GRUPO MERCANTIL

Política do Sistema de Controles Internos

Vigência a partir de

02/09/2024

Validade

01/10/2025

Versão

02

Divulgação EXTERNA

Sumário

1. APRESENTAÇÃO

A Política Institucional do Sistema de Controles Internos do Grupo Mercantil é aplicável a todos que estão indicados no item "Abrangência" deste documento e objetiva formalizar, padronizar, aculturar, facilitar e incentivar a adoção de controles internos adequados aos processos e sistemas inerentes às operações realizadas pela Instituição. Dessa maneira, este documento norteia os princípios, conceitos, papéis, responsabilidades e procedimentos relacionados ao tema.

O Sistema de Controles Internos visa proporcionar segurança razoável na realização dos processos da Instituição a partir da implementação de controles internos adequados, com respeito à realização dos objetivos relacionados a desempenho, informação e conformidade. Neste contexto, a conscientização de todos os níveis da organização quanto ao nível de risco presente em suas atividades é importante para melhorar a tomada de decisões sobre governança, estratégia, definição de objetivos e operações cotidianas, incluindo a avaliação sobre a eficácia e eficiência nas operações – considerando as análises, formalizações e alcance dos objetivos corporativos e operacionais - a confiabilidade e integridade das informações/ demonstrações financeiras e o cumprimento de leis e regulamentos internos e externos.

A composição do Sistema de Controles Internos visa a integração entre diversas esferas da Instituição podendo ser demonstrada conforme diagrama a seguir:

Um adequado e eficiente Sistema de Controles Internos contribui para o Grupo Mercantil alcançar objetivos estratégicos e a sustentar e melhorar o seu desempenho.

2. BASE LEGAL

Tipo	Número/Ano	Objetivo
Resolução CMN	4.968/2021 (alterada pela Resolução CMN 5.117/2024	Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Tipo	Número/Ano	Objetivo
Resolução CVM	35/2021 (alterada pelas resoluções 134/2022 e 179/2023)	Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.
Resolução CVM	21/2021 (alterada pelas resoluções 162/20222, 167,2022, e 179/2023)	Dispõe sobre o exercício profissional de administração de carteiras de valores mobiliários e revoga a Instrução CVM nº 426, de 28 de dezembro de 2005, a Instrução CVM nº 557, de 27 de janeiro de 2015, a Instrução CVM nº 558, de 26 de março de 2015, a Instrução CVM nº 597, de 26 de abril de 2018, a Deliberação CVM nº 51, de 25 de junho de 1987, a Deliberação CVM nº 740, de 11 de novembro de 2015 e a Deliberação CVM nº 764, de 4 de abril de 2017.
Resolução CMN	4.557/2017 (alterada pelas resoluções 4.745/2019, 4.926/2021, 4.943/2021, 5.049/2022, 5.076/2023, 5.077/2023 e 55/089/2023)	Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.
Circular Bacen	3.978/2020 (alterada pela circular 4.005/2020, e pelas resoluções 119/2021, 282/2022 e 344/2023)	Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.
Resolução CVM	161/2022 (alterada pela resolução 173/2022)	Dispõe sobre o registro de coordenadores de ofertas públicas de distribuição de valores mobiliários e sobre as regras, procedimentos e controles internos a serem

Tipo	Número/Ano	Objetivo
		observados na intermediação de tais ofertas.

As bases legais listadas acima possuem como foco o Sistema de Controles Internos e norteiam seus trabalhos. Contudo a atividade de controles internos se referência em todos os normativos que regem as atividades da Instituição nos diversos processos e/ou áreas de negócio do Grupo.

3. ABRANGÊNCIA

Esta Política se aplica ao Banco Mercantil e às empresas do Grupo Mercantil. A ciência e o cumprimento das diretrizes e regras aqui estabelecidas são obrigatórios a todos os seus colaboradores e terceiros.

4. GLOSSÁRIO DE TERMOS E SIGLAS

- COSO – Comitê das Organizações Patrocinadoras da Comissão Treadway (*Committee of Sponsoring Organizations of the Treadway Commission*);
- CRO – Diretor de Risco (*Chief Risk Officer*);
- RAS – Declaração de Apetite a Riscos (*Risk Appetite Statement*);
- ELC – Controles a Nível de Entidade (*Entity Level Controls*);
- CVM – Comissão de Valores Mobiliários;
- RCSA – Questionário de auto avaliação de riscos e controles (*Risk and Control Self-Assessment*);
- ICR – Indicador Chave de Risco;
- OKR – Objetivos e Resultados-Chave (*Objectives and Key Results*);
- LGPD – Lei Geral de Proteção de Dados.

5. ESTRUTURA DE GESTÃO DO SISTEMA DE CONTROLES INTERNOS

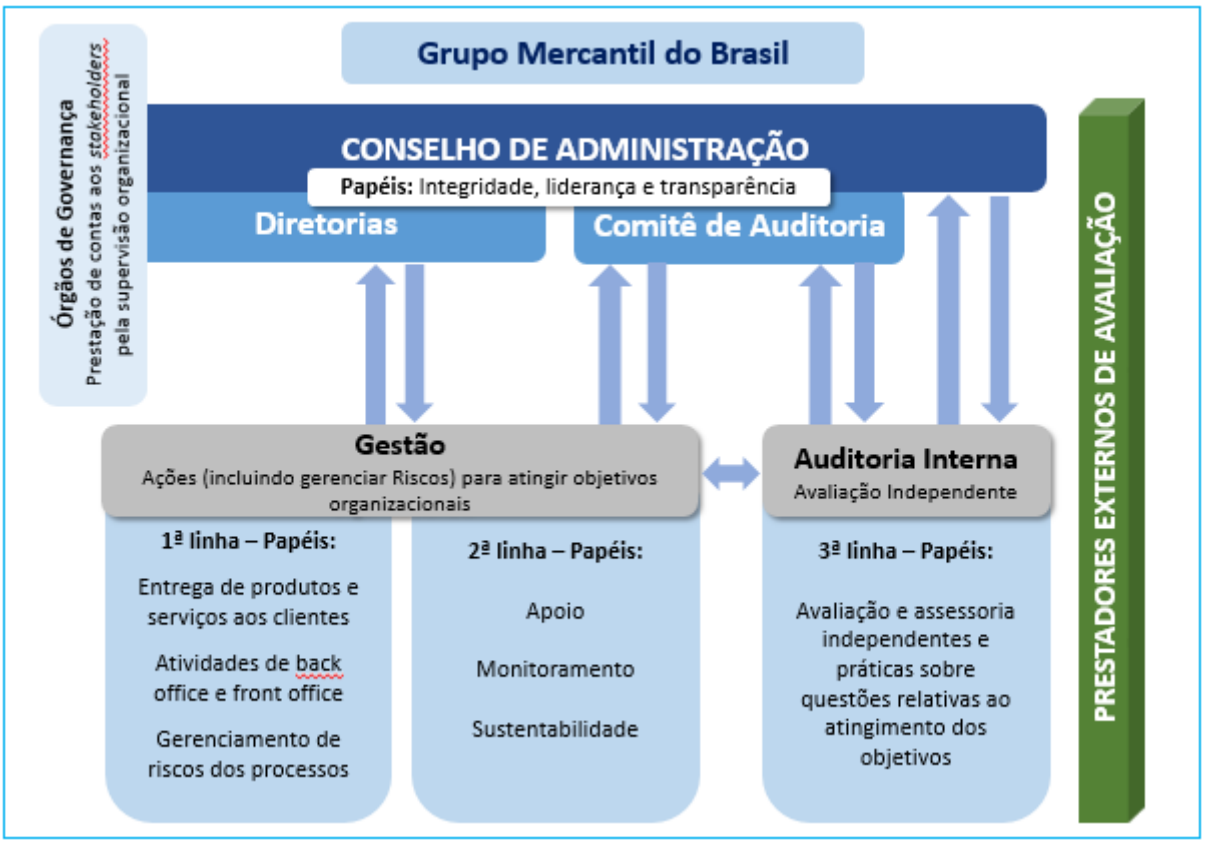
A Estrutura de Gestão do Sistema de Controles Internos do Grupo Mercantil está constituída em uma unidade única, centralizada na Gerência de Risco Operacional e Controles Internos, subordinada à Diretoria de Riscos e Compliance (CRO – *Chief Risk Officer*) e abrange todas as empresas do Grupo Mercantil.

O gerenciamento centralizado do Sistema de Controles Internos resulta em maior agilidade e assertividade na tomada de decisões e visa envolver todos os colaboradores e garantir a efetividade da gestão integrada dos controles internos. Dessa forma, todos os colaboradores devem atuar em prol de um ambiente operacional e de negócios mais seguro e aderente aos valores e objetivos do Grupo Mercantil.

6. GESTÃO DO SISTEMA DE CONTROLES INTERNOS

O Sistema de Controles Internos atua identificando oportunidades e propondo a adoção de atividades e procedimentos de controles que visam adaptar os ambientes operacionais e corporativos às constantes mudanças, mitigar riscos que estejam fora do apetite estabelecido pela Alta Administração - traduzido por meio da Declaração de Apetite a Riscos (RAS) – e apoiar um sólido processo de tomada de decisões e de governança da organização.

Aplicando-se o modelo das Três Linhas, representado no diagrama a seguir, o Grupo Mercantil visa minimizar o risco de erros e sua exposição a vulnerabilidades.



A **primeira linha** é constituída pelos gestores e áreas técnicas responsáveis pela entrega de produtos e serviços aos clientes e pela operacionalização dos processos, atuando de forma constante no monitoramento e proposição de controles adequados para gestão de seus próprios riscos.

As funções da **segunda linha** são executadas de forma coesa e coordenada pelas áreas de gerenciamento de riscos, conformidade, controles internos e segurança da informação que, juntamente a Comitês especialistas, atuam na gestão dos riscos, da conformidade e de controles da Instituição, permitindo o acompanhamento e avaliação das atividades, testes de desenho de controles, além de recomendações necessárias à primeira linha.

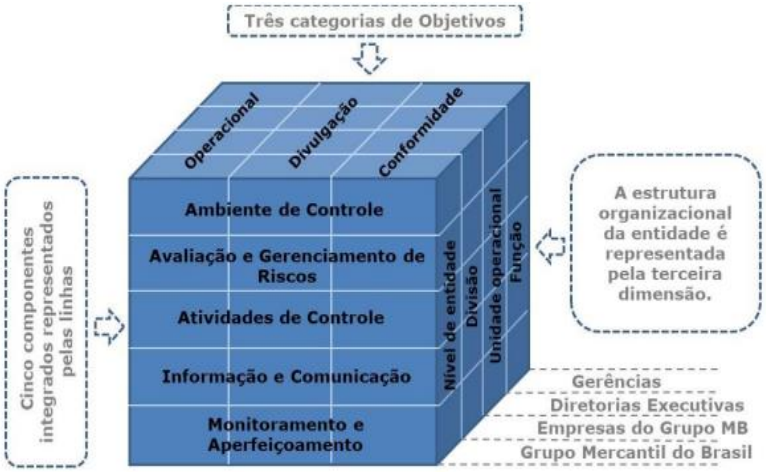
Já a **terceira linha**, constituída pela Auditoria Interna, atua de forma independente provendo avaliações sobre a adequação e a eficácia dos controles internos para mitigação dos riscos associados e sobre o ambiente de governança corporativa, realizando testes de controles e/ou testes substantivos a fim de garantir a efetividade da atuação das demais linhas no alcance dos seus objetivos.

De forma complementar, os prestadores externos de avaliação (auditorias externas e órgãos reguladores) desempenham um papel importante na estrutura geral de governança e controle, na medida em que prestam avaliações adicionais às partes interessadas da organização com a intenção de fortalecer processos e controles ou, ainda, de auxiliar no cumprimento de demandas regulatórias.

O Sistema de Controles Internos do Grupo Mercantil atua de forma a mitigar as exposições a riscos a partir da definição de controles consistentes e adequados de acordo com a natureza, complexidade e perfil de riscos da Instituição, favorecendo o processo de governança corporativa ao permitir tomadas de decisão com base em informações mais seguras e fidedignas.
Um efetivo sistema de controles internos sustenta a adaptação às mudanças geradas pelo ambiente externo, reduz a probabilidade de erros humanos e irregularidades em processos e sistemas, resulta na diminuição das perdas e falhas e fortalece os processos e procedimentos que refletem o modelo de governança adotado pelo Grupo Mercantil.

7. METODOLOGIA APLICADA

Baseado nos direcionamentos e orientações do COSO, o framework para gestão do Sistema de Controles Internos consiste no estabelecimento de um processo contínuo, constituído de cinco componentes inter-relacionados, os quais são traduzidos em princípios que baseiam o sistema:



Fonte: *Adaptado de Controles Internos – Estrutura Integrada (COSO, 2013).*

Componentes	Princípios
Ambiente de Controle	**1**. A organização demonstra ter comprometimento com a integridade e os valores éticos; **2.** A estrutura de governança demonstra independência em relação aos seus executivos e supervisiona o desenvolvimento e o desempenho do controle interno; **3**. A administração estabelece, com a definição da estrutura de governança, as estruturas, os níveis de subordinação e as autoridades e responsabilidades adequadas na busca dos objetivos; **4.** A organização demonstra comprometimento para atrair, desenvolver e reter talentos competentes, em linha com seus objetivos; **5**. A organização faz com que as pessoas assumam responsabilidade por suas funções de controle interno na busca pelos objetivos.

Avaliação e Gerenciamento de Riscos	**6**. A organização especifica os objetivos com clareza suficiente, a fim de permitir a identificação e a avaliação dos riscos associados aos objetivos; **7**. A organização identifica os riscos à realização de seus objetivos por toda a entidade e analisa os riscos como uma base para determinar a forma como devem ser gerenciados; **8**. A organização considera o potencial para fraude na avaliação dos riscos à realização dos objetivos; **9**. A organização identifica e avalia as mudanças que poderiam afetar, de forma significativa, o sistema de controle interno.
Atividades de Controles	**10**. A organização seleciona e desenvolve atividades de controle que contribuem para a redução, a níveis aceitáveis, dos riscos à realização dos objetivos; **11**. A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar a realização dos objetivos; **12**. A organização estabelece atividades de controle por meio de políticas que estabelecem o que é esperado e os procedimentos que colocam em prática essas políticas.
Informação e Comunicação	**13**. A organização obtém ou gera e utiliza informações significativas e de qualidade para apoiar o funcionamento do controle interno; **14**. A organização transmite internamente as informações necessárias para apoiar o funcionamento do controle interno, inclusive os objetivos e responsabilidades pelo controle; **15**. A organização comunica-se com os públicos externos sobre assuntos que afetam o funcionamento do controle interno.
Monitoramento e Aperfeiçoamento	**16**. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou independentes para se certificar da presença e do funcionamento dos componentes do controle interno; **17**. A organização avalia e comunica deficiências no controle interno em tempo hábil aos responsáveis por tomar ações corretivas, inclusive a estrutura de governança e alta administração, conforme aplicável.

Essa estrutura estabelece os requisitos para um sistema eficaz de controles internos, o qual reduz, a um nível aceitável, o risco de não se atingir os objetivos corporativos. O sistema de controles internos é considerado eficaz quando não há deficiências relevantes referentes ao funcionamento de um componente ou princípio.

A Resolução CMN n° 4.968/21 regulamenta, pois, os componentes do COSO, reafirmando a adequação da metodologia aplicada na Instituição, o que pode ser verificado no quadro a seguir, o qual apresenta a relação entre os componentes do COSO e da regulamentação vigente.

Componentes COSO	Aspectos Resolução 4.968
Ambiente de Controle	Cultura de Controle
Avaliação de Riscos	Identificação e Avaliação de Riscos
Atividades de Controle	Atividades de Controle e Segregação de Funções
Informação e Comunicação	Informação e Comunicação
Monitoramento e Aperfeiçoamento	Monitoramento

7.1. Cultura de Controle

Por cultura de controle entende-se o conjunto de normas, processos e estruturas que fundamentam o Sistema de Controles Internos por toda a Instituição, permeando todas as áreas e atividades executadas.

Neste contexto é importante ressaltar os princípios e valores éticos que norteiam a atuação daqueles que representam a Instituição, devendo estar alinhados ao **Propósito e Jeito M+ de Ser**. Além disso, o Grupo Mercantil conta com uma **estrutura de governança** onde são estabelecidos Comitês Estatutários e de Assessoria que suportam a Alta Administração em um processo adequado de tomada de decisões, bem como a responsabilização dos colaboradores nos sistemas de controle internos.

Ressaltam-se os **treinamentos e comunicações internas** que buscam a capacitação e alinhamento das equipes, resultando na adoção de controles adequados às operações e processos realizados.

O Grupo Mercantil conta ainda com um **Programa de Integridade,** que avalia e mitiga riscos de não conformidade, além de um robusto sistema de **Avaliação de Desempenho**, que monitora os resultados e o cumprimento dos objetivos estratégicos da Instituição, que conta com ferramentas de monitoramento e um sistema de indicadores (OKRs e KPIs) vinculados a programas de remuneração variável, o que garante um sistema meritocrático direcionado pela estratégia corporativa.

Todo esse ambiente está embasado em um processo de comunicação adequado e tempestivo em todos os níveis, por meio de comunicação interna, normatização de políticas e procedimentos, reportes, dentre outros.

7.2. Identificação e Avaliação de Riscos

Trata-se do processo dinâmico e interativo que visa identificar e avaliar exposições a riscos que afetem negativamente a busca pelos objetivos estratégicos do Grupo Mercantil, objetivando a mitigação dos riscos que estejam fora do apetite tolerado pela Instituição.

Dessa forma, o Sistema de Controles Internos deve estar bastante alinhado à gestão de riscos, formando uma estrutura sólida para garantir maior eficácia dos processos e operações realizados.

Destaca-se que o gerenciamento de riscos deve ser pautado no cumprimento das normas externas, das Políticas de Riscos, da Declaração de Apetite a Riscos (RAS) e das melhores práticas de mercado.

Trata-se de um processo contínuo que avalia tanto fatores internos como externos. Nesse sentido, ressalta-se a gestão da continuidade de negócios, a análise prévia de riscos envolvidos em novos produtos e serviços (risk by design), o monitoramento da base de perdas operacionais e suas causas raízes, o resultado dos mapeamentos de riscos e controles internos, e os testes de desenho e efetividade dos controles, objetivando mitigar o risco e garantir a integridade das operações junto aos clientes e a Instituição.

7.3. Atividades de Controle e Segregação de Funções

Refere-se a ações estabelecidas de forma tempestiva e adequada por meio de políticas e procedimentos que visam prevenir ou administrar os riscos inerentes, a fim de garantir o cumprimento dos objetivos estratégicos. É parte da atividade do gerenciamento dos riscos identificar as atividades de controles existentes nos processos mais relevantes para a instituição, classificando-os de acordo com as suas características, forma e frequência de execução, já que a formatação do controle define o nível de eficácia e consequente contribuição para a mitigação do risco a ele vinculado; além da avaliação dos resultados dos testes realizados.

A **Segregação de Funções** é geralmente inserida na seleção e no desenvolvimento das atividades de controles. No Grupo Mercantil, é estabelecida e formalizada em estrutura organizacional e tem importante papel de evitar conflitos de interesses e garantir a integridade das operações. É realizada pela atribuição adequada de papéis e responsabilidades, habilitada sobre os direitos e restrições de acesso ao sistema, e apoiada por controles de tecnologia da informação (CGTI). Compreende-se por:

- **Designação de autoridade e responsabilidade**: o estabelecimento e normatização por meio de políticas as quais definem os poderes e responsabilidades para o alcance dos objetivos da Instituição. O Conselho de Administração é o órgão máximo, responsável pela definição das diretrizes estratégicas e a aprovação do apetite ao risco. Há também a estrutura de governança baseada em decisões colegiadas, em que comitês de alto nível, estatutários e de assessoria, cumprem esse papel. Concomitantemente, para todos os cargos são definidos os pré-requisitos para sua ocupação, como nível de escolaridade, cursos técnicos, idiomas, tempo de experiência, conhecimentos específicos, além da descrição das atividades e as respectivas responsabilidades;

- **Direitos de acesso (físico e lógico):** define, através de políticas e procedimentos, as atividades de controles relacionadas à concessão e revogação dos acessos a rede, sistemas e banco de dados, além da segurança física dos ativos do grupo. A Política Institucional de Segurança da Informação tem o objetivo de preservar a integridade, a confidencialidade e a disponibilidade das informações e dos dados de propriedade do Grupo Mercantil. Todos os funcionários, parceiros de negócio e terceiros prestadores de serviços devem ficar cientes da sua responsabilidade pessoal no cumprimento rigoroso da conduta considerada adequada, conforme prescrito nos Manuais de Procedimentos vinculados à referida Política;

- **Controles Gerais de Tecnologia da Informação (CGTI):** responsáveis por estabelecer e preservar a integridade contínua dos processos e controles automatizados ou daqueles dependentes de componentes tecnológicos, assim como dos direitos de acesso aos sistemas. As restrições de acesso aos sistemas definidas nos processos de negócios são monitoradas pela Diretoria de Tecnologia, e são continuamente avaliadas pela 2ª e 3ª linhas, as quais verificam através de testes: (i) a existência de conflitos de acessos relacionados aos principais processos da Instituição, bem como a resposta a

esses conflitos; (ii) os processos para concessão ou revogação dos acessos de colaboradores; (iii) a existência de acessos conflitantes associados às principais funções de TI, com relação direta em atividades de administração nas diferentes plataformas e camadas, bem como, acesso a modificar e atualizar dados e programas considerados críticos.

7.4. Informação e Comunicação

O acesso a informações confiáveis, íntegras e tempestivas é vital para que o Sistema de Controles Internos seja adequado e eficaz aos seus objetivos. Este componente refere-se ao processo contínuo e interativo de obter, proporcionar e compartilhar as informações necessárias tanto internamente quanto externamente. Consiste na identificação, armazenamento e comunicação de informações relevantes, a fim de permitir a realização dos processos de acordo com as normas estabelecidas no Grupo Mercantil. Além de bases internas para divulgação de normas, comunicados, treinamentos, dentre outros, a Instituição conta com vários canais de atendimento e disponibilização de informações a clientes e investidores, tais como o site institucional e redes sociais.

7.5. Monitoramento

Realiza-se avaliações contínuas, por órgãos internos e externos, com o propósito de certificar a Instituição da presença e do funcionamento efetivo dos componentes de controles internos. Este monitoramento é realizado por meio de ferramentas que auxiliam na identificação de vulnerabilidades, podendo citar o questionário de auto avaliação de riscos - RCSA, o acompanhamento da base de perdas operacionais internas, a segurança da informação no ambiente tecnológico, testes sobre o desenho e a efetividade dos controles, monitoramento de incidentes, indicadores chaves de risco (ICRs), o acompanhamento dos OKR's estabelecidos pela Instituição, dentre outros.

Caso sejam identificadas vulnerabilidades em processos ou sistemas, recomendações são realizadas para o aperfeiçoamento da gestão no Grupo Mercantil, buscando-se o apoio da estrutura de governança corporativa para aquilo que é mais crítico à Instituição.

Como resultado do monitoramento do Sistema de Controles Internos são elaborados relatórios, emitidos conforme legislações vigentes e aprovados pela Alta Administração ou submetidos aos órgãos supervisores, quando requerido.

8. GERENCIAMENTO DO SISTEMA DE CONTROLES INTERNOS

O Sistema de Controles Internos é gerido por meio do desdobramento dos componentes do COSO em processos integrados que permeiam toda a organização e contribuem para o alcance dos objetivos estratégicos conforme descrito no tópico anterior "Metodologia Aplicada". No Grupo Mercantil, o Sistema contempla diversas ferramentas e processos, com destaque para os procedimentos de gestão formalizados internamente através da identificação, classificação e avaliação dos controles internos.

Este fluxo se dá através do mapeamento dos processos, que constitui em uma atividade que busca o adequado padrão de governança, ao formalizar os procedimentos necessários à consecução dos objetivos estratégicos com eficiência, eficácia e em conformidade com as regulamentações externas e internas aplicáveis. O mapeamento contribui para a identificação dos riscos potenciais inerentes às atividades executadas, bem como para com a avaliação qualitativa do ambiente de controles internos para mitigar esses riscos e para mensurar o nível de exposição residual dos riscos (após as ações de mitigação dos controles). Portanto, o

mapeamento permite uma análise e avaliação, com maior granularidade, das exposições a riscos e da qualidade dos controles internos. Este processo é composto pelas seguintes etapas:

- Levantamento dos processos críticos – compreende o entendimento de ponta a ponta (*end to end*) destes processos;
- Identificação dos riscos e categorização;
- Identificação e classificação de controles;
- Teste de desenho do controle: validação se o controle é suficientemente preciso para detectar o evento de risco antes de sua materialização, ou para detectar a não conformidade a ser solucionada. Avalia ainda, se o controle está projetado e operando de maneira adequada;
- Teste de efetividade do controle: validação se o controle está evitando ou detectando o evento de risco dentro de um determinado período de tempo conforme esperado em sua modelagem;
- Classificação das deficiências de controles: pode ser identificado um gap ou deficiência nas seguintes hipóteses: (i) quando não é identificado um controle atuando na mitigação do risco; (ii) quando o controle não possui os elementos necessários ou não é adequado para mitigar o risco; ou (iii) quando o controle é adequado mas há oportunidade de aprimoramento;
- Avaliação dos riscos com base na probabilidade e a consequência em caso de ocorrência e, considerando o resultado da qualidade dos controles de acordo com os testes executados;
- Elaboração da matriz de riscos residuais;
- Mitigação dos riscos por meio de planos de ação;
- Assunção de riscos, para os quais não haverá mitigação, aprovada pelo Comitê de Compliance, Controles Internos e Perdas Operacionais;
- Monitoramento dos riscos assumidos e das deficiências de controles em fase de remediação;
- Reavaliação dos processos, riscos e controles internos, reiniciando-se o ciclo.

Este processo se integra à gestão do risco operacional, formalizada na **Política Institucional de Risco Operacional**, cuja estratégia adotada é de não aceitar os riscos residuais, identificados após a avaliação da eficácia dos controles, classificados como "Alto" e "Muito Alto", visando manter a Instituição dentro dos limites de exposição pré-estabelecidos. Para estes, define-se planos de ação para mitigação dos riscos.

8.1. Classificação dos Controles

Com relação aos controles internos, a Instituição realiza tratamento por meio de classificação conforme a seguir:

Itens	Características
Tipologia	• Controles preventivos; • Controles detectivos; • Controles corretivos; • Controles no nível da entidade ou diretivos (ELCs).
Frequência	• Múltiplas vezes ao dia; • Diária; • Semanal; • Quinzenal; • Mensal; • Trimestral; • Semestral; • Anual; e • A cada transação/ação ou sob demanda (casos em que o controle seja de frequência esporádica ou por solicitação).
Natureza dos controles e tipo de evidências	• Controles manuais; • Controles sistêmicos (automáticos); • Controles híbridos (manuais dependentes de TI ou semiautomáticos)
Relevância	• Controle chave para mitigação do risco; • Controle não chave – não mitiga adequadamente o risco.

Ainda sobre controles, as vulnerabilidades são relatadas tempestivamente e as ações corretivas são planejadas e priorizadas de acordo com a relevância de cada item. O Comitê de Compliance, Controles Internos e Gestão de Perdas acompanha periodicamente as ações que possuem maior grau de impacto para a Instituição, de acordo com metodologia definida incluindo a priorização de planos de ação para mitigação de perdas operacionais. Maior detalhamento da metodologia está formalizada em procedimento interno específico.

8.2. Outros macroprocessos relevantes para o Sistema de Controles Internos

O Grupo Mercantil monitora continuamente os riscos e controles internos existentes, bem como desenvolve atividades de controles, especialmente no que se refere a **Tecnologia** e todo o ambiente de TI, incluindo infraestrutura, ambiente de dados e segurança cyber.

Destaca-se o processo denominado **"Grandes Mudanças de TI",** relativas a modificações no ambiente de TI da Instituição que interferem não somente em sistemas, mas principalmente em infraestrutura, envolvendo várias áreas de TI, e podendo impactar no atendimento ao cliente, sendo geralmente projetos de maior custo e complexidade. As áreas de Risco Operacional e Controles Internos e de Auditoria Interna são envolvidas a fim de identificar e qualificar riscos e controles envolvidos, acompanhar os testes realizados pela TI e requerer a mitigação dos riscos, bem como formalizar todo processo em base específica a fim de garantir a atuação integrada entre as áreas. Esse processo visa garantir que a mudança tenha o menor impacto possível para clientes, colaboradores e demais usuários.

Ainda nesse contexto, o Grupo Mercantil identifica, analisa e gerencia os **riscos de fraude**, sejam externas sejam internas, contando com estrutura dedicada às atividades de gestão. Diversas medidas preventivas antifraude são adotadas visando mitigar o risco e garantir a integridade das operações junto aos clientes e a Instituição. Além do risco de fraude, o Mercantil, por meio do Gerenciamento Integrado de Riscos e Capital, monitora toda e qualquer exposição a **riscos financeiros ou não-financeiros**, sejam relativas as situações de não conformidades,

conflito de interesses, imagem, conduta, lavagem de dinheiro, privacidade, além da responsabilidade social, ambiental e climática.

A **Auditoria Interna** realiza, de forma independente, exames nos diversos processos, inclusive nos relativos à gestão de riscos. O trabalho é contínuo e alinhado às diretrizes estratégicas, sendo conduzido com a aplicação técnica dos princípios que regulam a atividade de auditoria, quanto a adequada evidenciação, documentação, divulgação e acompanhamento das constatações e recomendações observadas.

Salienta-se ainda, o processo de **análise prévia dos riscos** envolvidos e controles a serem adotados quando do desenvolvimento de novos produtos e serviços, revisões ou alterações significativas (*risk by design*). Nesse processo, o gestor responsável apresenta as características do produto ou serviço para discussão e avaliação sob a ótica das áreas de riscos, Controles Internos, Ouvidoria, Jurídico, Conduta, Canais de Atendimento Eletrônico, LGPD, *Compliance*, Prevenção a Lavagem de Dinheiro, Controladoria, Prevenção a Fraude, Excelência Comercial e Experiência do Cliente, Segurança Cibernética e da Informação. Como resultado, podem ser solicitados ajustes e desenvolvimento de controles que busquem a viabilização dos negócios mediante a mitigação dos riscos envolvidos.

9. REPORTES

O **Relatório do Sistema de Controles Internos**, divulgado semestralmente. Destaca-se que no relatório emitido no primeiro semestre de cada ano, contempla aspectos da avaliação da qualidade e adequação dos controles internos da Instituição, incluindo reportes específicos referentes à Mercantil do Brasil Corretora, em atendimento às Resolução CVM nº. 35/2021 e Resolução CVM no. 21/2021. No segundo semestre, publica-se uma versão mais robusta desse documento, contemplando a visão sobre as características do Sistema de Controles Internos no Grupo Mercantil, sobre os riscos e controles no ambiente interno, testes de controles executados durante o ano, posicionamento dos planos de ação monitorados e definidos para sanar deficiências identificadas por diversos instrumentos e a remediações de controles e/ou GAP implementadas.

Além disso, destaca-se os relatórios regulamentares emitidos periodicamente conforme prevê as legislações vigentes citadas no item "Base Legal" desta política, não se limitando apenas as citadas, visto o cenário em constante alterações.

Os reportes objetivam posicionar a Alta Administração e gestores sobre a evolução da gestão do Sistema de Controles Internos na Instituição, bem como apresentar uma visão executiva e consolidada das conclusões das avaliações efetuadas. Neles estão contidas informações sobre os planos de ação originados de recomendações geradas por diversas fontes, tais como: Questionário RCSA, Risco Operacional, Auditorias Interna e Externa e Órgãos Supervisores. Ressalta-se que todas essas ações são classificadas por relevância, grau de vulnerabilidade e impacto ao negócio, sendo que as consideradas mais relevantes são foco de discussão do Comitê de *Compliance* e Controles Internos.

10. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades atinentes a esta Política estão distribuídos entre as alçadas abaixo indicadas:

- Conselho de Administração
- Comitê de Auditoria
- CEO, Vice-Presidências e Diretorias

- Comitê de *Compliance,* Controles Internos e Gestão de Perdas
- Diretoria de Riscos e *Compliance*
- Gerência de Risco Operacional e Controles Internos
- Gerência Executiva de Auditoria Interna
- Vice-Presidência de Produtos, Tecnologia e Serviços
- Demais Áreas
- Terceiros
  - Cumprir as diretrizes e cláusulas contratuais acordadas entre as partes, incluindo controle de qualidade na prestação do serviço;
  - Assegurar a adequada capacitação dos prestadores de serviços sobre os processos executados e manter as certificações obrigatórias;
  - Comunicar a área responsável pelo terceiro qualquer tipo de incidente que possa ocasionar problemas na prestação de serviços.

11. CONSIDERAÇÕES FINAIS

Esta Política deve ser objeto de avaliação mínima anual, com o intuito de que seja continuamente aprimorada e de que esteja sempre atualizada.

Este documento entra em vigor a partir de sua publicação, ficando à disposição dos órgãos de fiscalização e supervisão.

GRUPO MERCANTIL