

## POLÍTICA DE GESTÃO DE RISCOS E PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS DA SUMAUMA CAPITAL GESTÃO DE RECURSOS S.A.

### 1. INTRODUÇÃO

1.1 Esta Política de Gestão de Riscos e Plano de Contingência e Continuidade dos Negócios (“Política”) da Sumauma Capital Gestão de Recursos S.A. (“Sumauma Capital”) tem por objetivo estabelecer a política de gestão de riscos de mercado, riscos operacionais e riscos de liquidez, bem como estabelecer um plano de contingência e de continuidade dos negócios da Sumauma Capital, possibilitando assim que a instituição continue exercendo suas atividades e serviços mesmo em cenários de crise.

### 2. CONTROLE DE RISCOS

2.1 Visando estabelecer os fundamentos associados aos riscos, realizamos a seguinte subdivisão:

- (i) **Risco de Mercado/Concentração:** Para efeitos deste manual, entende-se o risco de mercado como a possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição em câmbio, taxas de juros, ações e mercadorias (*commodities*). Define-se o gerenciamento de risco de mercado como o processo contínuo de identificação, avaliação, monitoramento e controle das exposições decorrentes de posições detidas em tais ativos (Concentração) com o objetivo de mantê-los dentro dos limites regulatórios e dos limites estabelecidos por mandato.
- (ii) **Risco Operacional:** entende-se o risco de operacional como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos, riscos de natureza jurídica associados a contratos e acordos firmados pela empresa, bem como eventuais penalidades em razão de descumprimento de dispositivos legais e indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Sumauma Capital. Dentre os riscos operacionais estão: erros e práticas irregulares internas e externas, demandas trabalhistas, práticas inadequadas perante clientes, fornecedores e órgãos reguladores, quaisquer falhas que impactem a atividade desenvolvida pela empresa e

falhas em sistemas tecnológicos. O Diretor de Compliance e Risco é responsável por monitorar o risco operacional e reportar eventuais ocorrências no Comitê de Compliance e Riscos.

- (iii) **Risco de Liquidez:** entende-se por risco de liquidez (i) a possibilidade de a instituição não ser capaz de honrar efetivamente suas obrigações esperadas e inesperadas, correntes e futuras, inclusive as decorrentes de vinculação de garantias, sem afetar suas operações e sem incorrer em perdas significativas; e (ii) a possibilidade de a instituição não conseguir negociar a preço de mercado uma posição, devido ao seu tamanho elevado em relação ao volume normalmente transacionado ou em razão de alguma descontinuidade no mercado. Define-se o gerenciamento de risco de liquidez como o processo contínuo de identificação, avaliação, monitoramento e controle dos riscos associados, considerando os possíveis impactos na liquidez oriundos de distorções ou necessidades de caixa.
  
- (iv) **Risco de Crédito/Contraparte:** O Risco de Crédito consiste na possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas respectivas obrigações financeiras nos termos pactuados. Ao considerar o foco estratégico da Sumauma Capital, é possível observar que são poucos os momentos nos quais existem exposição a crédito privado, tais como contrapartes em operações de derivativos de balcão, empréstimo de ações fora do mercado de bolsa, aquisição de instrumentos com risco de crédito privado. O controle do Risco de Crédito privado da Sumauma Capital é feito por meio de análise de exposição por emissor, através da consolidação de posições de ativos e derivativos de um mesmo emissor. Os emissores que podem compor a carteira dos fundos devem ser aprovados e acompanhados pelo Comitê de Compliance e Riscos.
  
- (v) **Risco legal:** é possível que ocorram perdas decorrentes de multas, penalidades ou indenizações devidas a clientes e/ou órgãos reguladores ou de autorregulação, bem como perdas em processos administrativos ou judiciais. Para evitar esses riscos, os Colaboradores deverão acessar diariamente periódicos e informativos de órgãos reguladores e autorreguladores, entidades de classe e escritórios de advogados e, caso necessário, realizar a contratação de escritórios especializados para gerenciar eventuais questões jurídicas referentes ao exercício de suas funções.

- (vi) **Risco cibernético:** a Sumauma Capital compreende a possibilidade de riscos associados à estrutura de armazenamento de informações. Neste sentido, eventuais ataques cibernéticos podem ameaçar a integridade, confidencialidade e disponibilidade de informações, bem como dados empresariais e de clientes. Além das disposições já contidas no Manual de *Compliance* da Sumauma Capital, é importante que tais riscos sejam identificados por meio de um processo de análise de vulnerabilidades, ameaças e impactos relativos às informações da empresa, para que sejam recomendadas as proteções adequadas. Os cenários de riscos cibernéticos e de segurança da informação serão apontados, conforme o caso, pelo Comitê de *Compliance* para decisão e determinar eventuais ações de prevenção e proteção. Qualquer potencial ataque deverá ser prontamente informado à área de *Compliance* para providências.

### 3. ESTRUTURA E RESPONSABILIDADES

- 3.1 A responsabilidade pelos controles de riscos é do Diretor de Riscos devidamente designado no estatuto social da Sumauma Capital e junto à Comissão de Valores Mobiliários (CVM). O Diretor de Risco atua com total independência em relação à equipe de gestão no exercício desta Política e no cumprimento de suas responsabilidades, observadas as diretrizes que sejam aprovadas no Comitê de *Compliance* e Riscos, cujo funcionamento é disciplinado pelo Manual de *Compliance* da Sumauma Capital.

### 4. SISTEMAS E FERRAMENTAS

- 4.1 O sistema para o gerenciamento e controles de riscos será automatizado, contendo métricas para o controle de risco de mercado, liquidez e enquadramento dos fundos geridos pela Sumauma Capital. Além desses sistemas, são utilizadas informações obtidas junto ao(s) administrador(es) do(s) fundo(s) gerido(s) pela Sumauma, corretoras e, também, aos sistemas de informações de mercado (ex: Broadcast).

### 5. MONITORAMENTO E PLANO DE AÇÃO

- 5.1 O monitoramento dos riscos é realizado diariamente pelo Diretor de *Compliance* e Riscos que também irá disponibilizar acesso aos sistemas e ferramentas para

que a equipe de gestão acompanhe os riscos principalmente os de Mercado, Concentração, Liquidez e Enquadramento.

- 5.2 Eventuais desenquadramentos ativos deverão ser ajustados imediatamente e no caso de desenquadramentos passivos deve ser definido pela equipe de gestão um plano de ação que deverá ser aprovado pelo Diretor de *Compliance* e Riscos, observadas as disposições legais, regulatórias e autorregulatórias aplicáveis. Qualquer situação diferente das descritas anteriormente deverá ser levada aos membros do Comitê de *Compliance* e Riscos para uma decisão que deverá ser unânime e formalizada e arquivada.

## 6. LIMITES

### RISCO DE MERCADO/CONCENTRAÇÃO

- 6.1 Considerando a característica de gestão e dos produtos da Sumauma Capital, apesar do acompanhamento diário de métricas de risco de mercado como Var e Stress, os limites foram definidos em relação à exposição total do fundo e concentração por papel de um mesmo emissor (não aplicável a cotas de fundos e derivativos):

<b>Limite de exposição total:</b>	Entre -50% e 150%
<b>Limite de concentração por emissor:</b>	Entre -20% e 20%

- 6.2 Em caso de estrutura “Master-Feeder” os controles de Risco de Mercado são realizados no veículo “Master”.

### RISCO DE LIQUIDEZ

- 6.3 Os controles de Risco de Liquidez estão descritos no Manual de Liquidez da Sumauma Capital.

## 7. PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

- 7.1 O constante monitoramento das atividades da Sumauma Capital garante que em caso de ocorrência de contingências seja possível retomar as operações com os menores custos de transação, perdas de tempo e de recursos físicos e materiais possíveis. Para tanto, a Sumauma Capital mantém o backup permanente de todas suas informações, de tal modo que seja possível recuperá-las rapidamente;

mantém uma lista de fornecedores que possam prontamente atender às solicitações e providenciar os equipamentos danificados ou a reparação necessária; e vislumbra em seus comitês riscos possíveis e planos de ação caso tais riscos se verifiquem.

- 7.2** Para evitar contingências operacionais, a Sumauma Capital deverá manter um contingente de pessoal apto a realizar os trabalhos necessários; manter prestadores de serviços e fornecedores tanto quanto necessário para suprir as demandas da empresa; manter ampla sua base de clientes para garantir a continuidade da empresa em caso de perdas de clientes; executar as políticas estratégicas estabelecidas pelo Comitê Estratégico para que os riscos mercadológicos sejam mitigados; manter um fluxo de caixa que permita a continuidade da empresa em casos de perdas de clientes; também serão utilizados no-breaks com autonomia de 30 minutos para que seja concedido o tempo necessário a ações voltadas a mitigar riscos decorrentes de questões operacionais.
- 7.3** As crises possíveis a serem enfrentadas pela Sumauma Capital durante o exercício de suas atividades regulares incluem: perda de acesso ao escritório físico, perda de acesso às informações armazenadas em ambiente virtual, perda de Colaboradores, falhas operacionais resultantes de erros humanos ou problemas eletrônicos, queda de energia elétrica, acidentes dentro e fora do escritório, roubo, sabotagem, bem como outras crises geradas por caso fortuito ou força maior.
- 7.4** A Sumauma Capital estabelecerá local alternativo para processamento em situações de contingência com estrutura física e tecnológica adequadas, assim como versões de sistemas idênticas às do local de processamento principal, e que esteja localizado a uma distância razoável do local de processamento principal, assegurando a continuidade das suas atividades;
- 7.5** Em caso de crise, três etapas são necessárias: gestão de crise, recuperação e retomada.
- 7.5.1** A gestão de crise será realizada por meio de reunião extraordinária convocada exclusivamente para discutir acerca do ocorrido, visando compreender os motivos da crise, quais consequências ela gerou e/ou continua gerando, como manter as pessoas seguras, qual a dimensão do problema, se é necessário alguma comunicação oficial referente a crise que deve ocorrer naquele momento ou

chamar ajuda externa, se é necessário evacuar o prédio e/ou tomar qualquer providência imediata e, por fim, estabelecer os responsáveis por executar medidas necessárias para conter a crise.

**7.5.2** A recuperação consiste na aplicação dos planos desenvolvidos para o enfrentamento da crise e incluem a recuperação das estruturas e/ou informações perdidas, bem como a tentativa de restabelecer a normalidade das atividades da Sumauma Capital.

**7.5.2.1** A recuperação inicia-se quando a situação de normalidade for estabelecida, devendo, neste caso, novas medidas serem implementadas para evitar novas crises similares, caso aplicável. A fase de recuperação envolve a realização de reunião do Comitê de Compliance e Riscos para avaliar os impactos da crise e a necessidade de realizar informativos aos clientes, fornecedores e Colaboradores.

**7.5.3** A área de Compliance conduzirá, eventualmente com auxílio de terceiros contratados, validações e testes relativos aos itens estabelecidos nesta política, em intervalos mínimos de 12 meses ou periodicidade menor, conforme necessário.

## **8. VIGÊNCIA E ATUALIZAÇÃO**

**8.1** Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Elaborado por:	Matheus Soares Salgado Nunes de Matos.
Versão	5
Data:	Jun-2020
Revisado em:	Jun-2026