
Study Selection	16a	Results of selection process, ideally with a PRISMA flow diagram.	Results section and Figure 1
Study Selection (Exclusions)	16b	Cite studies excluded and reasons.	Not applicable (Scoping Review, broad inclusion)
Study Characteristics	17	Cite each included study/document and its characteristics.	Results (Tables 1 and longtable)
Risk of Bias in Studies	18	Present assessments of risk of bias.	Not assessed (Scoping Review)
Results of Individual Studies	19	For all outcomes, present summary statistics and effect estimates.	Results (Descriptive Synthesis in Tables)
Results of Syntheses	20a-d	Present results of syntheses, heterogeneity analysis, and sensitivity analysis.	Not applicable (Qualitative synthesis only)
Reporting Biases	21	Assessments of reporting bias for each synthesis.	Not assessed (Scoping Review)
Certainty of Evidence	22	Assessment of certainty in body of evidence.	Not assessed (Scoping Review)
DISCUSSION			
Discussion	23a-d	Interpretation of results, limitations of evidence, review process limitations, and implications for practice/policy.	Discussion section and Limitations subsection
OTHER INFORMATION			
Registration	24a	Provide registration information (if registered).	Not registered
Protocol	24b	Indicate where the review protocol can be accessed.	No protocol prepared
Protocol Amendments	24c	Describe amendments to protocol.	Not applicable
Support	25	Sources of funding and role of funders.	No external funding
Competing Interests	26	Declare any competing interests.	None declared