Política de Gerenciamento de Risco Operacional

Abril de 2025

Elaboração: Risco

Aprovação: Diretoria Executiva

Classificação do Documento: Público

ÍNDICE

1. INTRODUÇÃO

O gerenciamento de risco operacional no Conglomerado Prudencial Genial ("Conglomerado Genial") tem como objetivo identificar, avaliar e administrar riscos decorrentes de incertezas, integrando-se ao processo de criação e preservação de valor nas instituições que o compõem. Este processo é conduzido pela Diretoria Executiva e pelos demais colaboradores, sendo aplicado na definição de estratégias compatíveis com o apetite a risco estabelecido, proporcionando um alto nível de segurança quanto ao alcance dos objetivos organizacionais.

2. OBJETIVO

Esta política tem como objetivo estabelecer os princípios e diretrizes para o gerenciamento do risco operacional no Conglomerado Prudencial em conformidade com a Resolução CMN nº 4.557, de 23 de fevereiro de 2017.

3. ABRANGÊNCIA

As diretrizes estabelecidas nesta Política aplicam-se a:

i. Todas as empresas e instituições integrantes do Conglomerado Genial, incluindo suas controladas diretas e indiretas;
ii. Todos os colaboradores, independentemente do nível hierárquico ou função desempenhada; e
iii. Todos os Prestadores de serviços terceirizados e seus respectivos profissionais, sempre que atuarem em nome ou em benefício das entidades que compõem o Conglomerado Genial.

O cumprimento desta Política é obrigatório e visa garantir a uniformidade e a eficácia na gestão do risco operacional em todas as frentes de atuação da instituição.

4. DEFINIÇÕES

Este documento adota os conceitos estabelecidos na Resolução CMN nº 4.557, de 23 de fevereiro de 2017, e complementa com definições operacionais necessárias à compreensão e aplicação dos procedimentos relacionados ao gerenciamento do risco operacional no Conglomerado Genial.

4.1. Risco Operacional

Nos termos da regulamentação vigente, considera-se risco operacional a possibilidade de ocorrência de perdas resultantes de falhas, deficiências ou inadequações de processos internos,

pessoas, sistemas ou de eventos externos. Estão incluídos nessa definição os riscos legais, decorrentes da inadequação ou deficiência em contratos firmados pela instituição, do descumprimento de dispositivos legais e regulamentares, e de indenizações por danos a terceiros relacionados às atividades da instituição. O risco operacional também pode afetar diretamente a continuidade dos negócios, a reputação da instituição, sua exposição a sanções regulatórias e seus resultados financeiros.

4.2. Evento de Risco Operacional

Define-se como evento de risco operacional o incidente relativo à materialização de riscos operacionais, com impacto adverso, real ou potencial, sobre a instituição. Os principais eventos incluem:

- Fraudes internas;
- Fraudes externas;
- Demandas trabalhistas e segurança deficiente do local de trabalho;
- Práticas inadequadas relativas a usuários finais, clientes, produtos e serviços;
- Danos a ativos físicos próprios ou em uso pela instituição;
- Interrupções das atividades da instituição ou a descontinuidade da prestação de serviços essenciais;
- Falhas em sistemas, infraestrutura ou processos de tecnologia da informação;
- Erros na execução, falhas no cumprimento de prazos ou no gerenciamento de atividades institucionais.

4.3. Causas de Risco Operacional

As causas de risco operacional correspondem a ações ou circunstâncias que contribuem para a ocorrência de eventos de risco, normalmente relacionadas à deficiência ou ausência de controles efetivos. Para fins de análise e tratamento, as causas podem ser agrupadas nos seguintes fatores de risco:

- Pessoas: Compreende falhas humanas, intencionais ou não que possam resultar em perdas. Inclui a ausência de capacitação técnica, insuficiência de recursos humanos ou condutas inadequadas.
- Processos: Decorre de falhas, interrupções, ausência de controles ou desenho inadequado dos processos operacionais ou de apoio.
- Sistemas: Relaciona-se a falhas tecnológicas, sistemas obsoletos, não aderentes às necessidades do negócio, integrações inadequadas ou alterações não controladas. Envolve ainda falhas de comunicação interna e com terceiros.
- Fatores Externos: Referem-se a eventos alheios ao controle da instituição, como desastres naturais, pandemias, interrupções de serviços públicos ou outros eventos

externos que possam comprometer a operação ou gerar perdas materiais e/ou reputacionais.

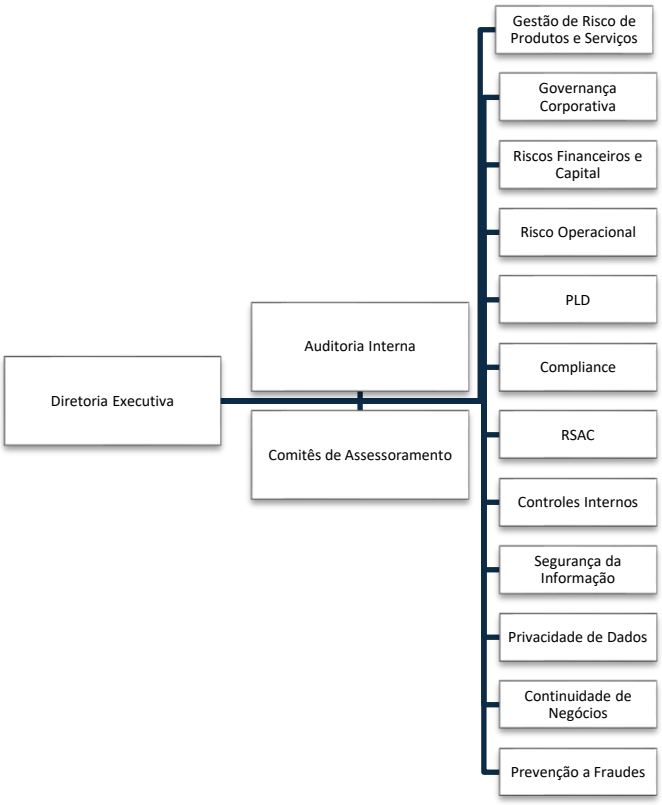
5. ESTRATÉGIA

A estratégia de gerenciamento de risco operacional do Conglomerado Genial é definida pela Diretoria Executiva e fundamenta-se na adoção das melhores práticas de mercado, com foco na prevenção, detecção e mitigação de riscos. Essa estratégia prevê a manutenção de um framework estruturado, robusto e compatível com a natureza, complexidade e relevância das exposições assumidas pelas instituições do Conglomerado.

A finalidade é garantir que o risco operacional – bem como os efeitos agregados de outros riscos relacionados – seja gerido de forma eficaz, contribuindo para a proteção dos processos críticos, o alcance das metas estratégicas e a sustentação da confiança dos clientes, investidores e demais partes interessadas.

6. ESTRUTURA DE GERENCIAMENTO DE RISCO OPERACIONAL

A estrutura de governança de risco do Conglomerado Genial tem como premissa a construção de um ambiente de gestão independente, robusto, integrado e abrangente, em conformidade com a regulamentação vigente e alinhada com as melhores práticas do mercado.
A Instituição adota uma postura prospectiva, buscando garantir que os riscos operacionais e seus efeitos agregados sejam identificados, mensurados, avaliados, monitorados, controlados, mitigados e adequadamente reportados. A responsabilidade pela operacionalização, desenvolvimento, monitoramento e aperfeiçoamento contínuo da estrutura de gerenciamento de riscos é atribuída ao *Chief Risk Officer* (CRO).
O envolvimento da Alta Administração – por meio da Diretoria Executiva e dos Comitês de Assessoramento – é permanente, tanto na condução das atividades diárias quanto no processo decisório, garantindo que a governança permaneça alinhada ao perfil de controle e aos princípios estratégicos definidos pela Administração. A seguir é apresentada a estrutura de riscos, controles e conformidade:



Como fundamento dessa estrutura, o Conglomerado Genial adota o modelo das Três Linhas de Defesa, reconhecido como um método eficaz para aprimorar a comunicação e a atuação no gerenciamento de riscos, por meio da clara definição de papéis e responsabilidades em toda a organização:

1ª LINHA DE DEFESA: Compreende os gestores e colaboradores responsáveis diretamente pelas atividades operacionais. Cabe a essa linha gerenciar os riscos inerentes às suas funções, identificando, avaliando, controlando e mitigando riscos em suas rotinas diárias, além de sugerir e, quando aplicável, implementar ações corretivas para sanar deficiências de controle. A atuação se dá por meio de uma estrutura hierárquica de responsabilidades, na qual os gestores devem estabelecer e supervisionar procedimentos de controle alinhados às metas e diretrizes institucionais.

2ª LINHA DE DEFESA: Constituída por funções específicas de gerenciamento de riscos e conformidade, estabelecidas pela Diretoria Executiva, com o objetivo de dar suporte à primeira linha e fortalecer os mecanismos de controle.

As funções da segunda linha de defesa incluem:

- Estabelecer rotinas e comitês que visem facilitar e monitorar a implementação de práticas eficazes de gerenciamento de riscos e conformidade por parte da 1ª Linha de defesa;
- Apoiar na definição do apetite a risco e na tomada de decisão das áreas de negócios, com reporte contínuo de informações relevantes;
- Monitorar riscos específicos, como o risco de não conformidade legal e regulatória, cuja responsabilidade é atribuída à área de Compliance, com reporte direto à Diretoria Executiva;
- Orientar as áreas operacionais quanto aos processos de gerenciamento de riscos e conformidade;
- Identificar alterações regulatórias ou no perfil de riscos, e alertar a 1ª Linha de Defesa.

3ª LINHA DE DEFESA: A Auditoria Interna compõe a 3ª Linha de Defesa e atua de forma independente e objetiva. Tem como principal atribuição avaliar a efetividade da governança, dos controles internos e do gerenciamento de riscos conduzidos pelas duas primeiras linhas. Os resultados são reportados diretamente à Diretoria Executiva e as comunicações são realizadas periodicamente, promovendo o aprimoramento contínuo da estrutura de controles e o reforço à segurança dos processos institucionais.

7. RESPONSABILIDADES

Em conformidade com os princípios estabelecidos nesta Política, as responsabilidades dos agentes envolvidos no processo de gerenciamento de risco operacional estão descritas a seguir:

7.1. Da Diretoria Executiva

- Aprovar, com periodicidade mínima anual, as políticas, estratégias e limites relacionados ao gerenciamento de risco operacional, bem como o programa de testes de estresse e as políticas para gestão de continuidade de negócios;
- Definir e revisar, com periodicidade mínima anual, os níveis de apetite a risco aplicáveis às entidades do Conglomerado Genial, com suporte do Comitê de Risco e *do Chief Risk Officer* (CRO);

- Analisar as recomendações contidas nos relatórios de Controles Internos, assegurando a inserção de manifestação formal quanto à responsabilidade pelas informações divulgadas;
- Garantir a aderência da instituição às políticas, estratégias e limites de gerenciamento de riscos;
- Assegurar que a estrutura de remuneração da instituição não incentive comportamentos incompatíveis com os níveis de apetite a risco dispostos na RAS;
- Assegurar a correção tempestiva das deficiências da estrutura de gerenciamento de riscos;
- Promover a cultura de gerenciamento de riscos em todos os níveis da instituição, incentivando boas práticas e a conscientização dos colaboradores;
- Autorizar, quando necessário, exceções à política, aos procedimentos, limites e níveis de apetite a risco definidos na RAS;
- Assegurar recursos adequados e suficientes para o exercício das atividades de gerenciamento de riscos, de forma independente, objetiva e efetiva, e
- Designar formalmente o diretor responsável pela Unidade de Gerenciamento de Riscos, conforme exigido pela regulamentação vigente.

7.2. Do Comitê de Risco

- Revisar anualmente a Política de Gerenciamento de Risco Operacional, assegurando sua atualização e aderência às melhores práticas e a regulamentação vigente;
- Analisar de forma integrada os riscos que podem impactar o capital, a liquidez e a continuidade das operações do Conglomerado Genial;
- Assessorar a Alta Administração no desempenho de suas atribuições relacionadas à adoção de estratégias, políticas e medidas voltadas à disseminação da cultura, mitigação de riscos e da conformidade com as normas aplicáveis;
- Estabelecer diretrizes e recomendações para o fortalecimento da governança de riscos, visando: (i) o cumprimento da legislação e regulamentações aplicáveis; (ii) a prevenção de exposições a riscos incompatíveis ou desnecessários ao perfil institucional; (iv) o aumento da eficácia e efetividade dos controles internos nas áreas de negócios e (v) a redução do impacto potencial dos riscos relevantes às quais as entidades do Conglomerado estão expostas.

7.3. Do Comitê de Segurança da Informação

- Revisar as políticas e diretrizes de segurança da informação e cibernética, e
- Avaliar os diversos tipos de riscos relacionados à Segurança Cibernética e continuidade de negócios e deliberar sobre as ações de mitigação apresentadas.

7.4. Do Chief Risk Officer (“CRO”)

- Supervisionar o desenvolvimento, a implementação e desempenho e o contínuo aperfeiçoamento da estrutura de gerenciamento de risco operacional;
- Avaliar a aderência e assegurar a compatibilidade da política, dos processos, dos relatórios, dos sistemas e dos modelos de risco operacional à Declaração de Apetite a Risco (RAS) e aos objetivos estratégicos da instituição;
- Capacitar adequadamente os integrantes da Unidade de Gerenciamento de Riscos, garantindo o entendimento pleno das políticas, dos processos, dos sistemas e dos modelos utilizados, ainda que que desenvolvidos por terceiros;
- Contribuir tecnicamente no processo de tomada de decisões estratégicas, oferecendo subsídios à Diretoria Executiva em temas relacionados ao gerenciamento de risco operacional, e
- Indicar as diretrizes a serem seguidas no programa de testes de estresse.

7.5. Da Área de Auditoria Interna

- Avaliar periodicamente os processos e procedimentos relativos ao gerenciamento de riscos;
- Identificar, analisar e documentar os riscos relevantes para o atendimento aos objetivos de negócio da Organização;
- Desenvolver um plano de auditoria anual baseado em risco e um planejamento cíclico de longo prazo com possibilidade de ajustes ao longo do tempo em caso de necessidade;
- Avaliar a adequação dos controles estabelecidos para assegurar conformidade com as políticas, procedimentos, leis, regras e objetivos do negócio;
- Avaliar os métodos de salvaguardas de ativos da organização e seus clientes;
- Avaliar a confiabilidade e segurança das informações financeiras e gerenciais, além dos sistemas e operações que geram esses dados, e
- Acompanhar (“follow-up”) os pontos identificados para assegurar o cumprimento das ações recomendadas, no prazo estabelecido.

7.6. Da Unidade de Gerenciamento de Riscos

- Elaborar e documentar as políticas e estratégias relacionadas ao gerenciamento do risco operacional;
- Implementar a estrutura de gerenciamento de riscos, disseminar o conhecimento e subsidiar as demais áreas para aderência às normas e regulamentações aplicáveis;
- Apoiar na definição de apetite a risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;

- Aplicar metodologias consistentes para identificar, avaliar, mensurar, monitorar, controlar e mitigar, de forma contínua, as causas e eventos de risco operacional, em conjunto com os gestores das áreas de negócios;
- Acompanhar e monitorar o desempenho da 1ª linha de defesa no que se refere ao gerenciamento do risco operacional;
- Elaborar, com periodicidade mínima anual, o relatório consolidado de risco operacional e submetê-lo a apreciação do Comitê de Risco;
- Documentar, armazenar, classificar e consolidar as informações referentes às perdas associadas ao risco operacional;
- Identificar previamente os riscos operacionais relacionados a novos produtos, serviços, alterações significativas em processos, sistemas, operações, modelo de negócio**,** bem como reorganizações societárias relevantes, e
- Disseminar institucionalmente o apetite a risco estabelecido na Declaração de Apetite a Risco (RAS) e promover o entendimento dos procedimentos de reporte relacionados à não conformidade com os limites de apetite a risco estabelecidos.

7.7. Da Área de Controles Internos

- Modelar novos processos operacionais ou atuar na reengenharia de processos e atividades existentes;
- Avaliar a eficiência dos controles internos com base em riscos;
- Apoiar na estruturação e gestão dos riscos corporativos;
- Fortalecer no processo de prevenção a fraude corporativa, e
- Apoiar a manutenção de processos operacionais alinhados com a estratégia e apetite a risco da instituição.

7.8. Da Área de Compliance

- Monitorar riscos específicos, como, por exemplo, a não conformidade com leis e regulamentos aplicáveis a instituição;
- Reportar eventuais inconsistências diretamente a Diretoria Executiva;
- Orientar sobre processos de gerenciamento de riscos e conformidade;
- Identificar mudanças no cenário regulatório e de riscos, e alertar a 1ª Linha de Defesa de tais inovações;
- Realizar testes e avaliações de aderência das atividades institucionais às normas legais, infralegais, às recomendações emitidas por órgãos de supervisão e autorreguladores, assim como às políticas internas, conforme plano anual de testes de conformidade aprovado pela Diretoria Executiva;

- Auxiliar na definição de apetite a risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;
- Identificar e reportar ao COAF os atos, omissões e operações que possam auxiliar ou cooperar de alguma forma para a identificação dos delitos de fraude, lavagem de dinheiro e/ou financiamento ao terrorismo, e
- Elaborar treinamentos e ações de disseminação da cultura de conformidade e controle de riscos.

7.9. Da Área de Segurança da Informação

- Identificar, classificar e documentar processos críticos do negócio, avaliando os impactos potenciais decorrentes de sua interrupção;
- Definir estratégias para assegurar a continuidade das operações da Instituição;
- Elaborar planos de continuidade de negócios que estabeleçam procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos do negócio, bem como as ações de comunicação necessárias;
- Realizar testes e revisões dos planos de continuidade de negócios com periodicidade adequada;
- Assegurar a integridade, segurança e disponibilidade de dados e dos sistemas de informação, promovendo a adequação contínua às mudanças no modelo de negócio e incorporando mecanismos de prevenção, detecção e mitigação de riscos cibernéticos e vulnerabilidades tecnológicas; e
- Implementar e manter uma estrutura de governança de tecnologia consistente com os níveis de apetite a risco estabelecidos na RAS.

7.10. Da Área de Antifraude

- Prevenir, identificar e responder a fraudes bancárias;
- Proteger os ativos do Grupo e dos seus clientes;
- Informar à Unidade de Gerenciamento de Riscos os eventos de risco operacional.

7.11. Dos Gestores e Colaboradores

- Identificar os riscos operacionais oriundos do exercício de suas atividades, considerando também os serviços terceirizados utilizados;
- Estabelecer e gerenciar os controles de risco inerentes as suas atividades do dia a dia;
- Avaliar regularmente o serviço pactuado com prestadores de serviços terceirizados;
- Informar à Unidade de Gerenciamento de Riscos os eventos de risco operacional.

7.12. Do Jurídico

- Identificar e mitigar o risco legal na elaboração dos contratos firmados pela instituição;
- Incluir nos contratos firmados pela instituição cláusulas que estabeleçam claramente os papéis e as responsabilidades dos prestadores de serviços terceirizados;
- Garantir a inclusão das cláusulas necessárias nos contratos de TI conforme Resolução N° 4.893.

8. DIRETRIZES DE GERENCIAMENTO DE RISCO OPERACIONAL

A metodologia utilizada está em linha com o *framework* definido nos documentos: (i) "*Principles for the Sound Management of Operational Risk"* emitido em junho de 2011 pelo *Basel Committee on Banking Supervision* e (ii) "*Integrated Framework: Application Techniques"* publicado em setembro de 2011 pelo COSO - *Committee of Sponsoring Organizations of the Treadway Commission*. Neste modelo, a gestão de riscos operacionais considera os seguintes elementos:

- Ambiente Interno
- Fixação de Objetivos
- Identificação de Eventos
- Avaliação de Riscos
- Atividade de Controle
- Resposta a Risco
- Informações e Comunicações
- Monitoramento

Desta forma, o Conglomerado Genial institui um ambiente interno propício para a prática de controles internos e gestão de riscos onde os objetivos estratégicos são fixados, os eventos de risco identificados e avaliados e uma resposta para a ocorrência dos riscos mapeados é estabelecida. A Genial possui atividades de controle, um fluxo de informações e comunicações e, por fim, um monitoramento contínuo dos riscos relevantes.

9. METODOLOGIA

A metodologia adotada para o gerenciamento do risco operacional segue uma abordagem estruturada, composta por etapas que visam garantir a identificação, avaliação, monitoramento, controle e mitigação dos riscos relevantes, conforme as diretrizes da Resolução CMN nº 4.557/2017 e as melhores práticas de mercado.

9.1. Identificação

A etapa de identificação constitui o ponto de partida do processo de gerenciamento do risco operacional, permitindo conhecer os riscos aos quais as empresas do Conglomerado Genial estão expostas. Essa fase tem como base o mapeamento de deficiências, vulnerabilidades e eventos de risco, utilizando ferramentas e práticas específicas adotadas pelas áreas de Controles Internos e de Risco.

As principais ferramentas utilizadas para a identificação de riscos operacionais são:

- **Base de Perdas:** utilizada para o registro, documentação e armazenamento estruturado de eventos de perdas operacionais, incluindo provisões, impactos relacionados a risco de mercado e crédito, bem como despesas vinculadas a cada ocorrência. Esta base visa a formação de um histórico confiável e a gestão estruturada do risco operacional. Os registros seguem os critérios mínimos abaixo:
  - ✓ Eventos de perda individuais com valor superior a R$ 1.000,00;
  - ✓ Eventos com mesma origem ou natureza, que de forma agregada, no mesmo dia, somem valor superior a R$ 1.000,00;
  - ✓ Eventos de perda superiores a R$ 10.000,00 devem conter justificativa formal registrada.
- ***Control Risk Self Assessment (CRSA):*** ferramenta qualitativa que promove a autoavaliação estruturada dos riscos e controles pelas áreas de negócio. O processo é conduzido por meio de entrevistas com gestores e responsáveis, que discutem processos críticos, potenciais riscos e controles existentes, bem como propõem planos de ação corretiva, quando necessário. O resultado dessa avaliação subsidia a construção da matriz de riscos operacionais, servindo como base para as próximas etapas do gerenciamento.

9.2. Avaliação e Mensuração

A etapa de avaliação e mensuração tem como finalidade quantificar ou dimensionar a exposição ao risco operacional, com o objetivo de analisar o potencial impacto sobre os negócios da instituição.

Esse processo envolve a estimativa da probabilidade de ocorrência dos eventos de risco e da magnitude de seus impactos, permitindo determinar o nível de risco residual associado a cada processo, atividade ou unidade de negócio.

A avaliação é conduzida com base em critérios objetivos e padronizados, de forma a promover comparabilidade, priorização e tratamento adequado dos riscos identificados. A seguir, são apresentadas as tabelas com as definições adotadas pela instituição para os critérios de probabilidade e impacto aplicáveis ao risco operacional:

PROBABILIDADE	REMOTA	POSSÍVEL	PROVÁVEL
FREQUÊNCIA	Há possibilidade de ocorrer de forma infrequente e incomum	Há possibilidade de ocorrer em algumas circunstâncias.	Provavelmente ocorra com frequência.

IMPACTO	BAIXO	MÉDIO	ALTO
FINANCEIRO (valores em Reais R$)	Perdas financeiras: **de: 0,01 até 1.000.000,00**	Perdas financeiras: **de: 1.000.000,01 até 10.000.000,00**	Perdas financeiras: **acima de 10.000.000,00**
IMAGEM	Menções negativas de baixa relevância: **Veículos de comunicações locais**	Menções negativas de média relevância: **Veículos de comunicações regionais e estaduais**	Menções negativas relevantes: **Veículos de comunicações nacionais e redes sociais**
CLIENTE	Indisponibilidades afetando até: **De 01% até 10% dos clientes**	Indisponibilidades afetando até: **de 11% até 25% dos clientes**	Indisponibilidade afetando: **Acima de 25% dos clientes**
LEGAL / COMPLIANCE	**Aplicação de Sanções de baixa relevância**, sem efeito midiático nem de imagem.	**Aplicação de sanções de média relevância,** podendo haver menção midiática pontual, com pequeno a médio potencial de dano a imagem.	**Aplicação de sanções relevantes,** com menção midiática relevante e dano à reputação causando empecilhos à concretização de negócios.

A tabela abaixo demonstra a **Exposição** ou **Grau de Risco** da relação probabilidade *versus* impacto:

IMPACTO

PROBABILIDADE	#	BAIXO	MÉDIO	ALTO
	REMOTA	Risco Baixo	Risco Baixo	Risco Moderado
	POSSÍVEL	Risco Baixo	Risco Moderado	Risco Alto
	PROVÁVEL	Risco Moderado	Risco Alto	Risco Alto

A Instituição define quatro respostas aos riscos mapeados:

EVITAR	MITIGAR	TRANSFERIR	ACEITAR
•Descontinuação das atividades que geram determinado risco.	•São adotados medidas e controles para reduzir a probabilidade ou o impacto dos riscos não tolerados e não controlados. Se necessários são alterados processos, sistemas e/ou pessoas.	•Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento do risco. Como aquisição de seguros e/ou terceirização de uma atividade.	•Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos. A Instituição aceita certo nível de risco devido ao custo para a mitigação ou irrelevância do risco.

9.3. Controle

A etapa de controle tem como finalidade avaliar a efetividade dos controles implementados para mitigação dos riscos operacionais identificados.

Essa avaliação é realizada por meio da execução de testes formais sobre a Matriz de Riscos e Controles, com o objetivo de verificar a aderência, suficiência e funcionamento adequado dos controles em relação aos riscos mapeados.

Os resultados obtidos subsidiam a identificação de necessidades de aprimoramento, a definição de ações corretivas e o fortalecimento contínuo da estrutura de controle da instituição.

9.4. Monitoramento e Reporte

O monitoramento consiste em uma atividade contínua e estruturada, voltada à identificação de deficiências, fragilidades e desvios no processo de gerenciamento do risco operacional. Essa etapa permite acompanhar a efetividade dos controles implementados, a aderência às políticas e diretrizes vigentes e a evolução dos planos de ação corretiva, quando aplicáveis.

As inconsistências e vulnerabilidades identificadas devem ser devidamente registradas, analisadas e reportadas à Alta Administração, de forma tempestiva e clara, garantindo suporte à tomada de decisão e ao aprimoramento da governança de riscos da instituição.

10. REVISÃO E APROVAÇÃO

Esta política deve ser revisada pelo Comitê de Risco e aprovada pela Diretoria Executiva no mínimo anualmente.

RIO DE JANEIRO
PHONE:
55 21 3923-3000
3500-3000

SÃO PAULO
PHONE:
55 11 3206-8000
2920-8000

MIAMI AFFILIATE
PHONE:
1 212 388-5600

NEW YORK
PHONE:
1 212 388-5600