



POLÍTICA DE GESTÃO DE RISCOS

POLÍTICA DE DEFINIÇÃO E RESPONSABILIDADES PARA A GESTÃO DE RISCOS

Sumário

1.	Objetivo.....	3
2.	Definições.....	3
3.	Ferramenta Suporte	5
4.	Conteúdo.....	5
5.	Referências.....	11
6.	Anexos	11

**POLÍTICA DE DEFINIÇÃO E
RESPONSABILIDADES PARA A GESTÃO DE RISCOS
DA IGUATEMI EMPRESA DE SHOPPING CENTER S.A.
("POLÍTICA DE GESTÃO DE RISCOS")**

1. Objetivo

- 1.1. Esta Política define diretrizes e responsabilidades para a Gestão de Riscos da Iguatemi ("Companhia"), integrando o processo decisório ao planejamento estratégico e à definição de apetite a risco, com foco em proteger e gerar valor à Companhia.
- Com isso, o documento visa promover na organização uma linguagem comum de gerenciamento de riscos, facilitando a disseminação do conhecimento e incorporando a Gestão de Riscos na cultura da Companhia.

2. Definições

Riscos: quaisquer eventos que, se materializados, podem impedir o alcance de objetivos específicos/ planejamento estratégico da Companhia. Abrange uma visão/ escopo de verificação da cadeia de forma integral, inclusive riscos e fatores de riscos que podem estar associados a outros *stakeholders*.

Fator de risco: ocorrência de evento ou alteração de um conjunto específico de circunstâncias que contribuem para que eventualmente um risco se materialize. O mesmo risco pode conter um ou mais fatores relacionados.

Oportunidade: refere-se a uma situação ou evento que, se aproveitado, pode levar a um resultado positivo ou benefício para a organização. Diferente dos riscos, que são potenciais ameaças, as oportunidades são potenciais ganhos que podem ser identificados e explorados para melhorar o desempenho, aumentar a eficiência ou alcançar objetivos estratégicos.

Risco Estratégico: riscos que possam impactar no alcance dos objetivos estratégicos e a execução da estratégia planejada.

Risco Operacional: risco de perda resultante de processos internos, pessoas e sistemas inadequados ou falhos, ou de eventos externos.

Risco Corporativo: riscos estratégicos e operacionais de uma Companhia.

Risco Inerente: é o risco intrínseco à atividade exercida pela Companhia. São aqueles que a Companhia está exposta, desconsiderando as ações (atividades de controle) que possam reduzir sua probabilidade e/ ou impacto.

Risco Residual: é o risco que permanece mesmo após a adoção de medidas utilizadas na mitigação do impacto e/ ou probabilidade de materialização do risco inerente.

Risco Emergente: risco novo ou em evolução que pode impactar significativamente uma organização, mas que ainda não é totalmente compreendido ou quantificado, caracterizado pela sua incerteza e complexidade.

Impacto: representação quantitativa e qualitativa da consequência do risco, caso venha se materializar.

Probabilidade: a probabilidade refere-se à chance de um risco específico se concretizar.

Exposição ao risco: é a classificação do risco avaliado em função do seu impacto e probabilidade, podendo ser Muito Alto, Alto, Médio e Baixo.

Apetite a risco: nível ao qual a Companhia está disposta a se expor em relação ao(s) risco(s) para cumprir seus objetivos estratégicos e agregar valor ao negócio.

Resposta do Risco: definição do tratamento que a Companhia dará ao risco residual.

Dicionário de riscos: catálogo de apresentação dos riscos devidamente organizado por natureza.

Dono do risco: colaborador que possui autoridade e responsabilidade para gerenciar o risco.

Elaboração de Cenários: processo para identificar, avaliar e projetar possíveis resultados de eventos futuros em situações de incerteza.

Matriz de Riscos: demonstração gráfica com base na análise geral dos riscos e de autoavaliação da Administração, em que são analisados os riscos da empresa, considerando impacto e probabilidade para sua materialização.

Key Risk Indicator (KRIs): componentes do processo de monitoramento de riscos, utilizados para fornecer indicadores antecipados (preventivos) ou atrasados (detectivos) de condições de risco em potencial.

Plano de Ação: proposta de melhoria ou correção de desvios e fatores de riscos identificados, com a finalidade de redução da probabilidade e impacto de materialização do risco a um limite que seja aceito pela Companhia.

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*): organização reconhecida mundialmente por prover diretrizes relacionadas a aspectos críticos de governança corporativa, ética nos negócios, Controles Internos, Gerenciamento de Riscos Corporativos e dissuasão de fraude.

ISO 31000:2018: norma criada com o objetivo de estabelecer uma padronização na Gestão de Riscos entre as Companhias, bem como das melhores práticas e abordagens para sua implantação.

IBGC (Instituto Brasileiro de Governança Corporativa): sugere as melhores práticas de governança corporativa, envolvendo especialistas do tema.

3. Ferramenta Suporte

N/A

4. Conteúdo

4.1. Abrangência

Esta Política se aplica a todas as empresas do Grupo Iguatemi S.A.

4.2. Diretrizes

4.2.1. Contexto

As organizações enfrentam diversos riscos relacionados à sustentabilidade, corrupção, fraude, ética nos negócios e reputação. No setor da Iguatemi, esses riscos são ampliados por fatores econômicos, sociais e operacionais, como flutuações econômicas, mudanças no comportamento do consumidor, inovações tecnológicas e eventos sociais e políticos.

Como consequência da condução de seus negócios, a Iguatemi assume riscos que, se não identificados e tratados de forma adequada, podem comprometer a sustentabilidade e perenidade dos seus negócios. Logo, é essencial estabelecer uma metodologia integrada com ferramentas, métricas, atividades e controles que suportem o processo de gestão de riscos, abrangendo todas as possíveis áreas de impacto.

Como o risco é inerente a qualquer atividade e impossível de eliminar, sua administração é primordial para não afetar as perspectivas da entidade. As atividades de gerenciamento de riscos corporativos devem ser vistas como fundamentais para a longevidade da organização e para a realização de seus objetivos, sejam eles de curto, médio e longo prazo (definidos de acordo com o Planejamento Estratégico da Iguatemi), além de ser analisadas à luz da realidade e do momento de cada entidade.

4.2.2. Sistema de Gestão de Riscos Iguatemi

Alinhado às melhores práticas de mercado, o Sistema de Gestão de Riscos Iguatemi adota como parte integrante da sua metodologia os *frameworks* COSO ERM, ISO 31.000:2018 e as diretrizes do IBGC. Essa abordagem combina critérios objetivos de avaliação com a visão estratégica da empresa.

Sendo assim, o processo de gestão de riscos da Iguatemi, está estruturado de acordo com as seguintes etapas:

4.2.2.1. Escopo, Contexto e Critérios

O contexto é estabelecido através da compreensão do ambiente interno, fundamentado no Planejamento Estratégico da Iguatemi e em seus objetivos, bem como do ambiente externo, relacionado aos fatores macroeconômicos, políticos, sociais, de sustentabilidade, tendências do setor,

concorrência, *benchmarking*, histórico com eventos de riscos materializados e notícias vinculadas na mídia.

4.2.2.2. Identificação de Riscos

A etapa de identificação de riscos e oportunidades envolve entender, reconhecer e registrar os riscos e fatores de risco estratégicos. O objetivo é identificar eventos que possam afetar os objetivos estratégicos da Iguatemi, levando em conta aspectos quantitativos e qualitativos.

Essa identificação geralmente é realizada por meio de reuniões periódicas (AGR – Análise Geral de Riscos) ou outras abordagens que se façam necessárias, com os principais executivos da empresa e membros independentes dos Comitês e Conselho. Além disso, são considerados os cenários internos e externos (incluindo riscos emergentes), bem como os resultados dos trabalhos de auditorias e controles internos.

4.2.2.3. Análise e Avaliação dos Riscos

A análise é realizada com base nos riscos e seus fatores, descritos no dicionário de riscos da Companhia, classificados conforme a natureza identificada: Estratégico, Financeiro, Operacional, Conformidade, Cyber e ESG (ambiental, social e governança).

A avaliação do risco identificado envolve a análise dos fatores de risco capturados e, quando aplicável, a criação de cenários. Esses elementos são combinados com a análise do possível impacto e sua probabilidade. Essa avaliação resulta na criação da Matriz de Riscos, que fornecem um mecanismo para priorizar esses riscos e direcionar os esforços para minimizar os riscos mais relevantes. As métricas para avaliar o impacto, a probabilidade e a exposição aos riscos são detalhadas em procedimento interno específico.

4.2.2.4. Tratamento dos Riscos

Após a avaliação dos riscos, é definido o tratamento a ser adotado, considerando as seguintes ações:

- i. Reduzir: implementar planos de ações/ controles que possam diminuir as causas ou as consequências dos riscos.
- ii. Compartilhar: definir ações que visam reduzir a probabilidade de ocorrência e/ ou impacto do risco, por meio da transferência ou compartilhamento total ou parcial do risco a terceiros, como, por exemplo, contratação de apólices de seguro, outsourcing etc.
- iii. Eliminar: consiste em descontinuar ou não se envolver com uma situação de risco (ex.: descontinuar uma operação).
- iv. Aceitar: a aceitação do risco pode ocorrer quando:
 - a. Se reconhece que a perda potencial de um risco não é suficientemente grande para justificar as possíveis ações mitigatórias.
 - b. Em situações em que o custo da ação mitigatória ultrapasse a exposição ao risco.
 - c. Por estratégia do negócio.

Para todas as situações descritas na resposta "Aceitar", é necessária a aprovação formal da instância de reporte, conforme a classificação final do risco (ver figura 1 a seguir). Caso a instância responsável concorde, o dono do risco fica isento da criação do plano de ação. No entanto, a área de Gestão de Riscos continua monitorando o risco em questão para garantir que a exposição não aumente.

Muito Alto	Conselho de Administração ¹
Alto	VPS/ CEO
Médio	Diretoria
Baixo	Gerência

¹ Devidamente recomendando pelo Comitê de Riscos e Compliance (CRC) e Comitê de Auditoria (COAUD).

Figura 1 – Exposição do Risco x Instância de Reporte

4.2.2.5. Monitoramento e Análise Crítica

O monitoramento e a análise crítica dos riscos, incluindo o reporte periódico aos órgãos de assessoramento do Conselho de Administração, são realizados pela área de Gestão de Riscos e o Dono do Risco. Neste reporte, são apresentados a evolução dos planos de ação/ controles e indicadores-chave de riscos (KRIs), quando aplicável, além da definição de novas ações para condução e/ ou mitigação.

A prorrogação dos prazos para a implementação dos planos de ação será permitida apenas com a devida autorização da instância responsável, acompanhada de sua correspondente justificativa aprovada pelo responsável da área, conforme tabela de alçada e detalhamentos a seguir:

<i>Classificação do Risco</i>	<i>Gerência</i>	<i>Diretoria</i>	<i>VP/ CEO</i>	<i>Conselho de Administração</i>
MUITO ALTO				X
ALTO			X	
MÉDIO		X		
BAIXO	X			

MUITO ALTO: a postergação somente será permitida se devidamente alinhada com o Comitê de Riscos e Compliance que submeterá ao Conselho de Administração.

ALTO: a postergação será permitida apenas 1 (uma) vez, desde que devidamente aprovada pela Vice-Presidência responsável e/ ou CEO que deverá submeter a justificativa ao Comitê de Riscos e Compliance.

MÉDIO: a postergação poderá ser realizada até 2 (duas) vezes, sendo a primeira com a devida aprovação da VP responsável e a segunda incluindo a aprovação do CEO.

BAIXO: a postergação poderá ser realizada quantas vezes forem necessárias, com a devida aprovação da Diretoria responsável.

Adicionalmente, a Companhia mantém outras atividades contínuas de monitoramento, realizadas pela área de Auditoria Interna ou por empresas terceirizadas (ex.: Auditoria Externa). A Iguatemi também realiza, com o envolvimento de seus executivos e membros independentes, a revisão anual de seus riscos, para reavaliar o alinhamento à sua estratégia e verificar continuamente a implementação e os resultados das medidas mitigadoras.

4.2.2.6. Comunicação e Consulta

A Iguatemi divulga informações dos seus riscos às partes interessadas de maneira que facilite a execução das responsabilidades dos colaboradores, incluindo a apresentação das informações em formatos adequados e dentro de prazos que permitam uma tomada de decisão assertiva. A Companhia assegura que essas informações sejam relevantes, transparentes, disponíveis, acessíveis e precisas.

Para garantir a integridade e a eficácia do processo de gestão de riscos, a área de Auditoria Interna tem a autonomia para realizar auditorias a qualquer momento.

4.3. Responsabilidades

4.3.1. Conselho de Administração

- i. Aprovar as diretrizes da estrutura de governança corporativa de gestão de riscos da Companhia, incluindo metodologia, políticas, processos, sistemas, integração com o Planejamento Estratégico, entre outros, quando devidamente recomendados pelo Comitê de Riscos e Compliance.
- ii. Monitorar o cumprimento das metodologias estabelecidas, as ações mitigatórias e os planos de ação dos riscos inerentes, especialmente aqueles que extrapolam o apetite ao risco da Companhia.
- iii. Apoiar as ações de conscientização dos gestores e colaboradores sobre a importância da gestão de riscos e a responsabilidade atribuída aos envolvidos no gerenciamento dos riscos da Companhia.
- iv. Assegurar a adequada gestão desta política, bem como a efetividade e a continuidade de sua aplicação.

4.3.2. Comitê de Riscos e Compliance

- i. Avaliar o processo de gerenciamento de riscos, incluindo metodologia, processos, sistemas, política e mecanismos de reporte, solicitando ajustes quando necessário e recomendando ao Conselho de Administração.
- ii. Acompanhar o mapeamento realizado pela gestão da Companhia, de todos os tipos de riscos relevantes, classificando-os segundo seus graus de impacto, sua probabilidade de ocorrência, sua origem e sua sensibilidade a ações preventivas ou mitigantes.
- iii. Reportar ao Conselho de Administração as exceções às diretrizes do processo de Gestão de Riscos e outros assuntos considerados relevantes.
- iv. Acompanhar o planejamento da Gerência de Riscos e Controles Internos, solicitando ajustes quando necessário, monitorando a execução do trabalho e avaliando a qualidade e efetividade do processo.

- v. Avaliar e monitorar as exposições e o gerenciamento dos riscos da Companhia.
- vi. Verificar se a administração está adotando os controles necessários para o gerenciamento de riscos que se julgue necessário um plano de ação para redução da sua exposição.
- vii. Recomendar ações para disseminar internamente a cultura de sensibilidade a riscos.

4.3.3. Comitê de Auditoria e Partes Relacionadas

- i. Avaliar e monitorar as exposições de risco da Companhia, solicitando reporte periódicos para conhecimento e eventual contribuição.
- ii. Opinar e recomendar, quando requerido, no processo de gerenciamento de riscos desde que devidamente acordado com o Comitê de Riscos e Compliance.
- iii. Opinar e recomendar, quando requerido, ações para disseminação da cultura de gestão de riscos.
- iv. Acompanhar as atividades de controles internos, uma vez que os planos de ação sejam implementados e façam parte da Matriz de Riscos e Controles (MRC).
- v. Garantir que o Plano de Auditoria Interna está baseado na Matriz de Riscos da Iguatemi.

4.3.4. Comitê de Pessoas, Cultura e ESG

- i. Conhecer e contribuir na definição da régua de impacto ESG (Ambiental, Social e Governança) para classificação dos riscos estratégicos.
- ii. Acompanhar o monitoramento realizados pelos donos de riscos conjuntamente com a Gerência de Riscos e Controles Internos as exposições das categorias de riscos/ fatores de riscos de ESG.
- iii. Propor planos de ação para mitigação de riscos ESG, quando requerido pelos donos dos riscos e/ ou Gerência de ESG.

4.3.5. Diretoria/ VPs e CEO

- i. Participar do processo de gerenciamento de riscos da Iguatemi, em concordância com a Política (papéis, responsabilidades, processos, entre outros) e garantir que esteja alinhado às boas práticas de Gestão de Riscos.
- ii. Auxiliar na disseminação da cultura do gerenciamento de risco.
- iii. Conhecer e contribuir na definição do apetite a risco (impacto financeiro), assim como nos demais critérios qualitativos.
- iv. Conhecer e contribuir na revisão do dicionário de riscos estratégicos.
- v. Indicar os riscos que serão priorizados para avaliação do Comitê de Riscos e Compliance e aprovação do Conselho de Administração.
- vi. Promover periodicamente ciclos de avaliação e revisões ao processo de gerenciamento de riscos (agentes internos ou externos), de modo a assegurar a eficácia do gerenciamento e do monitoramento dos riscos.

4.3.6. Gerência de Riscos e Controles Internos

- i. Disseminar o conhecimento de gestão de riscos aos colaboradores e integrantes dos órgãos independentes, com o objetivo de promover a cultura de gerenciamento de riscos, via trilha de capacitação por nível hierárquico, além de workshops ou outras capacitações que se julgue necessárias.

- ii. Propor diretrizes para a estrutura de governança corporativa de gestão de riscos da Companhia, incluindo metodologia, processos, sistemas, entre outros.
- iii. Estabelecer e manter atualizada a Política e Procedimento de Gestão de Riscos, bem como os padrões e mecanismos próprios de reporte de informações.
- iv. Assegurar que os gestores de riscos identifiquem, mitiguem e monitorem os riscos da Companhia, garantindo a integridade dos controles internos.
- v. Avaliar periodicamente os planos de ação, realizando testes e ajustes necessários, conforme reuniões com os gestores de riscos, e estabelecendo prazos e responsáveis pela execução e reporte das ações mitigatórias.
- vi. Aprimorar a metodologia de cálculo do apetite a risco, avaliando a probabilidade e o impacto dos riscos mapeados da Companhia.
- vii. Colaborar com os executivos e integrantes dos órgãos independentes na discussão sobre a definição do apetite a risco aceitável da Companhia.
- viii. Coordenar e monitorar o processo de identificação e avaliação dos riscos junto aos executivos da Companhia.
- ix. Atualizar e revisar periodicamente os fatores de risco, especialmente quando houver atualizações no planejamento estratégico e/ou quando ocorrerem fatos relevantes.
- x. Acompanhar e reportar mudanças na criticidade dos riscos ao Comitê de Riscos e Compliance, Comitê de Auditoria e Partes Relacionadas (quando requerido) e Conselho de Administração.
- xi. Apresentar ao Comitê de Riscos e Compliance e ao Comitê de Auditoria e Partes Relacionadas (quando requerido) os riscos a serem priorizados e os planos de ação propostos.
- xii. Avaliar periodicamente a Matriz de Riscos da Companhia com uma visão independente da área de negócio, consolidada, abrangente (considerando eventuais riscos emergentes) e integrada, bem como o apetite a riscos, recomendando ao Comitê de Riscos e Compliance os ajustes e atualizações necessárias.

4.3.7. Donos dos Riscos

- i. Gerenciar os riscos sob sua responsabilidade, identificando alterações nos ambientes externos e internos que possam impactá-los e avaliando a necessidade de planos de ação para garantir o correto tratamento.
- ii. Implementar as ações necessárias para a mitigação dos riscos, com o envolvimento de outras áreas, alinhadas ao plano de ação validado pela Gerência de Riscos e Controles Internos.
- iii. Realizar revisões técnicas periódicas dos riscos, dos fatores a eles relacionados, das respostas e das avaliações dos riscos.
- iv. Reportar periodicamente à Gerência de Riscos e Controles Internos sobre a evolução dos riscos sob sua responsabilidade, mudanças significativas nos fatores de risco ou em qualquer outra característica, além da identificação de novos riscos anteriormente não mapeados.
- v. Manter um ambiente de controle efetivo sobre os riscos sob sua responsabilidade, evidenciando as ações implementadas.

4.3.8. Auditoria Interna

De acordo com a definição do Instituto dos Auditores Internos (IIA), a Auditoria Interna na Companhia deve examinar e auditar a conformidade dos atos e fatos administrativos, avaliando processos, controles internos e gerenciamento de riscos. Assim, ela atuará como a Terceira Linha, apoiando a estruturação e o funcionamento adequado da Primeira Linha (Áreas de Negócios) e da Segunda Linha (Controles Internos e Gestão de Riscos), ou seja, ela analisa as duas linhas anteriores de forma independente, identificando as oportunidades de melhoria aplicáveis.

5. Referências

- i. Código de Conduta Ética – Iguatemi.
- ii. Política de *Due Diligence* de Terceiros – Iguatemi.
- iii. Estatuto Social – Iguatemi.
- iv. Regimento Interno do Conselho de Administração – Iguatemi.
- v. Regimento Interno do Comitê de Auditoria e Partes Relacionadas – Iguatemi.
- vi. Regimento Interno do Comitê de Riscos e Compliance – Iguatemi.
- vii. Relatório de Sustentabilidade – Iguatemi.
- viii. IFRS S1.
- ix. IFRS S2.
- x. Instrução CVM 80.
- xi. Instrução CVM 552.
- xii. Instrução CVM 586.
- xiii. Regulamento do Novo Mercado.
- xiv. Ofício Circular da CVM SEP 01/17.
- xv. COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework).
- xvi. Caderno de Governança Corporativa – Gerenciamento de Riscos Corporativos (Evolução em Governança e Estratégia).
- xviii. ISO (International Organization for Standardization) 31.000.
- xix. IIA (The Institute of Internal Auditors).

6. Anexos

N/A

7. Informações de Controle

7.1. Responsáveis pelo documento

Responsável	Área
Elaboração	Gerência de Riscos e Controles Internos
Revisão	Vice-Presidência Jurídica e CEO
Aprovação	Conselho de Administração

7.2 Registro de Versões

Versão	Data da Publicação
1ª	01/09/2022



IGUATEMI



IGUATEMI

RISK MANAGEMENT POLICY

RISK MANAGEMENT ROLES AND RESPONSABILITIES POLICY

Summary

1.	Objective	3
2.	Definitions	3
3.	Support Tool.....	5
4.	Content.....	5
5.	References.....	11
6.	Appendices	11

RISK MANAGEMENT

ROLES AND RESPONSABILITIES POLICY

1. Objective

This Policy establishes guidelines and responsibilities for Iguatemi's ("Company") Risk Management, integrating the decision-making process into strategic planning and risk appetite definition, aiming to protect and create value for the Company. It also promotes a common risk management language within the organization, facilitating knowledge dissemination and embedding Risk Management into the Company's culture.

2. Definitions

Risk: Any event which, if materialized, may hinder the achievement of specific objectives or the Company's strategic planning. This definition encompasses a comprehensive and integrated view of the value chain, including risks and risk factors that may be associated with other stakeholders.

Risk Factor: the occurrence of an event or a change in a specific set of circumstances that contributes to the potential materialization of a risk. A single risk may involve one or more related factors.

Opportunity: refers to a situation or event that, if leveraged, may result in a positive outcome or benefit for the organization. Unlike risks, which represent potential threats, opportunities are potential gains that can be identified and explored to enhance performance, increase efficiency, or achieve strategic objectives.

Strategic Risk: Risks that may impact the achievement of strategic objectives and execution of the planned strategy.

Operational Risk: Risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.

Corporate Risk: Strategic and operational risks of a Company.

Inherent Risk: the intrinsic risk associated with the Company's activities. It refers to exposures the Company faces before considering any control measures that may reduce their likelihood and/or impact. **Risk:** Any event which, if materialized, may hinder the achievement of specific objectives or the Company's strategic planning. This definition encompasses a comprehensive and integrated view of the value chain, including risks and risk factors that may be associated with other stakeholders.

Risk Factor: the occurrence of an event or a change in a specific set of circumstances that contributes to the potential materialization of a risk. A single risk may involve one or more related factors.

Opportunity: refers to a situation or event that, if leveraged, may result in a positive outcome or benefit for the organization. Unlike risks, which represent potential threats, opportunities are potential gains that can be identified and explored to enhance performance, increase efficiency, or achieve strategic objectives.

Strategic Risk: Risks that may impact the achievement of strategic objectives and execution of the planned strategy.

Operational Risk: Risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.

Corporate Risk: Strategic and operational risks of a Company.

Inherent Risk: the intrinsic risk associated with the Company's activities. It refers to exposures the Company faces before considering any control measures that may reduce their likelihood and/or impact.

Residual Risk: the risk that remains even after the implementation of measures aimed at mitigating the impact and/or likelihood of the inherent risk materializing.

Emerging Risk: A new or evolving risk that may significantly impact organization, but it is not yet fully understood or quantified, characterized by its uncertainty and complexity.

Impact: Quantitative and qualitative representation of the consequences of a risk if materialized.

Probability: Likelihood of a specific risk occurring.

Risk Exposure: Classification of risk based on impact and probability (Very High, High, Medium, Low).

Risk Appetite: The level of risk the Company is willing to accept to achieve strategic objectives and create value.

Risk Response: Definition of the treatment the Company will give to residual risk.

Risk Dictionary: Catalog presenting risks, organized by nature.

Risk Owner: Employee with authority and responsibility to manage the risk.

Scenario Development: Process for identifying, evaluating, and projecting possible outcomes of future events in uncertain situations.

Risk Matrix: Graphical representation based on the overall risk analysis and self-assessment by Management, analyzing company risks considering impact and probability of materialization.

Key Risk Indicator (KRIs): Components of the risk monitoring process, used to provide early (preventive) or delayed (detective) indicators of potential risk conditions.

Action Plan: Proposal for improvement or correction of identified deviations and risk factors, aiming to reduce the probability and impact of risk materialization to an acceptable limit for the Company.

COSO (Committee of Sponsoring Organizations of the Treadway Commission): Globally recognized organization providing guidelines on critical aspects of corporate governance, business ethics, Internal Controls, Corporate Risk Management, and fraud deterrence.

ISO 31000:2018: Standard created to establish risk management standardization among companies, as well as best practices and approaches for implementation.

IBGC (*Instituto Brasileiro de Governança Corporativa*): Suggests best practices in corporate governance, involving subject matter experts.

3. Support Tool

N/A

4. Content

4.1. Scope

This Policy applies to all companies within the Iguatemi S.A. Group.

4.2. Guidelines

4.2.1. Context

Organizations face various risks related to sustainability, corruption, fraud, business ethics, and reputation. In Iguatemi's sector, these risks are amplified by economic, social, and operational factors, such as economic fluctuations, changes in consumer behavior, technological innovations, and social and political events.

As a consequence of conducting its business, Iguatemi assumes risks that, if not properly identified and managed, may compromise the sustainability and longevity of its operations. Therefore, it is essential to establish an integrated methodology with tools, metrics, activities, and controls that support the risk management process, covering all possible areas of impact.

Since risk is inherent to any activity and impossible to eliminate, its management is essential to avoid affecting the entity's prospects. Corporate risk management activities should be viewed as fundamental to the organization's longevity and achievement of its objectives, whether short, medium, or long term (as defined by Iguatemi's Strategic Planning), and should be analyzed considering each entity's reality and timing.

4.2.2. Iguatemi Risk Management System

Aligned with market best practices, the Iguatemi Risk Management System incorporates COSO ERM, ISO 31000:2018 frameworks, and IBGC guidelines as part of its methodology. This approach combines objective evaluation criteria with the company's strategic vision.

Thus, Iguatemi's risk management process is structured according to the following steps:

4.2.2.1. Scope, Context, and Criteria

The context is established by understanding the internal environment, based on Iguatemi's Strategic Planning and objectives, as well as the external environment, related to macroeconomic, political, social, sustainability factors, industry trends, competition, benchmarking, history of materialized risk events, and media coverage.

4.2.2.2. Risk Identification

This step involves understanding, recognizing, and recording strategic risks and opportunities. The goal is to identify events that may affect Iguatemi's strategic objectives, considering quantitative and qualitative aspects.

Identification is usually carried out through periodic meetings (Risk Assessment) or other necessary approaches, with the company's main executives and independent members of Committees and the Board. Internal and external scenarios (including emerging risks), as well as audit and internal control results, are also considered.

4.2.2.3. Risk Analysis and Assessment

Analysis is based on risks and their factors, described in the Company's risk dictionary, classified by identified nature: Strategic, Financial, Operational, Compliance, Cyber, and ESG (Environmental, Social, and Governance).

Assessment involves analyzing captured risk factors and, when applicable, creating scenarios. These elements are combined with analysis of possible impact and probability. This assessment results in the creation of the Risk Matrix, which provides a mechanism to prioritize risks and direct efforts to minimize the most relevant risks. Metrics for evaluating impact, probability, and risk exposure are detailed in a specific internal procedure.

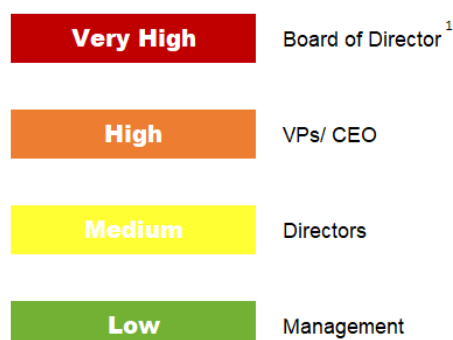
4.2.2.4. Risk Treatment

After risk assessment, the treatment to be adopted is defined, considering the following actions:

- i. Reduce: Implement action plans/controls to decrease causes or consequences of risks.
- ii. Share: Define actions to reduce the probability and/or impact of risk by transferring or sharing risk with third parties, such as insurance policies, outsourcing, etc.
- iii. Eliminate: Discontinue or avoid involvement with a risk situation (e.g., discontinuing an operation).
- iv. Accept: Risk acceptance may occur when:
 - a. The potential loss is not significant enough to justify mitigation actions.
 - b. The cost of mitigation exceeds risk exposure.
 - c. By business strategy.

For all situations described under "Accept," formal approval from the reporting authority is required, according to the final risk classification (see Figure 1 below). If the authority responsible agrees, the

risk owner is exempt from creating an action plan. However, the Risk Management area continues to monitor the risk to ensure exposure does not increase.



¹ Properly recommended by the Risk and Compliance Committee and Audit Committee.

Figure 1 – Risk Exposure x Reporting Authority

4.2.2.5. Monitoring and Critical Analysis

The monitoring and critical analysis of risks, including periodic reporting to the advisory bodies of the Board of Directors, are carried out by the Risk Management area and the Risk Owner. This report presents the progress of action plans/controls and key risk indicators (KRIs), when applicable, as well as the definition of new actions for management and/or mitigation.

Extension of deadlines for implementing action plans is only permitted with proper authorization from the authority responsible, accompanied by justification approved by the area manager, as per the approval table and details below:

<i>Risk Classification</i>	<i>Management</i>	<i>Directors</i>	<i>VP/ CEO</i>	<i>Board of Directors</i>
VERY HIGH				X
HIGH			X	
MEDIUM		X		
LOW	X			

VERY HIGH: Postponement will only be permitted if duly aligned with the Risk and Compliance Committee, which will submit it to the Board of Directors.

HIGH: Extension permitted only once, provided it is approved by the responsible Vice Presidency and/or CEO, who must submit justification to the Risk and Compliance Committee.

MEDIUM: Extension may be granted up to twice, the first with VP approval and the second including CEO approval.

LOW: Extension may be granted as many times as necessary, with approval from the Board responsible.

Additionally, the Company maintains other continuous monitoring activities, carried out by Internal Audit or third-party companies (e.g., External Audit). Iguatemi also conducts, with the involvement of

its executives and independent members, an annual review of its risks to reassess strategic alignment and continuously verify the implementation and results of mitigation measures.

4.2.2.6. Communication and Consultation

Iguatemi disseminates risk information to stakeholders in a way that facilitates the execution of employee responsibilities, including presenting information in appropriate formats and within deadlines that allow assertive decision-making. The Company ensures that this information is relevant, transparent, available, accessible, and accurate.

To ensure the integrity and effectiveness of the risk management process, the Internal Audit area has autonomy to conduct audits at any time.

4.3. Responsibilities

4.3.1. Board of Directors

- i. Approve guidelines for the Company's corporate governance structure for risk management, including methodology, policies, processes, systems, integration with Strategic Planning, among others, when properly recommended by the Risk and Compliance Committee.
- ii. Monitor compliance with established methodologies, mitigation actions, and action plans for inherent risks, especially those exceeding the Company's risk appetite.
- iii. Support awareness actions for managers and employees regarding the importance of risk management and the responsibility assigned to those involved in managing the Company's risks.
- iv. Ensure proper management of this policy, as well as its effectiveness and continuity.

4.3.2. Risk and Compliance Committee

- i. Evaluate the risk management process, including methodology, processes, systems, policy, and reporting mechanisms, requesting adjustments when necessary and recommending them to the Board of Directors.
- ii. Monitor mapping carried out by Company management of all relevant risk types, classifying them according to impact, probability, origin, and sensitivity to preventive or mitigating actions.
- iii. Report exceptions to the Board of Directors regarding risk management process guidelines and other relevant matters.
- iv. Monitor the planning of the Risk and Internal Controls Management, request adjustments when necessary, overseeing the execution of the work, and evaluating the quality and effectiveness of the process.
- v. Evaluate and monitor the Company's risk exposures and management.
- vi. Verify whether management is adopting necessary controls for risk management that require an action plan to reduce exposure.
- vii. Recommend actions to internally disseminate a risk sensitivity culture.

4.3.3. Audit and Related Parties Committee

- i. Evaluate and monitor the Company's risk exposures, requesting periodic reports for awareness and potential contribution.

- ii. Provide opinions and recommendations, when required, in the risk management process, provided it is duly agreed upon with the Risk and Compliance Committee.
- iii. Provide opinions and recommendations, when required, on actions to promote a risk management culture.
- iv. Monitor internal control activities, once action plans are implemented and included in the Risk and Control Matrix (RCM).
- v. Ensure that the Internal Audit Plan is based on Iguatemi's Risk Matrix.

4.3.4. People, Culture, and ESG Committee

- i. Understand and contribute to the definition of the ESG (Environmental, Social, and Governance) impact scale for classifying strategic risks.
- ii. Monitor the risk exposures in ESG categories/factors as assessed by the risk owners, in conjunction with the Risk and Internal Controls Management team.
- iii. Propose action plans to mitigate ESG risks, when requested by risk owners and/or the ESG Management.

4.3.5. Executive Board / VPs and CEO

- i. Participate in Iguatemi's risk management process in accordance with the Policy (roles, responsibilities, processes, among others) and ensure alignment with risk management best practices.
- ii. Promote the dissemination of the risk management culture.
- iii. Understand and contribute to the definition of risk appetite (financial impact), as well as other qualitative criteria.
- iv. Understand and contribute to the review of the strategic risk dictionary.
- v. Indicate the risks to be prioritized for evaluation by the Risk and Compliance Committee and approval by the Board of Directors.
- vi. Periodically promote evaluation cycles and reviews of the risk management process (internal or external agents), to ensure the effectiveness of risk management and monitoring.

4.3.6. Risk and Internal Controls Management

- i. Disseminate risk management knowledge to employees and members of independent bodies, aiming to promote a risk management culture through training paths by hierarchical level, as well as workshops or other necessary training.
- ii. Propose guidelines for the Company's corporate risk governance structure, including methodology, processes, systems, among others.
- iii. Establish and maintain updated the Risk Management Policy and Procedure, as well as proprietary standards and reporting mechanisms.
- iv. Ensure that risk managers identify, mitigate, and monitor the Company's risks, ensuring the integrity of internal controls.
- v. Periodically evaluate action plans, conduct tests and necessary adjustments, based on meetings with risk managers, and establish deadlines and responsible parties for execution and reporting of mitigation actions.
- vi. Improve the risk appetite calculation methodology by assessing the probability and impact of the Company's mapped risks.

- vii. Collaborate with executives and members of independent bodies in discussions regarding the definition of the Company's acceptable risk appetite.
- viii. Coordinate and monitor the risk identification and assessment process with the Company's executives.
- ix. Periodically update and review risk factors, especially when there are updates to strategic planning and/or relevant events occur.
- x. Monitor and report changes in risk criticality to the Risk and Compliance Committee, Audit and Related Parties Committee (when required), and Board of Directors.
- xi. Present to the Risk and Compliance Committee and the Audit and Related Parties Committee (when required) the risks to be prioritized and the proposed action plans.

4.3.7. Risk Owners

- i. Manage the risks under their responsibility, identifying changes in external and internal environments that may impact them and assessing the need for action plans to ensure proper treatment.
- ii. Implement necessary actions to mitigate risks, involving other areas, aligned with the action plan validated by Risk and Internal Controls Management.
- iii. Conduct periodic technical reviews of risks, related factors, responses, and risk assessments.
- iv. Periodically report to the Risk and Internal Controls Management on the evolution of risks under their responsibility, significant changes in risk factors or any other characteristics, as well as the identification of previously unmapped new risks.
- v. Maintain an effective control environment over the risks under their responsibility, evidencing the actions implemented.

4.3.8. Internal Audit

According to the definition of the Institute of Internal Auditors (IIA), Internal Audit in the Company must examine and audit the compliance of administrative acts and facts, evaluating processes, internal controls, and risk management. Thus, it will act as the Third Line, supporting the structuring and proper functioning of the First Line (Business Areas) and Second Line (Internal Controls and Risk Management), meaning it independently analyzes the previous two lines, identifying applicable improvement opportunities.

5. References

- i. Code of Ethical Conduct – Iguatemi
- ii. Third-Party Due Diligence Policy – Iguatemi.
- iii. Bylaws – Iguatemi
- iv. Internal Regulations of the Board of Directors – Iguatemi.
- v. Internal Regulations of the Audit and Related Parties Committee – Iguatemi.
- vi. Internal Regulations of the Risk and Compliance Committee – Iguatemi.
- vii. Sustainability Report – Iguatemi.
- viii. IFRS S1.
- ix. IFRS S2.
- x. CVM Instruction 80.
- xi. CVM Instruction 552.
- xii. CVM Instruction 586.
- xiii. Novo Mercado Regulation.
- xiv. CVM SEP Circular Letter 01/17.
- xv. COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework)
- xvi. Corporate Governance Handbook – Corporate Risk Management (Governance and Strategy Evolution)
- xvii. ISO (International Organization for Standardization) 31.000.
- xviii. IIA (The Institute of Internal Auditors).

6. Appendices

N/A

7. Control Information

7.1. Document Owners

Responsible	Area
Preparation	Risk and Internal Controls Management
Review	Legal Vice Presidency and CEO
Approval	Board of Directors

7.2 Version Record

Version	Publication Date
1st	01/Sep/2022



IGUATEMI