Universidade de Brasília

Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas

Departamento de Administração

FERNANDA DE ARAÚJO GONÇALVES

POR QUE OS GESTORES DE SEGURANÇA DA INFORMAÇÃO NÃO UTILIZAM A GESTÃO DE RISCOS?

Brasília – DF

2025

FERNANDA DE ARAÚJO GONÇALVES

POR QUE OS GESTORES DE SEGURANÇA DA INFORMAÇÃO NÃO UTILIZAM A GESTÃO DE RISCOS?

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Rafael Rabelo Nunes

Brasília – DF

2025

FERNANDA DE ARAÚJO GONÇALVES

Por que os Gestores de Segurança da Informação não utilizam a Gestão de Riscos?

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília da aluna

Fernanda de Araújo Gonçalves

Prof. Dr., Rafael Rabelo Nunes

Professor-Orientador

Prof. Dr., Victor Rafael Rezende Celestino

Professor-Examinador

Prof. Dr., Rildo Ribeiro de Santos

Professor-Examinador

Brasília, 17 de fevereiro de 2025

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, que me fortalece diariamente. À minha família, vocês foram essenciais em toda a minha caminhada e desenvolvimento, é visível em vocês o Amor de Deus que é incondicional, transformador e purificador. A minha mãe, uma mulher arretada que me ensinou a amar e escolher de forma correta, ao meu irmão que sempre zelou por mim e garante as vontades da queridinha, aos meus avós maternos e paternos, grandes exemplos do amor incondicional e que perdura por uma vida inteira. E pai, especialmente para o senhor, muito obrigada por acreditar em mim e embarcar nas minhas diversas "invenções de moda" como o senhor mesmo chama, é uma alegria poder partilhar cada conquista e dedicar a você, o primeiro gestor que tive contato e que para sempre será referência.

Aos meus amigos, que me permitiram continuar sorrindo e enxergando as belezas da vida no processo, especialmente ao cupcake que me acolhe mesmo sempre dormindo nos eventos não importando a altura do volume da música ou do barulho.

À Inframerica, que me recebeu no meu primeiro estágio e foi essencial para conhecer pessoas incríveis no TECA, além da oportunidade diária de estar em um dos meus lugares favoritos, o aeroporto, onde pude ter o primeiro contato com a gestão de riscos e logística.

À Embaixada do Reino unido, onde pude continuar minha carreira como estagiária no time de propriedades e facilities, e em seguida como Analista de Propriedades do FCDO no Brasil, é uma honra fazer parte deste time. À Andrea, minha primeira chefe, obrigada por me moldar e cada dia me orientar para sempre entregar meu máximo de forma completa e relevante, você é uma gestora de excelência e com certeza marcará minha carreira que está apenas começando. Phelipe e toda a turma do CS, a vida é mais bela com vocês, obrigada.

Professor Dr. Rafael, obrigada pela confiança com o projeto e os conselhos das nossas reuniões, todo esse processo foi marcante e será lembrado.

Equipe de estudos de Riscos e Seguranças cibernéticas, muito obrigada por todo apoio, recomendações e risadas, com certeza faziam as minhas sextas feiras serem melhores.

Gestores de Riscos da área de Segurança da informação apenas tenho a agradecer pela colaboração e disponibilidade em contribuir com o meu trabalho.

Obrigada UnB por me proporcionar experiências incríveis, desafiadoras e significantes.

“Reze como se tudo dependesse de Deus e trabalhe como se tudo dependesse de você.”

(Santo Inácio de Loyola)

RESUMO

A gestão de riscos desempenha um papel central na segurança da informação, garantindo a proteção e a continuidade operacional das organizações. No Brasil, desafios estruturais e culturais ainda impedem a implementação eficaz dessa prática, especialmente no setor público. O presente estudo visa identificar os fatores que dificultam o uso da gestão de riscos por Gestores de Segurança da Informação em órgãos públicos brasileiros, utilizando como referência os princípios estabelecidos pela ISO 31000:2018. A pesquisa foi conduzida em duas etapas por meio da aplicação de um questionário para Servidores Públicos Federais e posteriormente por entrevistas com Gestores Públicos Federais de Segurança da Informação, cujas respostas foram analisadas qualitativamente para identificar padrões e desafios recorrentes. Os resultados revelam barreiras estruturais e culturais como resistência organizacional, escassez de recursos humanos, restrições orçamentárias e baixa adesão da alta gestão que comprometem a implementação efetiva da gestão de riscos no setor público. Além disso, a pesquisa aponta a fragmentação na aplicação de frameworks e relações entre os fatores e os oito princípios da ISO 31000:2018. Por fim, são apresentadas recomendações para a aplicação de um questionário com assertivas baseadas na análise permitindo mensurar quantitativamente a aderência das instituições aos princípios da ISO 31000:2018, fortalecer a cultura organizacional, aprimorar processos e alinhar a gestão de riscos às diretrizes da ISO 31000:2018, promovendo um ambiente mais seguro e resiliente.

Palavras-chave: governança; conformidade; mitigação; estratégia; eficiência.

ABSTRACT

Risk management plays a central role in information security, ensuring organizational protection and operational continuity. In Brazil, structural and cultural challenges still hinder the effective implementation of this practice, particularly in the public sector. This study aims to identify the factors that impede the adoption of risk management by Information Security Managers in Brazilian public institutions, using the principles established by ISO 31000:2018 as a reference. The research was conducted in two phases: first, through a questionnaire administered to Federal Public Servants, followed by interviews with Federal Public Information Security Managers. The responses were qualitatively analyzed to identify recurring patterns and challenges. The results reveal structural and cultural barriers such as organizational resistance, shortage of specialized personnel, budget constraints, and limited support from senior management, all of which compromise the effective implementation of risk management in the public sector. Furthermore, the study highlights the fragmentation in the application of frameworks and the relationships between these factors and the eight principles of ISO 31000:2018. Finally, recommendations are presented for applying a questionnaire with statements based on the analysis, enabling the quantitative measurement of institutions' adherence to the principles of ISO 31000:2018, strengthening organizational culture, improving processes, and aligning risk management with ISO 31000:2018 guidelines, thereby fostering a safer and more resilient environment.

Keywords: governance; compliance; mitigation; strategy; efficiency.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

A gestão de riscos é um aspecto fundamental para a continuidade e o êxito das organizações modernas, especialmente em um cenário repleto de incertezas e complexidades (Lisboa, 2024). A habilidade de entender e aplicar de forma eficaz os princípios da gestão de riscos é vital para que as entidades possam não apenas reduzir ameaças, mas também aproveitar as oportunidades de maneira equilibrada. A trajetória histórica da percepção de risco, desde os primeiros tempos da humanidade, revela que o risco sempre esteve ligado à chance de recompensa, um conceito que continua a ser significativo no ambiente organizacional de hoje (Alves; Georg; Nunes, 2023).

Consoante a isso, a digitalização dos serviços públicos tem avançado significativamente, trazendo consigo um aumento proporcional dos riscos cibernéticos. De acordo com o Relatório de Riscos Globais (2025) do Fórum Econômico Mundial, o conflito armado entre Estados é apontado como o principal risco imediato, seguido por eventos climáticos extremos e pela desinformação. Embora o risco cibernético não esteja entre os três primeiros, a desinformação, que ocupa uma posição de destaque, está intrinsecamente ligada às ameaças cibernéticas, evidenciando a relevância dessas questões no cenário atual.

No contexto brasileiro, o governo tem implementado a Estratégia Nacional de Governo Digital (Governo Brasileiro, 2020), visando ampliar e simplificar o acesso aos serviços públicos por meio de soluções digitais. Essa estratégia busca um Estado mais inclusivo, eficaz, proativo, participativo e sustentável, adaptando processos às demandas atuais da sociedade com inovação e uso adequado de tecnologias.

Em 2022, o Brasil sofreu 103 bilhões de tentativas e ameaças de ataques cibernéticos (Jornal da Usp, 2023). Esses ataques, além de trazerem indisponibilidade de serviços e prejudicar a imagem da empresa, também geram um prejuízo médio que pode chegar a US$ 4,45 milhões (22 milhões de reais). Alguns desses incidentes, como foi o caso do ataque cibernético sofrido pelo sistema do SUS, demonstraram a necessidade de desenvolver uma política nacional de Cyber segurança e uma agência específica para tratar desses incidentes. (G1, 2021).

A mudança de cultura de resposta corretiva para preventiva se mostrou essencial na nova Política Nacional de Cibersegurança permitindo mais prevenção e preparo, de forma a

evitar os ataques cibernéticos e os prejuízos causados por eles. O decreto responsável por instituir a PNCiber também instituiu o Comitê Nacional de Cibersegurança (CNCiber), equipe responsável por propor atualizações à nova política, e os seus instrumentos (Estratégia Nacional e Plano Nacional de Cibersegurança), (Lumiun, 2024).

Apesar desses esforços, estudos indicam que apenas 5% das organizações no Brasil possuem um nível de preparação maduro para serem resilientes contra os riscos atuais de segurança cibernética (Cisco, 2024). Isso evidencia a necessidade de uma mudança cultural no gerenciamento de riscos, tanto cibernéticos quanto físicos, no setor público e privado. Portanto, é imperativo que o Brasil fortaleça suas estratégias de gestão de riscos cibernéticos, alinhando-se às melhores práticas internacionais e promovendo uma cultura de segurança da informação em todas as esferas governamentais e empresariais.

Dentro do ambiente organizacional, a administração de riscos vai além de uma simples ação de prevenção; ela se configura como uma ferramenta estratégica que potencializa a eficiência, a eficácia e a transparência das atividades (ABNT, 2018). Normas internacionais, como a ISO 31000:2018, disponibilizam orientações abrangentes sobre a gestão de riscos, incentivando uma abordagem proativa e estruturada (Coso, 2007).

A implementação dessas recomendações pode aprimorar a habilidade das organizações de realizar decisões embasadas, aumentar sua resiliência e atingir objetivos de forma sustentável (Moreira *et al*., 2021). No entanto, a administração de riscos no setor público brasileiro ainda lida com consideráveis obstáculos (Alves *et al*., 2021). O estudo proposto tem como objetivo examinar esses desafios, centrando-se nos princípios delineados pela ISO 31000:2018 e investigando os motivos pelos quais a gestão de riscos não foi amplamente incorporada na gestão da segurança da informação por gestores públicos (Lisboa, 2024; Queiroz; Nunes, 2023).

Apesar de a ISO 27.001 descrever que a gestão de segurança da informação deve ser feita com base em riscos, essa integração ainda não foi plenamente implementada. Ao abordar essas questões, a pesquisa busca contribuir para o desenvolvimento das práticas de gestão de riscos, ressaltando sua relevância na geração e na proteção de valor nas instituições (Shapira *et al*., 2021).

1.2 Formulação do problema

Dado o contexto explicitado, ainda cabe dúvidas sobre os fatores que dificultam a implementação da gestão de riscos em organizações públicas. Sendo assim, a questão que norteia a problemática deste trabalho é: Quais são os fatores que impedem a aplicação efetiva da gestão de riscos pelos responsáveis pela segurança da informação?

1.3 Objetivo Geral

A presente pesquisa tem como objetivo geral identificar os fatores que dificultam o uso da gestão de riscos por gestores de segurança da informação em órgãos públicos brasileiros.

1.4 Objetivos Específicos

Os objetivos específicos desta pesquisa são:

1. Mapear os desafios e dificuldades comuns enfrentados pelos responsáveis pela segurança da informação na aplicação da gestão de riscos.

2. Analisar como esses desafios afetam a eficácia da gestão de riscos nas organizações.

3. Identificar possíveis soluções ou melhores práticas para superar os obstáculos encontrados.

4. Propor recomendações para melhorar a implementação da gestão de riscos na segurança da informação.

5. Comparar os achados com as práticas e comportamentos esperados prescritos pelos princípios da gestão de riscos.

1.5 Justificativa

A gestão de riscos é um aspecto crítico para a segurança da informação, especialmente em um cenário onde as ameaças cibernéticas estão se tornando cada vez mais sofisticadas. A aplicação efetiva de estratégias de gestão de riscos é essencial para proteger dados sensíveis e garantir a continuidade das operações organizacionais. Conforme observado, a gestão de riscos

auxilia as organizações a estabelecer estratégias fundamentadas, alcançar objetivos e proteger o valor organizacional, especialmente em contextos sensíveis, como o Poder Judiciário brasileiro (Nunes; Perini; Pinto, 2022).

Os estudos apontam que existem barreiras significativas que dificultam a implementação de práticas eficazes, como a ausência de alinhamento estratégico, a falta de priorização de controles e a necessidade de avaliações contínuas para identificar e mitigar riscos. Tais desafios foram destacados na análise de riscos do Poder Judiciário, que mostrou a necessidade de controles mais robustos para reduzir vulnerabilidades críticas e proteger a integridade dos processos judiciais (Conselho Nacional de Justiça, 2021).

Este estudo é fundamental porque busca identificar e compreender esses obstáculos, preenchendo uma lacuna importante na teoria e na prática da gestão de riscos em segurança da informação. Embora existam diversos modelos e abordagens para a gestão de riscos, há uma falta de investigação aprofundada sobre os fatores específicos que dificultam sua implementação prática. Ao investigar essas barreiras, a pesquisa contribuirá para o avanço do conhecimento acadêmico e permitirá uma melhor compreensão das dificuldades enfrentadas pelos profissionais da área.

Além disso, a pesquisa tem potencial de impacto prático, já que identificar os desafios e fornecer recomendações para superá-los permitirá que as organizações desenvolvam estratégias mais eficazes para gerenciar riscos e proteger suas informações. Com a aplicação das soluções propostas, as organizações poderão melhorar sua resiliência contra ameaças e reduzir os impactos de incidentes de segurança.

A escolha da norma ISO 31000:2018 para o processo de análise é justificada pela sua significativa relevância na gestão de riscos em organizações. Por meio de suas diretrizes abrangentes, a norma oferece uma estrutura sólida e sistemática para identificação, avaliação e tratamento de riscos, permitindo que as empresas adotem uma abordagem proativa em relação aos desafios que possam surgir em seus ambientes operacionais. Ao seguir as orientações da ISO 31000:2018, as organizações podem fortalecer sua capacidade de tomar decisões informadas e embasadas, aumentar sua resiliência diante de situações adversas e, consequentemente, melhorar o desempenho geral, promovendo assim a criação e proteção de valor para a organização.

A presente pesquisa ganha relevância diante das circunstâncias, uma vez que, de acordo com um estudo realizado pela Marsh Risk Consulting em 2018, apenas 37% das empresas

brasileiras adotavam práticas de gestão de riscos até aquela época. Assim, torna-se essencial compreender não apenas a adoção de práticas e modelos, mas também os princípios que os fundamentam.

Contribuindo para o aprimoramento da gestão de riscos nas empresas do Brasil, essa pesquisa destaca a importância de compreender os princípios subjacentes a tais práticas e modelos, permitindo que as organizações melhorem sua resiliência e desempenho geral, antecipando, prevenindo e mitigando potenciais riscos.

Dada a urgência e a relevância do tema, a realização desta pesquisa é imperativa. Ela não apenas ampliará o entendimento sobre as dificuldades na gestão de riscos, mas também fornecerá orientações práticas para aprimorar a segurança da informação, contribuindo para a proteção eficaz de dados e a continuidade das operações empresariais.

2 REFERENCIAL TEÓRICO

2.1 Segurança da Informação

Segurança da Informação refere-se à proteção de informações contra acessos não autorizados, divulgação, alteração, destruição ou interrupção. O objetivo principal é garantir a confidencialidade, integridade e disponibilidade dos dados. Ela abrange um conjunto de práticas e controles destinados a proteger as informações em diversos formatos e mídias. Dessa forma, mostra-se extremamente necessária e importante numa realidade de constante desenvolvimento e inserção no mundo digital, especialmente no contexto do Poder Judiciário brasileiro, onde a transformação digital ampliou a exposição a riscos cibernéticos significativos (Hino; Cunha, 2020; Moura; Borges, 2022).

Além disso, a segurança da informação é essencial para prevenir impactos negativos que podem resultar de ataques cibernéticos. Casos recentes no Brasil demonstram que invasões a sistemas judiciais comprometeram não apenas a integridade dos dados, mas também a confiança pública e a continuidade operacional de tribunais, como evidenciado por ataques ao STJ e outros órgãos do Judiciário (Reina, 2022). Esses incidentes destacam a necessidade de controles de segurança mais robustos e integrados para mitigar riscos e garantir a continuidade das atividades essenciais (Nunes; Perini; Pinto, 2022).

Com a finalidade de padronizar, especificar e estabelecer requisitos para a segurança da informação globalmente, a ISO 27001 foi desenvolvida visando estabelecer, implementar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Ela fornece uma estrutura sistemática para gerenciar informações sensíveis, incluindo a implementação de controles e a realização de avaliações de risco.

A norma adota um ciclo de gestão contínuo que ajuda as organizações a protegerem seus dados e atenderem às exigências regulatórias, garantindo que esteja atualizada e condizente com a realidade mundial (ISO, 2022). Esta norma é amplamente adotada por organizações que buscam estruturar sua gestão de segurança da informação, a ISO 27001 ajuda as organizações promovendo um ambiente de maior segurança e conformidade quando corretamente implementada e alimentada (IFAC, 2024).

A segurança cibernética ou cibersegurança é um subconjunto da Segurança da informação que se concentra especificamente na proteção de sistemas e redes contra ameaças digitais, como ataques cibernéticos. Enquanto a Segurança da Informação aborda a proteção de

dados de forma ampla, a cibersegurança se dedica a mitigar riscos associados ao ambiente digital. É por meio dela que se é possível usufruir de ferramentas e técnicas específicas para enfrentar ameaças cibernéticas (Andress; Winterfeld, 2018).

A relação entre cibersegurança e Segurança da Informação é vital, pois a proteção digital é uma parte essencial da estratégia geral de segurança da informação. A integração de novas tecnologias, como o *blockchain*, no contexto da segurança digital, reflete a necessidade de um enfoque robusto em cibersegurança dentro dos sistemas de gestão de segurança da informação (Hanna, 2020).

Ataques cibernéticos podem ter impactos devastadores para as organizações, afetando a integridade dos dados, a confiança dos clientes e a continuidade dos negócios. Os impactos de uma violação cibernética incluem danos financeiros significativos e perda de reputação, destacando a necessidade urgente de implementar medidas de Cibersegurança eficazes (HBR, 2023). Dessa forma, é possível perceber a importância da gestão eficaz de riscos.

2.2 Gestão de Riscos

Nos primórdios da história humana, o risco físico e a recompensa material sempre caminharam juntos. O homem das cavernas que corria riscos para obter alimento tinha, naturalmente, mais chances de sobreviver, enquanto aquele que se esquivava acabava morrendo de fome (Damodaram, 2009). Desse modo, os riscos se apresentam como ponto inerente de toda e qualquer atividade humana, tornando-se, portanto, impossível eliminá-los por completo (Vieira; Barreto, 2019; Assunção; Lima, 2003).

Essa realidade, consequentemente, também se aplica ao âmbito organizacional (Montezano *et al.,* 2019). Afinal, assumir riscos é uma precondição essencial para o desenvolvimento humano; se parássemos de assumir riscos, inovações técnicas e sociais necessárias para solucionar muitos dos problemas mundiais desapareceriam (Wildavsky, 1979).

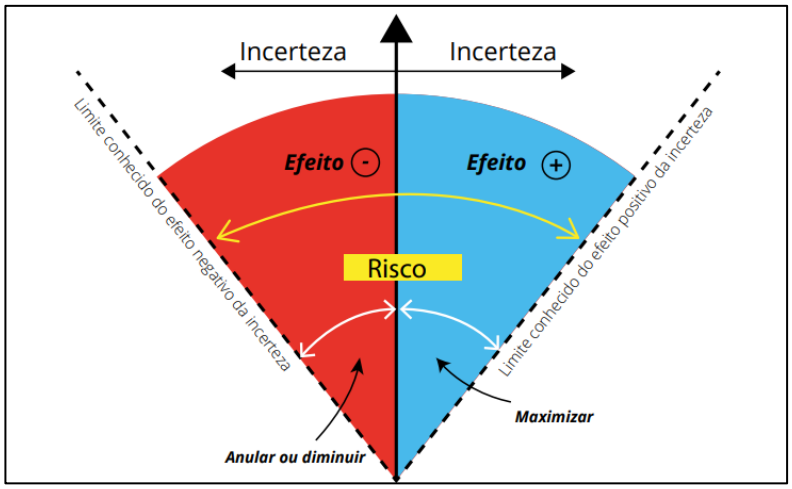
Conforme observado, a ideia de risco tem sido definida de maneiras diversas, não havendo consenso a respeito dessa temática (Jhunior; Abib, 2019). Knight (1921) definiu risco como um fato resultante de uma decisão tomada em condições de probabilidade conhecidas. No mundo das finanças, Damodaram (2009) definiu o construto como a variabilidade dos retornos observados em comparação com o retorno esperado de investimentos realizados. Aven

e Reen (2011), por sua vez, descreveram o risco como a incerteza sobre os resultados de uma atividade em relação a algo que as pessoas atribuem valor.

Dessa forma, é possível compreender o risco como a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos, combinada com o impacto dessa ocorrência sobre os resultados pretendidos (TCU, 2018). Contudo, para efeitos da presente pesquisa, adotou-se a definição estabelecida no normativo ISO 31000:2018. O normativo estabelece que risco é o efeito da incerteza sobre objetivos estabelecidos.

Os riscos podem ser algo que buscamos ou evitamos, no entanto, nossas percepções em relação a eles tendem a ser predominantemente negativas. Os riscos negativos, também conhecidos como ameaças, devem ser prevenidos ou minimizados, enquanto os riscos positivos, ou seja, as oportunidades, devem ser aproveitados ao máximo (Fonte, 2018). Portanto, é essencial que as organizações abordem os riscos de forma equilibrada, evitando efeitos negativos da incerteza e aproveitando os positivos, conforme exemplificado no diagrama a seguir.

Figura 1 – Abordagem de Riscos



Fonte: Rosa e Toledo (2015).

Dessa forma, para que o gestor possa potencializar os efeitos positivos das incertezas, é fundamental que ele estabeleça a gestão de riscos em seu contexto organizacional. A gestão de riscos é reconhecida como uma abordagem para aumentar a probabilidade de sucesso em tarefas complexas (Olechowski *et al.,* 2016) e, por sua natureza, é propensa a riscos de qualquer natureza. A gestão de riscos estimula a transparência organizacional, contribui para a gestão eficiente e eficaz dos recursos, além de fortalecer a reputação da imagem organizacional (Sousa

et al., 2018). Sendo assim, adotar práticas de gestão de risco permite identificar potenciais ameaças e oportunidades, possibilitando uma resposta proativa diante dos cenários de incertezas.

Gerenciar riscos envolve um conjunto de atividades coordenadas destinadas a orientar e controlar uma organização em relação a esses riscos (Sousa, 2018). Além disso, nos últimos anos, houve um rápido e generalizado desenvolvimento de modelos e práticas para o gerenciamento do risco operacional (Oliveira; Soares, 2018). No entanto, mais do que simplesmente aplicar esses modelos de gestão de riscos, é imprescindível que haja um foco nas diretrizes e nos princípios fundamentais que regem a gestão de riscos como um todo.

Foi conduzida uma pesquisa por Olechowski *et al*. (2016) que constatou que a adesão aos princípios de gerenciamento de riscos em alto nível desempenha um papel significativo no alcance bem-sucedido das metas de custo, cronograma, técnicas e satisfação dos clientes. Além disso, essa abordagem também contribui para uma execução mais estável do projeto. Diante de pesquisas como essa, a dúvida é por que os gestores da segurança de informação não utilizam a gestão de riscos de forma sistemática.

Destinado a pessoas que desejam criar e proteger valor nas organizações, gerenciando riscos, tomando decisões, estabelecendo e alcançando objetivos e melhorando o desempenho, a ISO 31000:2018 é uma norma internacional que oferece diretrizes para a gestão de riscos. Publicada pela International Organization for Standardization (ISO), essa norma estabelece um quadro abrangente e sistemático para a identificação, análise, avaliação, tratamento e monitoramento de riscos em diversos contextos organizacionais.

A ISO 31000:2018 incentiva as organizações a adotarem uma abordagem proativa em relação aos riscos, promovendo a melhoria contínua e uma cultura de conscientização sobre a importância do gerenciamento de riscos em todas as atividades empresariais. Ao seguir as orientações da norma, as empresas podem otimizar seus processos, tomar decisões mais informadas e fortalecer a resiliência para enfrentar desafios inesperados, contribuindo, assim, para o alcance de seus objetivos de maneira mais segura e sustentável (ABNT, 2018).

A ISO 31000:2018 oferece um guia sistemático e abrangente para a gestão de riscos, sendo estruturada em três pilares fundamentais: Princípios, Estrutura e Processos. Essa abordagem visa integrar a gestão de riscos em todos os níveis da organização, tornando-a parte integrante das decisões estratégicas e operacionais, bem como da cultura organizacional (Purdy, 2010). Essa integração permite às organizações enfrentarem incertezas de forma mais eficaz,

mitigando impactos negativos e aproveitando oportunidades. Segundo Rampini (2019), a versão revisada da norma trouxe uma abordagem mais estratégica, aprofundando os princípios e metodologias da gestão de riscos (ABNT, 2018)

A estrutura é o componente que fornece a base organizacional para a gestão de riscos. Ela envolve o comprometimento da alta liderança, a alocação de recursos adequados e a definição de responsabilidades claras em toda a organização. Essa estrutura também prevê a integração da gestão de riscos em todos os processos organizacionais, de forma a garantir que ela esteja alinhada com os objetivos estratégicos, o contexto externo e as partes interessadas. Além disso, a estrutura deve ser flexível e capaz de se adaptar às mudanças internas e externas para que seja eficaz (ISO 31000:2018).

Os processos são detalhados como uma série de etapas que devem ser seguidas para gerenciar os riscos de forma eficaz. Esses processos incluem a comunicação e consulta com as partes interessadas, o estabelecimento do contexto, a identificação, análise e avaliação de riscos, o tratamento de riscos e o monitoramento e revisão contínuos. Essa abordagem iterativa e dinâmica garante que a gestão de riscos seja atualizada regularmente, acompanhando mudanças no ambiente organizacional e permitindo decisões embasadas e proativas (ISO 31000:2018).

A próxima seção abordará os princípios da ISO 31000:2018, que formam a base para um sistema de gestão de riscos eficaz e integrado. Esses princípios incluem aspectos como inclusão, melhoria contínua e personalização, que ajudam as organizações a adaptar a gestão de riscos às suas necessidades específicas, maximizando os benefícios para a organização como um todo. Eles representam a essência da norma e são fundamentais para garantir sua aplicação prática em diferentes contextos organizacionais.

2.3 Os oito princípios da ISO 31000:2018

2.3.1 Integrada

Conforme estabelecido pela ISO 31000:2018, a gestão de riscos é uma parte essencial de todas as atividades realizadas em uma organização (Associação Brasileira de Normas Técnicas, 2018). Da mesma forma, a ISO 31004:2015, que serve como um guia normativo para a implementação da ABNT NBR ISO 31000:2018, reforça essa ideia, enfatizando que a gestão

de riscos não deve ser tratada como uma atividade isolada e independente das principais atividades e processos da organização.

Pelo contrário, a responsabilidade pela gestão de riscos recai sobre a direção da organização e está intrinsecamente conectada a todos os processos organizacionais, incluindo o planejamento estratégico, bem como os projetos e processos de gestão de mudanças (Associação Brasileira de Normas Técnicas, 2015). De acordo com Moreira *et al*. (2021), o princípio da integração na gestão de riscos vai além da mera adição de práticas de gerenciamento de riscos aos processos organizacionais.

De acordo com o grupo de pesquisadores, esse princípio ressalta a importância de promover ativamente o envolvimento e a participação de todos os membros da organização. Seguindo essa linha de pensamento, Araújo e Gomes (2021) enfatizam a necessidade de as organizações incorporarem e aprimorarem constantemente seus processos de gerenciamento de riscos, mantendo boas práticas para integrar o gerenciamento de riscos e construir uma cultura organizacional na qual todos sejam responsáveis pela gestão de riscos.

A ISO 31000:2018 estabelece a recomendação de que as organizações integrem de forma sistemática, transparente e confiável o processo de gerenciamento de riscos em sua governança, estratégia e processos gerais. Essa abordagem é respaldada pelos resultados da pesquisa conduzida por Olechowski *et al*. (2016), que ressaltam a importância de um processo de gerenciamento de riscos que esteja adequadamente integrado aos demais projetos e à organização como um todo. Assim, fica evidente que o primeiro princípio destacado na norma ISO 31000:2018 – integração – desempenha um papel fundamental na gestão de riscos ao promover a colaboração e a sinergia entre os diversos elementos envolvidos nesse processo.

Apesar da sua relevância, ainda é comum que a gestão de riscos, quando não integrada a outras atividades e processos, seja percebida como uma tarefa administrativa adicional, desprovida de valor agregado, ou até mesmo como um exercício burocrático que não contribui para a criação ou proteção de valor (Associação Brasileira de Normas Técnicas, 2015).

Em vista disso, é essencial integrar a gestão de riscos à cultura da organização e aos processos habituais, a fim de que sua importância seja reconhecida e para torná-la um processo efetivo. Dessa forma, ao incorporar a gestão de riscos de forma integrada, a organização poderá maximizar os benefícios dessa prática e fortalecer sua capacidade de tomar decisões informadas e proativas diante dos riscos enfrentados.

Como destacado anteriormente, a gestão de riscos é uma parte intrínseca de todas as atividades organizacionais, desde o planejamento estratégico até os projetos e processos de gestão de mudanças (Associação Brasileira de Normas Técnicas, 2015). Alinhado a isso, o Tribunal de Contas da União – TCU (2020) enfatiza que a gestão de riscos deve ser integrada ao processo decisório, desde que apresente uma relação custo-benefício favorável.

Portanto, é essencial que organizações e gestores estejam em conformidade com o princípio da integração a fim de garantir que a gestão de riscos seja devidamente incorporada em todas as áreas e processos. A integração efetiva da gestão de riscos fortalece a capacidade organizacional de identificar e enfrentar os riscos de forma proativa, garantindo a continuidade dos negócios e a obtenção de melhores resultados (ABNT, 2018). De acordo com Souza (2011), adotar uma abordagem integrada possibilita alcançar um desempenho consistentemente superior, ao mesmo tempo em que gerencia os riscos de maneira proativa.

A integração na gestão de riscos contribui para uma abordagem mais holística e proativa, garantindo que os riscos sejam tratados de maneira efetiva e que a organização esteja preparada para lidar com desafios e incertezas de forma mais eficiente e resiliente. Dessa forma, a gestão de riscos não deve ser considerada como um elemento à parte dos processos de gestão, mas sim como parte fundamental de cada um desses processos (ABNT, 2018). Vieira e Barreto (2019) ressaltam que uma cultura de integridade e cooperação dentro das instituições públicas é essencial para fortalecer a gestão de riscos, garantindo maior transparência e responsabilidade na tomada de decisões.

A ISO 31004:2015, norma guia para a implementação da ISO 31000:2018, apresenta diretrizes sobre as formas de aplicação do princípio da integração na gestão de riscos. De acordo com esse documento, a integração deve ocorrer em diversos aspectos organizacionais, incluindo a governança corporativa, a cultura organizacional, as estratégias e objetivos, os processos de tomada de decisão, a gestão de projetos e as atividades de monitoramento e revisão (Purdy, 2010).

De acordo com o documento, o princípio da integração pode ser aplicado de duas formas principais. Primeiro, no desenvolvimento, manutenção e melhoria da estrutura para gerenciamento de riscos. Isso implica integrar os componentes dessa estrutura ao sistema global de gestão e tomada de decisões da organização, independentemente de ser formal ou informal (Silva; Neves, 2019). Convém que a estrutura para gerenciar riscos seja compreendida pela integração de seus componentes ao sistema de gestão existente, e que os processos de gestão sejam aprimorados com base na ISO 31000:2018.

Além disso, é importante que o processo de gestão de riscos seja parte integrante das atividades que geram risco. Caso contrário, a organização pode perceber a necessidade de modificar as decisões posteriormente, quando os riscos associados forem melhor compreendidos. Se não houver um sistema formal de gestão, é possível que uma estrutura para gerenciar riscos seja utilizada para esse propósito (Rampini, 2019).

Ainda de acordo com os documentos que aqui são utilizados como base para as análises – ISO 31000:2018 e ISO 31004:2015 –, é recomendado que a organização expresse sua intenção em relação à gestão de riscos de forma consistente com suas outras intenções, garantindo alinhamento entre os diferentes aspectos da organização. É aconselhável incorporar os componentes da estrutura de gestão de riscos aos sistemas de gestão existentes, integrando-os às atividades e processos habituais da organização, evitando a percepção de ser uma tarefa administrativa adicional (Moreira *et al*., 2021).

Os organismos de auditoria têm um papel importante ao questionar as decisões da direção e garantir a aplicação adequada do processo de gestão de riscos, assegurando a efetiva implementação do princípio da integração em todas as decisões e atividades organizacionais.

Em resumo, a integração da gestão de riscos é um princípio-chave que permeia todas as atividades organizacionais. A ISO 31000:2018 destaca a importância de incorporar o processo de gerenciamento de riscos em todos os níveis da organização, desde a governança até as operações diárias. Essa abordagem promove a interação entre os diferentes elementos envolvidos no processo de gestão de riscos, facilitando uma compreensão abrangente dos riscos, tomada de decisões informadas e resiliência organizacional (Vieira; Barreto, 2019).

Ao integrar a gestão de riscos em sua cultura e práticas habituais, a organização pode garantir que a identificação, avaliação e tratamento de riscos sejam uma parte intrínseca de suas operações, contribuindo para a criação e proteção de valor (Silva; Neves, 2019). Portanto, aderir ao princípio da integração é essencial para uma gestão de riscos eficaz e bem-sucedida.

2.3.2 Estruturada e Abrangente

A norma ISO 31000:2018 define que a gestão de riscos deve ser conduzida de acordo com uma abordagem estruturada e abrangente, destacando a relevância da sistematização desse processo. A estruturação da gestão de riscos implica na definição e compartilhamento interno de políticas e processos que auxiliem na identificação de potenciais riscos. Por sua vez, a

abrangência da gestão de riscos refere-se à sua amplitude dentro da organização, abarcando todos os setores e níveis hierárquicos. Nesse sentido, Surya Prakash, Gunjan Soni e Ajay Pal Singh Rathore (2017) argumentam que, ao formular uma estratégia de combate ao risco, o foco principal é apresentar possíveis políticas e métodos para lidar com as consequências do risco.

Além disso, como enfatizado por Filyppova *et al*. (2019), é essencial adotar uma abordagem estruturada e abrangente para avaliar e controlar os riscos de maneira eficaz. Essa abordagem não apenas contribui para obter resultados consistentes e comparáveis, conforme ressaltado pela Associação Brasileira de Normas Técnicas (2018), mas também proporciona uma base sólida para uma gestão de riscos eficiente e proativa. No entanto, para garantir o sucesso dessas políticas e processos, é necessário o envolvimento de todas as partes interessadas e a implementação de mecanismos de monitoramento e revisão contínua.

A adoção de um modelo sistematizado de gestão de riscos, de acordo com Artur Araújo e Anailson Gomes (2021), alia confiabilidade, padronização e reconhecimento de boas práticas. Esse modelo proporciona uma abordagem estruturada e eficaz para lidar com os desafios dos riscos enfrentados pelas organizações. A confiabilidade é garantida por meio de processos comprovados, enquanto a padronização promove uma abordagem consistente na identificação e tratamento de riscos. Além disso, o reconhecimento de boas práticas fortalece a credibilidade e eficácia da gestão de riscos da organização.

O gerenciamento de riscos exige a consideração de diversos fatores, incluindo o contexto interno e externo da organização, bem como os aspectos humanos e culturais envolvidos (Moreira *et al*., 2021; Oliveira *et al*., 2017). Ao analisar o contexto interno, é necessário avaliar a estrutura organizacional, os processos de trabalho, os recursos disponíveis e as políticas internas que influenciam os riscos. Por sua vez, ao levar em conta o contexto externo, é essencial considerar regulamentações governamentais, condições de mercado, concorrência e mudanças tecnológicas que podem afetar os riscos enfrentados pela organização (Oliveira *et al*., 2017).

Como dito, além de levar em conta fatores puramente organizacionais, a gestão de riscos deve considerar os fatores culturais e humanos, reconhecendo as capacidades, percepções e intenções do pessoal interno e externo, que podem influenciar positiva ou negativamente os objetivos organizacionais (Inácio *et al*., 2021; Tribunal de Contas da União, 2020). Dessa forma, a gestão de riscos engloba as atitudes, comportamentos, valores e crenças dos indivíduos envolvidos, tanto dentro quanto fora da organização, para uma abordagem mais abrangente e eficaz.

Gabriel Rampinia, Harmi Takiab, Fernando Berssanetia (2019) defendem que a estruturação e abrangência são princípios fundamentais que garantem que a gestão de riscos seja um processo iterativo e possa ser aplicado nos diferentes níveis da organização, incluindo estratégico, operacional, de programa ou projeto. Diante disso, infere-se que a gestão de riscos é uma parte essencial de todos os processos e projetos de uma organização, sendo aplicada em todos os níveis para garantir a identificação, avaliação e mitigação dos riscos de forma sistemática e profícua. Ademais, a abordagem estruturada e abrangente contribui para a tomada de decisões informadas e a obtenção de resultados consistentes em toda a organização.

A norma ISO 31004:2015 – normativo que, embora cancelado, aborda minuciosamente as definições e aplicabilidade de cada um dos princípios – define o princípio da estruturação e abrangência como uma abordagem sistemática, oportuna e estruturada para a gestão de riscos, que contribui para a eficiência e a obtenção de resultados consistentes, confiáveis e comparáveis (Associação Brasileira de Normas Técnicas, 2015). Ao adotar uma abordagem estruturada, a organização estabelece uma base sólida para identificar, analisar, avaliar, tratar e monitorar os riscos. Isso envolve a definição de critérios de avaliação, a utilização de métodos e técnicas apropriados para análise de riscos e a implementação de medidas eficazes para mitigação ou aproveitamento dos mesmos.

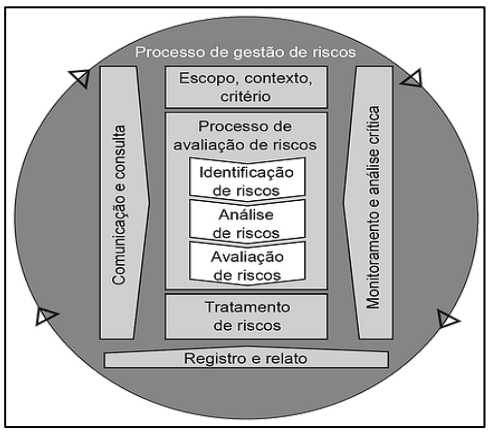
A aplicação de um processo de gestão de riscos estruturado e abrangente, de acordo com a norma ISO mencionada anteriormente, exige a criação e implementação de políticas e processos, juntamente com as devidas adaptações na estrutura organizacional para gerenciar os riscos (Associação Brasileira de Normas Técnicas, 2015). Essa abordagem auxilia o processo de integração, possibilitando a eficácia e o alinhamento da gestão de riscos com as práticas e objetivos da organização, conforme destacado por Artur Araújo e Anailson Gomes (2021).

O estudo conduzido pelos dois pesquisadores demonstrou que a implementação de sistemas e processos organizacionais que favorecem uma abordagem sistemática na gestão de riscos resulta em melhores decisões relacionadas aos riscos (Araújo; Anailson Gomes, 2021). Essa constatação fortalece a importância de estabelecer uma estrutura que considere não apenas os aspectos técnicos da gestão de riscos, mas também sua integração com as práticas existentes e os objetivos da organização. Dessa forma, a aplicação de um processo de gestão de riscos bem estruturado e alinhado torna-se ainda mais relevante para alcançar resultados consistentes e eficientes na tomada de decisões relacionadas aos riscos organizacionais.

Por fim, a aplicação do princípio da estruturação e abrangência na gestão de riscos, conforme a ISO 34001:2015, requer a adoção de uma abordagem sistematizada descrita na

ABNT NBR ISO 31000:2009 – aqui representada na imagem 1 –, junto com preparativos adequados. Essa abordagem estruturada deve ser flexível o suficiente para atender às necessidades específicas da organização, permitindo que o método de gestão de riscos seja consistente tanto com uma abordagem de cima para baixo quanto de baixo para cima, de modo a abordar o nível adequado de gestão (Associação Brasileira de Normas Técnicas, 2015). Isso garante que as atividades de gestão de riscos sejam conduzidas de maneira organizada, coerente e eficaz, proporcionando uma base sólida para a tomada de decisões relacionadas aos riscos.

Figura 2 – Processo de Gestão de Riscos



Fonte: ABNTNBR ISO 31000:2018

Com base nos argumentos apresentados, fica evidente que o segundo princípio estabelecido na norma ISO 31000:2018 não apenas está alinhado com a literatura recente, mas também a sustenta. Ao adotar uma gestão de riscos estruturada e abrangente, a organização fortalece sua capacidade de antecipar, avaliar e mitigar os riscos que possam impactar seus objetivos e resultados. Essa abordagem proporciona uma base sólida para identificar e lidar com os riscos potenciais, além de promover a eficiência e eficácia na tomada de decisões relacionadas aos riscos. Ao seguir esse princípio, a organização demonstra seu compromisso em gerenciar proativamente os riscos, salvaguardando seus interesses e aumentando sua resiliência diante de incertezas e ameaças.

2.3.3 Personalizada

O terceiro princípio da ISO 31000:2018 estabelece a necessidade de personalização do processo de gestão de riscos de acordo com as características e necessidades específicas de cada organização. Tanto a ISO 31000:2018 quanto a norma ISO 31004:2015 destacam a importância

de ajustar a gestão de riscos para atender aos contextos externo e interno da organização, considerando sua cultura, critérios de risco e objetivos. Essa personalização é fundamental para garantir a eficácia do processo de gestão de riscos, permitindo que seja adaptado e dimensionado conforme a realidade e as particularidades de cada organização.

A revisão sistemática realizada por Martins *et al*. (2018) reforça a ênfase da literatura sobre gestão de riscos na importância da personalização das categorias de riscos. Isso demonstra a adesão e concordância de teóricos e gestores de riscos ao terceiro princípio estabelecido na norma ISO. O enfoque atribuído a personalização é fundamental para incluir elementos específicos do negócio ou projeto em questão, evitando assim a possibilidade de negligenciar aspectos relevantes. O princípio da personalização reconhece que cada organização é única e enfrenta desafios distintos. Consequentemente, um modelo genérico de gestão de riscos pode não ser adequado para todas as situações.

A personalização da gestão de riscos implica que as organizações devem ajustar as diretrizes e estruturas fornecidas pela norma ISO 31000:2018 para se adequarem às suas circunstâncias específicas. Isso requer uma análise cuidadosa das atividades, objetivos e contexto operacional da organização, bem como das partes interessadas envolvidas. Ao compreender esses elementos específicos, a organização pode identificar e priorizar os riscos relevantes de maneira mais eficiente.

Um exemplo dos impactos da personalização pode ser observado nos resultados de uma pesquisa realizada por Inácio *et al*. (2021), que analisou a metodologia de gestão de riscos adotada pela Universidade Federal de Santa Catarina (UFSC). O estudo constatou que a criação de uma abordagem/metodologia própria para a elaboração do plano de gestão de riscos possibilitou que a instituição personalizasse sua gestão de riscos, aumentando, consequentemente, as chances de sucesso.

Além disso, a personalização do processo de gestão de riscos permite que a organização desenvolva abordagens e estratégias adaptadas às suas capacidades e recursos disponíveis. Isso é especialmente importante devido à escassez de recursos valiosos, o que impulsiona as empresas a encontrar formas eficientes de adquiri-los e aplicá-los (Massis *et al*., 2018). Sendo assim, a aplicação adequada desses recursos envolve naturalmente a adaptação dos métodos de avaliação de riscos, ferramentas de análise e processos de tomada de decisão para atender às necessidades e restrições da organização.

Incluir uma lista de categorias de riscos é considerado uma prática altamente benéfica no processo de personalização da gestão de riscos. No entanto, além de considerar as macros categorias geralmente utilizadas (como regulamentação, economia, concorrência, fornecedores, etc.), é fundamental incluir categorias específicas que orientarão o processo de identificação dos riscos (Martins *et al*., 2018).

Como mencionado anteriormente, a gestão de riscos é uma prática que está integrada a todas as atividades e processos de uma organização (Associação Brasileira de Normas Técnicas, 2015), o que ressalta a importância da personalização como um elemento intrínseco às atividades e processos organizacionais. Isso ocorre devido à variação que existe entre as organizações em relação às suas próprias atividades e processos.

Posto isso, verifica-se a relevância das micro categorias como mecanismos de personalização para uma gestão de riscos eficaz (Martins *et al*., 2018). Assim, a personalização possibilita que a gestão de riscos seja incorporada à essência da organização, tornando-se uma prática contínua e integrada em todas as atividades e decisões.

A personalização da gestão de riscos também impacta diretamente a comunicação organizacional. Uma comunicação intensa entre os participantes é essencial para um desempenho altamente confiável da avaliação e gestão de riscos (Paltrinieri; Comfort; Reiniers, 2019). Isso significa que uma comunicação efetiva e constante é um elemento fundamental para garantir o sucesso da abordagem personalizada de gerenciamento de riscos.

Ao personalizar a abordagem, a organização pode alinhar melhor as expectativas e garantir que todos os envolvidos tenham uma visão clara dos riscos e das medidas de mitigação necessárias. O normativo ISO 31000:2018 descreve a importância da personalização da gestão de riscos para atender às necessidades e características de cada organização. De acordo com a norma, não existe uma abordagem única correta, pois a concepção e implementação da estrutura e processos de gestão de riscos devem ser flexíveis e adaptáveis.

Diferentes áreas de risco podem exigir processos personalizados dentro da mesma organização, e é importante ajustar cada processo ao seu propósito específico. A concepção da estrutura de gestão de riscos deve refletir a forma como as decisões são tomadas, levando em consideração as obrigações legais e externas da organização. Além disso, é importante considerar questões internas e adaptar a estrutura para integrar os processos de tomada de decisão da organização. Em alguns casos, pode ser necessário modificar os processos existentes

para alinhá-los à estrutura de gestão de riscos estabelecida (Associação Brasileira de Normas Técnicas, 2015).

Para aplicar o terceiro princípio da ISO 31000:2018, é recomendado que a concepção da estrutura de gestão de riscos leve em consideração os pontos de vista dos envolvidos na sua implementação, conforme mencionado na ISO 31004:2015 (Associação Brasileira de Normas Técnicas, 2015). Além disso, é fundamental obter uma compreensão aprofundada dos conceitos fundamentais da ISO 31000:2018 para garantir que o ajuste da estrutura e do processo atenda aos atributos de uma gestão de riscos eficaz, conforme estabelecido na norma (Associação Brasileira de Normas Técnicas, 2015). Ao envolver os participantes e aprofundar o conhecimento das diretrizes, a organização estará melhor preparada para desenvolver uma estrutura de gestão de riscos personalizada e adaptada às suas necessidades específicas.

Em resumo, a personalização da gestão de riscos implica que os riscos semelhantes sejam percebidos e encarados de forma diferente, dependendo dos atores envolvidos em sua análise e avaliação. Isso destaca a importância de considerar as perspectivas individuais e as características específicas de cada organização ao desenvolver uma abordagem personalizada. Ao reconhecer essa diversidade de percepções e abordagens, é possível promover uma gestão de riscos mais eficaz e adaptada aos desafios enfrentados por cada organização.

2.3.4 Inclusiva

No contexto do gerenciamento de riscos, é essencial que o processo seja personalizado de acordo com o projeto e a organização em questão. Além disso, deve ser caracterizado pela transparência e, sobretudo, inclusão, garantindo a participação de todas as partes interessadas (Olechowski *et al*., 2016). De acordo com o quarto princípio da norma ISO 31000:2018, a inclusividade é enfatizada como uma importante diretriz no processo de gestão de riscos.

Isso implica envolver todas as partes interessadas relevantes de maneira apropriada e oportuna, a fim de considerar seus conhecimentos, perspectivas e percepções. Essa abordagem resulta em uma conscientização aprimorada e uma gestão de riscos mais fundamentada (Associação Brasileira de Normas Técnicas, 2018).

A inclusão de todas as partes interessadas, especialmente os tomadores de decisão, é fundamental na gestão de riscos. Ao envolver todos as partes, a gestão de riscos permanece pertinente e atualizada, permitindo decisões informadas (Associação Brasileira de Normas

Técnicas, 2015; Inácio *et al*., 2021). A participação inclusiva resulta em uma visão mais completa e eficaz para lidar com os riscos de forma adequada. Isso garante uma abordagem holística e abrangente, considerando diversas perspectivas.

Ou seja, a sistemática de gerenciamento de riscos estabelece uma estrutura que inclui processos e sistemas estabelecidos pelas partes interessadas, garantindo a incorporação da filosofia de risco nas atividades diárias da organização (Araújo; Gomes, 2021). Nesse sentido, o quarto princípio ISO busca promover a participação ativa de diferentes perspectivas e conhecimentos, além de incentivar a colaboração e a transparência.

A inclusividade na gestão de riscos é alcançada por meio do envolvimento das partes interessadas, resultando em maior conscientização e consideração de novos pontos de vista (Da Fonte, 2019). Isso envolve engajar funcionários, clientes, fornecedores, reguladores e a comunidade em geral. A comunicação desempenha um papel essencial nesse processo, permitindo a troca correta de informações entre diferentes áreas especializadas, fornecendo dados para a supervisão e tomada de decisão, e promovendo a inclusão e o senso de responsabilidade das partes afetadas pelo risco (Da Fonte, 2019).

A inclusão das partes interessadas no processo de gestão de riscos não apenas aumenta a probabilidade de identificação de riscos emergentes, mas também promove sua responsabilização (Oliveira *et al*., 2017). Isso resulta em um maior comprometimento das partes interessadas com a gestão de riscos, levando-as a se sentirem mais responsáveis e engajadas em tomar medidas para mitigar os riscos identificados (Ndlela, 2019).

Esse engajamento contribui para a criação de uma cultura organizacional que valoriza a gestão proativa de riscos, promovendo a segurança, a sustentabilidade e a continuidade dos negócios. Ao adotar uma abordagem inclusiva na gestão de riscos, a organização fortalece sua posição no mercado, demonstrando compromisso com a transparência e a governança corporativa.

Esse compromisso é ressaltado pelo alinhamento das partes interessadas em busca dos objetivos organizacionais, enfatizando a importância do gerenciamento de riscos como uma peça fundamental da governança corporativa (Montezano, 2019). Isso ajuda a construir confiança e relacionamentos sólidos com os diferentes grupos afetados pela organização, contribuindo para sua reputação e sustentabilidade a longo prazo. Ademais, a participação ativa das partes interessadas possibilita uma representação adequada e leva em consideração suas opiniões ao estabelecer os critérios de risco (Associação Brasileira de Normas Técnicas, 2015).

A inclusão das partes interessadas na consulta, como parte essencial do processo de gestão de riscos, requer um planejamento criterioso. É nesse momento que a confiança pode ser estabelecida ou abalada. Para garantir eficiência e fortalecer a confiança nos resultados, é recomendado envolver as partes interessadas relevantes em todos os aspectos do processo de gestão de riscos, inclusive na concepção do processo de comunicação e consulta (Associação Brasileira de Normas Técnicas, 2015).

Sendo assim, no que concerne à aplicação do quarto princípio na norma ISO 31004:2015, é recomendado que a adoção desse princípio leve em consideração aspectos de confidencialidade, segurança e privacidade. Um exemplo disso é a possibilidade de ser necessário separar as informações contidas nos registros de riscos, de forma a restringir o acesso a determinadas informações (Associação Brasileira de Normas Técnicas, 2015).

Adicionalmente, a ISO 31004:2015 ressalta a importância de incluir a simulação de papéis no contexto da comunicação e consulta durante a formação em gestão de riscos. Essa abordagem permite avaliar como os destinatários das informações percebem as mensagens transmitidas, garantindo que a comunicação seja eficaz e contribua para uma cultura organizacional mais robusta (Silva; Neves, 2019).

Além disso, é aconselhável realizar uma avaliação periódica para demonstrar o quão bem o que foi prometido ou concebido realmente funcionou na prática. A norma também encoraja a valorização e o reconhecimento de visões não solicitadas, incentivando que sejam apreciadas e, sempre que possível, fornecendo um feedback sobre essas contribuições (Souza, 2018).

Em resumo, o quarto princípio da ISO 31000:2018, a inclusividade, enfatiza a importância de envolver todas as partes interessadas relevantes no processo de gestão de riscos. Ao promover a participação ativa, a colaboração, a transparência e a equidade, a inclusividade fortalece a identificação e o tratamento dos riscos, promove a responsabilização e o comprometimento das partes interessadas e fortalece a credibilidade da organização (Vieira; Barreto, 2019). Essa abordagem impulsiona a melhoria contínua e contribui para a construção de uma cultura de gestão de riscos sólida e resiliente, garantindo que os riscos sejam compreendidos e tratados de forma eficaz em todos os níveis da organização (Pereira, 2019).

2.3.5 Dinâmica

A gestão de riscos deve ser sensível às mudanças, tanto internas quanto externas, que ocorrem nos contextos organizacionais. Assim, o acompanhamento e revisão dos riscos precisam ocorrer constantemente, permitindo a identificação de novos riscos, a modificação de alguns e o desaparecimento de outros (Associação Brasileira de Normas Técnicas, 2015). Diante da volatilidade dos contextos organizacionais, o quinto princípio da ISO 31000:2018, conhecido como "Dinâmica", refere-se à essa natureza de constante mudança dos riscos e da gestão de riscos.

A dinamicidade dos riscos, bem como da gestão de riscos é abordada mais detalhadamente na ISO 31004:2015. Conforme estabelecido no normativo, a gestão de riscos deve ser um processo adaptativo e flexível, capaz de reagir às mudanças, ajustando estratégias e medidas preventivas à medida que novos riscos surgem e outros se tornam obsoletos. Dessa forma, o referido princípio reconhece a evolução dos riscos e a importância de uma gestão de riscos ágil e flexível para lidar com essas mudanças.

Como dito, os riscos não são estáticos, mas sim dinâmicos. Portanto, podem surgir, evoluir (Oliveira; Silva; Leite, 2018) e desaparecer ao longo do tempo. Diante dessa perspectiva, é importante compreender que, assim como os riscos, a comunicação e o processo de gestão de riscos devem ser encarados como processos igualmente dinâmicos e interativos, envolvendo a troca de informações relevantes entre diversos agentes (Ndlela, 2019). A análise dos processos de gerenciamento de riscos na indústria da construção realizada por Zou, Kiviniemi e Jones (2017) demonstrou que, ao longo do desenvolvimento de projetos, sobretudo de longa duração, é frequente a ocorrência de mudanças inesperadas e riscos não planejados. Esta conclusão corrobora o que é estabelecido na norma ISO 31000:2018. Nesse sentido, a gestão do risco normalmente não consegue seguir rigorosamente o planejamento original.

Diante da natureza mutável e volátil dos contextos e eventos, as organizações devem estar preparadas para identificar e responder a novos riscos que possam surgir em seu ambiente operacional. Isso requer uma análise contínua e atualização dos riscos existentes, levando em consideração novas fontes de risco (Fonte, 2019; Sousa *et al*., 2018). Logo, infere-se que uma gestão de riscos dinâmica desempenha um papel fundamental ao antecipar, detectar, reconhecer e responder a essas mudanças e eventos de forma adequada e oportuna (Associação Brasileira de Normas Técnicas, 2018). O dinamismo da gestão de riscos sugere que esse deve ser um processo flexível o suficiente para se adaptar a mudanças nas circunstâncias e no contexto

operacional da organização. Isso significa que as estratégias e abordagens de gerenciamento de riscos precisam ser revisadas regularmente e ajustadas conforme necessário.

Sendo assim, para garantir uma gestão de riscos dinâmica eficaz, é importante estabelecer um sistema de monitoramento contínuo (kirilmaz; Erol, 2017). Esse tipo de processo envolve a coleta e análise regular de informações relevantes sobre os riscos, a fim de identificar mudanças e tendências (Oliveira *et al*., 2017). Com base nessas informações, a organização pode ajustar suas estratégias de gerenciamento de riscos e tomar medidas preventivas ou corretivas apropriadas. A dinâmica também implica em uma abordagem proativa para a gestão de riscos.

Em vez de apenas reagir a eventos ou incidentes adversos, as organizações devem antecipar e responder a mudanças nas circunstâncias que possam afetar seus riscos. Isso requer uma abordagem proativa na gestão de riscos, incorporando mecanismos de monitoramento contínuo e revisão das estratégias organizacionais para adaptar-se a novos cenários (Silva; Neves, 2019).

Isso pode incluir a implementação de medidas preventivas, como controles de segurança adicionais, treinamento de funcionários ou revisão de políticas e procedimentos. O fortalecimento dos controles internos e a capacitação contínua das equipes são estratégias essenciais para minimizar vulnerabilidades e melhorar a resiliência organizacional diante de ameaças emergentes (Souza, 2018). Além disso, a implementação de auditorias regulares e a adoção de boas práticas internacionais, como as diretrizes da ISO 31000:2018, contribuem significativamente para a eficácia da gestão de riscos (Moreira *et al*., 2021).

Além disso, a gestão de riscos dinâmica requer a participação de partes interessadas relevantes. Isso envolve a comunicação regular e colaborativa entre todas as partes envolvidas no processo de gestão de riscos, incluindo funcionários, clientes, fornecedores e parceiros de negócios (Ndlela, 2019). Ao compartilhar informações e conhecimentos, as organizações podem obter uma visão mais abrangente dos riscos e tomar decisões informadas sobre o gerenciamento adequado. Portanto, uma abordagem flexível e dinâmica de comunicação de risco, envolvendo as partes interessadas em todas as etapas, pode aumentar a eficácia e a credibilidade da comunicação de risco ao longo do ciclo de gerenciamento de crises (Ndlela, 2019).

As transformações tecnológicas e as mudanças nos comportamentos de consumo incentivam as organizações a implementarem mudanças internas para alcançar seus objetivos

estratégicos (Adair *et al.,* 2021). Nesse contexto dinâmico de mudanças organizacionais, o texto ISO 31004:2015 destaca que qualquer alteração nos objetivos da organização ou nas circunstâncias internas ou externas inevitavelmente modificará o risco (Associação Brasileira de Normas Técnicas, 2015, p. 21). Desse modo, o documento sugere que os processos de gestão de riscos devem ser concebidos de forma a refletir a dinâmica da organização.

No que diz respeito à aplicação do quinto princípio ISO, a norma ISO 31000:2018 destaca a importância do monitoramento e análise crítica como parte essencial do processo de gestão de riscos. A estrutura organizacional deve ser constantemente monitorada e analisada criticamente para garantir a implementação eficaz dos princípios da gestão de riscos, a aplicação da política de gestão de risco da organização e o suporte à tomada de decisões em toda a organização.

A norma recomenda que o monitoramento e a análise crítica sejam incorporados em cada etapa do processo de gestão de riscos, incluindo a revisão periódica dos controles para garantir sua contínua eficácia diante das mudanças. Além disso, o monitoramento e a análise crítica devem ser adaptados às circunstâncias em constante mudança e avaliar a relevância contínua dos indicadores monitorados (Associação Brasileira de Normas Técnicas, 2015).

A ISO 31000:2018 também diferencia o monitoramento e a análise crítica como atividades distintas. O monitoramento envolve a observação contínua de parâmetros-chave para determinar seu desempenho conforme o esperado. A análise crítica, por sua vez, é realizada periodicamente, de acordo com seu propósito específico, com o objetivo de verificar se as suposições que embasaram as decisões permanecem válidas e se as decisões resultantes necessitam de uma revisão crítica (Associação Brasileira de Normas Técnicas, 2015).

Por fim, ao aplicar o processo de gestão de riscos e desenvolver a declaração do contexto, é fundamental identificar os componentes mais propensos a mudanças e monitorá-los de perto. Qualquer alteração nesses componentes pode exigir uma reavaliação dos riscos documentados. Mesmo as pequenas empresas devem considerar as mudanças globais que inevitavelmente terão impacto direto ou indireto em suas operações (Associação Brasileira de Normas Técnicas, 2015). Eventos externos ou circunstâncias emergentes podem exigir mudanças proativas na estrutura de gerenciamento de riscos.

Resumidamente, o quinto princípio da ISO 31000:2018 enfatiza a importância da adaptabilidade e flexibilidade na gestão de riscos. A dinâmica dos riscos exige que as organizações estejam preparadas para mudanças e atualizem regularmente suas estratégias de

gerenciamento. A ISO 31000:2018 reforça que a gestão de riscos deve ser dinâmica, interativa e responder rapidamente a mudanças externas e internas, garantindo que a organização possa se ajustar de forma ágil aos desafios emergentes (Purdy, 2010).

Isso envolve monitoramento contínuo, abordagem proativa, envolvimento de partes interessadas e uma mentalidade de aprendizado contínuo. De acordo com Rampini (2019), a revisão da ISO 31000:2018 enfatizou a necessidade de uma gestão de riscos mais estratégica, destacando a importância da flexibilidade para garantir que as organizações possam se adaptar a novos cenários e ameaças de forma eficiente.

Ao adotar uma abordagem dinâmica, as organizações podem estar melhor preparadas para enfrentar os riscos em constante evolução e proteger seus objetivos e reputação. Estudos indicam que empresas que adotam um modelo de gestão de riscos contínuo e adaptável conseguem reduzir significativamente a exposição a perdas e melhorar a tomada de decisão estratégica (Silva; Neves, 2019). Além disso, a adaptação do gerenciamento de riscos ao contexto organizacional permite um alinhamento mais preciso entre a estratégia corporativa e as respostas a riscos, reforçando a resiliência e a capacidade de inovação das organizações (Pereira, 2019).

2.3.6 Melhor informação disponível

A Além dos princípios mencionados anteriormente, a ISO 31000:2018 estabelece que o processo de gerenciamento de riscos deve se basear na melhor informação disponível. De acordo com o documento, as entradas para o gerenciamento de riscos devem ser derivadas de informações históricas e atuais, levando em consideração também as expectativas futuras, considerando as limitações e incertezas associadas a essas informações e expectativas (Associação Brasileira de Normas Técnicas, 2018). Portanto, é inferido que o gerenciamento de riscos deve ser amplamente embasado em dados e informações coletadas ao longo da vida da organização.

Nesse sentido, é fundamental que as organizações utilizem tanto documentações e dados históricos como informações recentes e atualizadas para embasar suas decisões. O sexto princípio da norma ISSO 31000:2018, destaca a prioridade do uso dessas informações mais recentes. O referido princípio ressalta a necessidade de coletar informações relevantes para a identificação, análise e avaliação de riscos. Geralmente, o levantamento dessas informações

ocorre durante o processo de monitoramento de riscos ou na implementação de respostas adequadas aos mesmos. Através desse processo, decisões podem ser tomadas com base em informações atualizadas sobre o risco geral e os riscos individuais (Fonte, 2019).

De acordo com Ilbahar *et al*. (2018), a análise de risco consiste na utilização sistemática da informação disponível para determinar os perigos. Dessa forma, por meio desse processo, cada risco identificado é avaliado. Seguindo a mesma linha de pensamento, Andrade (2017) afirma que a análise de risco deve estar fundamentada na avaliação e compreensão de informações relacionadas aos ambientes interno e externo da organização. Isso implica na busca ativa por dados e evidências confiáveis, a fim de garantir que todos os riscos potenciais sejam considerados.

Além disso, esse princípio enfatiza a importância de atualizar constantemente a informação utilizada no gerenciamento de riscos (Olechowski *et al.,* 2016). Como abordado em tópicos anteriores, o ambiente de negócios é dinâmico e está sujeito a mudanças, portanto, é fundamental garantir que as informações utilizadas estejam atualizadas e reflitam a realidade atual da organização.

Oliveira e Soares (2018) argumenta que um outro aspecto relevante é a necessidade de avaliar a qualidade da informação disponível a fim de aperfeiçoar o processo de gestão de riscos. Isso implica verificar a fonte da informação, sua precisão, confiabilidade e relevância para o contexto específico em que e como está sendo aplicada (Associação Brasileira de Normas Técnicas, 2015).

A qualidade da informação influencia diretamente a eficácia das decisões de gerenciamento de riscos. Além disso, a norma ISO 31000:2018 destaca a importância de considerar diferentes perspectivas e opiniões ao avaliar a informação disponível. Isso significa buscar a diversidade de pontos de vista e experiências para enriquecer o processo de tomada de decisão e garantir uma visão mais abrangente dos riscos envolvidos.

Posto isso, o princípio também sugere a necessidade de comunicar adequadamente a informação relevante sobre riscos para todas as partes interessadas. A transparência na comunicação contribui para a compreensão compartilhada dos riscos e facilita a colaboração entre as partes envolvidas no processo de gerenciamento de riscos (Paltrinieri; Comfort; Reiniers, 2019).

Outro aspecto importante é a consideração dos limites da informação disponível. Sendo assim, gestores devem levar em consideração quaisquer limitações de dados ou de modelagem

utilizados, ou a possibilidade de divergência entre as partes interessadas (Associação Brasileira de Normas Técnicas, 2015). Reconhecer que nem sempre é possível obter informações completas ou precisas sobre todos os riscos é fundamental para tomar decisões informadas. Nesses casos, é necessário utilizar o conhecimento disponível da melhor maneira possível, reconhecendo e mitigando as incertezas associadas.

Por fim, o sexto princípio destaca a importância de revisar regularmente a informação utilizada no gerenciamento de riscos. Visto que, como dito anteriormente, a gestão de ricos deve fundamentar-se em documentos e informações atualizadas (Olechowski *et al.,* 2016). Isso significa que a informação deve ser periodicamente atualizada e validada, garantindo que o conhecimento sobre os riscos evolua e que as decisões sejam baseadas nas informações mais recentes e confiáveis.

Quanto à aplicação do sexto princípio, o normativo ISO 31004:2015 oferece orientações mais detalhadamente. De acordo com a norma, é importante que o gestor obtenha a melhor informação disponível para compreender os riscos. Para tanto, os arranjos de gestão de riscos devem incluir métodos de coleta ou geração de informações. Porém, deve-se considerar que as informações disponíveis podem ser limitadas e incertas. Diante desse fato, o julgamento de especialistas pode ser utilizado com cautela para evitar viés. Dessa forma, entende-se que, a confiabilidade da avaliação de riscos depende da clareza dos critérios, da coleta de dados relacionados (Associação Brasileira de Normas Técnicas, 2015) e, sobretudo, da análise do gestor.

A ISO 31004:2015 também enfatiza que, é imprescindível que o gestor considere cuidadosamente as decisões que a informação de incidentes pode auxiliar ao projetar o processo de relatório. Isso inclui identificar os usuários finais, organizar a informação, melhorar sua integridade e acessibilidade. Além disso, a descrição do contexto e a data devem ser incluídas nas descrições detalhadas dos riscos para que os usuários possam considerar eventuais mudanças subsequentes. É essencial justificar e registrar as suposições feitas durante a avaliação, incluindo suas limitações. Ao desenvolver tratamentos de risco, é importante considerar como o desempenho dos controles será monitorado e comunicado aos tomadores de decisão futuros que confiam nesses controles (Associação Brasileira de Normas Técnicas, 2015).

Em resumo, o princípio da Melhor Informação Disponível da norma ISO 31000:2018 enfatiza a importância de coletar, atualizar, avaliar a qualidade e comunicar adequadamente as informações relevantes para o gerenciamento de riscos. Também ressalta a necessidade de

considerar diferentes perspectivas, reconhecer os limites da informação disponível e revisar regularmente o conhecimento utilizado. Seguir esse princípio contribui para uma abordagem mais eficaz e informada na identificação, análise e tratamento de riscos nas organizações.

2.3.7 Fatores Humanos e culturais

A influência do comportamento humano e da cultura na gestão de riscos é de grande importância em todos os níveis e estágios (Associação Brasileira de Normas Técnicas, 2018, p. 4). O sétimo princípio da ISO 31000:2018 reconhece que as pessoas desempenham um papel fundamental no sucesso ou fracasso de um sistema de gestão de riscos. Nesse sentido, uma gestão de riscos eficaz deve levar em consideração a influência dos fatores humanos e da cultura organizacional na identificação, avaliação e tratamento dos riscos (Tribunal de Contas da União, 2020).

O termo "fator humano" abrange as capacidades físicas, mentais e perceptivas das pessoas, suas interações com o trabalho e o ambiente, e as características organizacionais que influenciam a segurança no comportamento do trabalho (HSE, 2002; Theobald; Lima, 2007). Contudo, ao se referir aos fatores humanos, a norma ISO 31000:2018 dá ênfase às características, habilidades, experiências e comportamentos dos indivíduos envolvidos na gestão de riscos. Reconhece-se que diferentes pessoas têm diferentes percepções, conhecimentos e capacidades para avaliar e lidar com riscos. Portanto, é essencial considerar essas diferenças ao identificar, avaliar e tratar os riscos.

Além dos fatores humanos, os fatores culturais também têm um impacto significativo na gestão de riscos em cada nível e estágio (Associação Brasileira de Normas Técnicas, 2018). As culturas organizacionais e sociais moldam as atitudes em relação aos riscos e a forma como eles são abordados (Klein *et al.,* 2021; Jhunior; Abib, 2019). Valores culturais, crenças, normas e práticas influenciam a maneira como os riscos são percebidos, comunicados e gerenciados dentro de uma organização (Jhunior; Abib, 2019).

Ao contextualizar o sétimo princípio, é importante reconhecer que os fatores humanos e culturais podem influenciar todo o ciclo de gestão de riscos. Na fase de identificação de riscos, a diversidade de perspectivas e conhecimentos pode levar a uma melhor compreensão dos riscos potenciais. Durante a análise de riscos, as diferenças culturais podem afetar a forma como as informações são interpretadas e priorizadas.

Na etapa de avaliação de riscos, os fatores humanos, como a experiência pregressa (TCU, 2018) e o julgamento, podem influenciar a precisão das estimativas de risco. Os fatores culturais também desempenham um papel importante na definição de tolerâncias a riscos (Fagundes *et al.,* 2021) e, consequentemente, na tomada de decisões relacionadas à aceitação ou mitigação de riscos.

Na implementação de medidas de controle de riscos, os fatores humanos entram em jogo na forma como as políticas e procedimentos são comunicados, entendidos e seguidos pelos funcionários. A cultura organizacional também pode influenciar a conformidade e a adesão a essas medidas. Ao monitorar e revisar o sistema de gestão de riscos, os fatores humanos desempenham um papel fundamental na coleta e interpretação de dados relevantes (Associação Brasileira de Normas Técnicas, 2015). A cultura organizacional pode afetar a transparência e a disposição das pessoas para relatar incidentes ou desvios dos procedimentos.

Desse modo, no que diz respeito à aplicação do referido princípio, a ISO 31004:2015 aponta a necessidade de considerar fatores sociais, políticos, culturais e conceitos de tempo. Além disso, é importante reconhecer os erros comuns que podem ocorrer, como a falha em detectar e responder aos alertas precoces, a indiferença em relação às opiniões dos outros ou a falta de conhecimento, o viés causado por estratégias simplificadas de processamento de informações para lidar com questões complexas e a falha em reconhecer complexidades (Associação Brasileira de Normas Técnicas, 2015).

Ao incorporar fatores humanos e culturais na estrutura e comunicação da gestão de riscos, são necessárias medidas específicas. A concepção da estrutura e a comunicação de risco devem considerar as características culturais e o conhecimento das partes envolvidas. Os gestores devem apoiar o respeito e a compreensão das diferenças individuais, encorajar a expressão de opiniões e reconhecer os esforços individuais. Além disso, é importante não depender exclusivamente de controles humanos para modificar riscos significativos e as organizações transnacionais devem reconhecer a influência da cultura no comportamento das pessoas (Associação Brasileira de Normas Técnicas, 2015).

A ISO 31004:2015 aduz que ao avaliar os fatores humanos e organizacionais, é essencial que o gestor considere a adequação das estruturas e processos. Também é essencial analisar as interfaces entre equipes, lidar com rumores de forma proativa e implementar políticas claras de recrutamento, remuneração e promoção, além de garantir a adesão e aplicação adequadas das políticas e procedimentos. Os gestores devem estar vigilantes em relação a comportamentos

inseguros ou antiéticos dentro da organização (Associação Brasileira de Normas Técnicas, 2015).

Em resumo, o sétimo princípio da ISO 31000:2018 destaca que a gestão de riscos não é apenas uma questão técnica, mas também depende dos fatores humanos e culturais. Sendo assim, considerar esses aspectos ao longo de todo o processo de gestão de riscos é fundamental para uma abordagem eficaz, promovendo uma compreensão mais completa dos riscos, melhorando a tomada de decisões e fortalecendo a cultura de gestão de riscos dentro de uma organização.

2.3.8 Melhoria Contínua

Por fim, o oitavo princípio ISO – melhoria contínua –, enfatiza a necessidade de buscar constantemente o aperfeiçoamento e o progresso no gerenciamento de riscos. A melhoria contínua consiste em avaliar, analisar e aprimorar de forma contínua os processos de gerenciamento de riscos de uma organização, com o objetivo de alcançar resultados melhores e reduzir a probabilidade de falhas ou eventos adversos.

De acordo com a ISO 31000:2018, a gestão de riscos é melhorada continuamente por meio do aprendizado e experiências. Para tanto a gestão de riscos orientada pela ISO baseia-se no método PDCA – método desenvolvido por Walter A. Shewhart em 1930. Composto pelas fases Plan (Planejar), Do (Executar), Check (Verificar) e Act (Agir) o ciclo pode ser utilizado de forma iterativa visando a melhoria contínua dos processos (Fonte, 2018).

Sendo assim, a melhoria contínua implica no aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento (TCU, 2020). O monitoramento, por sua vez, tem o objetivo de acompanhar a implementação das respostas aos riscos, identificar novos riscos e avaliar o processo de riscos ao longo do projeto (Fonte, 2018). Através dessa abordagem, as organizações podem identificar lacunas, áreas de risco aprimoráveis e tomar medidas corretivas necessárias (Inácio, 2021), incluindo a revisão regular de estratégias, políticas e práticas existentes, bem como a implementação de medidas de controle adicionais quando necessário.

A melhoria contínua também promove a aprendizagem e estimula a inovação no contexto organizacional (Neves, 2011). Ao revisar e analisar incidentes passados, erros e lições aprendidas, as organizações podem identificar oportunidades de melhoria e implementar mudanças para evitar a repetição de erros no futuro. As organizações são encorajadas a explorar

novas abordagens, tecnologias e melhores práticas para lidar com os riscos de forma mais eficaz e eficiente. Isso pode envolver a adoção de novas ferramentas, sistemas ou estratégias que permitam uma gestão mais proativa e preventiva dos riscos.

A ISO 31000:2018 também destaca que a melhoria contínua deve ser incorporada como um processo cíclico, integrado a todas as etapas do gerenciamento de riscos. Isso significa que a avaliação e o aprimoramento contínuos dos processos de gerenciamento de riscos devem ocorrer desde a identificação e análise inicial dos riscos até a implementação de medidas de controle e monitoramento.

Quanto à aplicação do princípio, a ISO 31004:2015 enfatiza que gestores e organização devem estar atentos a oportunidades de melhoria, tanto internas quanto externas, na gestão de riscos, sem complicar excessivamente o seu desempenho. Nesse sentido, a busca contínua por aprimoramentos pode englobar várias práticas, como a integração da atividade de gestão de riscos, uma melhor avaliação dos riscos, o acesso a informações de qualidade, a agilidade na tomada de decisões e a utilização de indicadores de progresso qualitativos e quantitativos (Associação Brasileira de Normas Técnicas, 2015). Com isso, a organização pode aprimorar significativamente seu sistema de gestão de riscos, tornando-o mais eficiente e eficaz no enfrentamento dos desafios que possam surgir.

Assim, a eficácia da gestão de riscos está ligada ao sucesso da organização em alcançar seus objetivos. Portanto, é importante que as melhorias sejam implementadas de forma ágil, considerando prioridades, benefícios e monitoramento contínuo do progresso. Algumas melhorias podem exigir tempo e recursos, exigindo um planejamento cuidadoso. O objetivo é aumentar a probabilidade de sucesso da organização por meio de uma gestão de riscos eficaz (Associação Brasileira de Normas Técnicas, 2015).

Dessa forma, o oitavo princípio da ISO 31000:2018, a melhoria contínua, destaca a importância de buscar constantemente aprimoramento no gerenciamento de riscos. Isso envolve a revisão regular das práticas existentes, a implementação de ações corretivas, a aprendizagem organizacional, a inovação, o envolvimento das partes interessadas e a integração contínua da melhoria em todas as etapas do processo de gerenciamento de riscos. Logo, para alcançar efetivamente a melhoria contínua, é essencial que gestores e organizações fundamentem sua política de gestão de riscos nos princípios anteriormente citados. Ao adotar a melhoria contínua, as organizações podem aperfeiçoar sua capacidade de antecipar, prevenir e mitigar os riscos, alcançando melhores resultados e aumentando a resiliência organizacional.

3 MÉTODOS E TÉCNICAS DE PESQUISA

Levando em consideração os objetivos de pesquisa estabelecidos, nesta seção são descritos os métodos e técnicas de pesquisa utilizada.

3.1 Tipologia e Descrição Geral dos Métodos de Pesquisa

Com a finalidade de identificar os fatores que dificultam o uso da gestão de riscos por gestores de segurança da informação em órgãos públicos brasileiros, optou-se por uma pesquisa tipo exploratória e de abordagem qualitativa, a fim de investigar e iniciar uma discussão ampliada da temática, permitindo que pesquisas futuras aprofundem o entendimento sobre a aplicação da ISO 31000:2018 nas atividades diárias dos gestores de segurança. De acordo com Gil (2019), pesquisas de finalidade exploratórias buscam clarificar conceitos e permitir o desenvolvimento de estudos posteriores com maior precisão na definição dos problemas ou hipóteses. Deste modo, pesquisas exploratórias também procuram apresentar uma visão geral sobre o fato estudado de forma aproximativa. Portanto, a escolha por este tipo de pesquisas se mostrou a mais adequada e alinhada ao objetivo proposto.

Inicialmente, desenvolveu-se uma revisão da literatura sobre os princípios da ISO 31000:2018, conceitos relativos ao uso da norma apresentam uma estrutura sólida e sistemática para identificação, avaliação e tratamento de riscos, permitindo que as empresas adotem uma abordagem proativa em relação aos desafios que possam surgir em seus ambientes operacionais, de forma que permitissem um entendimento preliminar a respeito do objeto da pesquisa. Em seguida, foi aplicado um questionário para 57 servidores públicos federais, alunos de um curso de especialização em Privacidade e Segurança da Informação. O questionário apresentou uma única questão aberta com o seguinte comando: “Por que os gestores de segurança da informação não utilizam a gestão de riscos?”. A partir dessas respostas, e considerando o referencial teórico, elaborou-se um roteiro de questões semiestruturadas para avaliar em profundidade o fenômeno. Entrevistou-se 12 gestores de segurança da informação atuantes em órgãos e contextos diversos (ministérios, agências reguladoras, institutos federais, universidades etc.) no setor público brasileiro. Esta técnica de entrevista tem como objetivo coletar respostas de uma fonte que possui as informações que se deseja conhecer baseando-se nas experiências subjetivas do entrevistado (Barros; Duarte, 2011).

Foi aplicada uma entrevista semiestruturada, que se caracteriza pelo conjunto de perguntas abertas, pré-estabelecidas onde não são oferecidas opções de resposta. Desta maneira, o entrevistado possui liberdade na forma de respondê-las (Gil, 2019). As perguntas se apresentam da forma mais aberta possível o que resulta em uma flexibilidade ao entrevistador que pode explorar a ordem das perguntas, sua profundidade e a forma em que se apresenta de acordo com as respostas e circunstâncias do entrevistado (Barros; Duarte, 2011).

3.2 Participantes da Pesquisa

Para aplicar o questionário servidores públicos federais, alunos de um curso de especialização em Privacidade e Segurança da Informação, foram selecionados para participar. O questionário apresentou uma única questão aberta com o seguinte comando: "Por que os gestores de segurança da informação não utilizam a gestão de riscos?", as respostas variaram em maturidade institucional em Segurança da Informação (SI), mas muitos problemas e padrões se repetiram.

Para realizar as entrevistas em profundidade e o questionário, foram escolhidos indivíduos que são Gestores de Riscos em organizações públicas e lidam diariamente com a aplicação da gestão de riscos. A escolha dos participantes, portanto, se deu de forma não probabilística por conveniência considerando a necessidade de entrevistar indivíduos que possuíssem experiências relacionadas a temática pesquisada, permitindo a obtenção das informações necessárias.

Na escolha dos entrevistados, levou-se em consideração critérios mínimos como a atuação no setor de gestão de riscos, excluindo assim pessoas que tivessem pouco ou nenhum contato com a norma em análise. Foram realizadas 12 entrevistas on-line com indivíduos residentes no Brasil. Decidiu-se por encerrar a etapa de entrevistas por entender que as informações coletadas estavam representando o pensamento coletivo do grupo e que o esforço em realizar novas entrevistas não produziriam resultados muito diferentes.

3.3 Procedimentos de Coleta e de Análise de Dados

Inicialmente, foram colhidas respostas de servidores públicos federais que foram questionados quanto aos motivos de não utilizarem a gestão de riscos nos ambientes que

gerenciam. A partir do tratamento de dados e distribuição por afinidades temáticas, foi possível determinar 6 categorias que permitiam uma melhor compreensão dos dados obtidos. A partir da análise dessas respostas, levantou-se uma hipótese a ser testada de que os gestores não utilizam a gestão de riscos, por descumprimento de um ou mais princípios da ISO 31000:2018 e influenciou a próxima etapa da pesquisa.

Sendo assim, foi desenvolvido um roteiro de 16 questões abertas e abrangentes de maneira a permitir que o entrevistado pudesse explorar, com liberdade, suas experiências e percepções individuais a respeito da aplicação da norma em sua rotina de trabalho. Algumas perguntas foram construídas com base nos princípios da ISO 31000:2018, com a finalidade de testar a hipótese.

Durante as entrevistas, o número de perguntas pode variar bastante, porém, usualmente são elaboradas poucas perguntas amplas que são feitas uma por vez e cabe ao entrevistador explorá-las ao máximo a partir das respostas do entrevistado até que se esgote a questão e depois, somente, passando para a pergunta seguinte (Barros; Duarte, 2011; Gil, 2019). A partir disso, foi possível explorar cada resposta dos entrevistando formulando outras questões que não estavam a princípio no roteiro a fim de aprofundar nas respostas obtidas e esgotar o tema abordado.

As entrevistas foram realizadas individualmente com cada entrevistado com duração aproximada de 40 minutos e foram realizadas em janeiro de 2025. Apesar de tradicionalmente serem conduzidas de forma presencial, a modalidade on-line é aceita pela metodologia científica principalmente pelo acesso aos meios de comunicação por grande maioria da população (Gil, 2019). Os áudios das entrevistas foram gravados mediante autorização dos entrevistados com o objetivo exclusivo de realizar a transcrição literal das perguntas e respostas obtidas e de forma anônima, serem utilizadas na pesquisa.

Optou-se, então, pela técnica de análise de conteúdo que por meio de procedimentos sistemáticos permite inferir conhecimento dos discursos analisados seguindo as etapas propostas em Bardin (2016): (i) pré-análise; (ii) exploração do material; e (iii) tratamento dos resultados, a inferência e a interpretação.

A etapa de pré-análise, consistiu na transcrição das entrevistas para organizar as informações e obter um material consistente e pronto para a análise. Assim, realizou-se uma análise prévia a fim de destacar trechos relevantes que poderiam estar alinhados ao objetivo da pesquisa de identificar os fatores que afetam a aplicação da norma na rotina diária.

Na segunda etapa, de exploração do material, os trechos destacados foram analisados e agrupados constituindo construtos, ou seja, temas ou frases capazes de representar um grupo de características citadas pelos entrevistados conforme o julgamento do pesquisador e das impressões observadas diretamente ligados aos princípios da ISO 31000:2018. Por fim, como etapa final, precedeu-se com o tratamento das informações obtidas através da análise anterior permitindo, assim, a sua interpretação e reflexão.

3.4 Roteiro

O presente questionário foi desenvolvido a partir da análise das respostas obtidas em turmas de especialização compostas por profissionais especialistas em privacidade e segurança da informação. A pesquisa teve como questão norteadora: "Por que os gestores de segurança da informação não utilizam a gestão de riscos?" Com o objetivo de aprofundar essa investigação, foi realizada a coleta de dados primários por meio de 12 entrevistas em profundidade. Para tanto, o questionário abaixo serviu como instrumento base para a condução das entrevistas, permitindo uma abordagem sistemática na identificação dos desafios, práticas e percepções relacionadas à gestão de riscos no setor público. A análise dos dados busca contribuir para a compreensão das barreiras estruturais, culturais e organizacionais que influenciam a adoção da gestão de riscos, bem como identificar oportunidades para a sua implementação mais eficaz no contexto da segurança da informação.

1. Em qual setor público você atua e qual é o seu cargo atual? Há quanto tempo você está na área de segurança da informação?

2. Como você gerencia a Segurança da Informação no seu setor? Poderia detalhar as práticas e abordagens adotadas?

3. Em quais situações você aplica a Gestão de Riscos no seu trabalho?

4. Quais são os principais desafios que você enfrenta ao implementar a Gestão de Riscos?

5. Você pode fornecer um exemplo concreto de como utiliza a Gestão de Riscos na prática?

6. De que maneira você coleta informações para fazer avaliação de riscos? Como você avalia a prioridade dos riscos identificados?

7. Como as estratégias de segurança da informação se alinham aos objetivos de longo prazo da sua organização?

8. De que maneira a estrutura organizacional atual impacta a implementação das políticas de segurança na empresa? Você percebe oportunidades de melhoria nos processos de gestão de riscos?

9. Quais características específicas da sua organização precisam ser consideradas ao adaptar as políticas de segurança para torná-las mais eficazes?

10. Como as partes interessadas, além do departamento de segurança, são envolvidas nas decisões sobre gestão de riscos? Todos têm a oportunidade de expressar suas preocupações ou sugerir melhorias relacionadas à segurança?

11. Quais ações sua organização toma para garantir que os planos de segurança sejam atualizados conforme mudanças rápidas no mercado ou no ambiente operacional? Como é feita a avaliação da segurança da sua organização?

12. Como sua organização gerencia e compartilha informações críticas para a tomada de decisões de segurança? Existem dificuldades nesse processo?

13. Como que é garantido que os riscos identificados serão tratados?

14. Como fatores culturais e comportamentais da equipe afetam a eficácia das políticas de segurança?

15. Como a organização lida com incidentes de segurança quando eles ocorrem? Existe um processo estruturado para análise, correção e prevenção de falhas? E se esse incidente for causado por um erro interno?

16. A organização utiliza algum Framework de referência? Como: CIS, NIST, ISO 27000, entre outras.

4 RESULTADOS E DISCUSSÃO

4.1 Questionário Aplicado

A análise das 57 respostas permitiu a identificação de seis grandes categorias de fatores que explicam por que a maioria dos gestores de segurança da informação não utiliza ou não implementa efetivamente a gestão de riscos. A ISO 31000:2018 estabelece que a governança de riscos deve estar integrada aos processos institucionais, contando com apoio gerencial, capacitação e estrutura adequada para sua aplicação (ABNT, 2018). No entanto, a literatura aponta que a ausência desses elementos compromete a implementação eficaz da gestão de riscos, resultando em abordagens fragmentadas e reativas (Associação Brasileira de Normas Técnicas, 2015).

Dentre os principais motivos identificados, destacam-se a falta de conhecimento ou capacitação, a ausência de apoio da alta gestão, a cultura organizacional frágil em relação à segurança da informação, a limitação de recursos, o foco em outras prioridades e a ausência de processos, governança ou metodologia formalizada. Moreira *et al*. (2021) ressaltam que a carência de um modelo estruturado para a gestão da segurança da informação reforça a lacuna na adoção de práticas preventivas e na mitigação de riscos institucionais. A seguir, cada uma dessas categorias será detalhada, com exemplos e subtemas extraídos dos depoimentos analisados, evidenciando os principais desafios enfrentados pelas organizações.

4.2 Detalhamento das Categorias

4.2.1 Falta de capacitação

A ausência de conhecimento sobre metodologias de gestão de riscos representa um desafio significativo para a efetividade das práticas organizacionais nessa área. Muitos gestores relatam a falta de treinamento adequado para a implementação desses processos, o que compromete a identificação, análise e mitigação dos riscos (ABNT, 2015). Além disso, a percepção de complexidade da gestão de riscos gera bloqueios e incertezas quanto ao seu início, dificultando a adoção de abordagens estruturadas. Conforme estabelecido pela norma ISO 31000:2018, a gestão de riscos deve ser baseada em princípios que assegurem sua integração

aos processos organizacionais, promovendo uma cultura de tomada de decisão informada e eficaz.

No entanto, a carência de capacitação adequada impede que esses princípios sejam plenamente aplicados, tornando essencial o investimento contínuo na formação de profissionais para garantir a implementação de uma governança eficiente de riscos. Essa realidade é evidenciada pelos próprios gestores de segurança da informação, cujos relatos incluem observações como: “Muitos gestores não compreendem plenamente os benefícios…” e “…a falta de conhecimento muitas vezes não é superada por não compreenderem a importância do processo…”.

4.2.2 Falta de apoio da alta gestão

A ausência de patrocínio e a escassez de recursos representam barreiras significativas para a implementação efetiva da gestão de riscos em segurança da informação. Muitos relatos indicam que a alta administração não prioriza nem destina investimentos adequados, sejam eles financeiros, humanos ou tecnológicos, para o desenvolvimento e a manutenção contínua de processos estruturados de gestão de riscos. Essa negligência está diretamente relacionada à falta de compreensão sobre o valor estratégico da segurança da informação, resultando na exigência de entregas rápidas que negligenciam abordagens sistemáticas de mitigação de riscos.

De acordo com a ISO 31000:2018, a governança eficaz de riscos depende do comprometimento da alta gestão, uma vez que decisões estratégicas precisam integrar a avaliação de riscos para garantir a resiliência organizacional. Essa limitação estrutural é reforçada na literatura, que aponta que a ausência de comprometimento da alta administração reduz a efetividade da gestão de riscos e compromete a governança organizacional (ABNT, 2015). No entanto, a percepção dos profissionais da área revela uma realidade distinta, como ilustrado por declarações como: *“A negligência na implementação da gestão de riscos frequentemente resulta da ausência de suporte adequado da alta administração…”* e *“Entende-se que a alta gestão não se preocupa com os riscos…”*.

4.2.3 Cultura organizacional frágil

A predominância de uma visão reativa na Segurança da Informação compromete a implementação de uma abordagem estratégica baseada na gestão de riscos. Muitos gestores relatam que a cultura organizacional ainda é voltada para a resolução de crises imediatas, adotando uma postura de "apagar incêndios" em vez de planejar preventivamente com base na identificação e mitigação de riscos. Essa mentalidade contribui para a subestimação dos riscos como parte essencial das operações diárias, dificultando a criação de um ambiente onde a segurança seja tratada de forma contínua e estruturada.

Nesse sentido, a ISO 31000:2018 enfatiza que a gestão de riscos deve ser integrada aos processos organizacionais e baseada em um modelo proativo, permitindo a tomada de decisões informadas para a redução de vulnerabilidades. Moreira *et al*. (2021) ressaltam que a ausência de uma cultura organizacional voltada à gestão de riscos dificulta sua efetiva implementação, tornando as práticas fragmentadas e descoordenadas. No entanto, relatos de profissionais indicam que essa integração ainda é deficiente, conforme demonstrado em declarações como: *"Não há uma cultura organizacional voltada para o gerenciamento de riscos."* e *"Prefere-se fechar os olhos, fingir que os riscos não existem…"*.

4.2.4 Limitação de recursos

A escassez de mão de obra e a falta de alocação adequada de pessoal comprometem a efetividade da gestão de riscos em segurança da informação, tornando-a uma atividade secundária diante das demandas operacionais diárias. Muitos gestores relatam que trabalham sozinhos ou com equipes reduzidas, acumulando diversas atribuições, o que dificulta a implementação de processos estruturados e a adoção de estratégias preventivas. Como consequência, a gestão de riscos sistemática é frequentemente postergada ou suprimida, já que o foco recai sobre tarefas urgentes, como o tratamento de incidentes e respostas a órgãos de controle.

A ISO 31000:2018 destaca que a governança de riscos deve contar com recursos adequados e apoio gerencial para garantir sua integração aos processos organizacionais. De acordo com Moreira *et al*. (2021), a falta de recursos humanos e financeiros reduz a capacidade das organizações de implementarem práticas contínuas e eficazes de gestão de riscos, resultando na priorização de demandas imediatas em detrimento de estratégias preventivas. No

entanto, relatos indicam que essa realidade ainda não se concretiza em muitas instituições, conforme evidenciado por declarações como: "…não possuem equipe disponível, trabalhando sozinho em inúmeras frentes…" e "…falta de um apoiador/patrocinador… resistência da alta gestão à mudança…".

4.2.5 Outras prioridades em foco

A necessidade de atender incidentes e cumprir requisitos legais frequentemente sobrepõe-se à implementação estruturada da gestão de riscos, relegando-a a uma posição secundária dentro das prioridades organizacionais. Muitos gestores relatam que a resposta a incidentes, a prestação de contas a órgãos de controle e a conformidade regulatória, como exigências da LGPD e da IN01/2020, consomem a maior parte do tempo e dos recursos disponíveis, dificultando a adoção de uma abordagem proativa para a mitigação de riscos. Essa dinâmica reforça a percepção de que a gestão de riscos é uma "tarefa extra" e não um elemento central da governança organizacional, especialmente em ambientes onde o cumprimento de prazos negociais é priorizado em detrimento da análise sistemática de ameaças.

A ISO 31000:2018 estabelece que a gestão de riscos deve ser integrada a todos os processos organizacionais, promovendo uma visão estratégica e preventiva. De acordo com Moreira *et al*. (2021), a priorização de demandas regulatórias e reativas, sem um planejamento adequado, compromete a efetividade da gestão de riscos e impede sua consolidação como parte essencial da governança corporativa. No entanto, conforme indicam os relatos dos profissionais da área, essa integração ainda não é plenamente adotada, como demonstrado em declarações como: *"Muitos gestores acabam vendo a gestão de riscos apenas como mais uma das tarefas…"* e *"Quando se tem pressão por resultados de curto prazo, perde-se a importância da segurança a longo prazo."*.

4.2.6 Falta de processos, governança ou metodologias de riscos atualizada

A ausência de frameworks estruturados e diretrizes claras para a gestão de riscos compromete a efetividade das ações de segurança da informação dentro das organizações. Muitos gestores relatam que não há uma política formalmente definida para a gestão de riscos ou, quando existe, não está adequadamente difundida e aplicada. Ademais, a falta de integração

entre áreas e a ausência de uma governança bem estabelecida dificultam a condução de avaliações de riscos de maneira abrangente, deixando o gestor de segurança isolado na tomada de decisões estratégicas.

A ISO 31000:2018 enfatiza que a gestão de riscos deve ser integrada aos processos organizacionais e contar com o apoio de uma estrutura clara de governança, garantindo alinhamento entre diferentes setores e níveis hierárquicos. Segundo Araújo; Gomes (2021), a falta de governança estruturada e a ausência de políticas consolidadas dificultam a integração da gestão de riscos, tornando-a fragmentada e limitando sua aplicabilidade estratégica. No entanto, relatos indicam que essa integração ainda é deficiente, como demonstrado em declarações como: *"Falta de uma estrutura clara de governança nas instituições…"* e *"O PPSI e os órgãos de controle atuam de forma colaborativa, mas é preciso liderança da alta gestão…"*.

4.3 Relação entre os Temas

A interdependência entre os fatores que dificultam a implementação da gestão de riscos em segurança da informação evidencia um ciclo vicioso que perpetua a vulnerabilidade organizacional. A falta de apoio da alta gestão resulta diretamente na limitação de recursos financeiros e humanos, tornando inviável a estruturação de equipes especializadas e a implementação contínua de processos de mitigação de riscos. Paralelamente, uma cultura organizacional frágil reforça a ausência de investimentos em capacitação, pois sem uma visão institucional que valorize a segurança da informação, o desenvolvimento profissional na área não se torna uma prioridade.

Além disso, a pressão por entregas imediatas, frequentemente impulsionada pela falta de planejamento estratégico da alta administração, reforça a ausência de governança e impede que a gestão de riscos seja incorporada ao dia a dia organizacional. Esse cenário culmina em um ciclo autossustentável: a ausência de uma cultura robusta faz com que a alta gestão não priorize o tema, resultando em poucos recursos e na sobrecarga dos gestores responsáveis, que, por sua vez, acabam focando apenas em respostas emergenciais a incidentes, deixando de lado a implementação estruturada da gestão de riscos. Com isso, os riscos continuam crescendo de forma oculta, sem que medidas preventivas sejam adotadas, agravando ainda mais a exposição das organizações a ameaças e vulnerabilidades.

4.4 Tendências Quantitativas

A análise das respostas revela uma forte recorrência de determinados desafios na implementação da gestão de riscos. A falta de cultura organizacional e o apoio da alta gestão aparecem em quase todos os relatos, evidenciando a ausência de priorização do tema no nível estratégico. Adicionalmente, a limitação de recursos e o foco excessivo em demandas imediatas são mencionados com frequência, indicando que restrições orçamentárias e operacionais dificultam a adoção de uma abordagem preventiva. A falta de conhecimento também se destaca como um fator crítico, sendo apontada direta ou indiretamente em diversas falas. Esses aspectos emergem como os mais recorrentes e impactantes no conjunto de respostas, reforçando a necessidade de mudanças estruturais para uma gestão de riscos mais eficaz.

4.5 Síntese

A análise das respostas dos 57 gestores revela que os principais desafios para a implementação eficaz da gestão de riscos estão concentrados em aspectos culturais, organizacionais e de recursos. A predominância de uma cultura voltada à reação imediata, aliada à pressão por entregas rápidas, resulta na subestimação dos riscos e dificulta a adoção de práticas preventivas. A ausência de governança estruturada e de patrocínio da alta gestão compromete a definição clara de processos, enquanto a falta de capacitação técnica e a percepção de burocracia aumentam a complexidade da gestão de riscos.

Nesse sentido, a limitação de recursos, manifestada por equipes reduzidas e acúmulo de funções, sobrecarrega os gestores de Segurança da Informação, impossibilitando a criação de um programa estruturado de gestão de riscos. Esse cenário perpetua um comportamento reativo, reduzindo a maturidade organizacional e ampliando a vulnerabilidade frente às ameaças cibernéticas.

4.6 Relações com os Princípios da ISO 31000:2018

A ISO 31000:2018 estabelece oito princípios fundamentais para garantir a efetividade da gestão de riscos nas organizações. No entanto, a análise das 57 respostas evidencia que esses

princípios não estão sendo plenamente atendidos ou sequer são observados na maioria das organizações relatadas. A ausência de integração da gestão de riscos aos processos organizacionais, a falta de comprometimento da alta administração e a limitação de recursos são fatores recorrentes que comprometem a implementação desses princípios.

Além disso, a cultura predominantemente reativa e a falta de clareza na governança impedem que a gestão de riscos seja percebida como um processo contínuo e estratégico. A seguir, será apresentada uma análise detalhada de cada princípio da ISO 31000:2018 em relação aos desafios identificados nas respostas dos gestores, evidenciando as lacunas existentes e os obstáculos à sua aplicação.

4.6.1 Integrada

A ISO 31000:2018 estabelece que a gestão de riscos deve ser integrada a todas as atividades organizacionais, alinhada à governança e aos processos institucionais (ABNT, 2018). No entanto, a literatura aponta que a falta de integração resulta na fragmentação dos processos, tornando a gestão de riscos meramente burocrática e pouco efetiva (Araújo; Gomes, 2021). Além disso, a segregação das áreas de negócio e de Segurança da Informação compromete a mitigação de riscos e reduz a resiliência organizacional (Moreira *et al*., 2021). Estudos indicam que essa desconexão amplia a vulnerabilidade institucional, pois os riscos deixam de ser considerados estrategicamente e passam a ser tratados de forma reativa e descoordenada (Olechowski *et al*., 2016).

Sendo assim, a análise das respostas indica que esse princípio não está sendo plenamente aplicado na maioria das organizações. Muitos gestores relatam a "falta de envolvimento da alta gestão" e a "falta de priorização" da gestão de riscos, o que sugere que essa prática não está integrada ao planejamento estratégico nem às decisões institucionais.

Ademais, há um isolamento das equipes de Segurança da Informação (SI), sem participação ativa das áreas de negócio, comprometendo a transversalidade da gestão de riscos. Como ilustrado pelos relatos "Entende-se que a alta gestão não se preocupa com os riscos…" e "A ausência de cultura organizacional voltada para o gerenciamento de riscos", a ausência de um patrocínio ativo da alta administração e a falta de colaboração entre setores demonstram que o princípio da integração não é atendido na maior parte das instituições analisadas.

4.6.2 Estruturada e abrangente

A ISO 31000:2018 estabelece que a gestão de riscos deve ser estruturada e abrangente, garantindo padronização e confiabilidade nos processos (ABNT, 2018). No entanto, a literatura aponta que a ausência de diretrizes formais e frameworks consolidados compromete a sistematização da gestão de riscos, tornando-a fragmentada e pouco efetiva (ABNT, 2015). A falta de estrutura e governança organizacional resulta na condução reativa dos processos, dificultando a comparabilidade e a integração entre setores (Moreira *et al*., 2021). Dessa forma, a inexistência de uma abordagem uniforme enfraquece a governança e aumenta a subjetividade das avaliações, reduzindo a eficácia da gestão de riscos (Araújo; Gomes, 2021).

Entretanto, a análise das respostas evidencia que esse princípio não é amplamente atendido. Muitos gestores relatam que a gestão de riscos é conduzida de forma reativa, sem um método ou fluxo bem definido, o que compromete a sistematização e a confiabilidade das avaliações. Há também menções à "falta de frameworks consolidados" e à "deficiência na formalização das diretrizes de risco", refletindo a ausência de padrões institucionais claros.

Nesse sentido, observa-se uma falta de padronização entre setores e órgãos, resultando em improvisação na abordagem dos riscos, sem uma visão corporativa abrangente. Conforme apontado nos relatos "A complexidade das avaliações… o Gestor de SI em muitos órgãos não possui equipe disponível, trabalhando sozinho em inúmeras frentes" e "Falta de uma estrutura clara de governança nas instituições são as maiores deficiências…", a predominância de processos desestruturados e não sistemáticos reforça que esse princípio não é cumprido na maioria dos casos relatados.

4.6.3 Personalizada

A ISO 31000:2018 estabelece que a gestão de riscos deve ser personalizada, considerando o contexto organizacional, seus objetivos e stakeholders (ABNT, 2018). No entanto, a literatura aponta que a falta de adaptação às necessidades específicas das instituições compromete a efetividade do processo, levando à adoção de modelos genéricos e pouco estratégicos (ABNT, 2015). A ausência de personalização resulta na mera conformidade regulatória, sem integração com os processos críticos da organização (Moreira *et al*., 2021). Além disso, a falta de envolvimento das áreas setoriais reduz a maturidade na gestão de riscos,

dificultando sua aplicação prática e impactando negativamente a governança institucional (Araújo; Gomes, 2021).

No entanto, a análise das respostas revela que esse princípio não tem sido plenamente aplicado. Muitas instituições apresentam baixa maturidade na gestão de riscos, sem adaptar metodologias ao seu contexto específico, como ambientes de sistemas legados ou particularidades do setor público.

Dessa forma, há uma falta de envolvimento das áreas setoriais, resultando na aplicação de modelos genéricos ou na completa omissão do processo. Em diversos casos, a prioridade é meramente atender requisitos regulatórios, como a conformidade com a IN 01/2020 ou a LGPD, sem a personalização necessária para os processos críticos de cada órgão. Como evidenciado nos relatos "Muitos gestores acabam vendo a gestão de riscos apenas como mais uma das tarefas… não dando prioridade ao conhecimento dos riscos" e "Falta de conhecimento do tema, falta de apoio da gestão…", a ausência de um alinhamento estratégico e a dependência de abordagens genéricas comprometem a efetividade da gestão de riscos, violando o princípio de personalização.

4.6.4 Inclusiva

A ISO 31000:2018 estabelece que a gestão de riscos deve ser inclusiva, garantindo a participação de diferentes stakeholders para uma abordagem mais abrangente e eficaz (ABNT, 2018). No entanto, a literatura destaca que a ausência de envolvimento das áreas finalísticas e a restrição da gestão de riscos à equipe de TI comprometem a integração e a visão sistêmica necessárias para sua efetividade (ABNT, 2015). A falta de colaboração entre jurídico, negócios, TI e alta administração dificulta a implementação de processos coesos, resultando em desalinhamento estratégico (Moreira *et al*., 2021). Dessa forma, a exclusão de setores essenciais na tomada de decisão fragiliza a governança e impede que os riscos sejam gerenciados de maneira integrada (Araújo; Gomes, 2021).

Nesse sentido, a análise das respostas evidencia que esse princípio não é plenamente atendido na maioria das organizações. Um problema recorrente é que a segurança da informação permanece restrita à equipe de TI, sem o envolvimento efetivo das áreas finalísticas e sem a colaboração dos gestores de negócio.

Além disso, há relatos de que a gestão de riscos está distante de quem realmente define e trata os dados, comprometendo a integração e a visão sistêmica necessária para uma abordagem eficaz. Também foram apontados desalinhamentos entre jurídico, negócios, TI e a alta administração, dificultando a implementação de processos coesos e bem coordenados. Conforme evidenciado nos relatos "… pessoas ligadas ao setor da administração ou de pessoal, com um certo distanciamento de quem, realmente, define e trata os dados" e "Falta de integração entre equipes (TIC versus Jurídica versus Negócios)", a ausência de uma abordagem inclusiva impede que os riscos sejam gerenciados de forma integrada, resultando na falha desse princípio na maior parte das organizações analisadas.

4.6.5 Dinâmica

A ISO 31000:2018 estabelece que a gestão de riscos deve ser dinâmica, permitindo adaptação contínua às mudanças internas e externas (ABNT, 2018). No entanto, a literatura aponta que a predominância de abordagens reativas, sem monitoramento sistemático e revisões regulares, compromete a capacidade de antecipação de riscos (ABNT, 2015). A sobrecarga de trabalho e a falta de tempo para atualização da matriz de riscos reduzem a efetividade do processo, tornando-o rígido e desatualizado (Moreira *et al*., 2021). Dessa forma, a ausência de uma cultura organizacional voltada à proatividade impede a evolução da gestão de riscos, limitando sua adaptação às transformações do ambiente institucional (Araújo; Gomes, 2021).

Seguindo essa linha de raciocínio, a análise das respostas indica que esse princípio não é atendido na maioria das organizações. Diversos gestores relatam que a prática predominante é reativa, focada em responder a incidentes em vez de antecipá-los. Ademais, a sobrecarga de trabalho e a falta de tempo dificultam o monitoramento contínuo e a atualização da matriz de riscos. Não há menções consistentes sobre a realização de revisões regulares ou o rastreamento sistemático de novas ameaças, o que compromete a adaptação às transformações do ambiente tecnológico e organizacional.

Como evidenciado nos relatos "Muitos gestores não se sentem confortáveis ou não têm coragem para empreender de fato esse trabalho com seriedade, preferindo fechar os olhos…" e "…falta de cultura na organização, talvez não conseguindo relacionar a gestão de risco como um apoio para fortalecer a segurança", a ausência de processos contínuos e a falta de envolvimento proativo inviabilizam a implementação de uma gestão de riscos dinâmica, impedindo sua evolução conforme as necessidades do contexto organizacional.

4.6.6 Melhor informação disponível

A ISO 31000:2018 estabelece que as decisões sobre riscos devem ser fundamentadas na melhor informação disponível, combinando dados concretos, experiência prática e contribuições dos stakeholders (ABNT, 2018). No entanto, a literatura destaca que a falta de mapeamento adequado de processos, a ausência de inventários de ativos e a deficiência na comunicação entre setores dificultam a coleta e o compartilhamento de informações essenciais para a gestão de riscos (ABNT, 2015). A priorização do atendimento a exigências regulatórias em detrimento de análises aprofundadas compromete a tomada de decisão estratégica e reduz a efetividade da gestão de riscos (Moreira *et al*., 2021). Dessa forma, a inexistência de um fluxo estruturado de informações enfraquece a governança e aumenta a incerteza na identificação e mitigação de riscos (Araújo; Gomes, 2021).

Entretanto, a análise das respostas evidencia que esse princípio não é plenamente atendido na maioria das organizações. Muitos gestores mencionam a falta de conhecimento sobre o contexto dos sistemas legados, a ausência de mapeamento adequado dos processos e a inexistência de um inventário de ativos, dificultando uma visão clara dos riscos. Além disso, há relatos de que a comunicação entre as áreas é falha, prejudicando a coleta e o compartilhamento de dados confiáveis para embasar decisões estratégicas.

Em alguns casos, a prioridade é simplesmente cumprir prazos regulatórios ou atender auditorias, sem uma análise aprofundada das evidências disponíveis. Como exemplificado nos relatos “No que se trata sobre gestão de risco… há uma deficiência e carência da condução… não há uma participação ou coparticipação da T.I…” e “…falta de conhecimento da infraestrutura de TI de sua organização, não conseguindo assim identificar potenciais fontes de riscos”, a ausência de um mapeamento estruturado e de um fluxo eficaz de troca de informações compromete a tomada de decisões baseadas em dados, evidenciando a fragilidade desse princípio na prática.

4.6.7 Fatores humanos e culturais

A ISO 31000:2018 estabelece que a gestão de riscos deve considerar fatores humanos e culturais, reconhecendo como percepções e comportamentos influenciam a efetividade do

processo (ABNT, 2018). Entretanto, a literatura aponta que a ausência de uma cultura organizacional voltada para riscos, aliada à resistência interna e à priorização de resultados imediatos, dificulta a implementação de práticas eficazes (ABNT, 2015). A concentração da gestão de riscos em poucos profissionais e a falta de engajamento institucional limitam a disseminação do conhecimento e reduzem a maturidade organizacional no tema (Moreira *et al*., 2021). Dessa forma, a negligência a esses fatores compromete a efetividade da governança de riscos, tornando a abordagem fragmentada e reativa (Araújo; Gomes, 2021).

Contudo, a análise das respostas demonstra que esse princípio é amplamente negligenciado na maioria das organizações. Muitos gestores destacam a ausência de uma cultura organizacional voltada para riscos, além da falta de engajamento e do temor de assumir responsabilidades, o que resulta em uma postura de negação ou minimização dos riscos existentes. Há uma resistência evidente ao tema, priorizando a entrega rápida de resultados em detrimento da implementação de práticas robustas de gestão de riscos.

Dessa forma, a dependência de poucos profissionais para lidar com segurança da informação e riscos sobrecarrega os gestores e limita a disseminação do conhecimento dentro das organizações. Como evidenciado nos relatos “Muitos gestores não compreendem plenamente os benefícios… pressão por resultados de curto prazo… preferindo soluções rápidas” e “A cultura organizacional não prioriza tal temática… preferindo assumir riscos, ignorá-los ou tratá-los pontualmente”, a baixa conscientização, a resistência interna e a falta de apoio institucional configuram o maior gap identificado, demonstrando o descumprimento claro desse princípio em larga escala.

4.6.8 Melhoria contínua

A ISO 31000:2018 estabelece que a gestão de riscos deve ser um processo contínuo de aprendizado e aprimoramento, incorporando lições extraídas de experiências passadas, incidentes e feedbacks (ABNT, 2018). Em contrapartida, a literatura aponta que a ausência de ciclos estruturados de avaliação e a realização de práticas pontuais voltadas apenas ao cumprimento de exigências regulatórias comprometem a melhoria contínua (ABNT, 2015). Além disso, a sobrecarga de trabalho e a escassez de recursos dificultam a implementação de revisões periódicas e o refinamento das metodologias empregadas (Moreira *et al*., 2021). Dessa forma, a falta de uma cultura organizacional voltada para a evolução constante da gestão de

riscos reduz a maturidade institucional, tornando-a reativa e pouco eficiente (Araújo; Gomes, 2021).

Apesar disso, a análise das respostas indica que esse princípio não está sendo plenamente aplicado. A maioria dos relatos aponta que, quando há alguma prática de gestão de riscos, ela ocorre de maneira pontual, geralmente para atender a exigências regulatórias, sem a estruturação de ciclos de avaliação e aprimoramento contínuo. Não há evidências consistentes de revisão periódica de planos ou de aplicação de lições aprendidas a partir de incidentes passados.

Ademais, a sobrecarga e a escassez de recursos dificultam a realização de retrospectivas ou refinamentos metodológicos, reforçando a ausência de uma cultura de melhoria contínua. Como demonstram os relatos "…os gestores podem optar por soluções de segurança rápidas e superficiais, em detrimento de investimentos em processos mais abrangentes" e "Não acho que não utilizam (sic)… mas a falta de pessoal… dificultam a elaboração e manutenção adequada do processo de gestão de risco", a falta de estrutura formal, alinhada a limitações culturais e de recursos, inviabiliza a aplicação desse princípio, comprometendo a evolução da maturidade organizacional em gestão de riscos.

4.7 Entrevistas em Profundidade

Buscando compreender os desafios enfrentados pelos responsáveis pela segurança da informação na aplicação da gestão de riscos, as entrevistas focaram em profissionais atuantes no setor público, representando partes interessadas essenciais nesse contexto organizacional. Esses profissionais, com conhecimento e experiência específicos em gestão de segurança, contribuíram significativamente para a identificação de práticas, dificuldades e soluções aplicadas em suas organizações.

As entrevistas exploraram aspectos fundamentais da gestão de riscos e segurança da informação, incluindo a influência da normatização, os desafios de integração, a resistência organizacional e as barreiras relacionadas à capacitação e ao engajamento dos profissionais. A ISO 31000:2018 enfatiza que a gestão de riscos deve ser compreendida e aplicada de forma estruturada em todas as áreas institucionais, reduzindo resistências e garantindo maior alinhamento com as diretrizes organizacionais (ABNT, 2018).

A literatura aponta que a falta de capacitação e envolvimento dos profissionais compromete a implementação de práticas eficazes, dificultando a consolidação de uma cultura organizacional voltada à mitigação de riscos (Associação Brasileira de Normas Técnicas, 2015). Durante as entrevistas, os participantes foram incentivados a compartilhar experiências sobre esses desafios, destacando fatores que impactam diretamente a eficácia da gestão de riscos em suas instituições.

Moreira *et al*. (2021) ressaltam que a abordagem qualitativa permite identificar barreiras institucionais e fornecer subsídios para aprimoramentos no processo de gestão de riscos. Além disso, a escolha de entrevistas individuais demonstrou-se eficaz, criando um ambiente confortável para que os entrevistados apresentassem percepções detalhadas e autênticas, minimizando vieses nas respostas (Araújo; Gomes, 2021).

O conhecimento técnico do pesquisador foi essencial para interpretar os depoimentos de maneira aprofundada, especialmente devido à natureza técnica e normativa do tema, que inclui termos específicos de frameworks como ISO 31000:2018, NIST e PPSI. Essa expertise permitiu elaborar perguntas adicionais durante as entrevistas, explorando nuances relevantes e assegurando a exaustividade das respostas obtidas.

Após a pré-análise do material coletado, trechos relevantes das entrevistas foram destacados, totalizando uma ampla gama de dados qualitativos. Esses trechos foram classificados e agrupados com base em afinidades temáticas, considerando desafios comuns, boas práticas e soluções mencionadas pelos participantes. Na etapa de exploração do material, os trechos foram consolidados em 8 construtos principais, definidos com base nas observações do pesquisador e alinhados aos princípios da ISO 31000:2018.

Os construtos identificados foram frequentes em diversas entrevistas e representam desafios estruturais e culturais enfrentados pelas organizações, principalmente na implementação eficaz de práticas de segurança. Esses construtos foram analisados quanto à frequência e impacto nos contextos organizacionais, permitindo uma visão detalhada sobre como os desafios afetam a gestão de riscos e destacando as oportunidades para implementação de melhores práticas.

A análise resultante possibilitou não apenas o mapeamento dos desafios mais frequentes, mas também a proposição de recomendações práticas e alinhadas aos princípios da ISO 31000:2018, visando melhorar a aplicação da gestão de riscos e elevar a maturidade das organizações no contexto da segurança da informação.

4.8 Afinidades Temáticas

4.8.1 Falta de cultura, conscientização e resistência

A análise das respostas evidencia uma constatação massiva: tanto as equipes operacionais quanto a alta gestão não possuem uma consciência aprofundada sobre a importância da gestão de riscos. A ISO 31000:2018 destaca que a gestão de riscos deve ser parte da cultura organizacional, promovendo a conscientização e o engajamento de todos os níveis institucionais (ABNT, 2018).

Contudo, a literatura aponta que a ausência dessa mentalidade contribui para a predominância de uma cultura reativa, na qual as ações são adotadas apenas após a ocorrência de incidentes, em vez de se estabelecer uma abordagem preventiva e estruturada (ABNT, 2015). Moreira *et al*. (2021) ressaltam que a falta de conscientização entre gestores e equipes técnicas dificulta a implementação de processos eficazes de gestão de riscos, resultando em respostas fragmentadas e pouco estratégicas. Dessa forma, a carência de uma cultura organizacional voltada à prevenção compromete a resiliência institucional e reduz a capacidade de mitigação de riscos (Araújo; Gomes, 2021).

Diversos gestores relatam resistência por parte dos usuários e setores a procedimentos básicos de segurança, como assinatura digital e autenticação em dois fatores, o que demonstra a falta de conscientização sobre boas práticas. Soma-se a isso a baixa priorização da gestão de riscos, refletida na pouca participação em comitês estratégicos e no engajamento restrito a momentos de crise. Essa postura compromete a evolução da maturidade organizacional e expõe as instituições a riscos contínuos que poderiam ser mitigados por meio de uma cultura de segurança mais proativa e integrada.

4.8.2 Escassez de equipe e sobrecarga

A escassez de profissionais dedicados à segurança da informação é um problema recorrente nas organizações analisadas. A ISO 31000:2018 enfatiza que a gestão de riscos deve contar com recursos humanos qualificados para garantir sua efetividade e continuidade (ABNT, 2018).

Entretanto, a literatura aponta que a falta de especialistas na área, somada à sobrecarga de trabalho e à ausência de formação específica em gestão de riscos, compromete a implementação de processos contínuos (Associação Brasileira de Normas Técnicas, 2015). Moreira *et al*. (2021) destacam que a limitação de recursos humanos inviabiliza o uso eficaz de ferramentas, dificulta o monitoramento constante e impede a evolução da maturidade organizacional em segurança da informação. Como consequência, a gestão de riscos se torna fragmentada e reativa, dificultando a criação de uma abordagem estruturada e sustentável (Araújo; Gomes, 2021).

4.8.3 Orçamento, contratações e burocracias

A burocracia nos processos de aquisição e as limitações orçamentárias representam obstáculos significativos para a implementação de soluções eficazes de segurança da informação. A ISO 31000:2018 destaca que a gestão de riscos deve ser integrada à governança organizacional, contando com suporte financeiro e administrativo adequado para garantir sua efetividade (ABNT, 2018).

Contudo, a literatura aponta que entraves em licitações, processos administrativos lentos e restrições financeiras dificultam a obtenção de ferramentas essenciais, como firewalls, antivírus corporativo e plataformas de análise de vulnerabilidades (ABNT, 2015). Moreira *et al*. (2021) ressaltam que, em diversas situações, as áreas técnicas identificam riscos e propõem medidas de mitigação, mas a alta gestão opta por aceitá-los devido à indisponibilidade de recursos. Esse contexto compromete a resiliência organizacional, expondo a infraestrutura de TI a vulnerabilidades que poderiam ser evitadas com investimentos preventivos e uma abordagem estruturada para a gestão de riscos (Araújo; Gomes, 2021).

4.8.4 Falta de estrutura formal e adoção parcial da gestão de riscos

A ausência de estruturas formais para a gestão de segurança da informação ainda é uma realidade em muitos órgãos, que não possuem ou estão apenas iniciando a criação de comitês de segurança e Equipes de Tratamento e Resposta a Incidentes (ETIR). A ISO 31000:2018 destaca que a governança de riscos deve ser estruturada e integrada aos processos institucionais, garantindo consistência e previsibilidade na mitigação de ameaças (ABNT, 2018).

No entanto, a literatura aponta que a falta de comitês e equipes especializadas compromete a efetividade da gestão de riscos, tornando-a fragmentada e dependente de abordagens informais (ABNT, 2015). Como consequência, a gestão de riscos ocorre de maneira não sistematizada, sendo conduzida por meio de planilhas, e-mails e discussões pontuais, sem uma metodologia consolidada. Moreira *et al*. (2021) ressaltam que a inexistência de processos formalizados reduz a capacidade organizacional de resposta a incidentes e dificulta a implementação de medidas preventivas eficazes.

Em diversos casos, a análise de riscos é realizada apenas para atender exigências legais nas contratações, como nos termos de referência, sem um acompanhamento contínuo. Contudo, algumas iniciativas recentes, como o Programa de Política de Segurança da Informação (PPSI) e os autodiagnósticos semestrais, têm impulsionado a adoção de uma estrutura mínima, incentivando maior formalização e governança sobre os riscos organizacionais.

4.8.5 Uso de ferramentas e frameworks

O Programa de Privacidade e Segurança da Informação (PPSI) é a iniciativa mais citada entre os esforços para estruturar a gestão de riscos e segurança da informação nas organizações analisadas. A literatura destaca que a adoção de frameworks reconhecidos contribui para a padronização das práticas de segurança, garantindo maior alinhamento com normas internacionais (Moreira *et al*., 2021).

Além disso, algumas referências normativas, como a ISO 27000 e os CIS Controls, são mencionadas como diretrizes para boas práticas, embora sua aplicação ainda seja limitada. A ISO 31000:2018 enfatiza que a gestão de riscos deve ser baseada em processos estruturados e ferramentas eficazes para possibilitar um monitoramento contínuo e integrado (ABNT, 2018).

No âmbito das soluções tecnológicas, plataformas como Zabbix são utilizadas para monitoramento, mas a fragmentação na sua implementação compromete a consolidação de uma abordagem abrangente. Araújo e Gomes (2021) ressaltam que a falta de integração entre ferramentas e processos reduz a efetividade da gestão de riscos, dificultando a criação de um ambiente organizacional mais resiliente.

A falta de processos integrados é um desafio recorrente, com diversas ferramentas operando isoladamente e pouca consolidação de informações, o que compromete a eficácia da gestão de riscos e dificulta uma visão abrangente da segurança organizacional.

4.8.6 Envolvimento da alta gestão e governança

A gestão de riscos e a segurança da informação dependem fortemente do apoio da alta administração para serem efetivamente implementadas. A ISO 31000:2018 enfatiza que a governança de riscos deve contar com o comprometimento da liderança, garantindo recursos adequados e integração com a estratégia organizacional (ABNT, 2018). Se líderes institucionais, como reitores, diretores ou secretários, não priorizam o tema, as iniciativas de segurança acabam ficando em segundo plano, sem os recursos e a governança necessários.

A literatura destaca que a ausência de envolvimento da alta gestão compromete a consolidação da cultura de riscos e reduz a efetividade das práticas de segurança (Moreira *et al*., 2021). Por outro lado, órgãos que contam com o envolvimento ativo da alta administração relatam avanços significativos, incluindo a criação de comitês atuantes, maior disponibilidade orçamentária e equipes dedicadas. Araújo e Gomes (2021) ressaltam que a liderança estratégica é essencial para consolidar a segurança da informação como um pilar fundamental da governança organizacional, promovendo uma gestão de riscos mais estruturada e proativa.

4.8.7 Exemplos concretos de incidentes e consequências

A recorrência de incidentes graves, como vazamento de credenciais, indisponibilidade de sistemas críticos e falhas físicas, como o superaquecimento de data centers, reforça a necessidade de uma gestão de riscos estruturada. A ISO 31000:2018 estabelece que a gestão de riscos deve ser contínua e integrada aos processos organizacionais, garantindo a antecipação e mitigação de ameaças antes que impactem as operações (ABNT, 2018).

No entanto, a maioria dos relatos indica que a resposta a esses eventos ocorre de forma reativa, em vez de preventiva. Moreira *et al*. (2021) destacam que a falta de monitoramento contínuo e de revisões periódicas compromete a capacidade de antecipação de riscos, tornando as ações corretivas mais onerosas e menos eficazes. Além disso, Araújo e Gomes (2021) ressaltam que a ausência de uma abordagem estruturada para a gestão de riscos na área de segurança da informação mantém a vulnerabilidade das instituições, impedindo a consolidação de práticas preventivas eficazes.

A falta de processos contínuos de monitoramento e mitigação deixa as organizações vulneráveis, tornando-as dependentes da remediação após o impacto. Esses incidentes evidenciam que a gestão de riscos não pode ser tratada apenas como uma resposta emergencial, mas sim como um elemento estratégico essencial para a resiliência institucional.

4.9 Relação aos Princípios da ISO 31000:2018

Este capítulo apresenta os resultados da pesquisa à luz dos oito princípios descritos no normativo ISO 31000:2018, oferecendo uma visão detalhada de como cada um deles se manifesta na prática das instituições analisadas. A norma estabelece que a gestão de riscos deve ser integrada, estruturada, personalizada e contínua, garantindo alinhamento estratégico e fortalecimento da governança organizacional (ABNT, 2018).

Para isso, cada seção do capítulo aborda um princípio específico, destacando as evidências empíricas coletadas nas entrevistas, as falas representativas dos participantes e as proposições em forma de assertivas. Segundo Moreira *et al*. (2021), a análise dos princípios da gestão de riscos permite identificar barreiras e oportunidades para a sua implementação, contribuindo para aprimoramentos na prática organizacional.

Além disso, conforme destacado por Araújo e Gomes (2021), a aplicação estruturada desses princípios pode ser avaliada de forma quantitativa por meio de instrumentos como a escala Likert, permitindo uma mensuração mais objetiva da aderência dos princípios à realidade institucional. Dessa forma, o capítulo busca integrar os achados qualitativos e quantitativos, oferecendo um panorama abrangente sobre os desafios e oportunidades na implementação da gestão de riscos.

Esse formato permite observar, de maneira sistemática, as razões que explicam tanto as potencialidades quanto as lacunas identificadas, possibilitando uma compreensão profunda de como a gestão de riscos tem sido incorporada na segurança da informação das organizações estudadas.

4.9.1 Integrada

O princípio Integrada, conforme a ISO 31000:2018, estabelece que a gestão de riscos deve ser incorporada a todos os processos e práticas organizacionais, garantindo alinhamento

com a governança e a estratégia institucional (ABNT, 2018). A partir das 12 entrevistas realizadas, verificou-se que a maioria das instituições não possui a gestão de riscos plenamente integrada, apresentando apenas esforços pontuais, geralmente motivados por auditorias externas ou exigências regulatórias. A literatura aponta que essa fragmentação compromete a efetividade da gestão de riscos, tornando-a reativa e desalinhada com os objetivos organizacionais (ABNT, 2015).

Moreira *et al*. (2021) destacam que a falta de integração leva à descontinuidade dos processos, limitando a adoção de práticas estruturadas e estratégicas. Além disso, a ausência de participação da alta administração dificulta a consolidação de uma cultura organizacional voltada à gestão de riscos, reduzindo sua efetividade e comprometendo a resiliência institucional (Araújo; Gomes, 2021). Assim, os resultados da pesquisa corroboram os desafios apontados na literatura, demonstrando que a gestão de riscos, quando não integrada, permanece fragmentada e com impacto limitado na tomada de decisões.

Em algumas organizações, a área de TI acaba assumindo sozinha a responsabilidade de identificar, avaliar e responder aos riscos, sem que haja envolvimento efetivo da alta administração ou das demais áreas finalísticas. Por outro lado, em determinados órgãos verifica-se um maior alinhamento entre a governança organizacional e a gestão de riscos de TI, promovendo a participação de diferentes áreas (jurídico, administrativo, negócio) e assegurando a disponibilidade de recursos e suporte para ações de segurança. Ainda assim, a integração não é plena: a dificuldade em reunir partes interessadas, a falta de cultura organizacional e a dispersão de setores em diferentes diretorias são apontadas como grandes barreiras. A seguir, falas dos entrevistados que corroboram para estes resultados:

> "Não temos um setor específico para riscos. A gente faz cada um por si, e quando estoura algum problema, reunimos um grupo. Fica solto, não é integrado a nenhum processo maior."
> "O Comitê de Segurança começou agora, mas ainda é muito incipiente. Precisa engajar as outras áreas para não ser só uma responsabilidade de TI."
> "A gente tem muita dificuldade de envolver a alta gestão. Sem esse suporte, a gestão de riscos não entra como parte do planejamento estratégico. Fica tudo fragmentado."
> "A TI costuma centralizar o assunto, mas o ideal é todo mundo participar. Precisamos que o RH, o Jurídico e as pró-reitoras entendam os riscos para incorporar no dia a dia."
> "Mesmo com a política de segurança, se ela não tiver alinhamento com a estratégia maior do órgão, cada setor faz do seu jeito. Falta uma visão realmente integrada de riscos em todos os processos."

A seguir, apresentam-se 6 assertivas que poderão ser utilizadas em um questionário, a fim de avaliar o grau de integração da gestão de riscos nas organizações. Essas assertivas podem

ser aplicadas numa escala Likert de 5 pontos (por exemplo, de 1 = Discordo totalmente até 5 = Concordo totalmente) ou conforme o modelo de preferência do pesquisador.

Quadro 1 – Integrada

A gestão de riscos deve ser parte integrante de todas as atividades organizacionais, alinhada com a estratégia, objetivos e processos de negócio.
1. A gestão de riscos em minha instituição está incorporada aos processos e práticas diários de todas as áreas. 2. O comitê (ou grupo responsável) de Segurança da Informação consegue envolver efetivamente diversos setores na identificação e avaliação de riscos. 3. Há uma política formal que descreve como a gestão de riscos deve ocorrer em cada etapa dos projetos e processos organizacionais. 4. Os líderes de diferentes áreas (administrativa, jurídica, negócios) participam ativamente das discussões sobre riscos e segurança. 5. As decisões estratégicas da instituição levam em conta os resultados das análises de riscos levantadas pela equipe de TI. 6. Sinto que as iniciativas de segurança da informação se encontram bem integradas à governança corporativa e ao planejamento estratégico da organização.

Fonte: Elaborado pelo autor.

4.9.2 Estruturada e abrangente

O princípio Estruturada e Abrangente, conforme a ISO 31000:2018, estabelece que a gestão de riscos deve ser conduzida de forma sistemática e consistente, abrangendo todas as áreas e processos organizacionais (ABNT, 2018). No entanto, as entrevistas realizadas indicam que a maioria dos órgãos avalia ou gerencia riscos de maneira pontual e reativa, muitas vezes limitada a incidentes de TI ou exigências regulatórias específicas, como a elaboração de Termos de Referência para contratações. A literatura destaca que essa falta de sistematização compromete a confiabilidade das avaliações e impede uma abordagem abrangente para a mitigação de riscos (Associação Brasileira de Normas Técnicas, 2015). Moreira *et al*. (2021) apontam que a ausência de metodologias documentadas, fluxos bem definidos e avaliações

periódicas reduz a efetividade da gestão de riscos e dificulta sua consolidação como um processo contínuo.

Além disso, a falta de padronização entre setores e a fragmentação dos esforços reforçam a percepção de que a gestão de riscos é uma atividade isolada e não parte essencial da governança organizacional (Araújo; Gomes, 2021). Dessa forma, os resultados da pesquisa confirmam que a ausência de uma estrutura formalizada compromete a abrangência e a eficácia da gestão de riscos nas instituições analisadas.

Em alguns casos, há menções ao uso parcial de frameworks como CIS ou ISO 27000, mas não se verifica uma aplicação sistemática que cubra a totalidade do ambiente. Também se notam iniciativas de mapeamento de processos por meio de um Escritório de Projetos ou de Governança, porém muitas vezes elas não incluem uma avaliação de riscos de segurança de forma ampla. Consequentemente, parte significativa dos riscos permanece subavaliada ou não é sequer identificada, comprometendo a efetividade geral da gestão de riscos. A seguir, falas dos entrevistados que corroboram para estes resultados:

> "Quando a gente fala de risco, geralmente só aparece no momento de elaborar os editais. Não temos uma abordagem geral para todos os serviços e sistemas."
> "Nossa gestão de riscos foca mais em incidentes maiores, mas os riscos que não são tão 'urgentes' ficam de lado. Falta um processo que mapeie tudo."
> "Não há um método formal que cubra todos os ativos e setores. A gente até faz uma planilha de riscos, mas cada área faz à sua maneira."
> "Usamos parcialmente o PPSI, mas é focado em alguns controles. Não temos uma matriz de riscos realmente abrangente de toda a instituição."
> "Há tentativa de fazer gestão de riscos corporativos, mas pouco se aplica especificamente às questões de TI, e aí fica incompleto. Precisamos padronizar tudo."

A seguir, 6 assertivas voltadas a avaliar o caráter estruturado e abrangente da gestão de riscos na organização. Essas assertivas podem ser aplicadas a uma escala Likert (por exemplo, de 1 = Discordo totalmente até 5 = Concordo totalmente), permitindo medir o nível de concordância e percepção dos participantes em relação à implementação do princípio Estruturada e Abrangente.

Quadro 2 – Estruturada e Abrangente

A abordagem de gestão de riscos deve ser estruturada e abrangente, assegurando consistência e comparabilidade nos processos de identificação, análise e avaliação de riscos.
1. Existe um processo formal documentado para identificar, analisar e tratar riscos em todos os ativos e setores da instituição.

2. A metodologia de gestão de riscos é padronizada, aplicando-se uniformemente em diferentes projetos e áreas.

3. As ferramentas e frameworks utilizados (CIS, ISO, NIST etc.) são aplicados de forma sistemática e cobrindo o ambiente de TI como um todo.

4. Todos os riscos, desde incidentes críticos até vulnerabilidades consideradas menores, são mapeados e registrados em um repositório comum.

5. Os riscos de segurança de TI são tratados em conjunto com outros riscos organizacionais, garantindo uma visão holística.

6. Existe um cronograma regular para revisar e atualizar as matrizes ou registros de riscos em toda a instituição.

Fonte: Elaborado pelo autor.

4.9.3 Personalizada

O princípio Personalizada, conforme a ISO 31000:2018, determina que a gestão de riscos deve ser adaptada ao contexto específico de cada organização, considerando suas necessidades, objetivos, cultura e stakeholders (ABNT, 2018). No entanto, as entrevistas revelam que, apesar do reconhecimento das peculiaridades institucionais, como grau de autonomia e diversidade de serviços, as ações de gestão de riscos permanecem genéricas, frequentemente limitadas a recomendações do PPSI ou de auditorias.

A literatura aponta que essa falta de customização compromete a efetividade do processo, tornando-o pouco aplicável às particularidades operacionais de cada instituição (ABNT, 2015). Moreira *et al*. (2021) ressaltam que a ausência de metodologias adaptadas reduz a aderência às práticas de gestão de riscos e impede sua consolidação como um mecanismo estratégico. Além disso, a não personalização dificulta a integração da gestão de riscos com as rotinas institucionais, reduzindo seu impacto na tomada de decisões (Araújo; Gomes, 2021).

Dessa forma, os achados da pesquisa demonstram que a gestão de riscos ainda não é plenamente customizada, o que limita sua efetividade e relevância organizacional. Mesmo em órgãos que reconhecem suas particularidades como a maior liberdade universitária ou a necessidade de lidar com dados sensíveis de saúde, por exemplo, o fator limitante costuma ser a falta de pessoal, orçamento ou mesmo o apoio formal.

Por isso, apesar de enxergarem a relevância de moldar a gestão de riscos ao seu perfil organizacional, muitos acabam aplicando apenas os requisitos mínimos estipulados por leis ou regulações, sem um aprofundamento genuíno para adequar metodologias de avaliação, classificação e tratamento de riscos. A seguir, falas dos entrevistados que corroboram para estes resultados:

> "A gente sabe que o ambiente de pesquisa aqui é muito diferente de um órgão administrativo. Só que, na prática, aplicamos controles genéricos, quase sem adaptação."
> "A universidade tem a questão de liberdade acadêmica, não dá pra impor bloqueios como numa empresa privada. Falta, no entanto, uma abordagem mais bem pensada pro nosso contexto."
> "Nós cuidamos de dados de alunos e servidores com perfis bem distintos. Precisaríamos de políticas específicas, mas acabamos usando regras gerais, sem tanta customização."
> "O PPSI ajuda, mas não cobre tudo do jeito que precisamos. A gente faz uns ajustes pontuais, mas nem sempre consegue customizar por falta de gente e de tempo."
> "Cada órgão tem suas prioridades, mas o setor público em geral segue o mesmo rascunho. Precisaríamos alinhar mais as regras de risco à realidade de cada ministério ou agência."

Abaixo, 6 assertivas para avaliar a personalização na gestão de riscos. Essas assertivas podem ser utilizadas com uma escala Likert (por exemplo 1 = Discordo totalmente a 5 = Concordo totalmente), permitindo verificar até que ponto as práticas de gestão de riscos se encontram personalizadas no contexto de cada organização.

Quadro 3 – Personalizada

A gestão de riscos deve ser alinhada e customizada ao contexto interno e externo da organização, considerando seu ambiente, objetivos, stakeholders e necessidades específicas.
1. A gestão de riscos em minha organização é moldada às particularidades do nosso setor de atuação (ex.: educação, saúde, fiscalização). 2. As metodologias e procedimentos de avaliação de riscos são adaptados aos processos internos e à cultura organizacional. 3. Nossas políticas de segurança e gestão de riscos levam em conta a autonomia/setores específicos (ex.: liberdade acadêmica, serviços de pesquisa, áreas finalísticas etc.). 4. As soluções e controles de segurança adotados são escolhidos após análise do contexto e necessidades exclusivas da instituição.

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.

Fonte: Elaborado pelo autor.

4.9.4 Inclusiva

O princípio Inclusiva, conforme a ISO 31000:2018, determina que a gestão de riscos deve envolver todas as partes interessadas, garantindo um processo construído com base em conhecimentos especializados e perspectivas diversas (ABNT, 2018). As entrevistas indicam que, na maioria das instituições, a segurança da informação e a gestão de riscos permanecem restritas à área de TI, sem participação efetiva de outros setores.

A literatura destaca que essa exclusão compromete a transversalidade da gestão de riscos, dificultando sua integração aos processos organizacionais (Associação Brasileira de Normas Técnicas, 2015). Moreira *et al*. (2021) apontam que a ausência de engajamento limita a compreensão dos riscos institucionais, resultando em decisões fragmentadas. Além disso, a baixa adesão a comitês ou fóruns de segurança demonstra que a gestão de riscos ainda não é percebida como uma responsabilidade coletiva, enfraquecendo a governança e a capacidade de mitigação de riscos (Araújo; Gomes, 2021).

Ao mesmo tempo, alguns órgãos relataram já possuir comitês de segurança ou de governança digital, incluindo diferentes setores, como: Gestão de Pessoas, jurídico, áreas finalísticas, o que propicia maior troca de informações e engajamento. Entretanto, mesmo nesses casos, a efetiva participação desses interessados muitas vezes permanece limitada por falta de conhecimento, prioridades concorrentes ou resistência cultural. Assim, a gestão de riscos tende a ser conduzida sem a contribuição e o comprometimento plenos de todos, resultando em decisões de segurança que podem não refletir as necessidades e realidades de cada área. A seguir, falas dos entrevistados que corroboram para estes resultados:

> “O Comitê de Segurança existe no papel, mas só o pessoal de TI comparece. Os outros setores só mandam representante quando têm interesse imediato.”
> “Falta a participação do negócio… eles não entendem que a segurança não é só firewall ou antivírus. Precisamos do engajamento de quem gerencia os dados.”

> “Criamos um fórum de gestão de riscos, mas as outras áreas não viam valor. Acabava sendo só TI discutindo sozinha e depois impondo medidas.”
> “Quando envolvemos o RH e o Jurídico, melhoram muito as ações de segurança, pois cada um traz seu ponto de vista. Mas isso ainda não é a rotina.”
> “Se a alta gestão e quem atua na ponta não estiver junto, a gestão de riscos fica incompleta. Mas convencer todos a participar ainda é um desafio.”

Abaixo, 6 assertivas que podem ser usadas para avaliar o grau de inclusão no processo de gestão de riscos. Essas assertivas, quando aplicadas em escala Likert (por exemplo: 1 = Discordo totalmente a 5 = Concordo totalmente), permitem avaliar em que medida a organização inclui efetivamente os diferentes stakeholders no processo de gestão de riscos.

Quadro 4 – Inclusiva

A gestão de riscos deve ser inclusiva, envolvendo diferentes stakeholders para que os pontos de vista e conhecimentos especializados sejam considerados.
1. Representantes de todas as áreas (administrativa, operacional e técnica) participam ativamente das discussões sobre riscos. 2. O comitê ou fórum de segurança da informação é composto por membros de diferentes setores, não se restringindo apenas à equipe de TI. 3. Antes de definir qualquer ação de tratamento de riscos, são consultadas as partes envolvidas e/ou impactadas. 4. A alta gestão (reitor, diretor, secretário etc.) contribui de forma efetiva, assegurando recursos e legitimidade às iniciativas de gestão de riscos. 5. As decisões sobre políticas e normas de segurança levam em conta as sugestões ou críticas dos demais departamentos, além do TI. 6. Há uma comunicação clara e frequente sobre riscos e segurança, estimulando a colaboração de toda a equipe.

Fonte: Elaborado pelo autor.

4.9.5 Dinâmica

O princípio Dinâmica, conforme a ISO 31000:2018, estabelece que a gestão de riscos deve antecipar e responder continuamente às mudanças, garantindo atualização constante diante de novos contextos, ameaças e exigências organizacionais (ABNT, 2018). As entrevistas

indicam que, na maioria dos órgãos, a prática ainda é reativa, com ações voltadas apenas para incidentes ou pressões externas, como auditorias e vazamentos de dados.

Embora alguns entrevistados mencionem o uso de ferramentas de monitoramento, como Zabbix e comitês periódicos, a literatura aponta que a ausência de revisões regulares e atualizações estruturadas compromete a adaptação da gestão de riscos às transformações do ambiente organizacional (ABNT, 2015). Moreira *et al*. (2021) destacam que, sem uma cultura voltada ao acompanhamento contínuo das ameaças, a gestão de riscos permanece fragmentada e limitada à resolução pontual de problemas, em vez de atuar preventivamente.

Em alguns casos, notou-se o uso pontual de atualizações de *firmware, patch management* ou revisões semestrais até por força do PPSI, o que mostra um movimento incipiente rumo a uma gestão de riscos mais proativa. Porém, problemas como a falta de equipe dedicada, orçamento restrito e resistência cultural dificultam a implementação de um ciclo dinâmico, em que a organização revise e reavalie os riscos conforme o ambiente interno e externo evolui. A seguir, falas dos entrevistados que corroboram para estes resultados:

> "A gente só corre atrás quando ocorre algum incidente grande ou quando o TCU pede justificativa. Do contrário, não há esse hábito de reavaliar e antecipar riscos."
> "Temos logs e algumas ferramentas de monitoramento, mas a cada problema que surge, é uma correria. Não há um ciclo de atualizar regularmente e revalidar nossos riscos."
> "Quando sai uma nova vulnerabilidade grave, tentamos agir rápido, mas não temos uma rotina de ficar acompanhando e testando o ambiente de forma contínua."
> "O PPSI nos obriga a preencher uns diagnósticos semestrais, o que já ajuda, mas ainda não é uma gestão que se antecipa aos problemas. Falta tempo e gente."
> "Se a gente tivesse um ciclo definido, com revisões mensais ou trimestrais, poderíamos antecipar várias questões. Mas hoje é só quando a água bate no pescoço."

Abaixo, 6 assertivas para avaliar a quão dinâmica é a gestão de riscos na organização. Essas assertivas, se usadas em uma escala Likert (por exemplo: 1 = Discordo totalmente a 5 = Concordo totalmente), ajudam a medir até que ponto a organização acompanha de forma contínua o cenário de ameaças e responde de modo ágil às mudanças, em vez de focar apenas em abordagens reativas.

Quadro 5 – Dinâmica

A gestão de riscos deve ser dinâmica, ou seja, capaz de antever, detectar e responder de forma contínua às mudanças internas e externas.

1. Nossa instituição revisa e atualiza sua matriz de riscos em intervalos regulares, mesmo sem ocorrer incidentes graves.
2. Há um processo formal de monitoramento contínuo que antecipa novas ameaças e vulnerabilidades, em vez de apenas reagir a incidentes.
3. Utilizamos ferramentas de logs e análise de vulnerabilidades de forma proativa, com alertas que geram revisões imediatas de risco.
4. As mudanças internas (novos projetos, contratações, sistemas) sempre incluem uma reavaliação dos riscos associados.
5. Mantemos um ciclo definido (mensal/trimestral/semestral) para reavaliar e priorizar riscos à luz de possíveis modificações no ambiente.
6. A equipe responsável por gestão de riscos recebe informações atualizadas sobre tendências de ataques e vulnerabilidades e ajusta os planos rapidamente.

Fonte: Elaborado pelo autor.

4.9.6 Melhor informação disponível

O princípio Melhor Informação Disponível, conforme a ISO 31000:2018, estabelece que a gestão de riscos deve ser fundamentada na coleta e análise contínua de dados atualizados e relevantes sobre ameaças e vulnerabilidades (ABNT, 2018). As entrevistas indicam que, embora os órgãos reconheçam a importância de informações para monitoramento e mapeamento de riscos, a ausência de mecanismos estruturados para consolidação e compartilhamento compromete a tomada de decisão.

A literatura aponta que a fragmentação de dados e a falta de integração entre setores reduzem a efetividade da gestão de riscos, limitando sua aplicação estratégica (ABNT, 2015). Moreira *et al*. (2021) destacam que, sem um fluxo organizado para a sistematização dessas informações, as decisões permanecem descentralizadas, dificultando a avaliação adequada dos riscos institucionais.

Além disso, ferramentas como *Zabbix* ou SIEM podem gerar alertas e indicadores, mas há relatos de que falta pessoal ou processos para analisá-los continuamente. Em algumas instituições, as atualizações vêm principalmente de exigências externas, como: relatórios de

auditoria do TCU ou do CGU, o que faz com que os dados sejam usados apenas quando existe uma demanda específica.

O resultado é que a maior parte dos entrevistados diz que o ciclo de informações sobre riscos não é tão dinâmico, nem tão robusto quanto poderia ser, e que há margem para melhorias tais como: unificar *logs*, realizar painéis executivos e compartilhar relatórios de forma mais ampla e contínua. A seguir, falas dos entrevistados que corroboram para estes resultados:

"Nós temos logs e alertas dispersos, mas não existe um painel central para consolidar tudo. Então ficamos sabendo de certas vulnerabilidades só quando estouram."

> "O uso de dados está mais focado em auditorias internas ou do TCU. Fora isso, não há um processo para compilar essas informações e municiar o comitê de riscos."
> "A gente recebe relatórios do fabricante, do CTIR, e da RNP, mas não há uma rotina pra tratar isso em conjunto e repassar pro resto da instituição."
> "Existem ferramentas de monitoramento, mas faltam pessoas pra correlacionar os dados e tirar insights sobre riscos novos ou emergentes."
> "Para cada incidente grande, a gente corre atrás de log e evidências. No dia a dia, não temos uma prática de analisar e difundir essas informações periodicamente."

A seguir, 6 assertivas para avaliar até que ponto a gestão de riscos em uma organização se fundamenta na melhor informação disponível. Com a aplicação de uma escala Likert (por exemplo: 1 = Discordo totalmente a 5 = Concordo totalmente), essas assertivas permitem verificar em que medida a organização emprega dados, evidências e relatórios atuais e robustos para embasar sua gestão de riscos, indo ao encontro do princípio de usar a Melhor Informação Disponível.

Quadro 6 – Melhor Informação Disponível

As decisões de risco devem ser tomadas com base na melhor informação disponível, incluindo dados, experiência, *insights dos stakeholders* etc.
1. Nossa instituição mantém um repositório central ou painel que consolida logs, indicadores de vulnerabilidades e alertas em tempo real. 2. As equipes de segurança analisam regularmente os dados coletados (logs de sistemas, relatórios de auditoria, boletins de vulnerabilidade) para apoiar decisões de risco. 3. Os relatórios ou análises de segurança são compartilhados com setores relevantes, auxiliando na compreensão e priorização dos riscos.

4. Quando surgem novos tipos de ataques ou vulnerabilidades, temos um canal eficiente para difundir e atualizar rapidamente nossa matriz de riscos.
5. Há ferramentas e processos definidos para correlacionar diferentes fontes de dados (logs, incidentes, boletins externos) e gerar insights confiáveis.
6. O comitê ou gestão de riscos utiliza sistematicamente informações atualizadas para redefinir prioridades e estratégias de segurança.

fFonte: Elaborado pelo autor.

4.9.7 Fatores humanos e culturais

O princípio Fatores Humanos e Culturais, conforme a ISO 31000:2018, reconhece que a percepção, o comportamento e o nível de engajamento das pessoas influenciam diretamente a efetividade da gestão de riscos (ABNT, 2018). As entrevistas evidenciam que a cultura organizacional e a postura das equipes, incluindo servidores, terceirizados e a alta gestão, representam um dos principais desafios para a adoção de práticas estruturadas de gestão de riscos.

A literatura aponta que a resistência interna e a falta de conscientização dificultam a incorporação da gestão de riscos na rotina institucional, tornando-a uma atividade secundária (ABNT, 2015). Araújo; Gomes (2021) destacam que, sem uma cultura organizacional voltada à gestão de riscos, as iniciativas se tornam fragmentadas e dependentes da iniciativa individual, comprometendo sua efetividade e continuidade.

Muitos entrevistados citaram resistência a mudanças, como: recusa em adotar ferramentas de assinatura digital ou multifatorial de autenticação, pouca compreensão de que segurança não é apenas TI e falta de priorização do tema. Em outros casos, há até conscientização maior, mas o engajamento acaba prejudicado por sobreposição de tarefas, escassez de pessoal e pouca efetividade de punições ou incentivos. Em suma, a eficiência da gestão de riscos fica comprometida quando fatores humanos não são bem trabalhados, seja por meio de capacitação, campanhas de conscientização ou apoio da alta liderança para legitimar procedimentos de segurança. A seguir, falas dos entrevistados que corroboram para estes resultados:

> “Mesmo com regras claras, muita gente ignora porque não enxerga valor ou acha que é burocracia demais. Falta uma cultura de prevenção.”
> “Alguns colegas mais antigos preferem o jeito antigo, sem tecnologia. Colocar MFA ou assinatura eletrônica vira briga.”
> “A gente faz capacitação, mas as pessoas acham que é perda de tempo. Só levam a sério após um incidente grave.”
> “Segurança é fortemente ligada a fatores comportamentais. Ter uma política não adianta se a equipe não comprar a ideia.”
> “Uma pessoa mal treinada pode vazar a credencial e comprometer o sistema inteiro. Fatores humanos são o elo mais fraco da cadeia de segurança.”

A seguir, 6 assertivas para avaliar em que medida fatores humanos e culturais são levados em conta e influenciam a gestão de riscos. Aplicando essas assertivas em uma escala Likert (por exemplo: 1 = Discordo totalmente a 5 = Concordo totalmente), é possível mensurar até que ponto a cultura organizacional e o comportamento das pessoas fortalecem ou comprometem a gestão de riscos, no espírito do Princípio Fatores Humanos e Culturais.

Quadro 7 – Fatores Humanos e Culturais

A gestão de riscos deve reconhecer as capacidades, percepções e intenções humanas que podem facilitar ou dificultar a consecução dos objetivos organizacionais.
1. Servidores e colaboradores compreendem claramente a importância de sua conduta para a segurança e gestão de riscos.
2. Existem treinamentos regulares de conscientização de segurança, que são bem aceitos pela equipe.
3. A resistência à adoção de novas ferramentas (ex.: autenticação multifator, assinatura digital) é facilmente superada.
4. A alta gestão apoia e reforça a cultura de segurança, demonstrando exemplo e priorizando iniciativas de conscientização.
5. Há incentivos ou reconhecimentos formais para as boas práticas de segurança adotadas pelos funcionários.
6. Quando um incidente ocorre por falha humana, a instituição investiga o processo para aprendizado, em vez de meramente culpar indivíduos.

Fonte: Elaborado pelo autor.

4.9.8 Melhoria contínua

O princípio Melhoria Contínua, conforme a ISO 31000:2018, estabelece que a gestão de riscos deve ser um processo cíclico, incorporando lições aprendidas e mudanças no ambiente para aprimorar continuamente políticas e controles (ABNT, 2018). As entrevistas indicam que a maioria das organizações não adota um ciclo formal de revisão e aprimoramento, limitando-se a ações pontuais motivadas por incidentes ou exigências regulatórias.

A literatura aponta que a ausência de revisões sistemáticas compromete a evolução da gestão de riscos, tornando-a reativa e desarticulada dos processos organizacionais (ABNT, 2015). Moreira *et al*. (2021) ressaltam que, sem mecanismos estruturados para registrar e analisar ocorrências passadas, as instituições perdem oportunidades de aprendizado, dificultando a adaptação e a maturidade da gestão de riscos.

Mesmo em órgãos com maior maturidade ou que desenvolvem práticas de auditoria interna/externa, a retroalimentação não é totalmente efetiva: poucos realizam, de fato, retrospectivas ou *workshops* sobre o que funcionou ou não, para então refinar a gestão de riscos. A falta de tempo, pessoal e cultura explicam parte do problema, mas também existe pouca pressão ou incentivo para que a segurança adote uma abordagem de melhoria incremental contínua. Alguns participantes ressaltaram que o PPSI, ao exigir verificações semestrais, tem funcionado minimamente como um gatilho periódico de revisão, embora ainda distante do ideal de avaliação e aprendizado permanentes. A seguir, falas dos entrevistados que corroboram para estes resultados:

> "Depois de um incidente, conseguimos resolver, mas não há um procedimento para registrar as lições aprendidas e aplicar melhorias no processo."
> "O relatório de auditoria sai, a gente faz o que eles pedem, mas não volta para replanejar nem atualizar a matriz de risco. Fica tudo muito pontual."
> "Se houvesse um ciclo de rever periodicamente o que foi implementado e o que não foi, ajustaríamos as metas. Mas isso não acontece de forma sistemática."
> "A gente até corrige falhas, mas não documenta o suficiente para mudar políticas ou procedimentos futuros."
> "O PPSI ajuda a rever algumas coisas de seis em seis meses, mas ainda não é uma prática robusta de melhoria contínua. É quase só para cumprir tabela."

Abaixo, 6 assertivas para aferir o nível de melhoria contínua na gestão de riscos. Essas assertivas, empregadas em uma escala Likert (por exemplo: 1 = Discordo totalmente a 5 = Concordo totalmente), podem ajudar a mensurar em que grau a organização evolui de forma cíclica e sistemática, fomentando a Melhoria Contínua na gestão de riscos e segurança da informação.

Quadro 8 – Melhoria Contínua

A gestão de riscos deve ser uma prática contínua de aprendizado e aperfeiçoamento, incorporando lições de experiências passadas, incidentes, *feedback* etc.
1. Após a resolução de um incidente, sempre realizamos uma análise aprofundada (post-mortem) para identificar causas-raiz e oportunidades de melhoria. 2. A organização possui um processo formal para revisar periodicamente as políticas e metodologias de gestão de riscos, incorporando lições aprendidas. 3. As auditorias externas ou internas resultam em ajustes estruturais permanentes, e não apenas em correções pontuais e reativas. 4. As equipes são estimuladas a propor aperfeiçoamentos contínuos na abordagem de riscos, registrando sugestões e acompanhando sua implementação. 5. Existe um calendário ou ciclo definido para reavaliar a efetividade dos controles e atualizar a matriz de riscos com base em novos aprendizados. 6. A cada implementação ou correção significativa de segurança, realizamos uma retrospectiva, documentando o que funcionou e o que pode ser aprimorado.

Fonte: Elaborado pelo autor.

5 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

A presente pesquisa teve como objetivo geral identificar os fatores que dificultam o uso da gestão de riscos por gestores de segurança da informação em órgãos públicos brasileiros, com base na análise de desafios, práticas e alinhamento aos princípios da norma ISO 31000:2018. A partir dos dados coletados e analisados, ficou evidente que essa problemática decorre, em larga medida, de barreiras culturais, escassez de recursos humanos, limitações orçamentárias e falta de apoio da alta gestão, culminando em uma abordagem predominantemente reativa em vez de proativa. Essas constatações reforçam a urgência de se alinhar governança, cultura organizacional e processos de TI para efetivamente incorporar a gestão de riscos como prática fundamental de segurança. Conforme exposto por Moreira *et al*. (2021), a integração e estruturação dos processos são fundamentais para garantir a implementação eficaz da gestão de riscos. Portanto, esses desafios evidenciam barreiras estruturais e culturais que comprometem a implementação efetiva da gestão de riscos no setor público.

5.1 Conclusão

Como primeiro objetivo específico, buscou-se mapear os principais desafios e dificuldades na adoção da gestão de riscos. O estudo evidenciou problemas como a resistência cultural tanto da equipe quanto de gestores, a falta de pessoal especializado, a ausência de processos integrados e a falha na disseminação de informações sobre riscos. Observou-se, ainda, que grande parte das instituições carece de uma estrutura formal como: equipe, comitê, política, que dê suporte e legitimidade às iniciativas de segurança, o que agrava a dificuldade de implantar uma abordagem de riscos estruturada e abrangente.

Em seguida, buscou-se analisar o impacto desses desafios sobre a eficácia da gestão de riscos. Ficou claro que, quando a cultura organizacional não prioriza a segurança, quando não há investimento em pessoal ou quando as ações ficam restritas à TI, a gestão de riscos torna-se desconexa, e os controles implementados não são suficientes para mitigar ameaças de modo efetivo. Na prática, a falta de integração entre setores e a ausência de métodos contínuos e proativos comprometem o valor da gestão de riscos, que passa a ser vista apenas como mais uma burocracia ou tarefa extra.

A pesquisa também permitiu identificar soluções e melhores práticas que podem auxiliar a superar esses entraves. Entre elas, destacam-se: campanhas sistemáticas de conscientização para fortalecer a cultura de segurança, estabelecimento de comitês interdisciplinares inclusivos e com participação de todas as áreas, adoção de frameworks como CIS, ISO 27000 e PPSI de modo personalizado ao contexto de cada órgão, além de um planejamento estratégico que vincule recursos orçamentários à implementação de ações de risco. Tais práticas, quando aliadas ao suporte efetivo da alta gestão, mostram potencial para viabilizar uma gestão de riscos sólida e contínua.

Com base nos achados, propõem-se recomendações que envolvem, em primeiro lugar, a formalização de uma política de gestão de riscos, garantindo que todos os ativos, processos e setores sejam mapeados, e que haja um ciclo de monitoramento e revisão periódica. É indispensável reforçar a capacitação das equipes e o engajamento da liderança, criando um ambiente propício para que a segurança seja percebida como parte integrante das decisões e não apenas uma exigência pontual. Além disso, a adoção de indicadores de desempenho (KPIs) e a definição de papéis e responsabilidades (inclusive no que tange à comunicação de incidentes) contribuem para a manutenção da gestão de riscos ao longo do tempo.

Por fim, realizou-se uma análise detalhada dos resultados à luz dos oito princípios da ISO 31000:2018 (Integrada, Estruturada e Abrangente, Personalizada, Inclusiva, Dinâmica, Melhor Informação Disponível, Fatores Humanos e Culturais, e Melhoria Contínua). Constatou-se que, embora alguns órgãos demonstrem certo alinhamento em aspectos pontuais como por exemplo, Inclusiva nos casos em que há comitês interdisciplinares; Dinâmica quando existem processos semestrais de verificação pelo PPSI, a maioria dos princípios não é plenamente atendida, sobretudo em virtude de restrições organizacionais devido a carência de pessoal, cultura resistente, pouca integração e de processos pouco estruturados que dificultam a incorporação do risco na governança. Tais achados validam a hipótese de que a gestão de riscos na segurança da informação ainda não está efetivamente consolidada em grande parte das instituições públicas analisadas.

5.2 Recomendações e pesquisas futuras

Diante desses achados, recomenda-se, como trabalho futuro de aprimoramento, a aplicação de um questionário baseado nas assertivas propostas ao longo da análise uma escala Likert de cinco pontos, por exemplo, de modo a mensurar quantitativamente o grau de aderência

de cada instituição aos princípios da ISO 31000:2018. Isso permitiria obter um panorama estatístico mais amplo, comparando diferentes órgãos e aprofundando o entendimento das variações de maturidade. Ademais, sugere-se que investigações futuras explorem casos de sucesso *(best practices)* em ambientes organizacionais semelhantes, de modo a fornecer diretrizes ainda mais direcionadas para superar os obstáculos mapeados.

5.3 Limitações

As limitações do presente estudo incluem, primeiramente, a amplitude ou quantidade das entrevistas realizadas, que podem não refletir totalmente a realidade de todos os órgãos públicos, dada a diversidade existente. Além disso, o método de coleta qualitativo, ou seja, entrevistas semiestruturadas, pode resultar em subjetividade das respostas, pois se baseiam na percepção dos gestores ou servidores específicos. Por fim, a falta de uma etapa quantitativa neste trabalho, que complementasse a análise qualitativa, pode ter restringido a profundidade com que se compararam diferentes cenários ou se aferiram estatisticamente os níveis de maturidade de cada órgão. Apesar disso, espera-se que a investigação aqui apresentada sirva de base para reflexões e ações concretas de melhoria na gestão de riscos em segurança da informação.

REFERÊNCIAS

ABNT. **NBR ISO 31000**. Gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018. Disponível em: https://dintegcgcin.saude.gov.br/attachments/download/23/2018%20-%20Diretrizes%20-%20Gestão%20de%20Riscos_ABNT%20NBR%20ISO%2031000.pdf. Disponível em:. Acesso em: 23 jan. 2025.

AIDAR, Soraia *et al*. Os desafios da gestão de mudanças em empresas privadas. **Enciclopedia Biosfera**, [*s*. *l*.], v. 18, n. 37, 2021.

ALVES, Dyego *et al*. Gestão de riscos no setor público: revisão bibliométrica e proposta de agenda de pesquisa. **Revista do Serviço Público**, [*s*. *l*.], v. 72, n. 4, p. 824-854, 2021. Disponível em: https://repositorio.enap.gov.br/jspui/handle/1/6802. Acesso em: 26 jan. 2025.

ALVES, Renato Solimar; GEORG, Marcus Aurelio Carvalho; NUNES, Rafael Rabelo. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. **Revista Ibérica de Sistemas e Tecnologias de Informação**, [*s*. *l*.], n. E56, p. 344-357, 2023. Disponível em: https://www.researchgate.net/publication/371510704_Judiciario_sob_ataque_hacker_riscos_de_negocio_para_seguranca_cibernetica_em_tribunais_brasileiros. Acesso em: 20 jan. 2025.

ANDRESS, Jason; WINTERFELD, S. **The basics of information security**: understanding the fundamentals of infosec in theory and practice. [*S. l.*]: Syngress, 2018.

ARAÚJO, Artur; GOMES, Anailson Marcio. Gestão de riscos no setor público: desafios na adoção pelas universidades federais brasileiras. **Revista Contabilidade & Finanças**, [*s*. *l*.], v. 32, p. 241-254, 2021.

AVEN, Terje; RENN, Ortwin. On risk defined as an event where the outcome is uncertain. **Journal of risk research**, [*s*. *l*.], v. 12, n. 1, p. 1-11, 2009.

CISCO. Estudo da Cisco revela que poucas empresas no Brasil estão preparadas para se defender contra ameaças de segurança. **Cisco News Blog**, 4 abr. 2024. Disponível em: https://news-blogs.cisco.com/americas/pt/2024/04/04/estudo-da-cisco-revela-que-poucas-empresas-no-brasil-estao-preparadas-para-se-defender-contra-ameacas-de-seguranca/. Acesso em: 28 ago. 2024.

COSO. Enterprise risk management: integrating with strategy and performance. **Coso**, 2007. Disponível em: https://www.coso.org/enterprise-risk-management. Acesso em: 25 jan. 2025.

DA FONTE, Eduardo Côrtes. Gerenciamento de riscos: uma comparação entre o Guia PMBOK 6ª edição e a ISO 31000: 2018. **Boletim do Gerenciamento**, [*s*. *l*.], v. 4, n. 4, p. 22-32, 2019.

DE ANDRADE, Felipe Scarpelli. Análise de Riscos e a Atividade de Inteligência. **Revista Brasileira de Ciências Policiais**, [*s*. *l*.], v. 8, n. 2, p. 90-116, 2017.

DE MASSIS, Alfredo *et al*. Innovation with Limited Resources: Management Lessons from the German Mittelstand. **Journal of Product Innovation Management**, [*s*. *l*.], v. 35, n. 1, p. 125-146, 2018.

DE OLIVEIRA, Ana Camila Rodrigues *et al*. Gestão de riscos em cadeia de suprimentos: aplicação em uma distribuidora de gás canalizado. **Revista Produção Online**, [*s*. *l*.], v. 18, n. 3, p. 1.076-1.101, 2018.

DE OLIVEIRA, Ualison Rébula *et al*. The ISO 31000:2018 standard in supply chain risk management. **Journal of Cleaner Production**, [*s*. *l*.], v. 151, p. 616-633, 2017.

FAGUNDES, Ernando *et al*. Tolerância ao risco de gestores: análise na tomada de decisões nos campos pessoal e organizacional. **Revista Evidenciação Contábil & Finanças**, [*s*. *l*.], v. 9, n. 1, p. 22-43, 2021.+++

FONTELAS, Audrey. Quais são os impactos dos ataques cibernéticos nas organizações?. **Phishx**, 2023. Disponível em: https://www.phishx.io/pt/post/impactos-dos-ataques-ciberneticos-nas-organizacoes. Acesso em: 28 ago. 2024.

G1. Ataque hacker ao site do Ministério da Saúde tira do ar o ConecteSUS. **G1 – Jornal Nacional**, 10 dez. 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml. Acesso em: 28 ago. 2024.

HANNA, Hany; HAROUN, Mai. H.; GOHAR, Nermin. TOE model: adoption of blockchain. **The Business and Management Review**, v. 11, n. 1, Aug. 2020. Disponível em: https://www.researchgate.net/profile/Hany-Hanna-2/publication/344793035_TOE_Model_Adoption_of_Block_Chain/links/5fecdaf1a6fdccdcb81ad7e3/TOE-Model-Adoption-of-Block-Chain.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9#page=288. Acesso em: 28 ago. 2024.

INÁCIO, Dauana Berndt *et al*. Estudo de caso sobre a metodologia de gestão de riscos utilizada na UFSC. *In*: COLÓQUIO INTERNACIONAL DE GESTÃO UNIVERSITÁRIA (CIGU), 10., 2021, [Florianópolis, SC]. **Anais** […]. [Florianópolis, SC]: UFSC, 2021. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/230248/210083.pdf?sequence=1&isAllowed=y. Acesso em: 16 fev. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27001**:2013 – Information technology – Security techniques – Information security management systems – Requirements. [*S. l.*: *s*. *n*.], 2022. Disponível em: https://www.iso.org/standard/54534.html. Acesso em: 28 ago. 2024.

JORNAL DA USP. Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano. Jornal da USP. **Jornal da USP**, 2023. Disponível em: https://jornal.usp.br/radio-usp/brasil-sofreu-mais-de-100-bilhoes-de-tentativas-de-ataques-ciberneticos-no-ultimo-ano/. Acesso em: 28 ago. 2024.

KIRILMAZ, Oguzhan; EROL, Serpil. A proactive approach to supply chain risk management: shifting orders among suppliers to mitigate the supply side risks. **Journal of Purchasing and Supply Management**, [*s*. *l*.], v. 23, n. 1, p. 54-65, 2017.

KLEIN, Leander Luiz *et al*. A influência do ambiente organizacional interno na gestão de riscos. **Revista de Gestão**, **Finanças e Contabilidade**, [*s*. *l*.], v. 11, n. 3, p. 85-107, 2021.

KNIGHT, Frank. **Risk**, **uncertainty and profit**. New York: Hart, Schaffner, and Marx, 1921.

LISBOA, Antonio Maria dos Reis. Análise de técnicas e estruturas de gestão de riscos dos tribunais brasileiros. Brasília, DF: Universidade de Brasília, 2024. Disponível em: https://bdm.unb.br/handle/10483/40889. Acesso em: 23 jan. 2025.

MARTINS, Adriano Luxi *et al*. Implementação de projetos de aerogeradores offshore no Brasil: um modelo para gestão de riscos segundo as melhores práticas em gestão de projetos. *In*: CONGRESSO INTERNACIONAL DE GESTÃO, PROJETOS & LIDERANÇA, 2018, Curitiba. Curitiba, PR: [*s*. *n*.], 2018.

MONTEZANO, Lana *et al*. Percepção de servidores públicos quanto à implantação da gestão de riscos em uma secretaria do governo federal do Brasil. **Revista Economia & Gestão**, [*s*. *l*.], v. 19, n. 54, p. 77-94, 2019.

MOREIRA, Fernando Rocha *et al*. Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. **Ieee Access**, [*s*. *l*.], v. 9, p. 129.605-129.618, 2021.

NDLELA, Martin; NDLELA, Martin N. A stakeholder approach to risk management. **Crisis Communication**, p. 53-75, 2019. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-97256-5_4. Acesso em: 16 fev. 2025.

NEVES, Edson Oliveira. Aprendizagem organizacional: considerações sobre metodologias de promoção e desenvolvimento. **Revista da Faculdade de Administração e Economia**, [*s*. *l*.], v. 3, n. 1, p. 2-16, 2011.

OLECHOWSKI, Alison *et al*. The professionalization of risk management: what role can the ISO 31000:2018 risk management principles play?. **International Journal of Project Management**, [*s*. *l*.], v. 34, n. 8, p. 1.568-1.578, 2016.

OLIVEIRA SANTOS JHUNIOR, Ronaldo de; ABIB, Gustavo. Percepção e gestão de riscos no contexto de internacionalização. **Gestão & Planejamento-G&P**, [*s*. *l*.], v. 20, 2019.

OLIVEIRA, Luiz Carlos Silva; SOARES, Gustavo Fernandes. Gestão de riscos operacionais e controles internos: o caso de uma instituição bancária. **Revista de Contabilidade da UFBA**, [*s*. *l*.], v. 12, n. 1, p. 227-249, 2018.

PALTRINIERI, Nicola; COMFORT, Louise; RENIERS, Genserik. Learning about risk: machine learning for risk assessment. **Safety science**, [*s*. *l*.], v. 118, p. 475-486, 2019.

PRAKASH, Surya; SONI, Gunjan; RATHORE, Ajay Pal Singh. Uma análise crítica do conteúdo da gestão de riscos da cadeia de suprimentos: uma revisão estruturada da literatura. **Journal of Advances in Management Research**, [*s*. *l*.], v. 14, n. 1, p. 69-90, 2017.

QUEIROZ, Carlos Eduardo Muniz; NUNES, Rafael Rabelo. Os tribunais têm estrutura para gerenciar riscos de segurança da informação? **Revista CEJ**, Brasília, DF, v. 27, n. 86, p. 145-160, 2023. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/2838. Acesso em: 26 jan. 2025.

SHAPIRA, Naama *et al*. Cybersecurity in water sector: stakeholders perspective. **Journal of Water Resources Planning and Management**, v. 147, n. 8, 2021. Disponível em: https://www.researchgate.net/publication/353623690_Cybersecurity_in_Water_Sector_Stakeholders_Perspective. Acesso em: 27 jan. 2025.

SOUSA, Monique Regina Bayestorff Duarte de *et al*. Gestão de risco nas instituições universitárias: uma análise comparativa da metodologia da Controladoria Geral da União e do Ministério do Planejamento, Desenvolvimento e Gestão. *In*: COLÓQUIO INTERNACIONAL DE GESTIÓN UNIVERSITÁRIA, 18., 2018, [*s*. *l*.]. **Anais** […]. [*S*. *l*.: *s*. *n*.], 2018.

STALLINGS, Williams. **Computer security**: principles and practice. [*S*. *l*.]: Pearson Education, 2013.

THEOBALD, Roberto; LIMA, Gilson Brito Alves. A excelência em gestão de SMS: uma abordagem orientada para os fatores humanos. **Sistemas & Gestão**, [*s*. *l*.], v. 2, n. 1, p. 50-64, 2007.

TIPTON, Harold F.; KRAUSE, Micki. **Information security management handbook**. 6. ed. Boca Raton: CRC Press, 2012.

TRANSFORMAÇÃO DIGITAL. **Gov.com**. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/transformacao-digital. Acesso em: 29 jan. 2025.

Tribunal de Contas da União. –. Brasília, DF: TCU, Secretaria de Planejamento, Governança e Gestão. (Seplan), 2020.

TRIBUNAL DE CONTAS DA UNIÃO. Brasília, DF: TCU, Secretaria Geral de Controle Externo (Segecex), 2018.

TSOHOU, Aggeliki; KARYDA, Maria; KOKOLAKIS. **Spyros information security management systems**: a handbook for practitioners. [S.l.]: Springer, 2020.

URSILLO, JR., Steve; ARNOLD, Christopher. **International Federation Of Accountants** (**IFAC**), 2023. Disponível em: https://www.ifac.org/knowledge-gateway/discussion/cybersecurity-critical-all-organizations-large-and-small#:~:text=Cybersecurity%20is%20making%20sure%20your,from%20unauthorized%20access%20%C2%BAr%20damage. Acesso em: 28 ago. 2024.

WIDDOWSON, Amanda; CARR, David. Human factors integration: implementation in the onshore and offshore industries. **Research Report**, [*s*. *l*.], n. 1, 2002a. Disponível em: http://www.hse.gov.uk/research/rrpdf/rr001.pdf. Acesso em: 28 set. 2004.

WILDAVSKY, Aaron. No risk is the highest risk of all. **American Scientist**, [s.l.], v. 67, n. 1, p. 32-37, 1979.

WORLD ECONOMIC FORUM. **The global risks report 2025**. 20th ed. Geneva: World Economic Forum, 2025. Disponível em: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf. Acesso em: 28 jan. 2025.

ZOU, Yang; KIVINIEMI, Arto; JONES, Stephen W. A review of risk management through BIM and BIM-related technologies. **Safety science**, [*s*. *l*.], v. 97, p. 88-98, 2017.