ITAÚSA

CNPJ 61.532.644/0001-15
Companhia Aberta

POLÍTICA DE GESTÃO DE RISCOS

(aprovada na RCA de 04.05.2017, alterada em 14.05.2018 e revisada em 22.02.2021)

1. OBJETIVO

A presente Política de Gestão de Riscos ("Política") estabelece as diretrizes a serem observadas no processo de Gestão de Riscos da Itaúsa S.A. ("Itaúsa" ou "Companhia"), de forma a possibilitar a identificação, avaliação, priorização e tratamento dos Riscos para a perpetuidade dos negócios.

2. PÚBLICO-ALVO

Esta Política aplica-se à Companhia e a todos os administradores (membros do Conselho de Administração e diretores), membros do Conselho Fiscal, membros de comitês de assessoramento ao Conselho de Administração, membros de comissões de assessoramento à Diretoria e colaboradores.

As sociedades controladas pela Itaúsa devem espelhar em suas respectivas políticas de gerenciamento de Riscos as considerações aqui formuladas, respeitadas suas eventuais peculiaridades procedimentais de gestão e o nível de complexidade de suas operações. As sociedades controladas que não tenham política própria devem seguir os termos desta Política, observadas as suas respectivas estruturas de gestão.

3. CONCEITOS

- **Apetite a Riscos:** grau de exposição a Riscos que a Companhia está disposta a aceitar para atingir seus objetivos e criar valor para seus acionistas.
- ***Compliance*:** designação utilizada na prevenção e detecção de falta de conformidade com leis e regulamentações nacionais e estrangeiras, que possa ser cometida pelos administradores, colaboradores e parceiros de negócios da Companhia.
- **Controles:** políticas, normas, procedimentos, atividades e mecanismos desenvolvidos para assegurar que os objetivos de negócios sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos.
- **Fator de Risco:** situação que pode potencializar a ocorrência de um Risco.
- **Gestão de Riscos:** atividades realizadas com a finalidade de identificar, classificar, formalizar, monitorar e/ou administrar os Riscos identificados. A Gestão de Riscos deve estar alinhada aos objetivos, estratégias e negócios da Companhia.
- **Impacto**: resultado de um evento ao qual a Companhia possa estar exposta em razão de suas atividades.

- **Indicadores de Riscos (*KRI's*):** métrica de avaliação ou monitoramento da exposição da Companhia aos seus Riscos.
- **Modelo de 3 Linhas:** identificam estruturas e processos que auxiliam no atingimento dos objetivos e fortalecem a governança e gerenciamento de Riscos.
- **Mapa de Riscos**: representação gráfica da classificação qualitativa e quantitativa dos Riscos, considerando possível Impacto e probabilidade de sua materialização.
- **Plano(s) de Ação**: definição das ações corretivas para reduzir a exposição aos Riscos residuais, a partir da identificação das deficiências ao longo do ciclo de avaliação do ambiente de Controle/Riscos.
- **Resposta(s) ao(s) Risco(s):** decisão que será tomada após a identificação do Risco Inerente ou avaliação do ambiente de Controle dos Riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de Controles internos da Itaúsa.
- **Risco(s):** ameaça de eventos ou ações que possam impactar o atingimento dos objetivos da Companhia. É inerente a qualquer atividade e pode afetar os ativos, resultados, imagem ou continuidade dos negócios.
- **Tolerância a Risco**: limite de nível de Risco ou incerteza que a Companhia suporta para atingir seus objetivos.
- **Risco Inerente:** Risco existente no processo antes de ser tratado/mitigado quanto à sua probabilidade de ocorrência e Impacto.
- **Risco Residual**: Risco remanescente após a Companhia ter implementado Controles ou Planos de Ação para reduzir a probabilidade de ocorrência e mitigar seu Impacto.
- ***Risk Owner***: pessoa ou área com responsabilidade e autoridade para gerenciar um Risco na primeira linha e apoiar na definição e implementação de Planos de Ação para mitigação ou remediação do Risco.
- **Vulnerabilidade:** nível de exposição da Companhia ao Risco considerando o ambiente de Controles internos em vigor.

4. PRINCÍPIOS e DIRETRIZES

Os princípios e as diretrizes de Gestão de Riscos corporativos têm como objetivo reforçar o compromisso da Itaúsa em agir em conformidade com os requisitos regulatórios e com as melhores práticas, alinhando seus negócios com a estratégia da Companhia. Além disso, também tem o papel de definir as responsabilidades dos colaboradores e da Administração na Gestão de Riscos, assegurar que as diretrizes de governança sejam cumpridas e fortalecer a filosofia e cultura de Riscos na Companhia.

4.1. Atividades de Controles

Conjunto de ações, políticas, normas, procedimentos e sistemas, com os quais se visa salvaguardar os ativos da Companhia, assegurando que seus Riscos sejam conhecidos e mitigados adequadamente.

As atividades de Controles devem ser desempenhadas em todos os níveis da Companhia e em vários estágios dentro dos processos corporativos.

4.2. Estrutura de Gestão de Riscos

Conforme as melhores práticas de mercado, a Itaúsa mantém uma estrutura organizada responsável pela aplicação do processo de Gestão de Riscos aqui descrito, em diferentes níveis da organização, conforme detalhado no item 5 desta Política.

A Companhia adota o Modelo de 3 Linhas do Instituto Internacional dos Auditores (IIA) na Gestão de Riscos corporativos, onde atuam de forma integrada as áreas de negócios, área de *Compliance* e Riscos Corporativos, a Auditoria Interna, Comitês, Comissões, Diretoria e Conselho de Administração.

- 1ª linha: gestores de negócios, que têm conhecimento e gestão de seus Riscos, bem como a responsabilidade de definir e implementar Planos de Ação para sua mitigação, de forma a garantir a adequada gestão dos processos;
- 2ª linha: área de *Compliance* e Riscos Corporativos, que auxilia a 1ª linha na identificação dos Riscos, causas e consequências associadas. Responsável pelo processo de Gestão de Riscos, utiliza metodologia e melhores práticas de mercado; e
- 3º linha: auditoria interna, que possui independência para avaliar os controles executados pela 1ª linha e a adequação da Gestão de Riscos.

4.3. Etapas da Gestão de Riscos:

4.3.1. Identificação dos Riscos

Os Riscos aos quais a Companhia está sujeita devem ser identificados periodicamente, documentados e formalizados de forma estruturada para que sejam conhecidos e tratados adequadamente.

Tais Riscos devem ser categorizados de acordo com sua natureza e origem, conforme abaixo indicado:

- **Estratégico:** Riscos associados à tomada de decisão da administração e que podem gerar perda substancial no valor econômico da Companhia. Além disso, podem ocasionar Impacto negativo na receita ou no capital da Companhia em consequência de um planejamento falho, da tomada de decisões adversas, da inabilidade da Itaúsa em implantar seus planos estratégicos apropriados e/ou de mudanças em seu ambiente de negócio.
- **Financeiro:** Riscos cuja materialização resulte em perdas de recursos financeiros pela Companhia, subdivididos nas seguintes categorias:
  - Risco de liquidez: é traduzido pela possibilidade de a Companhia não ser capaz de honrar seus compromissos no vencimento, ou somente fazê-lo com elevadas perdas. Este Risco pode também ser classificado como Risco de fluxo de caixa dada a possibilidade da ocorrência de descasamentos entre os pagamentos e os recebimentos que afetem a capacidade de pagamento da Companhia.
  - Risco de mercado: este Risco mede a possibilidade de perda econômica gerada pela variação nos Fatores de Risco de mercado aos quais os preços dos ativos, passivos e derivativos possuam sensibilidade. O horizonte de tempo da análise é tipicamente de curto prazo e inclui o Risco de variação: cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (*commodities*).

- Risco de crédito: é a possibilidade de perdas resultantes pelo não recebimento de valores contratados junto a terceiros em decorrência de sua incapacidade econômico-financeira.

- **Operacional:** Riscos relacionados à infraestrutura da Companhia (processos, pessoas e tecnologia), que afetam a eficiência operacional e a utilização efetiva e eficiente de seus recursos.
- **Regulatório:** Riscos relacionados ao descumprimento da legislação aplicável ao setor de atuação bem como da legislação em geral (ambiental, trabalhista, cível e tributário/ fiscal).
- **Cibernético:** Risco relacionado à possibilidade de uma ameaça interna ou externa de explorar Vulnerabilidades de um ativo, impactando na confidencialidade, integridade e disponibilidade dos sistemas e das informações.

A etapa de identificação contempla os Riscos corporativos inerentes às atividades da Companhia, inclusive nos serviços terceirizados. A identificação pode ocorrer a qualquer momento, desde o desenho de um novo processo até a sua operacionalização, e ter a participação de todos os envolvidos no processo em diferentes níveis. Devem ser definidas também as causas (Fatores de Risco, consequências e responsáveis pelos Riscos).

4.3.2. Análise dos Riscos

Esta etapa envolve a verificação das causas (Fatores de Risco) e consequências dos Riscos, bem como da probabilidade de concretização das referidas consequências.

4.3.3. Avaliação dos Riscos

A avaliação dos Riscos envolve processos dinâmicos e interativos que devem: (i) verificar quais Riscos necessitam de tratamento; e (ii) determinar a prioridade na implementação de referido tratamento. Para tanto, a Companhia adota critérios de Impacto e de Vulnerabilidade que são utilizados para a definição do Mapa de Riscos.

O Impacto considera as diretrizes da Administração em relação aos possíveis aspectos financeiros (perda), estratégicos, de imagem/reputação, operacionais, legais/regulatórios e reflexo nos valores mobiliários da Companhia. A Vulnerabilidade considera a magnitude de exposição da Itaúsa a diversos fatores externos e internos, ou seja, considera a probabilidade de ocorrência do Risco com base na robustez de seu ambiente de Controles internos.

A classificação final do grau de exposição da Companhia a cada Risco será definida em função da combinação entre o Impacto e a Vulnerabilidade, conforme abaixo:

- **Crítico:** Risco com Impacto crítico ou alto e Vulnerabilidade provável ou muito provável.
- **Alto:** Risco com Impacto crítico, alto ou médio e Vulnerabilidade possível, provável ou muito provável.
- **Médio:** Risco com Impacto crítico, alto, médio ou baixo e Vulnerabilidade remoto, possível, provável ou muito provável.
- **Baixo:** Risco com Impacto médio ou baixo e Vulnerabilidade remoto ou possível.

Essa classificação resultará no Mapa de Riscos que deverá auxiliar a Companhia na priorização do tratamento dos Riscos.

4.3.4. Tratamento dos Riscos

Os Riscos identificados devem ser abordados de acordo com sua criticidade. A Comissão de Sustentabilidade e Riscos deve determinar como responder aos Riscos, e definir os instrumentos para proteção da Companhia, equilibrando os efeitos da Resposta ao Risco com eventual custo/benefício decorrente de requisitos legais, regulatórios ou quaisquer outros que se provem relevantes à Companhia. A Comissão de Sustentabilidade e Riscos observará as seguintes alternativas para tratamento dos Riscos:

- **Aceitar:** nenhuma ação é tomada para influenciar a probabilidade de ocorrência e/ou severidade do Risco. Riscos cujo Impacto seja menor que o custo/benefício do seu gerenciamento podem ser mantidos, desde que conhecidos e aceitos pela Comissão de Sustentabilidade e Riscos, em linha com o Apetite a Riscos definido pelo Conselho de Administração. No entanto, devem ser estabelecidas medidas de monitoramento contínuo de modo a assegurar que, caso haja mudança de conjuntura que justifique alteração no tratamento do Risco, a Companhia implemente referido tratamento.
- **Rejeitar**: caso seja determinado que a Companhia não deseja conviver com o Risco nas condições em que este se apresenta, a Comissão de Sustentabilidade e Riscos aplicará um dos tratamentos a seguir:
  - Agir: ações são tomadas para reduzir a probabilidade de materialização e/ou severidade do Risco. Esta resposta envolve o aprimoramento ou criação de Controles e melhorias em processos com definição de responsáveis e prazos de implementação, além de estabelecer Indicadores de Riscos (*KRI's)* de monitoramento.
  - Planejar: definir ações ou Controles que reduzam a Vulnerabilidade ou o Impacto em caso de materialização do Risco.
  - Monitorar: não há necessidade de definição de ação ou Controle para o Risco. É realizado monitoramento periódico para reavaliar sua classificação de Impacto e Vulnerabilidade.

4.3.5. Monitoramento dos Riscos

Assegurar a efetividade e adequação dos Controles internos e obter informações que proporcionem melhorias no processo de gerenciamento de Riscos. O monitoramento deve ser realizado por meio de avaliações contínuas e isentas.

Os Indicadores de Riscos (*KRI's*) são ferramentas de monitoramento para acompanhar os limites de exposição estabelecidos pela Companhia, assim como os Planos de Ação definidos pela 2ª linha em conjunto com os *Risk Owners*.

O monitoramento é importante para acompanhar se o grau do Risco foi alterado, identificar a possível necessidade de tratamento adicional e assegurar a efetividade da Gestão de Riscos da Companhia.

4.3.6. Informação e comunicação

Comunicar, de forma clara e objetiva a todas as partes interessadas, os resultados de todas as etapas do processo de gerenciamento de Riscos, de forma a contribuir para o entendimento da situação atual da efetividade dos Planos de Ação e proporcionar a conscientização e capacitação da cultura de Gestão de Riscos na Companhia.

5. RESPONSABILIDADES

5.1. Conselho de Administração:

- definir o nível de Apetite e a Tolerância a Riscos da Companhia, com base nos princípios e diretrizes aqui estabelecidos;
- aprovar a Política de Gestão de Riscos da Companhia e suas futuras revisões;
- aprovar, mediante proposta da Diretoria, o Mapa e a priorização de Riscos, bem como suas revisões;
- supervisionar e aprovar planos de Resposta a Riscos, quando necessário;
- supervisionar e manifestar-se sobre a avaliação da efetividade das políticas, dos sistemas de gerenciamento de Riscos e de Controles internos e aprovar eventuais sugestões de alterações, caso entenda necessário.

5.2. Diretoria:

- propor ao Conselho de Administração o nível de Apetite e Tolerância a Riscos da Companhia;
- assegurar o funcionamento do modelo de 3 Linhas no processo de Gestão de Riscos da Companhia;
- realizar a Gestão de Riscos (quer sejam identificados pela própria Diretoria ou reportados pela Área de *Compliance* e Riscos) conforme previsto nesta Política;
- validar o relatório de consolidação de Riscos da Companhia, reportando-o ao Conselho de Administração;
- acompanhar os Planos de Ação para mitigação da exposição ao Risco, bem como definir os respectivos responsáveis e prazos de implementação;
- manifestar-se sobre a avaliação da efetividade das políticas, dos sistemas de gerenciamento de Riscos e de Controles internos, e encaminhar tal avaliação para apreciação do Conselho de Administração; e
- manifestar-se sobre as sugestões de alteração ou sugerir alterações a esta Política, e recomendar ao Conselho de Administração sugestões de aprimoramento, caso entenda necessário.

5.3. Comissão de Sustentabilidade e Riscos:

- aprovar a metodologia a ser utilizada na condução do processo de Gestão de Riscos;
- aprovar os Planos de Ação de Riscos críticos e altos propostos pelas áreas de negócios para mitigação dos Riscos;
- acompanhar de forma sistemática a Gestão de Riscos, incluindo Indicadores de Riscos *(KRI's*), assim como o estágio de realização das ações definidas para mitigação dos Riscos;

- avaliar, periodicamente, a efetividade das políticas, dos sistemas de gerenciamento de Riscos e de Controles internos, e encaminhar tal avaliação para apreciação da Diretoria;
- avaliar, periodicamente, a adequação da estrutura operacional de Gestão de Riscos na verificação de sua efetividade, e recomendar à Diretoria sugestões de aprimoramento, caso entenda necessário;
- aprovar o relatório de consolidação de Riscos da Companhia preparado pela área de *Compliance* e Riscos Corporativos, reportando-o à Diretoria; e
- apreciar as exceções, eventuais violações e casos omissos a esta Política e encaminhá-los ao Conselho de Administração para sua deliberação e/ou aprovação, sendo tal comunicação enviada simultaneamente para ciência da Diretoria.

5.4. Áreas de Negócios:

- atuar diretamente na Gestão de Riscos de sua área, privilegiando: a identificação, avaliação, tratamento e monitoramento, de acordo com as diretrizes desta Política;
- realizar, em conjunto com a 2ª linha, o processo de avaliação de Riscos (*Self-Assessment*);
- reportar ativamente à 2ª linha alterações que possam impactar a Gestão de Riscos, como mudanças nos processos ou Controles, novos negócios, desinvestimentos de determinada operação, alterações relevantes nas rotinas ou objetivos e revisões de planejamentos;
- assegurar a implementação dos Planos de Ação definidos para tratamento dos Riscos;
- desenvolver, em conjunto com a Área de *Compliance* e Riscos Corporativos, Indicadores de monitoramento dos Riscos (*KRI's*), critérios de classificação e propostas de limite;
- reportar à Comissão de Sustentabilidade e Riscos as informações relacionadas às suas atividades no gerenciamento de Riscos e de conformidade;
- comunicar à Área de *Compliance* e Riscos Corporativos tempestivamente sobre Riscos antes não identificados, sejam eles novos ou não;
- aprovar as normas e procedimentos que direcionem as ações individuais na implementação dos conceitos de gerenciamento de Riscos na sua área de atuação, a fim de assegurar que as Respostas aos Riscos sejam executadas; e
- detalhar o Plano de Ação, alinhá-lo com a Área de *Compliance* e Riscos Corporativos e implantá-lo segundo a prioridade nele definida.

5.5. Auditoria Interna

- verificar, de forma independente e periódica, a adequação dos processos e procedimentos de identificação e gerenciamento dos Riscos, conforme as diretrizes estabelecidas nesta Política e em normativos internos; e
- apresentar ao Conselho de Administração os resultados das avaliações do sistema de Gestão de Riscos e efetividade dos Controles internos

5.6. Área de *Compliance* e Riscos Corporativos:

- propor responsabilidades relacionadas às atividades de Gestão de Riscos, assim como alçadas de aprovações e escopos de atuação;
- disponibilizar ferramentas, sistemas, infraestrutura e governança que suportam o gerenciamento de Riscos da Companhia;
- desenvolver a metodologia de Gestão de Riscos e submetê-la à aprovação da Comissão de Sustentabilidade e Riscos;
- conscientizar a 1ª linha sobre a importância da Gestão de Riscos e a responsabilidade inerente dos administradores e colaboradores da Companhia;
- coordenar as atividades de Gestão de Riscos junto às áreas da 1ª linha, mantendo independência no exercício de suas funções;
- desenvolver com os gestores de negócios modelos e/ou Indicadores de Riscos para monitoramento dos Riscos, critérios de classificação e propostas de limite;
- preparar relatórios periódicos de consolidação dos Riscos da Companhia e submetê-los à Comissão de Sustentabilidade e Riscos;
- apoiar os gestores de processo na definição dos Planos de Ação necessários para tratamento dos Riscos e assegurar a implementação dos Planos de Ação;
- disseminar o conhecimento e a cultura de Gestão de Riscos na Companhia;
- reportar as informações relacionadas às suas atividades de gerenciamento de Riscos à Comissão de Sustentabilidade e Riscos; e
- viabilizar os trabalhos de auditoria interna para assegurar seu reporte ao Conselho de Administração.
