Manual de Controles Internos e Riscos

Sumário

1. Introdução

A gestão de controles internos e riscos é um pilar fundamental para a perenidade, sustentabilidade e o sucesso de qualquer organização, especialmente no setor de seguros, onde a confiança e a integridade são ativos indispensáveis. Em um ambiente altamente regulado e dinâmico, devemos adotar práticas robustas de gerenciamento de riscos para proteger clientes, acionistas e a própria continuidade do negócio.

Este manual tem como objetivo estabelecer diretrizes claras e eficazes para a identificação, avaliação, monitoramento e mitigação de riscos, bem como para a implementação de controles internos que assegurem a conformidade com normativas regulatórias e boas práticas de governança. A estrutura aqui apresentada visa alinhar as operações do Grupo Wiz Co às exigências dos órgãos reguladores, além de promover uma cultura organizacional voltada para a mitigação de riscos e a melhoria contínua dos processos.

Ao longo deste documento, serão abordados os principais conceitos e metodologias aplicáveis ao gerenciamento de riscos e controles internos, incluindo a definição dos papéis e responsabilidades, os tipos de riscos de acordo com o nosso apetite a riscos e definição do dicionário de riscos e as estratégias para sua mitigação. Também serão detalhados os procedimentos de monitoramento e reporte, essenciais para garantir a efetividade do processo de gestão de riscos.

A correta aplicação deste manual permitirá ao Grupo Wiz Co aprimorar sua capacidade de resposta a eventos adversos, fortalecer a tomada de decisões estratégicas e aumentar sua resiliência frente às incertezas do mercado. Dessa forma, reforçamos o compromisso com a transparência, a ética e a segurança operacional.

2. Objetivo e Aplicabilidade

Objetivo

Este Manual tem como objetivo estabelecer diretrizes e melhores práticas para os controles internos e o gerenciamento de riscos nas operações da Wiz Co e de suas Unidades de Negócio.

Com ele, buscamos garantir a conformidade regulatória, fortalecer a governança corporativa e criar um ambiente de controle eficaz, reduzindo perdas e protegendo o Grupo contra riscos financeiros, operacionais e reputacionais.

As orientações foram apresentadas de maneira resumida para facilitar a compreensão do processo de gestão de riscos. No entanto, este manual não contempla todos os aspectos do tema. Por isso, recomenda-se a busca por aprofundamento adicional, bem como a consulta à equipe de Riscos e Controles Internos da Companhia para esclarecimentos e orientações complementares.

Aplicabilidade

As orientações aqui descritas constituem a linha de conduta adotada pelo Grupo e se aplica à Wiz Co Participações e Corretagem de Seguros S.A., suas empresas controladas, áreas internas, colaboradores, diretores, membros do conselho de administração e quaisquer outros órgãos com funções técnicas e consultivas do Grupo, com exceção das unidades de negócio, a saber: Inter Seguros, BRB Seguros e CMG Corretora de Seguros.

3. Definições

As definições listadas abaixo foram definidas utilizando-se como referência a ISO 31000:2018, o COSO ERM, a Resolução CNSP nº 416/2021 e fontes relacionadas.

Processo: Processo definido como um **conjunto estruturado de atividades** ou etapas inter-relacionadas, que são executadas para alcançar um determinado objetivo.

Risco: Evento que possa afetar negativamente os resultados da Companhia e sua capacidade de atingir seus objetivos estratégicos e de negócios.

Apetite a risco: Nível de exposição ao risco que a Companhia está disposta a aceitar para atingir seus objetivos estratégicos de curto, médio e longo prazos, esse apetite é limitado pelo nível de tolerância ao risco.

Atividade de Controle: são ações estabelecidas para atuar na mitigação dos riscos e contribuir para que os objetivos estratégicos e operacionais sejam alcançados dentro dos padrões estabelecidos.

Tolerância ao risco: Medida do nível de aceitação aos riscos, é quantificável e estabelece o limite para o apetite a risco declarado pela Companhia.

Impacto: É a potencial consequência da materialização de um risco, medido em termos financeiros e/ou não financeiros.

Probabilidade: Possibilidade de ocorrência de um evento. Na terminologia de gerenciamento de riscos, a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer.

Exposição ao risco: Representa a combinação do impacto e da probabilidade de a Companhia ser afetada por um determinado risco, podendo ser alto, médio ou baixo.

Matriz de riscos: Relação dos riscos identificados e avaliados para a Companhia e suas unidades de negócio, classificados de acordo com seu nível de exposição.

Gestão de riscos: Processos e procedimentos empregados de forma coordenada para identificar, avaliar, mensurar, tratar, monitorar e reportar os riscos da Companhia, tendo por base a adequada compreensão dos tipos de risco, de suas características e interdependências, das fontes de riscos e de seu potencial impacto sobre o negócio.

Controle: Atividades periódicas ou contínuas executadas visando a mitigação de um risco. Compreendem políticas, normas e procedimentos cuja finalidade é minimizar os riscos que estão sendo observados nos processos executados. As atividades de controle ocorrem em todos os níveis da Companhia.

Controles internos: Conjunto coerente, abrangente e contínuo de processos e procedimentos realizados pela Companhia com o objetivo de assegurar minimamente i) a eficiência operacional de suas atividades; ii) a existência e prestação de informações financeiras e não financeiras às partes interessadas internas e externas, de forma tempestiva, fidedigna e completa; iii) a conformidade de suas operações com as leis e regulamentações aplicáveis, boas práticas e suas próprias políticas e normativos internos; e iv) a condução prudente dos negócios.

Sistema de controles internos (SCI): Conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, operacionalização, monitoramento, análise crítica e melhoria contínua dos controles internos através de toda a Companhia.

Unidades de negócio: Unidades integrantes da estrutura organizacional e que desempenham atividades diretamente relacionadas ao negócio da Companhia.

Gestão de continuidade de negócios: Processo essencial para garantir que uma organização possa manter suas operações essenciais diante de incidentes inesperados, como falhas tecnológicas, desastres naturais, crises econômicas e ataques cibernéticos.

Cadeia de valor: A definição de cadeia de valor, de acordo com Michael Porter, refere-se ao conjunto de atividades primárias e de suporte que uma organização executa para criar valor para o cliente final, desde a entrada de insumos até o pós-venda.

4. Referências Normativas

- **Política de Gestão de Riscos Wiz Co:** descreve as definições, o processo e as responsabilidades para a gestão de riscos
- **Código de Conduta Ética**: Estabelece o padrão de conduta dentro da Wiz, objetiva orientar como proceder de acordo com os princípios éticos e valores da instituição.
- **NBR ISO 31000:2018:** Fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A aplicação destas diretrizes pode ser personalizada para qualquer organização e seu contexto.
- **COSO ERM:** Fornece uma estrutura de processo de gestão de riscos, contribuindo para uma adoção mais adequada ao abordar os riscos inerentes dos processos institucionais em prol do cumprimento dos objetivos estratégicos e de negócio.

5. Papéis e Responsabilidades

Em uma organização, todos os colaboradores compartilham a responsabilidade pela gestão de riscos e, cada equipe deve ter suas funções bem definidas para entender seu papel e os limites de atuação dentro da gestão de riscos da empresa.

Os gestores são os principais responsáveis por planejar, organizar e implementar a gestão de riscos em suas áreas. Devem promover a cultura de gestão de riscos e controlar os riscos dentro dos limites aceitáveis estabelecidos pela empresa.

Os papéis e responsabilidades estão definidos na Política de Gestão de Riscos da Wiz.

6. Estrutura dos Controles Internos

A estrutura de controles internos na Wiz Co busca assegurar a existência de um processo efetivo de identificação e avaliação dos riscos por meio da análise e monitoramento dos controles existentes.

A Wiz adota o modelo das três linhas de defesa que estão envolvidas no alinhamento das normas internas com o ambiente de controle necessário para prevenir e combater qualquer ato de natureza ilícita, bem como assegurar que os principais riscos envolvidos nas operações sejam conhecidos, monitorados e tratados adequadamente. A figura abaixo apresenta, de forma adaptada, o modelo das linhas de defesa:

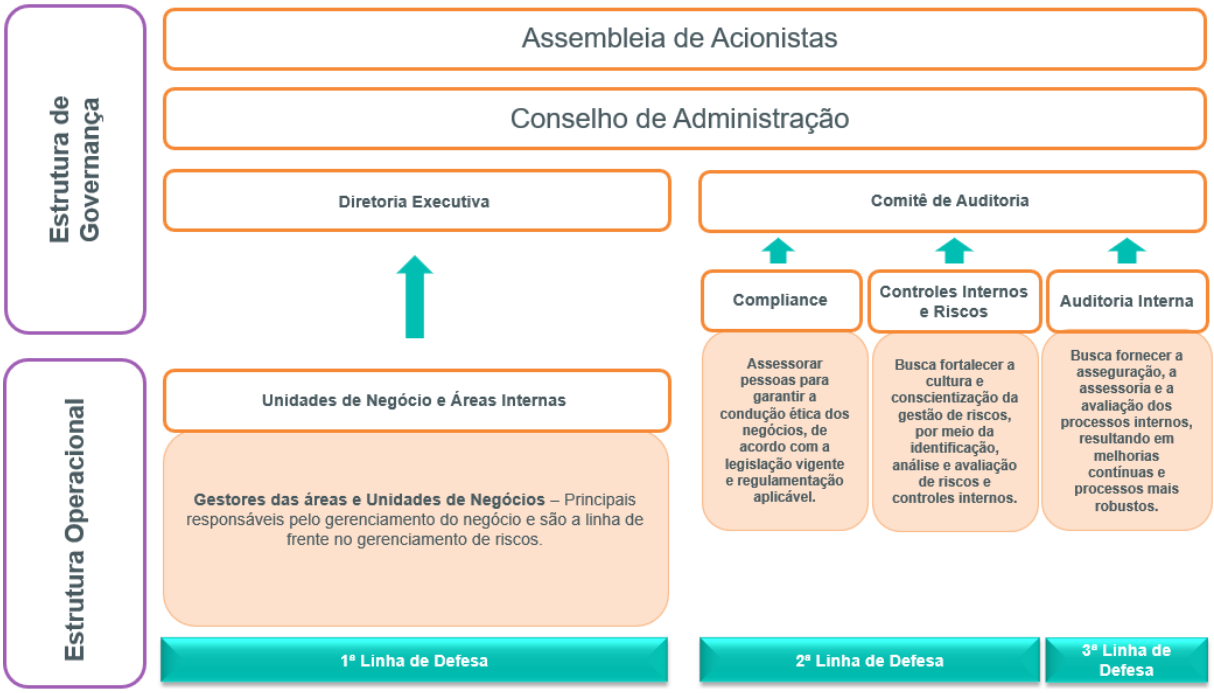

Figura 1: Modelo das três linhas de defesa

7. Gestão de Riscos Corporativos e Ferramentas de Apoio

Processo de Gestão de Riscos

O processo de gestão de riscos é constituído pelo conjunto de procedimentos e ações coordenadas que buscam garantir que os objetivos sejam realizados dentro de limites aceitáveis de risco. Para tanto, o Grupo Wiz Co segue as etapas cruciais no processo de gestão de riscos, quais sejam: identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos inerentes que ameaçam as atividades da Companhia, considerando aspectos de curto, médio e longo prazos.

O processo de gestão de riscos foi definido com base nas orientações consolidadas do COSO – *Committee of Spornsoring Organizations of the Treadway Commission,* no processo de gestão de riscos sugerido pela norma ISO 31000:2018, e nas exigências previstas na Resolução CNSP n° 416/21.

Etapas do Processo de Gestão de Riscos

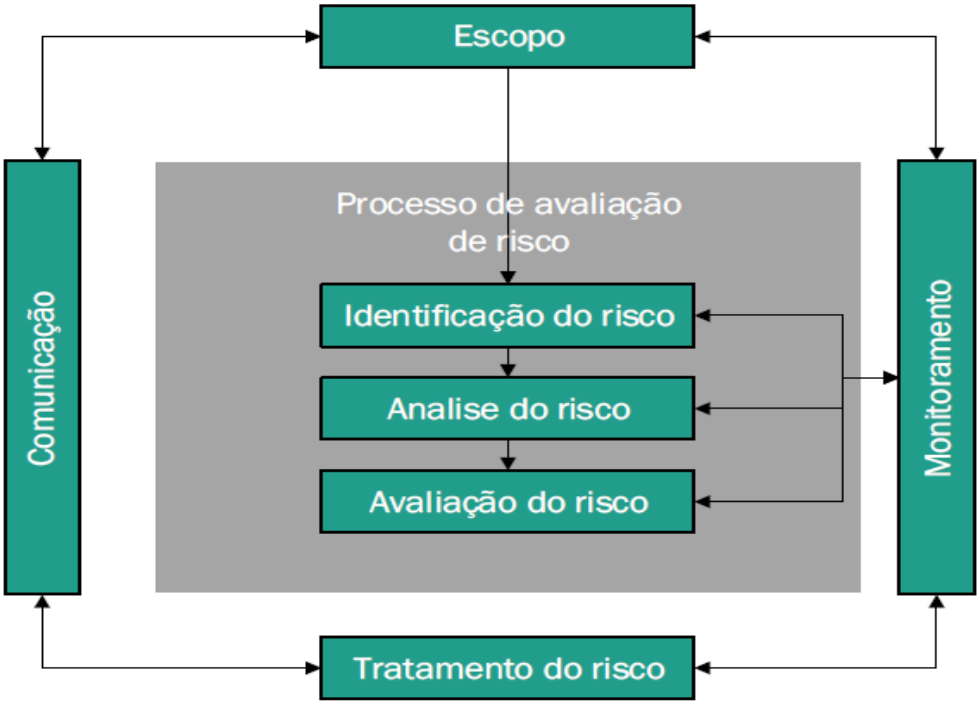

Figura 2: Fluxo das etapas do processo de gestão de riscos

- **Escopo (Análise do ambiente e objetivos):**

  Esta etapa compreende, dentre outros, a documentação do(s):

  - Contexto e ambiente sob o qual a Companhia está inserida;
  - Objetivos estratégicos do processo e/ou da Companhia;
  - Fatores internos ou externos que possam impactar o atingimento dos objetivos, incluindo a lista de diretrizes legais e normativos aplicáveis e a lista de sistemas e outras ferramentas que operacionalizam o processo;
  - Mapeamento das partes interessadas do processo, preferencialmente, através de utilização da Matriz RECI (RACI *matrix* ou *chart*, em inglês);
  - Mapeamento do fluxo de atividades, destacando decisões, entradas, saídas e classificações por criticidade.

  Se a área/unidade de negócio já tiver cadeia de valor, macroprocesso, processo e fluxos mapeados, tais documentos serão de fundamental relevância para esta etapa.

- **Identificação do Risco (Mapeamento dos eventos de riscos):**

  O processo consiste em identificar e descrever riscos que possam afetar o alcance dos objetivos organizacionais, avaliando as causas, eventos, vulnerabilidades e mudanças no contexto.

  Após este levantamento, os riscos são analisados de forma crítica, priorizando aqueles com maior relevância para os processos.

- **Análise do Risco:** A análise de riscos é o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos (ABNT, 2009).

  O risco resulta da interação entre a **probabilidade** de um evento ocorrer e a **magnitude** de suas consequências. Portanto, o grau de risco é determinado pela análise conjunta da chance de ocorrência e do impacto que esse evento pode causar aos objetivos estabelecidos, conforme avaliado na matriz de risco abaixo.

			PROBABILIDADE				
			Muito Baixa	Baixa	Média	Alta	Muito Alta
			1	2	5	8	10
IMPACTO	Insignificante	10	10	20	50	80	100
	Não relevante	20	20	40	100	160	200
	Moderado	50	50	100	250	400	500
	Extensivo	70	70	140	350	560	700
	Significativo	100	100	200	500	800	1000

BAIXO	Mitigação recomendada - Avaliar propostas de melhorias continuas
MÉDIO	Mitigação necessária - Avaliar alternativas de médio prazo e melhorias continuas
ALTO	Mitigação urgente - Implantar ações de curto prazo

Figura 3: Matriz de Impacto x Probabilidade

As perguntas a seguir poderão ser utilizadas como referência para avaliar a probabilidade de ocorrência do risco:

- Há controles automáticos implementados que mitigam esse risco?
- Há validações manuais ou revisões independentes que reduzam a chance de ocorrência?
- Existe uma alçada de aprovação formal no processo associada a esse risco?
- Esse processo passou recentemente por auditorias internas ou externas? Se sim, houve apontamentos?
- Já houve histórico de ocorrência deste risco na organização ou no mercado?
- O risco depende de fatores externos fora do controle da organização (ex.: fornecedores, governo, clima)?
- Qual o grau de variabilidade ou incerteza do processo relacionado ao risco?
- O processo está formalizado e os envolvidos são capacitados e conscientes do risco?

As perguntas a seguir orientam a análise do impacto potencial desse risco:

- Qual seria o impacto financeiro estimado, em caso de ocorrência do risco?
- Esse risco pode afetar diretamente a experiência ou a confiança do cliente?
- A ocorrência desse risco impactaria outras áreas, processos ou unidades de negócio?

- O risco pode resultar em penalidades legais, sanções regulatórias ou não conformidades?
- A falha relacionada ao risco pode interromper a operação crítica do negócio?
- Haveria exposição negativa à reputação da empresa, na mídia ou junto aos *stakeholders*?
- O risco compromete o atingimento de metas estratégicas ou indicadores-chave da organização?
- Esse risco pode acarretar perda de dados, informações sensíveis ou ativos relevantes?

A **documentação da análise de riscos** costuma conter: (a) o método aplicado, as fontes de informação utilizadas e os envolvidos no processo; (b) os critérios adotados para classificar probabilidade e impacto; (c) a estimativa de ocorrência dos eventos, seus possíveis efeitos nos objetivos e respectivas análises; (d) os controles internos existentes, sua efetividade e o risco associado; e (e) a avaliação dos riscos antes (inerente) e após (residual) os controles.

Os **riscos** serão **classificados** nas seguintes **categorias**:

- Risco de Conformidade – Possibilidade de perdas, sanções ou penalidades devido ao descumprimento de leis, regulamentações, normas externas ou diretrizes internas.

- Risco Estratégico – Possibilidade de não alcançar os objetivos estratégicos devido a decisões ou estratégias inadequadas, ineficazes ou malsucedidas.

- Risco Financeiro – Possibilidade de perdas decorrentes de decisões financeiras, variações econômicas (juros, câmbio, inflação) ou incapacidade de cumprir obrigações financeiras.

- Risco de Governança – Possibilidade de falhas perda ou deficiências ocasionadas por inadequações dos processos e da estrutura organizacional de governança corporativa;

- Risco de Informação - Possibilidade de sanções ou prejuízos causados por falhas na confidencialidade, na integridade ou na disponibilidade das informações, incluindo uso indevido ou tratamento inadequado de dados;

- Risco Operacional - Possibilidade de perdas por falhas em processos, sistemas, contratos, eventos externos ou descumprimento legal, incluindo danos a terceiros;

- Risco de Pessoas - Perdas decorrentes de falhas na gestão de pessoas, como contratação, alocação ou retenção de profissionais qualificados, gerando impactos operacionais; e

- Risco de Reputação e Imagem - Danos à imagem da empresa e seus resultados, causados por eventos ou percepções negativas junto ao mercado e partes interessadas.

As definições completas das categorias de risco estão no Dicionário de Riscos do Grupo. Em caso de dúvidas, recomenda-se consultar o Dicionário de Riscos ou a equipe de Riscos e Controles Internos da Companhia.

- **Avaliação do Risco:** A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis ou se algum tratamento é exigido (ABNT, 2009).

  Nesta etapa, com base na avaliação dos riscos feita anteriormente, são tomadas decisões importantes, tais como: (a) determinar quais riscos demandam ações e a ordem de prioridade; (b) decidir se determinadas atividades devem ser mantidas ou suspensas; e (c) avaliar a necessidade de implementar novos controles internos ou ajustar os já existentes, seja para mantê-los, modificá-los ou eliminá-los.

- **Tratamento do Risco:** Define-se se o risco será corrigido, mitigado ou aceito, com base em análises técnicas e financeiras, incluindo a avaliação do Apetite ao Risco* da Companhia, e aprovação da liderança. Em seguida, elabora-se um plano de ação.

*O **Apetite a Riscos** representa o nível de risco que a organização está disposta a assumir para alcançar seus objetivos estratégicos. A **Declaração de Apetite a Riscos (RAS)** é elaborada pela área de Controles Internos e Riscos, e considera as principais categorias de risco definidas nas políticas e dicionários do Grupo, orientando decisões alinhadas à estratégia, evitando exposições excessivas e promovendo o aproveitamento de oportunidades dentro de limites aceitáveis. A versão atual foi elaborada em 2025.

- **Monitoramento:** O monitoramento e análise crítica é etapa essencial da gestão de riscos e tem por finalidade: (a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes; (b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos; (c) analisar eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles; e (d) assegurar que os controles sejam eficazes e eficientes no projeto e na operação (ABNT, 2009).

  Nessa etapa, é comum realizar o acompanhamento dos planos de ação relacionados às recomendações de melhoria nos processos identificadas pela auditoria interna. Os planos de ação referem-se a **ações definidas por gestores**, visando melhorar processos, minimizar riscos ou solucionar problemas identificados nos processos.

- A área de Controles Internos e Riscos recomenda que os planos sigam a metodologia 5W2H, que é uma ferramenta eficaz para planejar ações de forma clara e estruturada. Além disso, a área de Controles Internos e Riscos realiza o acompanhamento das ações corretivas propostas nos planos de ação, garantindo o cumprimento dos prazos que acontece de acordo com a criticidade dos riscos. Assim, apontamentos com maior criticidade precisam ser sanados com maior tempestividade. As comunicações acontecem por e-mail tanto para validação e aceite do plano de ação, quanto para acompanhamento da sua execução e solicitação de evidências de seu cumprimento, para este é realizada a reavaliação e testes de efetividade para verificar se as ações implementadas corrigiram os problemas.

5W2H	Pergunta Norteadora	Descrição e Orientações
WHAT	O que será feito?	Informar qual será o plano de ação executado para mitigar o problema levantado no apontamento de auditoria.
WHY	Por que será feito?	Esta pergunta terá uma resposta padrão já preenchida na base: Aprimoramento dos processos conforme sugestão da Auditoria Interna e Controles Internos e Riscos do Grupo Wiz Co.
WHERE	Onde será feito?	Informar se o plano de ação será executado em algum sistema, base e etc. Informar em quais locais, departamentos e/ou áreas esse plano de ação será executado.
WHEN	Quando será feito?	Informar quando o plano de ação será concluído. É importante se atentar para o prazo máximo de conclusão do Plano de Ação informado na Tabela de Prazos.
WHO	Por quem será feito?	Informar quem será o responsável por colocar o plano de ação em prática. Se possível, informar primeiro o time responsável e posteriormente o nome do gestor.
HOW	Como será feito?	Informar como o plano de ação será colocado em prática. Quais ferramentas serão utilizadas? Quais atividades serão necessárias?
HOW MUCH	Quanto vai custar?	Informar se o plano de ação envolverá a necessidade de gastos e se esses gastos estão em orçamento.

Figura 4: Tabela de Orientação de Preenchimento do Plano de Ação

- **Comunicação:** Informe periódico sobre os riscos identificados, mitigados e aceitos.

  - Processo de Escalonamento de Riscos: Identificação do risco pela área > Reporte ao gestor imediato > Submissão ao Comitê de Auditoria, se necessário > Submissão à alta administração.

8. Aprovação e Vigência

Aprovação

Este Manual tem sua aprovação pelo *Chief Audit Executive* (CAE), tendo sua aplicação monitorada pelo Comitê de Auditoria, sendo a área de Controles Internos e Riscos a unidade responsável pela elaboração e avaliação da eficácia dos controles e gestão de riscos.

Vigência e Versão do Documento

Este Manual terá vigência de 02 anos a contar da data de sua publicação, podendo ser revisto a qualquer momento diante de mudanças relevantes na estratégia do negócio, mudanças nas exigências regulatórias, novos cenários ou direcionamentos do Grupo Wiz Co.

Versão	Data	Histórico
01	15 de julho de 2025	Elaboração do Documento.

9. Considerações Finais

O fortalecimento dos controles internos e da gestão de riscos é um compromisso contínuo das organizações que buscam eficiência, conformidade e mitigação de riscos. A adoção de boas práticas, aliada à implementação de metodologias eficazes, assegura não apenas a proteção dos ativos e a conformidade regulatória, mas também contribui para a tomada de decisões estratégicas baseadas em informações confiáveis.

Para garantir a eficácia do sistema de controles internos, é essencial que haja um envolvimento ativo de todas as áreas e unidades de negócios do Grupo Wiz Co, com treinamentos regulares, revisões periódicas e um ambiente de controle fortalecido pela cultura organizacional.

Este manual foi elaborado para fornecer diretrizes claras e práticas sobre os princípios, dos controles internos e gerenciamento de riscos. Seu objetivo é assegurar que todos os envolvidos no processo de controles e gestão de riscos compreendam suas responsabilidades e reconheçam a importância de aderir às políticas e procedimentos estabelecidos.

Por fim, este manual deve ser utilizado como um guia prático e atualizado constantemente para refletir as melhores práticas e a evolução do ambiente de negócios. O compromisso com a integridade, transparência e melhoria contínua dos controles internos fortalece a governança corporativa e contribui para o sucesso sustentável da organização.

Marcus Vinícius
CAE

Matrizes

Brasília
SCN Qd. 02, Liberty Mall, Torre B
13º andar, sala 1.301
Brasília - DF / CEP: 70.712-904

São Paulo
Rua Olimpíadas, 66, 12º andar
Edifício Capital Center
São Paulo - SP / CEP: 04551-000

Curitiba
Avenida João Gualberto, 1259
Edifício Laís Peretti, 15º, Alto da Glória
Curitiba – PR / CEP: 80030-001

www.wiz.co