

**POLÍTICA DE
GERENCIAMENTO DE
RISCOS DA CIABRASF – CIA.
BRASILEIRA DE SERVIÇOS
FINANCEIROS S.A.**



Sumário

INTRODUÇÃO	3
1 OBJETIVOS	3
2 ABRANGÊNCIA.....	3
3 REFERÊNCIAS	3
4 DEFINIÇÕES	3
5 PROCESSO DE GERENCIAMENTO DE RISCOS.....	5
6 RESPONSABILIDADES.....	8
7 DISPOSIÇÕES GERAIS	10

INTRODUÇÃO

Esta Política de Gerenciamento de Riscos (“**Política**”) da CIABRASF – Cia. Brasileira De Serviços Financeiros S.A. (“**Companhia**”) descreve a forma por meio da qual a Companhia identifica, avalia, monitora e gerencia os riscos aos quais a Companhia está sujeita.

1 OBJETIVOS

1.1 Esta Política estabelece os princípios e parâmetros a serem observados com relação ao processo de gerenciamento de risco da Companhia com vistas a identificar, avaliar, priorizar e gerenciar Riscos (conforme abaixo definido).

1.2 Esta Política também descreve o processo de gerenciamento de risco, os procedimentos de comunicação e as responsabilidades dos principais órgãos societários da Companhia.

2 ABRANGÊNCIA

2.1 Esta Política vincula todos os departamentos, administradores e empregados da Companhia. As subsidiárias da Companhia também deverão cumprir as disposições ora previstas.

3 REFERÊNCIAS

- (i) O Código de Conduta Ética;
- (ii) A Política de Divulgação de Informações da Companhia;
- (iii) A Política de Negociação de Valores Mobiliários da Companhia;
- (iv) A Política de Transações entre Partes Relacionadas da Companhia; e
- (v) *COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework*

4 DEFINIÇÕES

4.1 Os seguintes termos usados nesta Política têm os significados abaixo especificados:

- | | |
|---------------------------------|---|
| “Apetite para o Risco” | significa o nível de risco associado à consecução dos objetivos da Companhia. Periodicamente a Companhia avalia e revisa o nível de risco aceitável assumido pela Companhia como um todo, para assegurar que o equilíbrio entre risco e benefício seja adequadamente gerenciado e alinhado. |
| “Gerenciamento do Risco” | significa o processo de avaliação e resposta ao risco relacionado aos negócios da Companhia com vistas a reduzir tais riscos a níveis aceitáveis. O gerenciamento do |

risco é parte do processo de avaliação e utiliza os resultados oriundos de tal processo para tomar decisões sobre a aceitação de riscos ou a tomada de medidas para reduzi-los.

“Risco”	significa a incerteza relacionada a certos eventos e seu potencial resultado que possa ter um efeito significativo sobre as atividades da Companhia. Todas as atividades da Companhia podem representar algum risco decorrente de potenciais ameaças ou da não concretização de oportunidades, que podem prejudicar, impedir, afetar ou interferir na consecução dos objetivos sociais.
“Risco Estratégico”	significa o risco de implementação de uma estratégia errada, inadequada ou ineficaz que deixe de atingir os objetivos da Companhia.
“Risco Operacional”	significa o risco de prejuízo devido a falhas, deficiências ou inadequação de processos, pessoal e sistemas internos de suporte às atividades da Companhia ou, ainda, eventos externos, incluindo, mas não se limitando, risco de compliance associado à inadequação ou deficiência em contratos, assim como sanções devidas ao não cumprimento de leis e regulamentos e indenizações de danos causados a terceiros resultantes das atividades da Companhia. Também inclui fraudes internas e externas.
“Risco de Liquidez”	significa o risco de falta de capacidade financeira da Companhia para pagar suas dívidas previstas e imprevistas, efetivas e futuras, incluindo operações com garantias, sem afetar suas operações do dia e sem incorrer em perdas significativas.
“Risco de Compliance”	significa o risco de estar sujeito a quaisquer sanções legais de cunho reputacional ou regulatórias, ou prejuízo financeiro que a Companhia possa sofrer em decorrência de sua falha em cumprir as leis e regulamentos aplicáveis, políticas internas, códigos de conduta e padrões de boas práticas.
“Risco de Informação”	significa o risco relacionado à perda, ao mau uso ou à divulgação não autorizada de dados pessoais sensíveis ou informações confidenciais de clientes, fornecedores, parceiros de negócios, acionistas internos ou externos que possam causar danos ou transtornos a qualquer indivíduo, ameaçar os negócios da Companhia ou prejudicar sua reputação.

5 PROCESSO DE GERENCIAMENTO DE RISCOS

5.1 O gerenciamento do risco é um elemento crucial das estratégias da Companhia, já que fornece um processo sistemático para identificar riscos relacionados às atividades da Companhia bem como ao mercado de atuação da Companhia. Tal processo envolve a categorização e a avaliação de cada risco e a aplicação de controles gerenciais para mitigar o risco, baseados em um julgamento acerca do impacto provável caso nenhuma medida seja tomada, combinado com uma avaliação da probabilidade de nova ocorrência do risco.

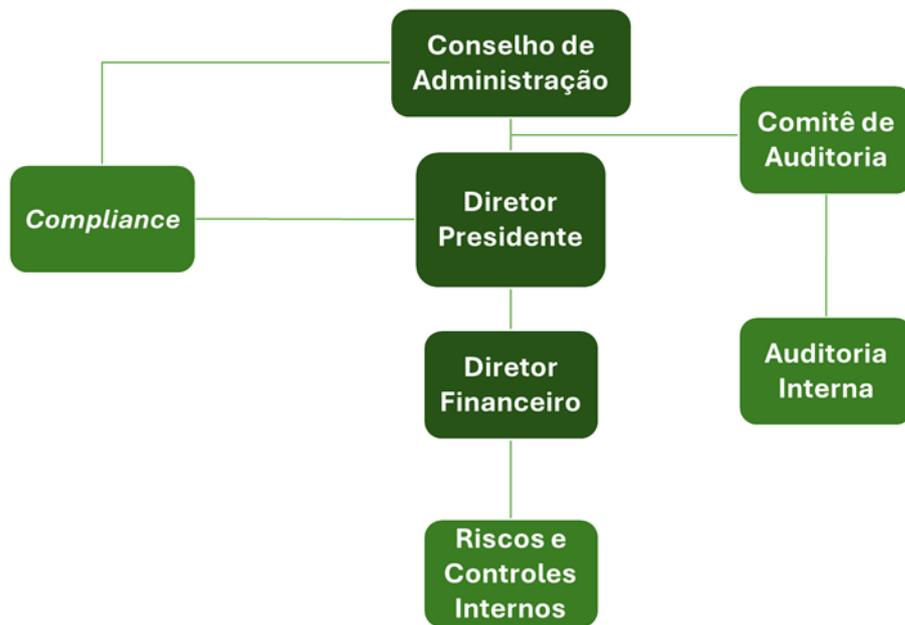
5.2 A estrutura de detecção e prevenção aos riscos é composta da seguinte forma:

(i) 1ª Linha: Áreas de Negócios. As áreas de negócio e operações da Companhia e de suas investidas constituem a primeira linha de defesa, sendo as principais responsáveis pela identificação, avaliação e mitigação de riscos no nível operacional. Cada unidade de negócio realizará monitoramentos contínuos para identificar possíveis vulnerabilidades e assegurará a execução de controles preventivos e corretivos. O objetivo é garantir que os processos estejam alinhados com as políticas corporativas e com os requisitos regulatórios aplicáveis.

(ii) 2ª Linha: Área de Riscos, Controles Internos e Compliance da Companhia. A segunda linha de defesa é composta pela Área de Riscos, Controles Internos e *Compliance* da Companhia, que atua como suporte às áreas de negócio e aos administradores da Companhia na tomada de decisões.

(iii) 3ª Linha: Auditoria Interna. A Auditoria Interna constitui a terceira linha de defesa.

(iv) Adicionalmente ao acompanhamento do ambiente por meio dessas três linhas de defesa, o Conselho de Administração da Companhia conta com a atuação do Comitê de Auditoria para auxiliá-lo no acompanhamento e gerenciamento de riscos.



5.3 A Companhia estabelece um processo de gerenciamento dos riscos estruturado e contínuo, composto pelas seguintes etapas:

(i) ambiente interno: A Área de Riscos, Controles Internos e *Compliance* da Companhia realiza a análise de ambiente interno, por meio da avaliação envolve o estabelecimento da base de como riscos e são percebidos controles são visualizados e tratados pelos empregados da Companhia;

(ii) fixação de objetivos: Em linha com as recomendações da Área de Riscos, Controles Internos e *Compliance* da Companhia, a Diretoria propõe, e submete à aprovação do Conselho de Administração, a definição dos objetivos estratégicos, operacionais, de comunicação e de confiabilidade, por meio de um processo de desenvolvimento e de alinhamento entre os objetivos priorizados à missão e aos princípios da Companhia;

(iii) identificação de eventos: A Área de Riscos, Controles Internos e *Compliance* da Companhia realiza análises para identificar eventos, fatores internos e externos que configurem risco reais ou potenciais. Esses riscos são categorizados como estratégicos, operacionais, de *compliance*, de liquidez e de informação;

(iv) avaliação do risco: Cada risco identificado é avaliado pela Área de Riscos, Controles Internos e *Compliance* da Companhia, considerando sua probabilidade de ocorrência e impacto. A Companhia utiliza métodos como *benchmarking* e modelos probabilísticos para

priorizar e classificar os riscos de forma objetiva. O relatório de riscos é revisado pela Auditoria Interna e reportado à Diretoria e ao Conselho de Administração;

(v) resposta ao risco: Em linha com as recomendações da Área de Riscos, Controles Internos e Compliance da Companhia, a Diretoria propõe, e submete à aprovação do Conselho de Administração, respostas aos riscos identificados, incluindo:

- Evitar o risco, ajustando processos ou atividades;
- Mitigar o risco, implementando controles internos;
- Transferir o risco, por meio de seguros ou contratos;
- Aceitar o risco, dentro do apetite definido pelo Conselho de Administração.

(vi) atividades de controle: Para assegurar a eficácia das respostas, a Área de Riscos, Controles Internos e *Compliance* da Companhia elabora planos de ação alinhados às políticas e procedimentos internos da Companhia, com responsáveis definidos e prazos estabelecidos. Tais planos são revisados pela Auditoria Interna e reportados à Diretoria e ao Conselho de Administração;

(vii) informação e comunicação: A Área de Riscos, Controles Internos e *Compliance* da Companhia estabelece o fluxo de governança de informações e define a estratégia de comunicação, de forma que as informações relevantes sejam identificadas, coletadas e comunicadas para os empregados da Companhia, para que todos possam compreender e desempenhar suas funções e responsabilidades com relação ao enfrentamento dos riscos priorizados; e

(viii) monitoramento: O monitoramento contínuo da integridade do processo de gerenciamento de riscos é realizado pela Área de Riscos, Controles Internos e *Compliance* da Companhia, pela Auditoria Interna, pela Diretoria e pelo Conselho de Administração. Esse monitoramento permite ajustes rápidos e adequados às mudanças de cenário e aos riscos emergentes.

5.4 O processo de gerenciamento de riscos é integrado à cultura organizacional da Companhia, assegurando flexibilidade e proatividade na mitigação de riscos e na resposta a mudanças no ambiente de negócios. Essa estrutura reforça o compromisso da Companhia com as melhores práticas de controles internos, gestão de processos, mitigação de riscos, *compliance* e continuidade de negócios.

5.5 O processo de gerenciamento do risco será realizado por meio de auditoria interna e externa visando a minimizar as consequências da ocorrência de um risco com base em impacto e probabilidade, reconhecendo-se que o risco propriamente dito pode não ser eliminado.

5.6 A adequação da estrutura operacional e de controles internos para verificação da efetividade da política de gerenciamento de riscos deverá ser reavaliada anualmente pelo Conselho de Administração da Companhia, com assessoramento do Comitê de Auditoria.

6 RESPONSABILIDADES

6.1 A estrutura organizacional de gerenciamento de riscos é composta pelo Conselho de Administração, pela Diretoria da Companhia, pelo Comitê de Auditoria, pela Área de Riscos, Controles Internos e *Compliance* e pela Auditoria Interna, bem como pelos colaboradores da Companhia, no desempenho de suas funções.

6.2 Conselho de Administração: O Conselho de Administração da Companhia é responsável pela aprovação desta Política, suas revisões e atualizações, bem como por:

- (i) determinar o Apetite para o Risco e estabelecer a cultura da gestão do risco dentro da Companhia, especialmente com relação a novas iniciativas e riscos emergentes;
- (ii) tomar as decisões principais com relação ao processo de gestão de riscos da Companhia, incluindo os que possam afetar o perfil de risco ou exposição da Companhia;
- (iii) avaliar a efetividade do sistema de controles internos, com o assessoramento do Comitê de Auditoria;
- (iv) aprovar quaisquer mudanças nesta Política; e
- (v) revisar, monitorar e aprovar as estratégias gerais da Companhia para a gestão do risco e os papéis e relatórios elaborados pelo Comitê de Auditoria e pela Área de Riscos e Controles Internos.

6.3 Diretoria: A Diretoria da Companhia é responsável por:

- (i) implementar as estratégias da Companhia aprovadas pelo Conselho de Administração com relação à Gestão do Risco;
- (ii) propor ao Conselho de Administração o Apetite para o Risco da Companhia;
- (iii) avaliar periodicamente a Avaliação de Risco, relatando quaisquer descobertas ao Conselho de Administração;
- (iv) avaliar e monitorar o Risco Estratégico; e
- (v) identificar quaisquer Riscos antecipadamente e conduzir o

Gerenciamento de Risco correlata.

6.4 Comitê de Auditoria Não Estatutário: O Comitê de Auditoria da Companhia é encarregado de:

- (i) rever o cumprimento pela Companhia das leis, padrões e regulamentos aplicáveis;
- (ii) avaliar e analisar o uso e a confiabilidade dos controles internos, riscos de compliance e corporativos;
- (iii) monitorar as exposições de Risco da Companhia;
- (iv) fiscalizar o desempenho de terceiros contratados para dar suporte ao staff designado para desempenhar funções de compliance, controles internos e risco corporativo;
- (v) revisar as principais políticas da Companhia, incluindo as políticas internas e o Código de Conduta Ética, propondo quaisquer mudanças ao Conselho de Administração;
- (vi) coordenar e monitorar as atividades de canal de denúncias (*whistleblower*) assegurando a autonomia, sigilo, confidencialidade e um ambiente livre de retaliações;
- (vii) avaliar e monitorar o Risco de Liquidez;
- (viii) investigar e monitorar eventos que possam prejudicar os controles internos da Companhia e esta Política;
- (ix) fornecer treinamento recorrente ao pessoal da Companhia com vistas a assegurar que sejam capazes de identificar, evitar, avaliar, monitorar e mitigar Riscos;
- (x) conduzir uma revisão periódica da Política de Gerenciamento de Riscos e apresentar quaisquer sugestões ao Conselho de Administração; e
- (xi) avaliar periodicamente a Avaliação de Risco, relatando quaisquer descobertas ao Conselho de Administração.

6.5 Área de Riscos, Controle Internos e Compliance: Os colaboradores da Companhia designados para desempenhar funções de compliance, controles internos e de riscos corporativos são encarregados de:

- (i) rever o cumprimento pela Companhia das leis, padrões e regulamentos aplicáveis;
- (ii) estabelecer o processo de gestão do risco da Companhia;
- (iii) coordenar e determinar as diretrizes a serem seguidas no tocante aos procedimentos de compliance, controles internos e risco corporativo;
- (iv) preparar relatórios que descrevam os riscos da Companhia e a avaliação de Risco correlata, e submetê-los periodicamente à avaliação do Comitê de Auditoria;

- (v) avaliar e monitorar o Risco de *Compliance*, o Risco Operacional e o Risco de Informação;
- (vi) mapear e conduzir treinamentos de *compliance* às áreas de interesse;
- (vii) auxiliar a área de ouvidoria na apuração e análise das medidas disciplinares a serem aplicadas em decorrência de violação do Código de Ética e Conduta da Companhia;
- (viii) realizar no mínimo uma revisão anual do sistema de controles internos da Companhia; e
- (ix) coordenar a força de trabalho interna destinada a detectar quaisquer Riscos e monitorar a eficácia do processo de Gerenciamento do Risco.

6.6 Auditoria Interna: A área responsável pela auditoria interna da Companhia responderá diretamente ao Comitê de Auditoria, e estará encarregada de:

- (i) monitorar, avaliar e realizar recomendações visando a aperfeiçoar os controles internos e as normas e procedimentos estabelecidos pelos administradores;
- (ii) aferir a qualidade e efetividade dos processos de Gerenciamento do Risco, controle e governança da Companhia;
- (iii) determinar a extensão do cumprimento das normas, dos planos e procedimentos vigentes;
- (iv) determinar o grau de confiança, das informações e dados contábeis e de outra natureza, preparados dentro da Companhia;
- (v) avaliar os riscos estratégicos e de negócio da Companhia; e
- (vi) avaliar a eficácia, suficiência e aplicação dos controles contábeis, financeiros e operacionais.

7 DISPOSIÇÕES GERAIS

7.1 Esta Política foi aprovada pelo Conselho de Administração e vigorará por prazo indeterminado. Os casos omissos serão decididos pelo Conselho de Administração da Companhia.

7.2 A presente Política somente poderá ser alterada por deliberação do Conselho de Administração da Companhia.

* * *

Versão 03 - Aprovada em 03/07/2025	
Elaboração:	Departamento Jurídico e <i>Compliance</i>
Revisão/Aprovação:	Conselho de Administração