Levantamento da Percepção dos Princípios da ISO 31000:2018 para Proposição de Medidas de Controle de Gestão de Riscos de Segurança da Informação no Setor Público

Patrícia Araújo de Oliveira[1], **Rafael Rabelo Nunes**[1]

[1]Especialização em Privacidade e Segurança da Informação
Programa de Pós-Graduação em Engenharia Elétrica – Universidade de Brasília (UnB)
DF – Brazil

patricia.araoli@gmail.com, rafaelrabelo@unb.br

Resumo. *A gestão de riscos de segurança da informação é amplamente reconhecida por organismos internacionais e nacionais como eixo estratégico para assegurar resiliência institucional, continuidade de serviços e confiança da sociedade. No Brasil, embora diferentes instrumentos normativos estabeleçam diretrizes e responsabilidades para o setor público, existe o desafio de fomentar a operacionalização da gestão de riscos em todos os órgãos. Este artigo apresenta uma pesquisa exploratória aplicada a 75 profissionais da administração pública, majoritariamente da esfera federal, com base em questionário estruturado a partir dos princípios da ISO 31000:2018, com o objetivo de aferir a percepção quanto à condução da gestão de riscos em segurança da informação nos órgãos públicos. A análise das respostas evidenciou a percepção de boas práticas institucionais, mas também fragilidades relevantes, como indefinições sobre a revisão periódica de riscos, lacunas na comunicação transversal e baixa valorização de fatores humanos e culturais. Com base nessas percepções, foram propostas medidas de controle alinhadas ao Programa de Privacidade e Segurança da Informação (PPSI) de modo a apoiar o avanço de práticas de gestão de riscos, relacionadas aos princípios da ISO 31000:2018, no setor público brasileiro.*

1. Introdução

A Gestão de Riscos de Segurança da Informação (SI) é amplamente reconhecida por organismos internacionais - entre eles a Agência da União Europeia para a Cibersegurança (*European Union Agency for Cybersecurity* – ENISA)[1], a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[2] e a *International Organization for Standardization* (ISO)[3] - como elemento essencial para assegurar resiliência institucional, continuidade de serviços e confiança da sociedade. Em especial, a ISO 31000:2018 [ISO 2018] busca orientar a gestão de riscos e estabelecer princípios fundamentais que norteiam sua aplicação. Na literatura, diversos autores [Wallace and Keil 2004, Kutsch and Hall 2009, Olechowski et al. 2016,

[1]https://www.enisa.europa.eu
[2]https://www.oecd.org
[3]https://www.iso.org

de Bakker et al. 2010] reforçam a relevância da gestão de riscos, destacando que sua aplicação eficaz pode determinar o sucesso ou fracasso de projetos e organizações.

No Brasil, o tema de Gestão de Riscos de SI tem se consolidado em diferentes normativos, como a Instrução Normativa GSI/PR nº 3/2021 [GSI/PR 2021], a Política Nacional de Segurança da Informação (PNSI 2025) [Brasil 2025a] e a Portaria SGD/MGI nº 852/2023, que instituiu o Programa de Privacidade e Segurança da Informação (PPSI) [SGD/MGI 2023]. A IN nº 3/2021 constitui o principal normativo operacional, ao estabelecer processos obrigatórios para mapeamento de ativos, análise e tratamento de riscos de SI, continuidade de negócios, gestão de mudanças e avaliação de conformidade. A PNSI 2025 fornece a base estratégica da segurança da informação no país, consolidando princípios e objetivos que reforçam a centralidade da gestão de riscos. Entre seus princípios, destaca-se o inciso VI, que estabelece "o foco na gestão de riscos", e, entre seus objetivos, o inciso III, que dispõe sobre "estimular a gestão de riscos, a proteção e o controle da informação". O PPSI, por sua vez, tem como foco elevar a maturidade dos órgãos em privacidade e segurança da informação, estabelecendo entre seus objetivos o aprimoramento da gestão de riscos relacionados a essas áreas, de modo a apoiar a tomada de decisão e a alocação eficiente de recursos. Em conjunto, esses (e outros) instrumentos contribuem para direcionar a gestão de riscos de segurança da informação no setor público, articulando diretrizes estratégicas, mecanismos operacionais e parâmetros de governança.

Observa-se, contudo, um dilema recorrente: a busca por uniformidade regulatória, embora necessária para consolidar práticas comparáveis, nem sempre contempla a diversidade de contextos organizacionais. Soma-se a isso a heterogeneidade dos níveis de maturidade em gestão de riscos entre os órgãos, o que torna ainda mais desafiadora a implementação de diretrizes comuns. Esse cenário evidencia uma tensão entre a padronização, que favorece a governança, e a flexibilidade, que possibilita práticas ajustadas às realidades institucionais. O desafio consiste em desenvolver mecanismos de acompanhamento e apoio capazes de orientar sem impor prescrições rígidas, mas que também considerem as diferentes etapas de evolução das instituições.

Diante desse contexto, o presente artigo tem como propósito verificar a percepção de profissionais da administração pública sobre os princípios da ISO 31000:2018, buscando compreender em que medida tais diretrizes são incorporadas às práticas institucionais de gestão de riscos de segurança da informação. A pesquisa concentra-se em três eixos: (i) analisar a mentalidade de riscos no setor público; (ii) avaliar o grau de aderência institucional aos princípios da ISO 31000:2018; e (iii) propor medidas de controle alinhadas aos princípios da ISO 3100:2018 de forma a equilibrar a padronização metodológica com a adaptação às especificidades de cada órgão.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta o referencial teórico, com ênfase nos princípios da ISO 31000:2018, em sua integração com a ISO/IEC 27005:2022 e nos principais normativos nacionais aplicáveis; a Seção 3 descreve o contexto da gestão de riscos de segurança da informação no setor público brasileiro; a Seção 4 detalha a metodologia adotada; a Seção 5 expõe os resultados obtidos; a Seção 6 reúne as proposições de medidas de controle derivadas da análise; e, por fim, a Seção 7 apresenta as considerações finais.

2. Referencial Teórico

2.1. Princípios da ISO 31000:2018

A ISO 31000:2018 [ISO 2018] é uma norma internacional que estabelece diretrizes para a gestão de riscos em qualquer tipo de organização, independentemente de porte, setor ou natureza. Seu propósito central é apoiar a criação e a proteção de valor, fornecendo um referencial capaz de estruturar processos decisórios mais seguros, resilientes e alinhados às estratégias institucionais.

No campo específico da segurança da informação, a ISO/IEC 27005:2022 [ISO 2022] complementa a ISO 31000 ao detalhar processos de identificação, análise, avaliação e tratamento de riscos, articulando-se diretamente com a família ISO/IEC 27000 [ISO 2018]. Essa família inclui a ISO/IEC 27001:2022 [ISO 2022a], que define requisitos para Sistemas de Gestão de Segurança da Informação (SGSI), e a ISO/IEC 27002:2022 [ISO 2022b], que apresenta controles de referência amplamente adotados. Dessa forma, a ISO/IEC 27005 atua como elo metodológico entre os princípios gerais da ISO 31000 e a implementação prática dos controles normativos de segurança da informação.

A ISO 31000:2018 não define etapas prescritivas, mas estabelece oito princípios fundamentais que orientam a gestão de riscos e asseguram que ela seja conduzida de maneira consistente, eficaz e legitimada [Purdy 2010]. A literatura reforça que sua adoção exige adequação cultural e estrutural, sob pena de reduzir-se a um exercício meramente formal [Olechowski et al. 2016]. A seguir, são apresentados os oito princípios com maior detalhamento.

1. Integrada

A gestão de riscos deve ser parte essencial da governança, da estratégia e dos processos organizacionais, não sendo tratada como atividade paralela. A responsabilidade recai sobre a alta direção e deve permear todos os níveis hierárquicos e atividades, desde o planejamento estratégico até a execução operacional. A integração evita que a gestão de riscos seja percebida apenas como obrigação burocrática e reforça seu papel como processo que gera valor e apoia decisões críticas [ABNT 2015]. A integração também fortalece a cultura institucional de riscos, exigindo comprometimento da liderança, alinhamento aos processos decisórios e envolvimento das partes interessadas [Vieira and Barreto 2019, Moreira and Lima 2021].

2. Estruturada e Abrangente

Este princípio exige que a gestão de riscos seja conduzida de maneira sistemática, padronizada e documentada. A estruturação garante consistência, comparabilidade e transparência, enquanto a abrangência assegura que todos os níveis organizacionais e tipos de riscos sejam contemplados [ABNT 2015]. Políticas claras, critérios definidos e processos bem estabelecidos possibilitam decisões informadas, mitigando vieses e inconsistências [Filypova 2019]. Além disso, a adoção de uma abordagem estruturada e abrangente favorece o alinhamento da gestão de riscos com os objetivos estratégicos e a governança institucional.

3. Personalizada

A personalização implica que a gestão de riscos deve ser ajustada às características próprias da organização, levando em conta o contexto interno e externo, a cultura organizacional, as partes interessadas e os objetivos institucionais. Não há modelo único de gestão de riscos aplicável a todas as instituições. Cada organização deve adaptar metodologias, categorias de riscos e instrumentos de análise à sua realidade [Martins 2018]. Esse princípio garante relevância prática, evita o uso de modelos genéricos pouco eficazes e promove maior legitimidade das ações de gerenciamento.

4. Inclusiva

A inclusão envolve a participação ativa e o engajamento das partes interessadas, garantindo legitimidade, transparência e colaboração. O processo de gestão de riscos deve incorporar percepções, conhecimentos e expectativas de diferentes atores — incluindo servidores, gestores, fornecedores, órgãos de controle e a sociedade [Olechowski et al. 2016]. A consulta e o diálogo aumentam a qualidade da análise de riscos e fortalecem a confiança nos resultados obtidos, além de promover uma cultura de corresponsabilidade e engajamento coletivo [Oliveira 2017, Ndlela 2019].

5. Dinâmica

O princípio da dinamicidade reconhece que riscos e contextos mudam continuamente. Por isso, a gestão de riscos deve ser adaptativa, proativa e capaz de responder a transformações internas e externas [ABNT 2015]. A natureza mutável dos riscos exige monitoramento contínuo, revisões periódicas e ajustes ágeis dos planos de ação [Zou et al. 2017]. Uma abordagem dinâmica evita que o gerenciamento se torne obsoleto e fortalece a capacidade de antecipar cenários emergentes, tornando a organização mais resiliente [Silva 2019].

6. Melhor Informação Disponível

As decisões de risco devem apoiar-se em informações confiáveis, atualizadas e verificáveis, provenientes tanto de dados históricos quanto de projeções futuras [ABNT 2015]. A qualidade da informação é determinante para a eficácia do processo, exigindo análise crítica de fontes, confiabilidade, precisão e relevância [Ilbahar and Cebi 2018, Andrade and Figueiredo 2017]. O uso da melhor informação disponível deve ser acompanhado do reconhecimento de limitações e incertezas, evitando uma falsa sensação de certeza absoluta.

7. Fatores Humanos e Culturais

A gestão de riscos deve considerar que valores, percepções, condutas e competências das pessoas influenciam diretamente a sua efetividade [ABNT 2015]. Esse princípio reconhece a centralidade do fator humano, exigindo investimento em treinamento, conscientização, comunicação e engajamento. A cultura organizacional deve ser fortalecida para que os servidores se percebam como corresponsáveis pela gestão de riscos, em vez de tratar o tema como responsabilidade exclusiva de áreas técnicas [Vieira and Barreto 2019, Souza 2011].

8. Melhoria Contínua

A gestão de riscos é um processo iterativo que deve incorporar constantemente lições aprendidas de incidentes, auditorias e avaliações internas [ABNT 2015]. A melhoria contínua promove a evolução permanente das práticas institucionais, ajustando controles e metodologias à medida que novos desafios surgem [Olechowski et al. 2016]. Esse princípio garante que a gestão de riscos permaneça atualizada, eficiente e integrada às estratégias organizacionais.

Os oito princípios da ISO 31000:2018 oferecem um arcabouço que orienta a gestão de riscos de forma consistente, eficaz e adaptada a diferentes contextos organizacionais. No campo da segurança da informação, a ISO/IEC 27005:2022 constitui o principal guia metodológico para operacionalizar esses princípios, conectando-os aos requisitos da ISO/IEC 27001:2022 e aos controles recomendados pela ISO/IEC 27002:2022, assegurando uma abordagem prática e aderente às melhores práticas internacionais.

A Tabela 1 sintetiza os oito princípios, destacando suas definições centrais segundo a ISO 31000:2018 e exemplos de aplicação prática nas organizações, conforme levantado por Gonçalves (2025) [Gonçalves 2025].

Table 1. Os oito princípios da ISO 31000:2018 — Definição e aplicação prática

Princípio	Definição segundo a ISO 31000:2018	Aplicação prática nas organizações
1. Integrada	A gestão de riscos deve ser parte essencial da governança, da estratégia e dos processos organizacionais.	Envolvimento da alta direção; integração em planos estratégicos, processos de decisão e gestão de mudanças; cultura organizacional baseada em riscos.
2. Estruturada e Abrangente	Deve ser conduzida de forma sistemática, coerente e comparável, abrangendo todos os níveis da organização.	Definição de políticas e critérios de risco; padronização de metodologias; maior transparência e comparabilidade de resultados.
3. Personalizada	Deve ser adaptada ao contexto interno e externo, considerando cultura, recursos e objetivos organizacionais.	Ajuste de metodologias às especificidades institucionais; categorização de riscos própria; adequação a restrições orçamentárias e de pessoal.
4. Inclusiva	Deve envolver as partes interessadas, assegurando legitimidade, transparência e colaboração.	Participação de gestores, servidores, fornecedores e sociedade; consultas públicas; comitês multidisciplinares de riscos.
5. Dinâmica	Deve acompanhar mudanças internas e externas, reconhecendo a natureza mutável dos riscos.	Monitoramento contínuo; revisões periódicas dos planos de risco; respostas ágeis a novas ameaças ou oportunidades.
6. Melhor Informação Disponível	Deve basear-se em informações confiáveis, históricas, atuais e projeções futuras, reconhecendo limitações e incertezas.	Uso de *logs*, relatórios, auditorias, *benchmarks* e boletins técnicos; análise crítica da qualidade e confiabilidade das informações.
7. Fatores Humanos e Culturais	Deve reconhecer que percepções, condutas e competências das pessoas influenciam a efetividade da gestão de riscos.	Capacitação contínua; campanhas de conscientização; engajamento dos servidores; redução da resistência à mudança.
8. Melhoria Contínua	Deve incorporar lições aprendidas, auditorias e avaliações para promover evolução permanente.	Realização de *post-mortems*, auditorias periódicas, indicadores de desempenho; atualização contínua de controles e políticas.

Fonte: Adaptado de ISO 31000:2018 [ISO 2018], ISO 31004:2015 [ABNT 2015], Olechowski et al. (2016) [Olechowski et al. 2016], Vieira e Barreto (2019) [Vieira and Barreto 2019], Gonçalves (2025) [Gonçalves 2025].

2.2. Normativos Brasileiros em Segurança da Informação

A Instrução Normativa número 3 de 2021, do Gabinete de Segurança Institucional da Presidência da República (IN GSI/PR nº 3/2021) [GSI/PR 2021], constitui o principal normativo operacional sobre gestão de riscos de segurança da informação no setor público federal. Ela determina que os órgãos implementem cinco processos obrigatórios: (i) mapeamento de ativos de informação, (ii) gestão de riscos de segurança da informação, (iii) gestão de continuidade de negócios, (iv) gestão de mudanças em segurança da informação e (v) avaliação de conformidade.

Para viabilizar esses processos, a norma exige instrumentos como o Plano de Gestão de Riscos de Segurança da Informação e o Relatório de Tratamento de Riscos, além de atribuir responsabilidades à alta administração, gestores e equipes técnicas. Embora forneça diretrizes estruturantes, não define uma metodologia única, permitindo que os órgãos se apoiem em referenciais como a ISO 31000:2018 [ISO 2018] e a ISO 27005:2022 [ISO 2022]. Essa flexibilidade amplia a adaptação, mas também gera heterogeneidade na aplicação entre instituições. A IN nº 3/2021 complementa a IN GSI/PR nº 1/2020 [GSI/PR 2020], que institui a Política de Segurança da Informação na Administração Pública Federal, a qual já previa a necessidade de gestão de riscos, mas de forma mais genérica.

A PNSI, atualizada pelo Decreto nº 12.572/2025 [Brasil 2025a], fornece a base estratégica e política da segurança da informação no país. Seu objetivo é assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação em qualquer meio. Entre seus princípios fundamentais, está a gestão de riscos, considerada eixo estruturante da política nacional. Sua governança é atribuída ao GSI/PR, por meio do Comitê Gestor de Segurança da Informação.

A PNSI reafirma a centralidade da gestão de riscos, mas não detalha mecanismos operacionais, o que demanda articulação com normas técnicas (ISO 31000:2018, ISO 27005:2022) e normativos (IN nº 3/2021). Nesse contexto, o Decreto nº 9.203/2017 [Brasil 2017], que institui a Política de Governança da Administração Pública Federal, reforça a gestão de riscos como princípio fundamental da governança pública, aplicável também à segurança da informação.

O PPSI é um programa de governança voltado a elevar a maturidade e a resiliência em privacidade e segurança da informação na Administração Pública Federal, instituído pela Portaria SGD/MGI nº 852/2023 [SGD/MGI 2023]. Ele estrutura-se em cinco dimensões complementares: governança, metodologia, pessoas, tecnologia e maturidade.

O PPSI possibilita aos órgãos do SISP uma visão estruturada de suas capacidades, funcionando como guia prático para transformar exigências normativas em ações concretas. Entre seus objetivos, destaca-se o fortalecimento da gestão de riscos de privacidade e segurança da informação, em alinhamento à IN GSI/PR nº 3/2021, à PNSI 2025 e também à IN SGD/ME nº 117/2020 [SGD/ME 2020], que trata da governança de TIC e prevê a consideração de riscos como elemento essencial para a gestão e o planejamento de tecnologia no setor público.

Além dos instrumentos já detalhados, o cenário brasileiro conta ainda com marcos estratégicos complementares. A Estratégia Nacional de Cibersegurança (E-Ciber) [Brasil 2025b] estabelece diretrizes para o fortalecimento da resiliência cibernética nacional e inclui a gestão de riscos entre o conjunto de medidas de cibersegurança necessárias para proteger o ciberespaço, bem como os ciberativos de usuários e organizações. A Política Nacional de Cibersegurança (PNCiber) [Brasil 2024a] organiza princípios e objetivos para a atuação no ciberespaço, destaca-se, entre eles, o inciso V, que prevê "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". No campo da transformação digital, a Estratégia Federal de Governo Digital (EFGD), instituída pelo Decreto nº 12.198/2024 [Brasil 2024c], es-

tabelece iniciativas de médio prazo para o governo federal, incluindo o eixo "Governo Confiável e Seguro". De forma articulada, a Estratégia Nacional de Governo Digital (ENGD), formalizada pelo Decreto nº 12.069/2024 e Portaria SGD/MGI nº 4.248/2024 [Brasil 2024b, SGD/MGI 2024], amplia essas diretrizes para todos os entes federados, priorizando eficiência, transparência, participação cidadã, privacidade e segurança.

A Tabela 2 apresenta uma síntese dos principais instrumentos normativos relacionados à gestão de riscos e segurança da informação, agrupando normas internacionais e políticas nacionais.

Table 2. Principais instrumentos normativos relacionados à gestão de riscos e segurança da informação

Instrumento	Natureza / Abrangência	Finalidade principal
ISO 31000:2018 [ISO 2018]	Norma internacional (gestão de riscos)	Estabelece princípios gerais para a gestão de riscos em qualquer organização, com foco na criação e proteção de valor.
ISO/IEC 27005:2022 [ISO 2022]	Norma internacional (segurança da informação)	Fornece metodologia específica para identificação, análise, avaliação e tratamento de riscos em SI, conectando a ISO 31000 com a série ISO 27000.
ISO/IEC 27001:2022 [ISO 2022a]	Norma internacional (SGSI)	Define requisitos para implantação, manutenção e melhoria de Sistemas de Gestão de Segurança da Informação (SGSI).
ISO/IEC 27002:2022 [ISO 2022b]	Norma internacional (controles de SI)	Apresenta boas práticas e controles de referência em segurança da informação.
Decreto nº 9.203/2017 [Brasil 2017]	Decreto (Brasil)	Institui a Política de Governança da Administração Pública Federal, estabelecendo a gestão de riscos como princípio fundamental da boa governança, aplicável também à segurança da informação.
IN GSI/PR nº 1/2020 [GSI/PR 2020]	Normativo estratégico (Brasil)	Institui a Política de Segurança da Informação no âmbito da APF, prevendo a necessidade de gestão de riscos de forma geral, com foco em diretrizes e governança.
IN GSI/PR nº 3/2021 [GSI/PR 2021]	Normativo operacional (Brasil)	Determina processos obrigatórios de gestão de riscos de SI na APF: mapeamento de ativos, análise de riscos, continuidade de negócios, gestão de mudanças e avaliação de conformidade.
IN SGD/ME nº 117/2020 [SGD/ME 2020]	Normativo de governança de TIC (Brasil)	Define diretrizes de governança e gestão de TIC no setor público, incluindo a obrigatoriedade da consideração de riscos no planejamento e execução de ações de tecnologia.
Política Nacional de Segurança da Informação (PNSI 2025) [Brasil 2025a]	Política estratégica (Brasil)	Define princípios e objetivos nacionais de SI, reafirmando a gestão de riscos como eixo estruturante e atribuindo governança ao GSI/PR.
Programa de Privacidade e Segurança da Informação (PPSI) [SGD/MGI 2023]	Programa governamental (Brasil)	Estabelece framework de governança com dimensões de governança, metodologia, pessoas, tecnologia e maturidade para órgãos do SISP, incluindo objetivo específico de fortalecimento da gestão de riscos.
Estratégia Nacional de Cibersegurança (E-Ciber) [Brasil 2025b]	Estratégia nacional (Brasil)	Define diretrizes para aumentar a resiliência cibernética nacional.
Política Nacional de Cibersegurança (PNCiber 2024) [Brasil 2024a]	Política nacional (Brasil)	Organiza princípios, objetivos e eixos de atuação para proteção do ciberespaço.
Estratégia Federal de Governo Digital (EFGD) [Brasil 2024c]	Estratégia nacional (Brasil)	Estabelece objetivos estratégicos e iniciativas para a transformação digital no governo federal, incluindo o eixo "Governo Confiável e Seguro".
Estratégia Nacional de Governo Digital (ENGD) [Brasil 2024b, SGD/MGI 2024]	Estratégia nacional (Brasil)	Define diretrizes de médio e longo prazo para transformação digital entre entes federados, priorizando eficiência, transparência, participação cidadã, privacidade e segurança.

Nota: A tabela agrupa instrumentos internacionais e nacionais, evidenciando sua complementaridade para estruturar a gestão de riscos em segurança da informação no setor público brasileiro.

3. Contexto

A segurança da informação no setor público brasileiro é um campo em constante evolução, marcado pela consolidação de referenciais normativos internacionais, como a

ISO 31000:2018 e a ISO 27005:2022, e pela adoção de normativos nacionais, como a IN GSI/PR nº 3/2021 e a PNSI 2025. Esse debate tem sido reforçado pela literatura, que tem buscado compreender tanto os avanços quanto as fragilidades na institucionalização das práticas de gestão de riscos de segurança da informação.

Batista [Batista 2022] propôs o MISASI STI, um modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES), baseado no OCTAVE Forte, destacando a necessidade de apoio institucional da alta administração. No mesmo sentido, Vasconcelos et al. [Vasconcelos et al. 2025] adaptaram a ISO/IEC 27005:2022 com uso de *Business Process Management* (BPM), oferecendo um processo mais claro e replicável. Lisboa [Lisboa 2021] enfatiza a aplicação prática da ISO/IEC 27005 em empresas privadas, mostrando como melhorias incrementais na infraestrutura reduzem riscos e aumentam a resiliência operacional. De forma complementar, Cruz [Cruz 2025] discute o papel do Sistema de Gestão de Segurança da Informação (SGSI) e *frameworks* como a ISO 27001, reforçando a importância de ferramentas como matriz de probabilidade e impacto e análise SWOT para reduzir incidentes e fortalecer a resiliência organizacional.

Silva, Souza Neto e Orlandi [Silva et al. 2025] apresentaram um modelo de maturidade em governança de SI para a Administração Pública Federal, aplicável a diferentes órgãos, e alinhado à ISO/IEC 27002. Furlan [Furlan 2021] reforça a importância de comitês de riscos e mecanismos de governança para superar barreiras institucionais. No campo do Judiciário, Alves, Queiroz e Nunes [Alves et al. 2023] analisam a estrutura dos tribunais à luz do Modelo das Três Linhas, destacando a fragilidade da segunda linha de defesa em diversos órgãos e a relevância de estruturas apartadas de SI para fortalecer a resiliência institucional. De forma aplicada, Cancellier [Cancellier 2020] realizou um estudo pioneiro no Tribunal de Contas da União (TCU) sobre a gestão de riscos de segurança da informação, identificando fragilidades em controles internos, na institucionalização da segunda linha de defesa e na atualização periódica dos inventários de riscos. Esse estudo é relevante porque mostra, de maneira concreta, os desafios enfrentados mesmo em órgãos de controle.

Aceiro [Aceiro 2022] evidenciou a importância da dimensão pessoal, incluindo autoconsciência e ética na alta gestão, como fator de resiliência em programas de integridade. Dorneles, Araújo e Costa [Dorneles et al. 2024] destacaram riscos e critérios de segurança da informação na contratação de serviços de nuvem pela Administração Pública Federal. No campo tecnológico emergente, Lento [Lento 2024] desenvolveu um modelo adaptativo de gestão de riscos em IoT, utilizando lógica probabilística, redes Bayesianas e cadeias de Markov. Esse trabalho mostra como riscos em ecossistemas distribuídos e críticos, como saúde e cadeias de suprimento, exigem abordagens dinâmicas e adaptativas.

Silva et al. [Silva et al. 2021] realizaram uma revisão bibliométrica da produção nacional sobre riscos no setor público, identificando lacunas na aplicação prática. Nesse contexto, Gonçalves [Gonçalves 2025] construiu um instrumento inicial com 48 assertivas para avaliar a aderência dos órgãos da Administração Pública Federal aos princípios da ISO 31000:2018. O estudo foi elaborado a partir de revisão bibliográfica e de evidências empíricas coletadas por meio de entrevistas e questionários, dialogando com lacunas já destacadas em pesquisas internacionais sobre a baixa institucionalização da

gestão de riscos [Wallace and Keil 2004, Kutsch and Hall 2009]. Em continuidade, Gama [Gama 2025] realizou a validação de conteúdo [Polit and Beck 2006] desse instrumento junto a especialistas em tecnologia da informação, segurança da informação e gestão de riscos, resultando na reformulação de 18 assertivas e na validação unânime de 6. Essa etapa reforçou a importância de metodologias sistematizadas e legitimadas, em consonância com recomendações de Olechowski et al. [Olechowski et al. 2016] e de Bakker et al. [de Bakker et al. 2010], que defendem a necessidade de instrumentos empíricos validados para a profissionalização da área.

O estudo de Olechowski et al. [Olechowski et al. 2016] é particularmente relevante por analisar empiricamente os 11 princípios da então ISO 31000 de 2009 (ISO 31000:2009) [International Organization for Standardization 2009] em projetos de engenharia, evidenciando que sua adoção está associada a maior estabilidade organizacional e ao alcance de objetivos de custo, prazo, desempenho e satisfação do cliente. Os autores identificaram dois agrupamentos de princípios: (i) integração organizacional (criação de valor, integração a processos, apoio à decisão e melhoria contínua) e (ii) estrutura do processo (sistematização, melhor informação, adaptação, inclusão e dinamicidade). Essa categorização reforça a relevância dos princípios como medidas de maturidade e como caminho para a profissionalização da gestão de riscos, mais do que como prescrições rígidas de métodos.

Esses trabalhos de Gonçalves (2025) e Gama (2025) consolidaram um instrumento robusto, fundamentado na norma ISO 31000:2018, criando condições para aplicação de assertivas validadas acerca dos princípios da ISO 31000:2018. Este artigo dá prosseguimento a essa linha, aplicando o questionário validado a profissionais da administração pública, de forma exploratória, para identificar padrões de fragilidade e propor medidas de controle alinhadas aos princípios da ISO 31000:2018.

Table 3. Evolução dos estudos sobre gestão de riscos de segurança da informação no setor público brasileiro

Estudo	Objetivo principal	Metodologia	Contribuição	Limitações
Gonçalves (2025)	Construir um instrumento inicial para avaliar a aderência à ISO 31000:2018 na Administração Pública Federal	Revisão bibliográfica + entrevistas e questionários exploratórios	Criação de 48 assertivas organizadas por princípio da ISO 31000:2018	Necessidade de validação de conteúdo
Gama (2025)	Validar o instrumento proposto por Gonçalves	Validação de conteúdo por especialistas (Polit & Beck, 2006)	Reformulação de 18 assertivas e validação unânime de 6, resultando em instrumento mais robusto	Estudo restrito à etapa de validação
Este artigo (2025)	Aplicar o instrumento validado e propor medidas de controle	Pesquisa exploratória com 75 respondentes + análise normativa	Diagnóstico preliminar de fragilidades e proposição de medidas	Potencial de orientar políticas e práticas institucionais

4. Metodologia

Este estudo caracteriza-se como uma pesquisa exploratória e descritiva, de abordagem quantitativa e qualitativa, com o objetivo de identificar fragilidades e avanços nas práticas de gestão de riscos de segurança da informação no setor público brasileiro. A pesquisa foi conduzida por meio da aplicação de um questionário estruturado, baseado nos princípios

da ISO 31000:2018 e previamente validado em estudos anteriores [Gonçalves 2025, Gama 2025]. O instrumento é composto por 48 assertivas distribuídas entre os oito princípios da norma.

4.1. Amostra

O questionário foi disponibilizado eletronicamente a profissionais de diferentes órgãos e entidades da administração pública. Foram obtidas 75 respostas válidas, contemplando majoritariamente participantes da esfera federal (96%), com pequena participação da esfera estadual (4%) e ausência de representantes da esfera municipal. Quanto ao poder, a amostra reuniu representantes do Executivo (79%) e do Judiciário (19%), enquanto 3% não informaram.

A diversidade de perfis profissionais reforça a representatividade da amostra: 25% atuam como analistas ou técnicos de segurança da informação, 15% como gestores de TI, 12% como gestores de segurança da informação, e 7% em funções ligadas diretamente à privacidade (encarregados e técnicos). Outros 41% desempenham papéis correlatos. Observou-se ainda ampla variação no tempo de experiência: 25% possuem menos de três anos de atuação, 19% entre três e seis anos, 8% entre seis e nove anos e 24% mais de nove anos, enquanto 24% afirmaram não atuar diretamente em atividades da área.

4.2. Instrumento de Coleta

As assertivas foram avaliadas em escala Likert de seis pontos:

- 0 — Não sei/Não quero responder;
- 1 — Discordo totalmente;
- 2 — Discordo;
- 3 — Não concordo, nem discordo;
- 4 — Concordo;
- 5 — Concordo totalmente.

Para fins de análise quantitativa, as categorias foram agrupadas como: (i) Concordam (4 e 5), (ii) Discordam (1 e 2), (iii) Não concordam, nem discorda (3) e (iv) Não sabem/Não querem responder (0). Para fins de análise qualitativa, em muitos casos, foi considerada a soma das respostas (iii) Não concordam, nem discorda (3) e (iv) Não sabem/Não querem responder, de modo a identificar situações de indefinição ou ausência de posicionamento por parte dos respondentes.

4.3. Procedimentos de Análise

A análise dos dados foi conduzida em duas etapas:

1. Quantitativa: cálculo das frequências absolutas e relativas das respostas, organizadas por princípio da ISO 31000:2018, permitindo identificar padrões de concordância, discordância, neutralidade e ausência de opinião.
2. Qualitativa: destaque das assertivas com maiores índices de discordância, neutralidade ou ausência de resposta, tratadas como fragilidades potenciais e transformadas em perguntas orientadoras para proposição de medidas de controle.

As tabelas da Seção 5 apresentam a distribuição das respostas por assertiva e princípio, sintetizando o diagnóstico obtido.

5. Resultados

O questionário contou com a participação de 75 respondentes (*N=75*). Em relação à formação acadêmica, a maioria possui especialização (63%, 47 respondentes), seguida por mestrado (21%, 16), graduação (11%, 8) e doutorado (5%, 4). Quanto à esfera institucional, 96% (72) atuam em órgãos da esfera federal e 4% (3) na esfera estadual, não havendo representantes da esfera municipal. Em relação ao poder, 79% (59) pertencem ao Executivo e 19% (14) ao Judiciário, enquanto 3% (2) não informaram.

No que diz respeito ao papel desempenhado nas organizações, observa-se diversidade de funções. Os analistas ou técnicos de segurança da informação correspondem a 25% (19), seguidos por gestores de TI (15%, 11) e gestores de segurança da informação (12%, 9). Os encarregados de proteção de dados (3%, 2) e analistas/técnicos em privacidade (4%, 3) são minoria, enquanto 41% (31) atuam em outras funções relacionadas.

A estrutura institucional dos órgãos também foi analisada. A maioria já dispõe de mecanismos formais de governança em segurança da informação: 92% (69) possuem políticas e normas internas, 84% (63) contam com gestor de segurança designado, 80% (60) têm comitê gestor instituído e o mesmo percentual (80%) dispõe de equipe de resposta a incidentes cibernéticos (ETIR ou equivalente). Apesar disso, apenas 44% (33) indicaram participação efetiva da alta administração na implementação de políticas, e 3% (2) afirmaram que sua instituição não possui nenhuma dessas alternativas.

Em relação ao tempo de atuação, 25% (19) possuem menos de três anos de experiência, 19% (14) entre três e seis anos, 8% (6) entre seis e nove anos e 24% (18) mais de nove anos. Outros 24% (18) afirmaram não atuar diretamente em atividades ligadas à área de segurança ou privacidade.

Por fim, quanto à gestão de riscos, 33% (25) declararam atuar especificamente em riscos de privacidade e segurança da informação, 11% (8) em riscos de negócio e 25% (19) já atuaram anteriormente, mas não de forma contínua. Entretanto, 31% (23) afirmaram nunca ter atuado na área.

5.1. Princípio Integrada

O princípio integrada estabelece que a gestão de riscos deve estar incorporada a todas as atividades organizacionais, permeando processos, estruturas de governança e rotinas operacionais. A Tabela 4 apresenta a distribuição das respostas para as seis assertivas relacionadas a este princípio.

De forma geral, os resultados revelam percepções de concordância quanto ao grau de integração da gestão de riscos na instituição. Destacam-se a busca por integrar iniciativas de segurança da informação aos mecanismos de governança e ao planejamento estratégico (55% de concordância) e a existência de políticas formais que orientam a gestão de riscos em projetos e processos (52%). Esses achados indicam que parte significativa das instituições aparentemente já reconhece a importância de estruturar mecanismos formais de integração.

No entanto, existem pontos relevantes a serem destacados. A assertiva sobre a consideração da gestão de riscos nos processos das principais áreas, apesar de ter apresentado 35% de concordância, apresentou 32% de discordância, sendo este o maior índice de discordância entre as seis, sugerindo que a prática não está plenamente consolidada como atividade transversal. Além disso, observa-se uma proporção expressiva de respostas neutras (23–24%) em temas centrais, como o envolvimento do comitê de segurança e a participação de líderes de diferentes áreas. Essa tendência à neutralidade pode refletir desconhecimento, baixa visibilidade ou mesmo incerteza quanto à efetiva incorporação da gestão de riscos no cotidiano institucional.

Em síntese, os achados apontam para um cenário positivo para este princípio, porém que requer atenção: coexistem avanços em políticas formais e integração estratégica, mas ainda há desafios significativos na consolidação da gestão de riscos como prática rotineira e transversal a todas as áreas das instituições.

Table 4. Distribuição das respostas — Princípio 1: Integrada (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
Sempre que possível as decisões estratégicas da instituição consideram os resultados das análises de riscos levantadas pela equipe de TI e por outras áreas.	41% (31)	25% (19)	19% (14)	15% (11)
O comitê (ou grupo responsável) de Segurança da Informação busca envolver setores relevantes da instituição na identificação e avaliação de riscos.	48% (36)	15% (11)	23% (17)	15% (11)
Os líderes de diferentes áreas (administrativa, jurídica, negócios) são convidados a participar de discussões sobre riscos e segurança.	43% (32)	19% (14)	24% (18)	15% (11)
A gestão de riscos em minha instituição é considerada nos processos das principais áreas e é gradualmente incorporada às práticas diárias.	35% (26)	32% (24)	20% (15)	13% (10)
Há uma política formal que orienta a gestão de riscos nos projetos e processos organizacionais conforme as diretrizes institucionais.	52% (39)	16% (12)	17% (13)	15% (11)
As iniciativas de segurança da informação buscam integrar-se progressivamente aos mecanismos de governança institucional e ao planejamento estratégico.	55% (41)	9% (7)	23% (17)	13% (10)

Nota: As células em cinza indicam o maior percentual de cada assertiva.

5.2. Princípio Estruturada e Abrangente

O princípio da estruturada e abrangente reforça que a gestão de riscos deve ser realizada de forma consistente, comparável e alinhada a metodologias bem definidas. A Tabela 5 apresenta a distribuição das respostas para as seis assertivas relacionadas a esse princípio.

As respostas revelam percepções variadas entre os participantes. A utilização de

frameworks reconhecidos (ITIL, COBIT, NIST, CIS, ISO) foi a assertiva com maior concordância (48%), seguida da existência de processos formais para identificação, análise e tratamento de riscos (40%) e da padronização e adaptabilidade da metodologia de gestão de riscos (39%). Esses dados sugerem que parte dos respondentes reconhece a importância de metodologias estruturadas e percebem em sua instituição sua aplicação de forma planejada.

Por outro lado, surgem percepções críticas. A maior taxa de discordância (37%) concentrou-se na assertiva sobre o mapeamento de todos os riscos, inclusive vulnerabilidades menores. Nesse mesmo caso, a soma de neutralidade (23%) e não resposta (16%) alcançou 39%, superando o maior percentual individual. Esse resultado evidencia predominância de indefinição ou ausência de posicionamento por parte dos participantes em relação a essa prática.

Na assertiva sobre a existência de um cronograma regular para revisar e atualizar o inventário de riscos, registrou-se concordância de 35%. Entretanto, o mesmo percentual (35%) resultou da soma de neutralidade (16%) e não resposta (19%), configurando um empate. Esse equilíbrio reforça a percepção de indefinição, indicando que, para uma parte significativa dos respondentes, não há clareza sobre a consolidação de ciclos de revisão.

Em outras assertivas, observam-se ainda percentuais expressivos de neutralidade (16% a 23%), como na integração dos riscos de TI aos riscos organizacionais e na formalização de processos. Esse padrão sugere incertezas ou falta de consenso entre os participantes sobre a efetiva aplicação de mecanismos estruturados de gestão. Essa mesma assertiva teve um elevado percentual de discordância, 32%, contra 37% de concordância.

Em síntese, o quadro é heterogêneo: embora haja reconhecimento sobre a relevância de referenciais e *frameworks*, a percepção predominante em alguns pontos revela indefinição, seja porque a soma de neutralidade e não resposta superou o maior percentual individual, seja porque houve empate entre posições afirmativas e a indefinição.

Table 5. Distribuição das respostas — Princípio 2: Estruturada e Abrangente (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
Os riscos de segurança de TI são tratados em conjunto com outros riscos organizacionais garantindo uma visão holística.	37% (28)	32% (24)	17% (13)	13% (10)
A metodologia de gestão de riscos é padronizada e adaptável, sendo aplicada conforme as necessidades de diferentes unidades organizacionais e projetos.	39% (29)	25% (19)	21% (16)	15% (11)
Existe um processo formal documentado para identificar, analisar e tratar riscos nos principais ativos e setores da instituição, de forma centralizada e com aplicação gradativa às demais áreas.	40% (30)	23% (17)	21% (16)	16% (12)
Todos os riscos, desde incidentes críticos até vulnerabilidades consideradas menores, são mapeados e registrados em um repositório comum.	24% (18)	37% (28)	23% (17)	16% (12)
A instituição busca implementar um cronograma regular para revisar e atualizar o inventário de riscos na instituição.	35% (26)	31% (23)	16% (12)	19% (14)
A instituição utiliza *frameworks* reconhecidos (como ITIL, COBIT, NIST, CIS, ISO) para apoiar a gestão de riscos, aplicando-os de forma planejada e progressiva no ambiente de TI.	48% (36)	16% (12)	19% (14)	17% (13)

Nota: As células em cinza indicam o maior percentual de cada assertiva. As células em laranja indicam casos em que a soma das respostas "Não concordam, nem discordam" e "Não sabem/Não querem responder" superou ou igualou o maior percentual individual.

5.3. Princípio Personalizada

O princípio personalizada estabelece que a gestão de riscos deve ser adaptada ao contexto específico de cada organização, contemplando suas características institucionais, setoriais e legais. A Tabela 6 sintetiza as respostas para as seis assertivas relacionadas a esse princípio.

De modo geral, os resultados indicam níveis consistentes de concordância em pontos centrais. Mais da metade dos respondentes (53%) afirmou que a gestão de riscos é moldada às particularidades do setor de atuação, e 52% indicaram a escolha de soluções e controles após análise do contexto institucional. Percentuais próximos (44% a 45%) também destacaram a adaptação de metodologias, a consideração de características próprias na definição de prioridades e a flexibilidade para ajustar normas, sugerindo a busca por práticas adaptativas e evitando modelos genéricos.

Por outro lado, emergem sinais de indefinição em aspectos específicos. Na assertiva sobre o alinhamento das políticas de segurança e gestão de riscos às especificidades institucionais, a soma de neutralidade e não resposta (24% + 19% = 43%) superou o maior percentual individual (36% de concordância), evidenciando baixa clareza ou visibilidade quanto ao grau real de personalização nessas políticas. Esse padrão de indefinição não se repetiu nas demais assertivas desta seção.

Em síntese, há avanços na incorporação da personalização à gestão de riscos, mas permanece o desafio de consolidar políticas e práticas que traduzam de forma clara e verificável as particularidades institucionais, setoriais e legais no cotidiano das organizações.

Table 6. Distribuição das respostas — Princípio 3: Personalizada (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
A gestão de riscos em minha organização é moldada às particularidades do nosso setor de atuação (ex.: educação, saúde, fiscalização).	53% (40)	16% (12)	16% (12)	15% (11)
As soluções e controles de segurança adotados são escolhidos após análise do contexto e necessidades exclusivas da instituição.	52% (39)	12% (9)	20% (15)	16% (12)
As metodologias e procedimentos de avaliação de riscos são adaptados, conforme necessário, aos processos e características específicas dos diferentes setores da organização.	44% (33)	17% (13)	19% (15)	19% (14)
Nossas políticas de segurança e gestão de riscos levam em conta a autonomia/setores específicos (ex.: liberdade acadêmica, serviços de pesquisa, áreas finalísticas etc.).	36% (27)	21% (16)	24% (18)	19% (14)
Quando definimos prioridades de risco, consideramos características próprias (p. ex.: dados sensíveis, perfis de usuários, legislação setorial).	45% (34)	20% (15)	19% (14)	16% (12)
Há flexibilidade para ajustar normas de risco e segurança de acordo com variações regionais ou departamentais, evitando um modelo genérico.	45% (33)	19% (14)	21% (15)	15% (11)

Nota: As células em cinza indicam o maior percentual de cada assertiva. As células em laranja indicam casos em que a soma das respostas "Não concordam, nem discordam" e "Não sabem/Não querem responder" superou ou igualou o maior percentual individual.

5.4. Princípio Inclusiva

O princípio inclusiva estabelece que a gestão de riscos deve envolver diferentes partes interessadas, promovendo legitimidade, transparência e colaboração entre setores. A Tabela 7 apresenta a distribuição das respostas para as seis assertivas relacionadas a esse princípio.

As respostas indicam que parte dos participantes percebe a existência de mecanismos participativos em suas instituições. Destacam-se, nesse sentido, a pluralidade na composição dos fóruns ou comitês de segurança da informação (64% de concordância) e a consideração de sugestões de diferentes departamentos nas decisões sobre políticas e normas (61% de concordância) — ambos os maiores percentuais entre as assertivas.

Por outro lado, alguns resultados mostram que a soma das respostas de neutralidade e de não resposta superou o maior percentual individual de concordância ou discordância. Esse cenário foi observado em dois casos: na assertiva sobre comunicação clara e frequente sobre riscos (36% de concordância contra 40% de indecisão e não resposta) e na participação de representantes de todas as áreas (33% de discordância contra 40% de

indecisão e não resposta). Esses dados sugerem que, para parte significativa dos respondentes, ainda há indefinição quanto à efetividade da inclusão no processo de gestão de riscos.

Em outras assertivas, como a consulta às partes envolvidas antes do tratamento de riscos (47% de concordância) e a participação da alta gestão (43% de concordância), a percepção predominante foi de concordância, embora índices de neutralidade e ausência de resposta também tenham sido relevantes (32% e 40%, respectivamente). Isso indica que, mesmo quando a maioria tende a concordar, há uma parcela considerável dos participantes que não manifesta percepção clara sobre o tema.

Em síntese, os resultados revelam percepções heterogêneas: em algumas situações prevalece a concordância quanto à inclusão, enquanto em outras o destaque recai sobre a indefinição ou a ausência de respostas. Essa diversidade de percepções sugere que a inclusão na gestão de riscos ainda é percebida como prática em consolidação, variando entre instituições e contextos.

Table 7. Distribuição das respostas — Princípio 4: Inclusiva (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
O comitê ou fórum de segurança da informação é composto por membros de diferentes setores, não se restringindo apenas à equipe de TI.	64% (48)	11% (8)	13% (10)	12% (9)
As decisões sobre políticas e normas de segurança levam em conta as sugestões ou críticas dos demais departamentos, além do TI.	61% (46)	8% (6)	15% (11)	16% (12)
Antes de definir qualquer ação de tratamento de riscos, são consultadas as partes envolvidas e/ou impactadas.	47% (35)	21% (16)	17% (13)	15% (11)
Há uma comunicação clara e frequente sobre riscos e segurança, estimulando a colaboração de toda a equipe.	36% (27)	24% (18)	28% (21)	12% (9)
Representantes de todas as áreas (administrativa, operacional e técnica) participam ativamente das discussões sobre riscos.	27% (20)	33% (25)	27% (20)	13% (10)
A alta gestão e outras partes interessadas relevantes participam e apoiam as iniciativas de gestão de riscos, assegurando recursos e legitimidade.	43% (32)	17% (13)	25% (19)	15% (11)

Nota: As células em cinza indicam o maior percentual de cada assertiva. As células em laranja indicam casos em que a soma das respostas "Não concordam, nem discordam" e "Não sabem/Não querem responder" superou ou igualou o maior percentual individual.

5.5. Princípio Dinâmica

O princípio dinâmica ressalta que a gestão de riscos deve ser responsiva às mudanças internas e externas, com processos, controles e prioridades revisados de forma contínua. A Tabela 8 apresenta a distribuição das respostas referentes a esse princípio.

Os resultados refletem percepções diversas dos participantes quanto à institucionalização de práticas dinâmicas. O maior índice de concordância foi ob-

servado no uso de ferramentas de *logs* e análise proativa de vulnerabilidades (48%), o que indica que muitos participantes reconhecem a existência de tais práticas técnicas. De modo semelhante, 41% afirmaram que as equipes de gestão de riscos recebem informações atualizadas e ajustam rapidamente seus planos, embora 21% tenham se mostrado neutros e 15% não tenham respondido, sugerindo que essa percepção não é uniforme.

Em contraste, práticas mais estruturais foram percebidas como frágeis ou pouco consolidadas. Na revisão periódica do inventário de riscos, 32% concordaram, mas a soma das respostas neutras (25%) e de não resposta (15%) alcançou 40%, superando o maior percentual individual. Isso evidencia que parte significativa dos participantes não percebe clareza ou regularidade nessa prática. O mesmo ocorre na definição de ciclos de reavaliação: 33% discordaram, enquanto a soma das respostas neutras (17%) e de não resposta (17%) superou o maior percentual isolado, reforçando a percepção de que não há padronização consolidada.

O monitoramento contínuo também foi avaliado de forma dispersa: 35% concordaram com sua existência, mas a soma de neutralidade (29%) e não resposta (12%) totalizou 41%, superando o maior percentual isolado. Esse resultado sugere que, na percepção dos respondentes, ainda há indefinições sobre a efetividade e formalização desses mecanismos.

Por fim, a reavaliação de riscos diante de mudanças internas — como novos projetos, contratações ou sistemas — foi percebida de forma dividida: 36% concordaram e 33% discordaram, revelando falta de consenso entre os participantes.

Em síntese, as percepções dos participantes apontam para maior reconhecimento de práticas técnicas ligadas a ferramentas e ajustes pontuais, enquanto dimensões mais institucionais — como revisão periódica, ciclos de reavaliação e monitoramento contínuo — são vistas como insuficientes ou pouco consistentes. Esse descompasso ressalta a necessidade de fortalecer mecanismos de governança para que a dinamicidade se torne uma característica efetiva da gestão de riscos.

Table 8. Distribuição das respostas — Princípio 5: Dinâmica (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
A equipe responsável por gestão de riscos recebe informações atualizadas sobre tendências de ataques e vulnerabilidades e ajusta os planos rapidamente.	41% (31)	23% (17)	21% (16)	15% (11)
Utilizamos ferramentas de *logs* e análise de vulnerabilidades de forma proativa, com alertas que geram revisões imediatas de risco.	48% (36)	20% (14)	20% (15)	13% (10)
A instituição revisa e atualiza seu inventário de riscos periodicamente, independentemente da ocorrência de incidentes.	32% (24)	28% (21)	25% (19)	15% (11)
Mantemos um ciclo definido (mensal/trimestral/semestral) para reavaliar e priorizar riscos à luz de possíveis modificações no ambiente.	32% (24)	33% (25)	17% (13)	17% (13)
Há um processo formal de monitoramento contínuo que antecipa novas ameaças e vulnerabilidades, em vez de apenas reagir a incidentes.	35% (26)	24% (18)	29% (22)	12% (9)
Mudanças internas, como novos projetos, contratações, sistemas ou processos, incluem reavaliação dos riscos associados.	36% (27)	33% (25)	17% (13)	13% (10)

Nota: As células em cinza indicam o maior percentual de cada assertiva. As células em laranja indicam casos em que a soma das respostas "Não concordam, nem discordam" e "Não sabem/Não querem responder" superou ou igualou o maior percentual individual.

5.6. Princípio Melhor Informação Disponível

O princípio melhor informação disponível estabelece que a gestão de riscos deve ser sustentada por dados confiáveis, evidências consistentes e informações atualizadas. A Tabela 9 apresenta a distribuição das respostas para as seis assertivas associadas a este princípio, destacando em cinza os maiores percentuais e em laranja os casos em que a soma da neutralidade com a ausência de resposta superou ou igualou o maior percentual individual.

As percepções dos participantes indicam que a análise regular, pelas equipes de segurança, de dados coletados (como *logs* de sistemas, relatórios de auditoria e boletins de vulnerabilidades) foi o aspecto mais reconhecido, com 52% de concordância. Também se sobressaem a existência de canais para difusão rápida de novas vulnerabilidades (45%) e o compartilhamento de relatórios com setores relevantes (40%), sugerindo que parte dos respondentes percebe práticas de coleta, atualização e disseminação de informações voltadas ao apoio das decisões de risco.

Entretanto, os resultados também apontam percepções de fragilidade. A assertiva sobre ferramentas para correlacionar diferentes fontes de dados registrou 37% de concordância, mas a soma das respostas neutras e de não resposta (41%) superou esse valor, revelando dúvidas quanto à efetividade desses mecanismos. Situação semelhante ocorreu na utilização de informações atualizadas pelo comitê de riscos: o maior índice individual foi de 29% de neutralidade, sugerindo que, para muitos participantes, o processo decisório ainda não se apoia plenamente em dados recentes. No caso da manutenção de um

repositório central de informações, 35% concordaram com sua existência, mas a soma de neutralidade e não resposta (36%) superou este percentual, reforçando a percepção de ausência ou insuficiência de práticas consolidadas.

Em síntese, as respostas evidenciam que, embora haja reconhecimento de práticas voltadas à coleta, monitoramento e compartilhamento de informações, prevalece a percepção de que ainda faltam mecanismos centralizados, integrados e sistemáticos. Isso indica que a confiança e a efetividade da informação como suporte às decisões de risco permanecem como desafios a serem enfrentados pelas instituições.

Table 9. Distribuição das respostas — Princípio 6: Melhor Informação Disponível (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
As equipes de segurança analisam regularmente os dados coletados (*logs* de sistemas, relatórios de auditoria, boletins de vulnerabilidade) para apoiar decisões de risco.	52% (39)	15% (11)	17% (13)	16% (12)
Quando surgem novos tipos de ataques ou vulnerabilidades, temos um canal eficiente para difundir e atualizar rapidamente nossa matriz de riscos.	45% (34)	21% (16)	16% (12)	17% (13)
Há ferramentas e processos definidos para correlacionar diferentes fontes de dados (*logs*, incidentes, boletins externos) e gerar insights confiáveis.	37% (28)	21% (16)	25% (19)	16% (12)
O comitê ou gestão de riscos utiliza sistematicamente informações atualizadas para redefinir prioridades e estratégias de segurança.	24% (18)	27% (20)	29% (22)	20% (15)
Nossa instituição mantém um repositório central ou painel que consolida logs, indicadores de vulnerabilidades e alertas em tempo real.	35% (26)	29% (22)	20% (15)	16% (12)
Os relatórios ou análises de segurança são compartilhados com setores relevantes, auxiliando na compreensão e priorização dos riscos.	40% (30)	29% (22)	17% (13)	13% (10)

Nota: As células em cinza indicam o maior percentual de cada assertiva. As células em laranja indicam casos em que a soma das respostas "Não concordam, nem discordam" e "Não sabem/Não querem responder" superou ou igualou o maior percentual individual.

5.7. Princípio Fatores Humanos e Culturais

O princípio fatores humanos e culturais reconhece que a efetividade da gestão de riscos depende diretamente das pessoas, de suas percepções, capacidades e condutas. A Tabela 10 apresenta a distribuição das respostas para as seis assertivas relacionadas a esse princípio.

Os resultados refletem percepções variadas dos participantes. Parte significativa dos respondentes reconhece o papel da alta gestão no apoio à cultura de segurança, com 51% de concordância quanto ao seu exemplo e priorização de iniciativas de conscientização. De modo semelhante, 52% concordam que existem ações de comunicação e capacitação voltadas a reduzir resistências na adoção de novas ferramentas, índice mais elevado entre as assertivas deste princípio. Além disso, 44% percebem que incidentes decorrentes

de falhas humanas são tratados como oportunidades de aprendizado, em vez de mera culpabilização individual, sinalizando uma visão construtiva em algumas instituições. A mesma porcentagem (44%) tem a percepção de que existem treinamento regulares de conscientização na instituição.

Por outro lado, também emergem percepções críticas. Apenas 43% concordaram que servidores e gestores compreendem a importância de sua conduta para a segurança, enquanto 32% permaneceram neutros, o que sugere falta de clareza sobre a corresponsabilidade humana na gestão de riscos em algumas instituições. De forma ainda mais evidente, 41% discordaram da existência de incentivos ou reconhecimentos formais para estimular boas práticas, revelando uma percepção de ausência de mecanismos de valorização institucional.

Em síntese, os dados mostram que, embora haja percepções positivas quanto ao apoio da alta gestão, à comunicação e à capacitação, fatores humanos e culturais ainda não são vistos como plenamente incorporados à cultura organizacional. A percepção dos participantes evidencia que a consolidação desse princípio exige maior clareza sobre responsabilidades individuais e institucionais, além de políticas de incentivo mais consistentes para promover condutas seguras.

Table 10. Distribuição das respostas — Princípio 7: Fatores Humanos e Culturais (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
Existem treinamentos regulares de conscientização de segurança, que são bem aceitos pela equipe.	44% (33)	29% (22)	23% (17)	4% (3)
Quando um incidente ocorre por falha humana, a instituição investiga o processo para aprendizado, em vez de meramente culpar indivíduos.	44% (33)	21% (18)	21% (16)	11% (8)
A alta gestão apoia e reforça a cultura de segurança, demonstrando exemplo e priorizando iniciativas de conscientização.	51% (38)	16% (12)	27% (20)	7% (5)
Os servidores e colaboradores, inclusive da alta gestão, compreendem a importância de sua conduta para a segurança e a gestão de riscos.	43% (32)	16% (12)	32% (24)	9% (7)
A organização utiliza incentivos ou reconhecimentos formais como estratégia para estimular as boas práticas de segurança.	33% (25)	41% (31)	19% (14)	7% (5)
A instituição adota ações de comunicação e capacitação para reduzir a resistência à adoção de novas ferramentas (ex.: autenticação multifator, assinatura digital).	52% (39)	17% (13)	27% (20)	4% (3)

Nota: As células em cinza indicam o maior percentual de cada assertiva.

5.8. Princípio Melhoria Contínua

O princípio melhoria contínua estabelece que a gestão de riscos deve ser entendida como um processo iterativo e sistemático, capaz de incorporar aprendizados decorrentes de

incidentes, auditorias, retrospectivas e revisões periódicas. A Tabela 11 apresenta a distribuição das respostas para as seis assertivas que compõem este princípio.

As percepções dos participantes revelam que as auditorias internas e externas são vistas como principal mecanismo de indução de melhorias, com 55% de concordância — o maior índice do conjunto. Também há uma percepção significativa de utilização de incidentes passados como fonte de aprendizado, com 47% de concordância, sugerindo que práticas de análise pós-incidente (*post-mortem*) estão parcialmente presentes nas organizações.

Por outro lado, a marcação em laranja indica situações em que prevalece a neutralidade ou a ausência de posicionamento. No estímulo às equipes para propor aperfeiçoamentos contínuos, a soma das respostas neutras e de não resposta (41%) igualou a concordância (41%). Na prática de retrospectivas após implementações críticas, em que predominou a discordância (31%), a soma das respostas neutras e de não resposta (40%) mostrou-se superior. Quanto ao processo formal de revisão periódica das políticas e metodologias de riscos, embora 36% tenham concordado, a soma de neutralidade e não resposta (38%) foi maior, evidenciando percepções de indefinição ou baixa institucionalização da prática.

Outro ponto relevante refere-se à existência de ciclos regulares para reavaliar a efetividade dos controles e atualizar a matriz de riscos. Houve empate entre concordância e discordância (29% cada), mas a soma de neutralidade e não resposta (41%) foi ainda maior, revelando percepção de que esse planejamento não está consolidado como rotina em muitas instituições.

Em síntese, as percepções coletadas indicam que, embora incidentes e auditorias sejam reconhecidos como elementos de aprendizado, ainda há dúvidas quanto à regularidade e formalização de processos de revisão e aprimoramento contínuo. Isso sugere que a internalização do princípio permanece dependente de práticas pontuais, exigindo maior alinhamento às diretrizes da ISO 31000:2018 e aos normativos nacionais para se transformar em processo institucionalizado.

Table 11. Distribuição das respostas — Princípio 8: Melhoria Contínua (N=75; % e n)

Assertiva	Concordam	Discordam	Não concordam, nem discordam	Não sabem/Não querem responder
Após a resolução de um incidente, sempre realizamos uma análise aprofundada (post-mortem) para identificar causas-raiz e oportunidades de melhoria.	47% (35)	20% (15)	19% (14)	15% (11)
As equipes são estimuladas a propor aperfeiçoamentos contínuos na abordagem de riscos, registrando sugestões e acompanhando sua implementação.	41% (31)	17% (13)	28% (21)	13% (10)
A cada implementação ou correção significativa de segurança, realizamos uma retrospectiva, documentando o que funcionou e o que pode ser aprimorado.	29% (22)	31% (23)	25% (19)	15% (11)
A organização possui um processo formal para revisar periodicamente as políticas e metodologias de gestão de riscos, incorporando lições aprendidas.	36% (27)	27% (20)	23% (17)	15% (11)
As auditorias internas ou externas contribuem para a implementação de melhorias nos processos de gestão de riscos.	55% (41)	16% (12)	16% (12)	13% (10)
Existe um calendário ou ciclo definido para reavaliar a efetividade dos controles e atualizar a matriz de riscos com base em novos aprendizados.	29% (22)	29% (22)	21% (16)	20% (15)

Nota: As células em cinza indicam o maior percentual de cada assertiva. As células em laranja indicam casos em que a soma das respostas "Não concordam, nem discordam" e "Não sabem/Não querem responder" superou ou igualou o maior percentual individual.

5.9. Perguntas Abertas

Duas perguntas abertas foram incluídas no questionário: (1) Quais sugestões você teria para a melhoria das práticas de gestão de riscos de segurança da informação na sua instituição? e (2) Quais sugestões você teria para fortalecer a gestão de riscos de segurança da informação na Administração Pública?

As respostas revelaram um conjunto expressivo de percepções, que foram agrupadas em seis eixos temáticos. A Tabela 12 apresenta a síntese dessas contribuições, destacando desde a importância de ações de conscientização e capacitação até a necessidade de estruturas formais, apoio da alta administração e auditorias independentes.

Table 12. Síntese das sugestões qualitativas dos participantes para melhoria da gestão de riscos

Categoria	Exemplos de Sugestões dos Participantes
Conscientização, cultura e capacitação	- Campanhas de conscientização em todos os níveis; - Treinamentos contínuos e simulações de ataques (ex.: phishing); - Inclusão do tema no cotidiano das atividades institucionais.
Estruturas formais e governança	- Criação de diretorias ou coordenações de segurança; - Comitês de segurança e privacidade; - Maior participação da alta administração.
Integração e visão holística	- Integração com áreas jurídicas, administrativas e finalísticas; - Visão transversal incluindo ativos físicos e processos; - Cooperação interinstitucional e repositórios centrais.
Recursos, equipes e ferramentas	- Ampliação das equipes de cibersegurança; - Adoção de metodologias (ISO 27005, NIST); - Valorização de soluções abertas e auditáveis.
Apoio da alta administração	- Engajamento efetivo da liderança; - Alocação de recursos humanos e financeiros; - Reconhecimento da gestão de riscos como prática estratégica.
Normatização e auditoria	- Auditorias independentes e periódicas; - Atualização constante de políticas e manuais; - Divulgação de objetivos e resultados de forma transparente.

As respostas abertas dos participantes reforçam os achados quantitativos: apesar da existência de estruturas e iniciativas formais, ainda se identificam fragilidades relacionadas à cultura organizacional, ao apoio da alta administração e à integração efetiva da gestão de riscos às estratégias institucionais.

6. Proposição de Medidas de Controle para o PPSI

A análise quantitativa e qualitativa das assertivas aplicadas ao questionário (N=75) permitiu identificar dois grupos críticos de atenção: (i) assertivas com maior discordância e (ii) assertivas com maior neutralidade e/ou ausência de resposta. Cada grupo evidencia fragilidades de natureza distinta: ausência de práticas consolidadas ou percepções de incerteza quanto aos processos institucionais.

As medidas derivadas das assertivas com maior discordância estão apresentadas na Tabela 13. Observa-se que os maiores pontos de fragilidade concentram-se nos princípios *Estruturada e Abrangente*, *Inclusiva* e *Fatores Humanos e Culturais*. Além disso, assertivas relacionadas ao princípio *Melhoria Contínua* também revelaram fragilidades, incluindo um caso de empate entre concordância e discordância, o que demonstra percepções institucionais divididas.

Na Tabela 14, estão reunidas as medidas propostas a partir das assertivas com maior neutralidade. O destaque recai sobre os princípios *Dinâmica* e *Melhor Informação Disponível*, evidenciando desafios no monitoramento contínuo de ameaças, na consolidação de informações em tempo real e na utilização sistemática de dados atualizados para subsidiar decisões estratégicas.

Em conjunto, as duas tabelas sintetizam recomendações que visam reduzir incertezas, reforçar práticas organizacionais e consolidar uma cultura de gestão de riscos mais integrada e eficaz. As fragilidades identificadas distribuem-se em cinco dos oito princípios da ISO 31000:2018, reforçando a necessidade de ação coordenada e transversal para o fortalecimento do PPSI.

Table 13. Propostas de medidas derivadas de assertivas com maior discordância (N=75)

Princípio	Assertiva	% discordância	Medida Proposta	Descrição da Medida
Estruturada e Abrangente	Todos os riscos, desde incidentes críticos até vulnerabilidades consideradas menores, são mapeados e registrados em um repositório comum.	37%	Todos os riscos de segurança da informação, desde incidentes críticos até vulnerabilidades menores, são mapeados e registrados em um repositório comum?	Consolidar em um único repositório todos os riscos, abrangendo desde incidentes críticos até vulnerabilidades menores, garantindo atualização contínua e acesso institucional.
Inclusiva	Representantes de todas as áreas (administrativa, operacional e técnica) participam ativamente das discussões sobre riscos.	33%	Representantes de todas as áreas (administrativa, operacional e técnica) participam ativamente das discussões sobre riscos?	Instituir fóruns de governança participativa, com presença obrigatória de representantes das áreas administrativa, operacional e técnica, assegurando registro formal das deliberações.
Dinâmica	Mantemos um ciclo definido (mensal/trimestral/semestral) para reavaliar e priorizar riscos à luz de possíveis modificações no ambiente.	33%	A organização mantém um ciclo definido (mensal/trimestral/semestral) para reavaliar e priorizar riscos à luz de possíveis modificações no ambiente?	Definir periodicidade mínima para reavaliação de riscos e priorização de controles, ajustando o planejamento às mudanças do ambiente organizacional.
Fatores Humanos e Culturais	A organização utiliza incentivos ou reconhecimentos formais como estratégia para estimular as boas práticas de segurança.	41%	A organização utiliza incentivos ou reconhecimentos formais como estratégia para estimular as boas práticas de segurança?	Desenvolver programas internos de valorização, premiação ou certificação voltados a equipes e servidores que adotem práticas exemplares de segurança.
Melhoria Contínua	A cada implementação ou correção significativa de segurança, realizamos uma retrospectiva, documentando o que funcionou e o que pode ser aprimorado.	31%	A cada implementação ou correção significativa de segurança, realizamos uma retrospectiva, documentando o que funcionou e o que pode ser aprimorado?	Formalizar a prática de retrospectivas após mudanças significativas, com registro de lições aprendidas e encaminhamentos de melhoria.
Melhoria Contínua	Existe um calendário ou ciclo definido para reavaliar a efetividade dos controles e atualizar a matriz de riscos com base em novos aprendizados.	29% (empate com concordo; 41% neutralidade)	Existe um calendário ou ciclo definido para reavaliar a efetividade dos controles e atualizar a matriz de riscos com base em novos aprendizados?	Implementar calendário oficial para reavaliar periodicamente controles e atualizar a matriz de riscos, com base em resultados e aprendizados obtidos.

Table 14. Propostas de medidas derivadas de assertivas com maior neutralidade (N=75)

Princípio	Assertiva	% neutralidade/ não resposta	Medida Proposta	Descrição da Medida
Melhor Informação Disponível	O comitê ou gestão de riscos utiliza sistematicamente informações atualizadas para redefinir prioridades e estratégias de segurança.	29%	O comitê ou gestão de riscos utiliza sistematicamente informações atualizadas para redefinir prioridades e estratégias de segurança?	Estabelecer rotina de coleta e análise de logs, relatórios de auditoria e boletins de vulnerabilidade para subsidiar deliberações de comitês de risco.
Estruturada e Abrangente	A instituição busca implementar um cronograma regular para revisar e atualizar o inventário de riscos na instituição.	35% (16% nem discordam, 19% não sabem)	A instituição busca implementar um cronograma regular para revisar e atualizar o inventário de riscos na instituição?	Definir periodicidade e responsabilidades para a atualização do inventário de riscos, garantindo registro e acompanhamento sistemático.
Personalizada	Nossas políticas de segurança e gestão de riscos levam em conta a autonomia/setores específicos (ex.: liberdade acadêmica, serviços de pesquisa, áreas finalísticas etc.).	43% (24% nem discordam, 19% não sabem)	As políticas de segurança e gestão de riscos levam em conta a autonomia/setores específicos (ex.: liberdade acadêmica, serviços de pesquisa, áreas finalísticas etc.)?	Incorporar critérios de autonomia acadêmica e especificidades setoriais nas políticas de segurança, assegurando maior legitimidade e aplicabilidade.
Inclusiva	Há uma comunicação clara e frequente sobre riscos e segurança, estimulando a colaboração de toda a equipe.	40% (28% nem discordam, 12% não sabem)	Há uma comunicação clara e frequente sobre riscos e segurança, estimulando a colaboração de toda a equipe?	Estabelecer canais de comunicação recorrente (boletins, reuniões periódicas, painéis digitais) para garantir transparência e engajamento das equipes.
Dinâmica	Há um processo formal de monitoramento contínuo que antecipa novas ameaças e vulnerabilidades, em vez de apenas reagir a incidentes.	41% (29% nem discordam, 12% não sabem)	Há um processo formal de monitoramento contínuo que antecipa novas ameaças e vulnerabilidades, em vez de apenas reagir a incidentes?	Implementar sistemas de monitoramento proativo, integrando inteligência de ameaças e análise preditiva para reduzir riscos emergentes.
Melhor Informação Disponível	Há ferramentas e processos definidos para correlacionar diferentes fontes de dados (logs, incidentes, boletins externos) e gerar insights confiáveis.	41% (25% nem discordam, 16% não sabem)	Há ferramentas e processos definidos para correlacionar diferentes fontes de dados (logs, incidentes, boletins externos) e gerar insights confiáveis?	Estabelecer plataformas integradas que consolidem diferentes fontes de dados, permitindo análise cruzada e insights estratégicos.
Melhor Informação Disponível	Nossa instituição mantém um repositório central ou painel que consolida logs, indicadores de vulnerabilidades e alertas em tempo real.	36% (20% nem discordam, 16% não sabem)	A instituição mantém um repositório central ou painel que consolida logs, indicadores de vulnerabilidades e alertas em tempo real?	Implantar solução institucional que reúna indicadores de segurança em tempo real, acessível a gestores e equipes operacionais.
Melhoria Contínua	As equipes são estimuladas a propor aperfeiçoamentos contínuos na abordagem de riscos, registrando sugestões e acompanhando sua implementação.	41% (28% nem discordam, 13% não sabem)	As equipes são estimuladas a propor aperfeiçoamentos contínuos na abordagem de riscos, registrando sugestões e acompanhando sua implementação?	Criar mecanismos permanentes de registro, avaliação e implementação de sugestões de equipes sobre práticas de segurança.
Melhoria Contínua	A organização possui um processo formal para revisar periodicamente as políticas e metodologias de gestão de riscos, incorporando lições aprendidas.	38% (23% nem discordam, 15% não sabem)	A organização possui um processo formal para revisar periodicamente as políticas e metodologias de gestão de riscos, incorporando lições aprendidas?	Definir processo formal de revisão periódica de políticas de segurança, incorporando resultados de auditorias e análises pós-incidentes.

7. Considerações Finais

A pesquisa realizada com 75 profissionais do setor público brasileiro permitiu identificar avanços e fragilidades na adoção dos princípios da ISO 31000:2018 aplicados à gestão de riscos de segurança da informação. Os resultados evidenciaram que, embora já exista a formalização de políticas, equipes especializadas e comitês de segurança em grande parte das instituições, a integração efetiva da gestão de riscos às decisões estratégicas e operacionais ainda se mostra incipiente. As percepções coletadas revelaram níveis elevados de neutralidade e ausência de posicionamento em temas centrais, como a revisão sistemática de inventários de riscos, a comunicação clara entre setores e a participação efetiva da alta gestão. Fragilidades adicionais foram observadas nos princípios estruturada e abrangente, inclusiva, fatores humanos e culturais e melhoria contínua, evidenciando um estágio de maturidade desigual entre os órgãos respondentes.

A partir desses achados, foram propostas medidas de controle alinhadas ao Programa de Privacidade e Segurança da Informação (PPSI), à Instrução Normativa GSI/PR nº 3/2021 e à Política Nacional de Segurança da Informação (PNSI 2025). Essas medidas buscam transformar as fragilidades identificadas em ações concretas, fortalecendo processos de revisão contínua, ampliando mecanismos de participação e comunicação transversal, incentivando a valorização de condutas seguras e consolidando a gestão de riscos como prática institucionalizada.

O estudo reforça a necessidade de compreender a gestão de riscos como prática transversal e estruturante, capaz de sustentar a resiliência institucional, a continuidade dos serviços públicos e a confiança da sociedade. Ao oferecer evidências empíricas e recomendações aplicáveis ao setor público, esta pesquisa contribui tanto para o avanço acadêmico da área quanto para a consolidação de políticas públicas em segurança da informação. Trabalhos futuros podem aprofundar a validação das medidas propostas, explorar metodologias quantitativas para cálculo de índices de maturidade e expandir a aplicação do instrumento para diferentes esferas e níveis da administração pública.

References

ABNT (2015). ABNT NBR ISO 31004: Gestão de riscos — Orientações para a implementação da ISO 31000. Norma técnica.

Aceiro, A. Y. (2022). A dimensão pessoal como quesito metodológico ao aperfeiçoamento da gestão de riscos no combate à fraude e à corrupção no âmbito da administração pública federal. Dissertação (mestrado profissional em administração pública), Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

Alves, R. S., Queiroz, C. E. M., and Nunes, R. R. (2023). Os tribunais têm estrutura para gerenciar riscos de segurança da informação? um estudo à luz das três linhas. *Revista CEJ*, 27(86):145–160. Trabalho apresentado no EnAJUS 2022.

Andrade, M. E. and Figueiredo, A. C. (2017). Gestão da informação e apoio à tomada de decisão em processos de risco. *Revista Brasileira de Administração Científica*, 8(1):45–62.

Batista, R. R. (2022). *Análise de riscos em segurança da informação: modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES)*. Tese (doutorado em ciência da informação), Universidade Federal da Paraíba.

Brasil (2017). Decreto nº 9.203, de 22 de novembro de 2017: Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Presidência da República.

Brasil (2024a). Decreto nº 11.856, de 31 de dezembro de 2024. institui a política nacional de cibersegurança (pnciber). https://www.in.gov.br/web/dou/-/decreto-n-11.856-de-31-de-dezembro-de-2024. Diário Oficial da União, Edição Extra, Seção 1, p. 1.

Brasil (2024b). Decreto nº 12.069, de 21 de junho de 2024. formaliza a estratégia nacional de governo digital (engd). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12069.htm. Diário Oficial da União.

Brasil (2024c). Decreto nº 12.198, de 24 de setembro de 2024. institui a estratégia federal de governo digital (efgd) e a infraestrutura nacional de dados. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12198.htm. Diário Oficial da União.

Brasil (2025a). Decreto nº 12.572, de 14 de fevereiro de 2025. Diário Oficial da União, Brasília. Institui a Política Nacional de Segurança da Informação (PNSI).

Brasil (2025b). Estratégia nacional de segurança cibernética (e-ciber). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Disponível em: Portal GSI/PR.

Cancellier, R. (2020). Gestão de riscos de segurança da informação no tribunal de contas da união: estudo de caso. Relatório técnico. Estudo aplicado.

Cruz, J. M. R. d. (2025). Aplicação da gestão de risco para reduzir incidentes de segurança da informação em organizações. Trabalho de conclusão de curso em administração, Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB).

de Bakker, K., Boonstra, A., and Wortmann, H. (2010). Does risk management contribute to it project success? a meta-analysis of empirical evidence. *International Journal of Project Management*, 28(5):493–503.

Dorneles, S., Araújo, W. J. d., and Costa, P. R. S. (2024). Segurança da informação e contratação de serviços de computação em nuvem na administração pública federal. *Revista RACIn*, 12(2).

Filypova, M. (2019). Systematic approaches to risk management in organizations. *International Journal of Risk Management*.

Furlan, L. d. M. (2021). Governança de riscos para superação dos desafios na

implementação da gestão de riscos corporativos na administração pública federal. Dissertação (mestrado em administração universitária), Universidade Federal de Santa Catarina.

Gama, P. H. R. (2025). *AVALIAÇÃO DE PRÁTICAS DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO: Estudo de Validade de Conteúdo de Instrumento Baseado na ISO 31.000:2018*. Monografia, Universidade de Brasília.

Gonçalves, F. D. A. (2025). *POR QUE OS GESTORES DE SEGURANÇA DA INFORMAÇÃO NÃO UTILIZAM A GESTÃO DE RISCOS?* Monografia, Universidade de Brasília.

GSI/PR (2020). Instrução normativa gsi/pr nº 1, de 27 de maio de 2020: Política de segurança da informação no âmbito da apf. Gabinete de Segurança Institucional da Presidência da República.

GSI/PR (2021). Instrução normativa gsi/pr nº 3, de 9 de junho de 2021. Diário Oficial da União, Brasília. Dispõe sobre a gestão de riscos de segurança da informação e comunicações na Administração Pública Federal.

Ilbahar, E. and Cebi, S. (2018). The role of data quality in decision-making for risk management. *Safety Science*, 102:281–292.

International Organization for Standardization (2009). ISO 31000:2009 — Risk management — Principles and guidelines. Standard.

ISO (2018). Iso 31000:2018 — risk management – guidelines.

ISO (2018). *ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary*. International Organization for Standardization, Geneva.

ISO (2022a). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization, Geneva.

ISO (2022b). *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization, Geneva.

ISO (2022). Iso/iec 27005:2022 — information security, cybersecurity and privacy protection – guidance on information security risk management.

Kutsch, E. and Hall, M. (2009). The rational choice of not applying project risk management in information technology projects. *Project Management Journal*, 40(3):72–81.

Lento, L. O. B. (2024). *Um modelo adaptativo para gestão de riscos de segurança em IoT*. Tese de doutoramento em informática, Universidade de Évora.

Lisboa, L. H. (2021). Gestão de riscos em segurança da informação.

Martins, J. A. (2018). Gestão de riscos organizacionais: adaptações contextuais e desafios práticos. *Revista de Administração Pública*.

Moreira, R. S. and Lima, P. H. (2021). Cultura organizacional e a efetividade da gestão de riscos. In *Anais do Encontro Nacional da ANPAD (EnANPAD)*, Rio de Janeiro. ANPAD.

Ndlela, L. T. (2019). Stakeholder involvement in risk governance: a practical perspective. *Journal of Risk Research*.

Olechowski, A., Oehmen, J., Seering, W., and Ben-Daya, M. (2016). The professionalization of risk management: What role can the iso 31000 risk management principles play? *International Journal of Project Management*, 34(8):1568–1578.

Oliveira, R. S. (2017). Participação e governança em processos de risco. In *Anais do EnANPAD*.

Polit, D. F. and Beck, C. T. (2006). *The Content Validity Index: Are You Sure You Know What's Being Reported? Critique and Recommendations*, volume 29. Research in Nursing & Health.

Purdy, G. (2010). Iso 31000:2009 — setting a new standard for risk management. *Risk Analysis*, 30(6):881–886.

SGD/ME (2020). Instrução normativa sgd/me nº 117, de 19 de novembro de 2020: Indicação do encarregado pelo tratamento dos dados pessoais no âmbito da apf. Secretaria de Governo Digital do então Ministério da Economia.

SGD/MGI (2023). Portaria sgd/mgi nº 852, de 28 de dezembro de 2023. Diário Oficial da União, Brasília. Institui o Programa de Privacidade e Segurança da Informação (PPSI).

SGD/MGI (2024). Portaria sgd/mgi nº 4.248, de 26 de junho de 2024. estabelece recomendações para cumprimento da engd no período de 2024–2027. `https://www.in.gov.br/en/web/dou/-/portaria-sgd-mgi-n-4.248-de-26-de-junho-de-2024`. Diário Oficial da União.

Silva, A., Souza Neto, J., and Orlandi, T. R. C. (2025). Aplicação de um modelo de maturidade em governança de segurança da informação para a administração pública federal. *Perspectivas em Gestão & Conhecimento*, 15(1):15–37.

Silva, D. A. d., Silva, J. A. d., Alves, G. d. F., and Santos, C. D. d. (2021). Gestão de riscos no setor público: revisão bibliométrica e proposta de agenda de pesquisa. *Revista do Serviço Público*, 72(4):824–854.

Silva, M. E. (2019). Risco dinâmico e adaptação organizacional. *Revista Brasileira de Gestão e Inovação*.

Souza, F. C. (2011). *Cultura organizacional e gestão de riscos*. Atlas.

Vasconcelos, V. N., Lins, F. A. A., Valença, G., Losse, M. A. P. F., Morais, A. C. C. M., and Sousa, E. T. (2025). Instanciação do processo de gestão de riscos de segurança da informação da iso 27005 em organizações públicas. In *Anais do LASDiGov 2025*.

Vieira, A. F. and Barreto, M. L. (2019). Gestão de riscos e governança: uma análise da integração em organizações públicas. *Revista de Administração Pública*, 53(2):321–340.

Wallace, J. C. and Keil, M. (2004). Software project risks and their effect on outcomes. *Communications of the ACM*, 47(4):68–73.

Zou, P. X. W., Zhang, G., and Wang, J. (2017). Understanding the key risks in construction projects in china. *International Journal of Project Management*, 25(6):601–614.

Apêndice A – Termo de Consentimento Livre e Esclarecido

Você está sendo convidado(a) a participar de uma pesquisa que tem como objetivo entender sobre práticas e princípios adotados na Gestão de Riscos de Segurança da Informação na Administração Pública.

A participação é voluntária, e você pode desistir a qualquer momento. As respostas serão anônimas, e os dados coletados serão utilizados exclusivamente para fins acadêmicos e científicos, garantindo o sigilo, privacidade e confidencialidade das informações.

Ao prosseguir com o preenchimento deste formulário, você declara que compreendeu os objetivos da pesquisa e autoriza voluntariamente sua participação, de forma livre e esclarecida.

Apêndice B – Instrumento Validado para Diagnóstico de Aderência aos Princípios da ISO 31000:2018

Este apêndice apresenta o instrumento validado, composto por 48 assertivas organizadas de acordo com os princípios estabelecidos pela ISO 31000:2018. As assertivas foram reformuladas e validadas em Gama (2025), e avaliadas quanto à concordância em escala *Likert* de 1 (discordo totalmente) a 5 (concordo totalmente).

Princípio 1 – Integrada

1. Sempre que possível as decisões estratégicas da instituição consideram os resultados das análises de riscos levantadas pela equipe de TI e por outras áreas.
2. O comitê (ou grupo responsável) de Segurança da Informação busca envolver setores relevantes da instituição na identificação e avaliação de riscos.
3. Os líderes de diferentes áreas (administrativa, jurídica, negócios) são convidados a participar de discussões sobre riscos e segurança.
4. A gestão de riscos em minha instituição é considerada nos processos das principais áreas e é gradualmente incorporada às práticas diárias.
5. Há uma política formal que orienta a gestão de riscos nos projetos e processos organizacionais conforme as diretrizes institucionais.
6. As iniciativas de segurança da informação buscam integrar-se progressivamente aos mecanismos de governança institucional e ao planejamento estratégico.

Princípio 2 – Estruturada e Abrangente

1. Os riscos de segurança de TI são tratados em conjunto com outros riscos organizacionais garantindo uma visão holística.
2. A metodologia de gestão de riscos é padronizada e adaptável, sendo aplicada conforme as necessidades de diferentes unidades organizacionais e projetos.
3. Existe um processo formal documentado para identificar, analisar e tratar riscos nos principais ativos e setores da instituição, de forma centralizada e com aplicação gradativa às demais áreas.

4. Todos os riscos, desde incidentes críticos até vulnerabilidades consideradas menores, são mapeados e registrados em um repositório comum.
5. A instituição busca implementar um cronograma regular para revisar e atualizar o inventário de riscos na instituição.
6. A instituição utiliza *frameworks* reconhecidos (como ITIL, COBIT, NIST, CIS, ISO) para apoiar a gestão de riscos, aplicando-os de forma planejada e progressiva no ambiente de TI.

Princípio 3 – Personalizada

1. A gestão de riscos em minha organização é moldada às particularidades do nosso setor de atuação (ex.: educação, saúde, fiscalização).
2. As soluções e controles de segurança adotados são escolhidos após análise do contexto e necessidades exclusivas da instituição.
3. As metodologias e procedimentos de avaliação de riscos são adaptados, conforme necessário, aos processos e características específicas dos diferentes setores da organização.
4. Nossas políticas de segurança e gestão de riscos levam em conta a autonomia/setores específicos (ex.: liberdade acadêmica, serviços de pesquisa, áreas finalísticas etc.).
5. Quando definimos prioridades de risco, consideramos características próprias (p. ex.: dados sensíveis, perfis de usuários, legislação setorial).
6. Há flexibilidade para ajustar normas de risco e segurança de acordo com variações regionais ou departamentais, evitando um modelo genérico.

Princípio 4 – Inclusiva

1. O comitê ou fórum de segurança da informação é composto por membros de diferentes setores, não se restringindo apenas à equipe de TI.
2. As decisões sobre políticas e normas de segurança levam em conta as sugestões ou críticas dos demais departamentos, além do TI.
3. Antes de definir qualquer ação de tratamento de riscos, são consultadas as partes envolvidas e/ou impactadas.
4. Há uma comunicação clara e frequente sobre riscos e segurança, estimulando a colaboração de toda a equipe.
5. Representantes de todas as áreas (administrativa, operacional e técnica) participam ativamente das discussões sobre riscos.
6. A alta gestão e outras partes interessadas relevantes participam e apoiam as iniciativas de gestão de riscos, assegurando recursos e legitimidade.

Princípio 5 – Dinâmica

1. A equipe responsável por gestão de riscos recebe informações atualizadas sobre tendências de ataques e vulnerabilidades e ajusta os planos rapidamente.

2. Utilizamos ferramentas de *logs* e análise de vulnerabilidades de forma proativa, com alertas que geram revisões imediatas de risco.
3. A instituição revisa e atualiza seu inventário de riscos periodicamente, independentemente da ocorrência de incidentes.
4. Mantemos um ciclo definido (mensal/trimestral/semestral) para reavaliar e priorizar riscos à luz de possíveis modificações no ambiente.
5. Há um processo formal de monitoramento contínuo que antecipa novas ameaças e vulnerabilidades, em vez de apenas reagir a incidentes.
6. Mudanças internas, como novos projetos, contratações, sistemas ou processos, incluem reavaliação dos riscos associados.

Princípio 6 – Melhor Informação Disponível

1. As equipes de segurança analisam regularmente os dados coletados (logs de sistemas, relatórios de auditoria, boletins de vulnerabilidade) para apoiar decisões de risco.
2. Quando surgem novos tipos de ataques ou vulnerabilidades, temos um canal eficiente para difundir e atualizar rapidamente nossa matriz de riscos.
3. Há ferramentas e processos definidos para correlacionar diferentes fontes de dados (logs, incidentes, boletins externos) e gerar insights confiáveis.
4. O comitê ou gestão de riscos utiliza sistematicamente informações atualizadas para redefinir prioridades e estratégias de segurança.
5. Nossa instituição mantém um repositório central ou painel que consolida logs, indicadores de vulnerabilidades e alertas em tempo real.
6. Os relatórios ou análises de segurança são compartilhados com setores relevantes, auxiliando na compreensão e priorização dos riscos.

Princípio 7 – Fatores Humanos e Culturais

1. Existem treinamentos regulares de conscientização de segurança, que são bem aceitos pela equipe.
2. Quando um incidente ocorre por falha humana, a instituição investiga o processo para aprendizado, em vez de meramente culpar indivíduos.
3. A alta gestão apoia e reforça a cultura de segurança, demonstrando exemplo e priorizando iniciativas de conscientização.
4. Os servidores e colaboradores, inclusive da alta gestão, compreendem a importância de sua conduta para a segurança e a gestão de riscos.
5. A organização utiliza incentivos ou reconhecimentos formais como estratégia para estimular as boas práticas de segurança.
6. A instituição adota ações de comunicação e capacitação para reduzir a resistência à adoção de novas ferramentas (ex.: autenticação multifator, assinatura digital).

Princípio 8 – Melhoria Contínua

1. Após a resolução de um incidente, sempre realizamos uma análise aprofundada (post-mortem) para identificar causas-raiz e oportunidades de melhoria.
2. As equipes são estimuladas a propor aperfeiçoamentos contínuos na abordagem de riscos, registrando sugestões e acompanhando sua implementação.
3. A cada implementação ou correção significativa de segurança, realizamos uma retrospectiva, documentando o que funcionou e o que pode ser aprimorado.
4. A organização possui um processo formal para revisar periodicamente as políticas e metodologias de gestão de riscos, incorporando lições aprendidas.
5. As auditorias internas ou externas contribuem para a implementação de melhorias nos processos de gestão de riscos.
6. Existe um calendário ou ciclo definido para reavaliar a efetividade dos controles e atualizar a matriz de riscos com base em novos aprendizados.