POLÍTICA DE GESTÃO DE RISCOS - CONGLOMERADO MAGALUPAY

CONTROLE DE ALTERAÇÕES

Revisão	Data	Local da Revisão	Descrição
0	09/10/2025	-	Emissão inicial, revogando a Política de Gestão de Riscos da MagaluPay Instituição de Pagamento S.A.

LISTA DE DISTRIBUIÇÃO

Função
Todos os administradores, colaboradores, prestadores de serviços e parceiros de todas as empresas do Conglomerado MagaluPay.

LISTA DE TREINAMENTO

Áreas funcionais
Todos os administradores e colaboradores de todas as empresas do Conglomerado MagaluPay e colaboradores das áreas de Gestão de Riscos.

Elaborado/Revisado por:

Diretoria de *Compliance*, Integridade e PLD
Diretoria de Riscos e Prevenção à Fraude

Aprovado por:

Fabio Itiro Bonifácio Murakami
Diretor de Produtos

Kahuê Souza Cardoso
Diretor de Riscos

Leandro Hespanhol
Diretor Comercial

Rebeca Virginia Villagra Lima
Diretora de *Compliance*, Integridade e PLD

Lelio Marcos Rodrigues Bertoni
Diretor Jurídico e Ouvidoria

Paulo Augusto Pannunzio de Castro
Diretor de Auditoria Interna

Marcio Henrique Oliveira
Diretor de Tecnologia e Segurança da Informação

Ciência:

JÖRG DETLEF FRIEDEMANN JUNIOR
Diretor Presidente

1. OBJETIVO

Estabelecer diretrizes e responsabilidades relacionadas à identificação, análise e monitoramento dos riscos que podem afetar o plano estratégico e operacional do Conglomerado MagaluPay, a fim de subsidiar o processo decisório, na busca do cumprimento dos objetivos, da criação, preservação e crescimento de valor.

2. TERMOS E DEFINIÇÕES

- **Apetite a risco:** nível de risco que uma organização está disposta a assumir para atingir seus objetivos, que serve como guia para a tomada de decisões. O apetite a riscos deve ser aprovado pela alta administração da companhia.
- **Comitê de Auditoria, Riscos e *Compliance* ("CARC") da Controladora:** órgão colegiado instituído pela controladora Fintech Magalu, que tem como uma de suas principais finalidades assessorá-la com o monitoramento das atividades de gerenciamento de riscos e com o acompanhamento das funções de controles internos e de conformidade regulatória relativos aos principais processos operacionais e corporativos do Conglomerado MagaluPay.
- **Comitê de Crédito e Liquidez:** órgão colegiado instituído pela Diretoria Estatutária da MagaluPay, que tem a finalidade de analisar, avaliar e decidir acerca das questões relacionadas ao crédito e à liquidez da MagaluPay, buscando assegurar sua solidez, eficiência e conformidade com as regulamentações aplicáveis.
- **Conglomerado MagaluPay:** grupo de empresas controladas pela MagaluPay Holding. Inclui a MagaluPay Instituição de Pagamento S.A., a Sociedade de Crédito, Financiamento e Investimento S.A. e as empresas controladas pelas instituições.
- **Evento:** ocorrência ou alteração em um conjunto específico de circunstâncias. Um evento pode consistir de uma ou mais ocorrências, e pode ter várias causas. Também pode consistir em não ocorrência de alguma coisa.
- **Gestão de Riscos:** atividades coordenadas e estruturadas para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos em uma organização, visando auxiliar no processo decisório.
- ***Key Risk Indicators* (KRIs) -** principais indicadores de riscos: consiste em uma medida quantitativa usada para avaliar e monitorar o nível de exposição ao risco relacionado a uma área, processo ou atividade. Os KRIs são componentes fundamentais de uma estrutura de controles e das boas práticas de gestão de risco. É desejável que os indicadores possuam as

características de efetividade (ser específico, mensurável e preditivo), comparabilidade (ser consistente e auditável), e facilidade (ter coleta automatizada, de baixo custo e transparente).

- ***Key Performance Indicators* (KPIs) -** principais indicadores de performance: auxiliam no monitoramento do desempenho do negócio e das áreas funcionais de suporte, permitindo avaliar e implantar melhorias necessárias para se atingir os objetivos da organização.
- **PLD/FT:** prevenção à lavagem de dinheiro e ao financiamento do terrorismo.
- **Riscos:** fatores ou eventos incertos que podem causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos da organização. Podem subsidiar o processo de tomada de decisão e representam, por vezes, uma oportunidade.
- **Risco inerente:** risco para o qual ainda não foram aplicadas ações de resposta/tratamento, para alterar a probabilidade de ocorrência e/ou impacto (mitigação).
- **Risco residual:** risco que permanece após aplicação de ações de resposta/tratamento.
- **Riscos de negócio e/ou estratégicos:** relacionados à estratégia da organização na busca de criação, proteção e crescimento sustentável de valor. Decorrem de causas internas e externas.
- **Riscos operacionais:** decorrem da inadequação ou falha na gestão de processos internos, de pessoas, sistemas, eventos externos e demais recursos, que possam dificultar ou impedir o alcance dos objetivos da organização. Estes riscos estão associados tanto à operação do negócio como *marketing*, vendas e comercial; quanto à gestão de áreas de suporte ao negócio tais como: administrativas (contabilidade, controladoria, controles), de tecnologia, suprimentos, saúde e segurança do trabalho, fraudes e relações sindicais.
- **Riscos financeiros:** aqueles que derivam, entre outros, de eventos relativos a finanças (ambiente econômico, geração de caixa operacional, rentabilidade, endividamento, alavancagem, aplicação e captação de recursos financeiros). Contempla: (i) Risco de Mercado - decorre da possibilidade de perdas que podem ser ocasionadas por mudanças no comportamento das taxas de juros, do câmbio, dos preços das ações e dos preços de commodities; (ii) Risco de Crédito - definido como a possibilidade de perda resultante da incerteza quanto ao recebimento de valores pactuados com tomadores de empréstimos/financiamentos, contrapartes de contratos ou emissões de títulos; (iii) Risco de Liquidez - possibilidade de perda decorrente da incapacidade de realizar uma transação em tempo razoável e sem perda significativa de valor, ou a falta de recursos para honrar os compromissos assumidos.
- **Riscos inesperados ou "cisne negro":** se caracterizam por sua probabilidade remota, mas que, caso ocorram, geram impacto gigantesco.

- **Riscos de conformidade:** ocorrem pela possibilidade de aplicação de sanções legais ou regulatórias, acarretando em perdas financeiras ou danos à reputação e à imagem. Resultam do descumprimento de leis, normas, acordos, regulamentos, código de ética e conduta e políticas internas, além de atos de corrupção, fraude, desvios de ativos ou divulgação de informações incorretas nas demonstrações financeiras.
- **Riscos de tecnologia:** para fins desta Política, referem-se à possibilidade de perdas ou danos resultantes de falhas, vulnerabilidades, interrupções, inadequações ou obsolescência da tecnologia e dos ativos digitais de todo o ecossistema tecnológico, incluindo prestadores de serviço e fornecedores de *softwares* e *hardwares*. Esses riscos podem interromper operações, apresentar ameaças à segurança cibernética, ou comprometer a relevância e funcionalidade dos sistemas, e abrangem todo o ciclo de vida dos ativos digitais, desde a concepção e desenvolvimento até a operação, segurança, e a capacidade de evolução da infraestrutura, plataformas, algoritmos, dados e uso da inteligência artificial.
- **Riscos socioambientais:** riscos relacionados a fatores ambientais, sociais e de governança corporativa, que podem impactar a sustentabilidade financeira, a reputação e a perenidade ou continuidade do negócio a longo prazo.
- **Riscos prioritários:** grupo de riscos com impacto considerado alto e muito alto para o negócio, cujo tratamento deve ser priorizado e, portanto, os seus indicadores devem ser monitorados regularmente.
- **Riscos emergentes:** riscos que surgem de mudanças rápidas e inesperadas no ambiente econômico, socioambiental, tecnológico, político e de ações de competidores. Esses riscos podem ser difíceis de identificar e avaliar no início, pois muitas vezes estão associados a inovações, tendências ou eventos novos que não foram amplamente estudados e compreendidos ou mesmo previstos.
- **Sociedade de Crédito, Financiamento e Investimento (SCFI):** instituição autorizada pelo Banco Central a atuar na concessão de crédito, como financiamentos e empréstimos, utilizando recursos próprios ou captados no mercado, sem realizar captação de depósitos à vista.

3. ATRIBUIÇÕES E RESPONSABILIDADES

Áreas funcionais:	Responsável por:
Diretoria Estatutária	• Estabelecer as diretrizes gerais das estratégias de gestão de riscos do Conglomerado MagaluPay; • Avaliar e aprovar a matriz de riscos estratégicos e as diretrizes gerais para estabelecimento dos limites aceitáveis para exposição do Conglomerado MagaluPay aos riscos (apetite a riscos); • Supervisionar as atividades do processo de gerenciamento de riscos, diretamente ou por meio dos Comitês de Assessoramento; • Assegurar a adequação da estrutura de gestão de riscos e garantir a disponibilidade de recursos humanos, financeiros e tecnológicos, destinados ao processo de gerenciamento de riscos das instituições membro do Conglomerado; • Aprovar a aceitação de riscos residuais, que estiverem em não conformidade com o apetite a riscos; • Aprovar a Declaração de Apetite a Riscos (RAS) e acompanhar a aderência do Conglomerado; • Aprovar esta Política de Gestão de Riscos e suas revisões futuras.
Comitê de Auditoria, Riscos e *Compliance* da Controladora	Por delegação da Diretoria Estatutária: • Propor à Diretoria Estatutária as definições gerais das estratégias de gestão de riscos; • Acompanhar e supervisionar, dentro de suas atribuições e especialidades, o processo de gestão de riscos e a correta aplicação dos KRIs/KPIs, por meio dos trabalhos das áreas de Gestão de Riscos, de Controles Internos e de Auditoria Corporativa; • Analisar, monitorar e informar, periodicamente, à Diretoria Estatutária, sobre os riscos prioritários identificados pelas revisões das áreas de Gestão de Riscos e de Auditoria Interna e os planos de ação e recomendações aplicáveis; • Avaliar a adequação da estrutura (recursos humanos, financeiros e sistemas) destinada ao processo de gerenciamento de riscos.
Comitê de Crédito e Liquidez	Por delegação da Diretoria Estatutária: • Propor à Diretoria Estatutária as definições gerais das estratégias de gestão dos riscos financeiros do Conglomerado MagaluPay; • Monitorar o nível de exposição do Conglomerado MagaluPay a riscos de mercado, de crédito e de liquidez; • Acompanhar e supervisionar o processo de gestão de riscos financeiros para geração de valor do Conglomerado MagaluPay - planejamento financeiro, orçamento, monitoramento de indicadores, definições e revisão de limites, análises de cenários de estresse, decisões de investimento e captação de recursos.

Diretorias de Negócios e Operações	• Promover a integração da gestão de riscos com os ciclos de gestão e planejamento do Conglomerado MagaluPay; • Fomentar a cultura de gestão de riscos nas suas respectivas áreas e em todas as entidades do Conglomerado; • Garantir a implantação de modelo eficiente de gestão de riscos, alinhado aos objetivos de negócios e metas operacionais; • Acompanhar os riscos gerenciados no nível de cada macroprocesso e/ou operação, para verificar a efetividade dos controles existentes em todo o Conglomerado; • Identificar e priorizar riscos de suas respectivas áreas, com o apoio do time de Gestão de Riscos; • Acompanhar os KRIs/KPIs e as estratégias de mitigação dos riscos prioritários; • Avaliar e monitorar o tratamento dos riscos de negócio quando da execução do planejamento estratégico; • Avaliar, ao menos anualmente, a eficácia dos critérios instituídos nesta Política e do sistema de gerenciamento de riscos, e prestar contas ao Comitê de Auditoria, Riscos e *Compliance* da Controladora.
Diretoria de *Compliance*, Integridade e PLD	• Identificar os riscos de conformidade legal, regulatória e de integridade, garantindo o seu adequado gerenciamento; • Quando pertinente, propor, adotar e implantar mecanismos ou instrumentos de controle, a fim de evitar riscos de que as operações e/ou negócios, de qualquer empresa do Conglomerado, sejam utilizados para prática de corrupção, fins irregulares, ilegais e ilícitos; • Revisar e acompanhar o planejamento anual das atividades de gestão de riscos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais e reportando o resultado dos seus trabalhos ao CARC; • Avaliar, em conjunto com cada Diretoria, os riscos operacionais por macroprocesso, por unidade de negócio ou portfólio; • Elaborar, treinar, disseminar e recomendar os processos e procedimentos para a gestão de riscos; • Desenvolver, testar e implantar os modelos e metodologias para mensuração e gestão dos riscos; • Emitir parecer sobre a viabilidade das operações em relação aos riscos de integridade/*compliance*; • Assegurar, em conjunto com as áreas envolvidas, a eficácia desta Política e verificar o seu cumprimento; • Suportar as áreas de negócio na definição dos planos de ação para tratamento de riscos; • Realizar a *Due Diligence* de Integridade/*Compliance* e Socioambiental, para identificação de riscos, visando minimizar impactos reputacionais negativos em transações de M&A.

Diretoria de Riscos e Prevenção à Fraude	• Mapear riscos transacionais e adotar medidas efetivas para mitigação de riscos identificados; • Promover, sistematicamente, melhorias nos procedimentos de prevenção, monitoramento e identificação de fraudes transacionais; • Monitorar, identificar e analisar transações e operações realizadas por clientes, fornecedores e parceiros, que sejam consideradas suspeitas; • Acompanhar e reportar, periodicamente, indicadores de riscos de sua respectiva área; • Informar, à Gerência de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, fraudes e/ou operações suspeitas de lavagem de dinheiro ou de financiamento ao terrorismo; • Efetuar investigações de fraudes e reportar à Diretoria Estatutária para avaliação e deliberação, se necessário.
Gerência de Gestão de Riscos da Diretoria de *Compliance*, Integridade e PLD	• Definir a metodologia corporativa de gestão de riscos, pautada na visão integrada e sistêmica das atividades do Conglomerado MagaluPay, subsidiada pelas metodologias adotadas no mercado e melhores práticas de governança; • Propor o planejamento anual das atividades de gestão de riscos e assegurar sua operacionalização; • Consolidar e comunicar os riscos prioritários do Conglomerado MagaluPay às Diretorias de Negócios e Operações; • Assessorar e capacitar as áreas funcionais e de negócios na identificação e avaliação dos riscos mapeados; • Elaborar, em conjunto com os gestores das áreas, as matrizes de riscos dos processos/áreas mapeadas e classificá-los de acordo com a metodologia aprovada; • Elaborar a Declaração de Apetite a Riscos (RAS); • Avaliar/validar os riscos identificados pelos agentes de integridade em suas respectivas áreas; • Executar as tarefas que permitam o adequado monitoramento dos riscos, reportando os resultados de suas avaliações ao CARC; • Apoiar as áreas na elaboração e manutenção dos planos de continuidade de negócios e operacionais; • Elaborar, em conjunto com a Gerência de PLD/FT, a Avaliação de Risco de LD/FT do Conglomerado.

Gerência de Privacidade e ASG da Diretoria de *Compliance*, Integridade e PLD	• Identificar os riscos relacionados à privacidade de dados pessoais nos processos e negócios do Conglomerado MagaluPay e adotar medidas efetivas para a sua mitigação; • Efetuar a análise de *score* de risco de incidentes que impactem a privacidade de dados pessoais e, se for o caso, comunicar à ANPD e/ou os titulares; • Acompanhar as ações de contenção e remediação relacionadas aos incidentes de dados pessoais; • Efetuar a análise de risco de fornecedores/terceiros, nos casos em que o objeto da contratação envolva o tratamento de dados pessoais; • Elaborar e/ou revisar cláusulas de proteção de dados pessoais nos contratos cujo objeto envolva qualquer tipo de tratamento de dados pessoais; • Ministrar treinamento de privacidade e proteção de dados pessoais.
Gerência de Prevenção à Lavagem de Dinheiro e/ou financiamento do terrorismo da Diretoria de *Compliance*, Integridade e PLD	• Identificar os riscos dos produtos ou negócios serem utilizados para lavagem de dinheiro (LD) e/ou para financiamento do terrorismo (FT); • Monitorar todas as transações e/ou operações a fim de identificar, tempestivamente, operações e/ou transações atípicas e/ou suspeitas; • Propor, adotar e/ou implantar mecanismos ou instrumentos de controle para mitigar os riscos das operações e/ou negócios, de qualquer empresa do Conglomerado, sejam utilizadas para LD/FT; • Elaborar, em conjunto com a Gerência de Gestão de Riscos, a Avaliação de Risco de LD/FT do Conglomerado.
Agentes de Integridade das Áreas Funcionais e Operacionais	• Apoiar suas respectivas áreas na identificação, classificação e gerenciamento dos riscos operacionais; • Contribuir para o estabelecimento de mitigantes para os riscos das suas áreas de atuação; • Apoiar na implantação dos planos de ação e acompanhar as ações corretivas e/ou preventivas em suas áreas; • Fazer a *interface* das áreas de negócios e funcionais com a área de gestão de riscos e controles internos.
Áreas Funcionais (Primeira linha de defesa)	• Assegurar a operacionalização da gestão de riscos, fazendo parte do processo de identificação, avaliação e mensuração, implantando ações de tratamento dos riscos identificados; • Participar, de forma ativa, das atividades de comunicação e de treinamento, de gestão de riscos no Conglomerado; • Aprovar os riscos residuais classificados como médios e baixos, conforme definidos na matriz de riscos, assegurando a aderência ao apetite de risco e a efetividade dos controles e planos de tratamento.

4. DIRETRIZES GERAIS

A gestão de riscos está inserida no compromisso do Conglomerado MagaluPay, com a criação e preservação de valor da organização, devendo estar integrada ao processo de tomada de decisão.

A gestão de riscos contribui para: (i) a consecução dos objetivos estatutários e estratégicos do Conglomerado; (ii) sua sustentabilidade; (iii) a preservação do patrimônio tangível e intangível; (iv) a segurança das pessoas; e, (v) a integridade do meio ambiente e comunidades, por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos risco e possíveis externalidades negativas decorrentes de sua materialização.

O Conglomerado MagaluPay adota um *framework* de gestão de riscos para identificação, análise, tratamento e monitoramento dos riscos de forma estruturada, abrangente e aplicada a todas as suas entidades e processos críticos.

Este *framework,* que se baseia nas melhores práticas de mercado e em diretrizes como o COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management*) e a norma ISO 31000:2018, visa integrar as decisões estratégicas e operacionais com os riscos mapeados, de forma consistente e em linha com as diretrizes dos órgãos reguladores.

O Conglomerado MagaluPay identifica e trata riscos estratégicos, operacionais, de tecnologia, de conformidade, financeiros e socioambientais de forma a garantir o cumprimento das metas estabelecidas em seu planejamento estratégico e seus principais objetivos. Além disso, deve monitorar potenciais situações de riscos emergentes, proporcionando uma base sólida para decisões estratégicas e reduzindo incertezas.

A gestão de riscos do Conglomerado MagaluPay fundamenta-se nas diretrizes abaixo, as quais devem estar alinhadas com as considerações e recomendações do CARC, de órgãos reguladores externos, e com as melhores práticas de mercado e metodologias relacionadas:

- Cultura de riscos integrada na organização;
- Independência da função da área de Gestão de Riscos;
- Foco nos riscos oriundos das atividades das áreas de negócios para a adequada gestão e controle; e

- Adoção de metodologia que garanta à organização e sua governança conhecer os riscos e os respectivos responsáveis por seu controle e gestão.

Os riscos são identificados e avaliados de acordo com a probabilidade de ocorrência e seu impacto sobre o negócio, inclusive, sobre a imagem e reputação do Conglomerado MagaluPay e sua potencial repercussão no Grupo Magazine Luiza. Cada decisão deve levar em consideração os benefícios, os aspectos negativos e os riscos atrelados, mensurando a relação entre custo e benefício e entre a severidade e mitigação.

4.1 Objetivos da Gestão de Riscos

O Processo de Gestão de Riscos foi definido com base nas orientações consolidadas no COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management*) e na norma ISO 31000:2018, com o intuito de:

- Aumentar a probabilidade de realização/alcance dos objetivos estratégicos estabelecidos;
- Aprimorar a identificação de oportunidades e ameaças;
- Assegurar conformidade com políticas, normas e requisitos legais e regulatórios, padronizando conceitos e práticas;
- Implantar sistema de gestão de riscos robusto para proteger sistematicamente os ativos da organização;
- Melhorar o reporte das informações ao mercado, elevando a confiança das partes interessadas e garantindo a transparência para todas as partes interessadas;
- Garantir base confiável de dados para a tomada de decisão e planejamento, fornecendo um fluxo dinâmico e eficiente de informação, bem como prevenir ou minimizar perdas, envolvendo todos os agentes da estrutura em alguma etapa;
- Alocar e utilizar eficazmente os recursos, melhorando o ambiente de controles; e
- Aperfeiçoar a eficácia e eficiência operacional, aumentando a resiliência das operações do Conglomerado MagaluPay, buscando garantir a continuidade do negócio e a rápida recuperação de serviços críticos diante de adversidades.

4.2 Natureza dos riscos

Os riscos são classificados como: riscos estratégicos, riscos operacionais, riscos socioambientais, riscos de tecnologia, riscos de conformidade e riscos financeiros, conforme definição no item “2.

TERMOS E DEFINIÇÕES".

4.3 Estrutura para Gestão de Riscos

O compromisso com a integridade, os valores éticos e a disseminação da cultura de gestão de riscos no Conglomerado MagaluPay é responsabilidade de todos os colaboradores, sendo estes responsáveis, também, pela gestão de riscos de suas respectivas áreas.

De acordo com a premissa acima, a estrutura de gestão de riscos do Grupo Magazine Luiza e do Conglomerado MagaluPay, como parte do seu ecossistema, considera a atuação conjunta dos órgãos de governança corporativa e de gestão, alinhado com o conceito das 3 (três) linhas de defesa:

➔ **Primeira Linha de Defesa:** refere-se à gestão operacional, representada pelas diretorias, gerências e pelos demais colaboradores, que atuam nas operações do Conglomerado MagaluPay. São os chamados "donos dos riscos". É responsável por:

- Identificar, avaliar, tratar e monitorar os riscos de acordo com as diretrizes desta Política;
- Implantar planos de ação e controles em conjunto com as áreas de Gestão de Riscos e de Controles Internos;
- Comunicar/reportar, em tempo hábil, informações relevantes relacionadas à gestão de riscos.

➔ **Segunda Linha de Defesa:** refere-se às áreas de controle do Grupo Magazine Luiza, compreendendo, essencialmente, as funções de Gestão de Riscos e Controles Internos e, no que tange à execução orçamentária, a Controladoria. Reporta-se à Diretoria Executiva e, também, ao Conselho de Administração do Grupo Magazine Luiza e seus Comitês de Assessoramento. A Segunda Linha de Defesa tem as seguintes responsabilidades, no âmbito de suas respectivas competências:

- Analisar, avaliar e monitorar os riscos identificados pela gestão operacional;
- Facilitar e monitorar a implantação das práticas de gestão de riscos pela gestão operacional (1ª linha de defesa) de acordo com o apetite a risco;
- Comunicar/reportar, em tempo hábil, informações relevantes relacionadas à gestão de riscos;
- Auxiliar na identificação de riscos, riscos emergentes e no desenvolvimento de processos

e controles; e,

- Elaborar as matrizes de riscos e controles das áreas.

➔ **Terceira Linha de Defesa:** Diz respeito à atuação da Auditoria Interna e do *Compliance,* Integridade e PLD na avaliação e supervisão da aderência e eficácia do processo de gerenciamento de riscos. Atua de forma independente e objetiva, reportando-se à Diretoria Colegiada, ao Conselho de Administração do Grupo Magazine Luiza e seus Comitês de Assessoramento.

Figura 1: Estrutura das 3 linhas de defesa

Fonte: elaboração própria

4.4 Etapas da Gestão de Riscos

O processo de Gestão de Riscos considera a identificação do perfil de exposição e tolerância a riscos (apetite a risco) pela avaliação do ambiente interno, bem como a fixação dos objetivos e diretrizes estratégicas.

O processo de avaliação dos riscos é aplicado inicialmente aos riscos inerentes, e posteriormente, a partir das medidas de tratamento e resposta aos riscos, é aplicado aos riscos residuais.

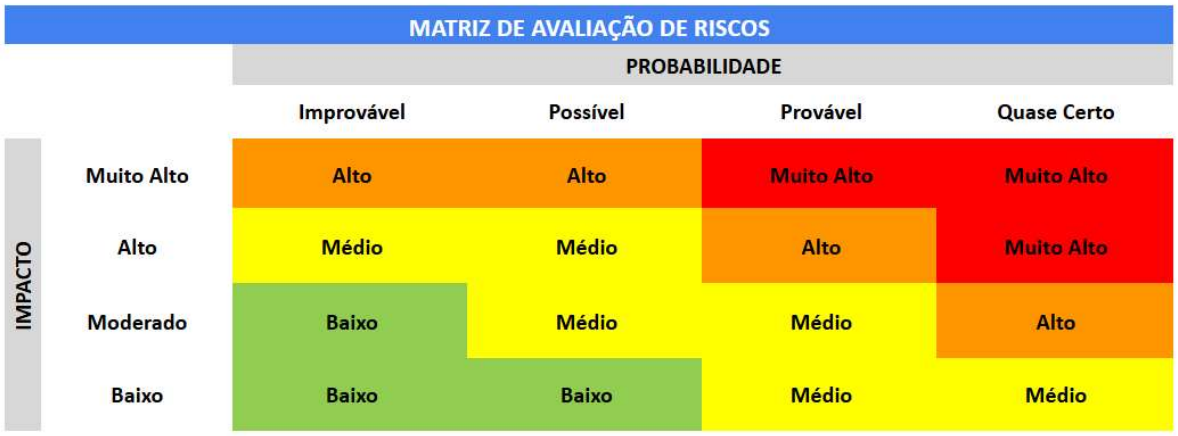
1ª	**Identificação e Mapeamento**	• Consiste na identificação dos riscos inerentes que afetam o negócio, com o objetivo de gerar uma lista abrangente de riscos. O mapeamento descreve os eventos (incluindo causas e consequências) que podem criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos, impactando as metas, a operação eficaz dos processos e a alocação eficiente de recursos.
2ª	**Análise e Quantificação**	• A Análise e Quantificação representa o cálculo do nível de exposição do Conglomerado MagaluPay a determinado risco. Essa etapa compreende a categorização dos riscos identificados com base em sua probabilidade ou frequência de ocorrência e impacto nos objetivos da organização. O resultado fornece a base para a avaliação de riscos e para tomada de decisões quanto ao seu tratamento. **Avaliação do Risco = Probabilidade x Impacto** Para fins de análise e quantificação, adota-se a matriz de avaliação de riscos 4x4, que avalia o impacto e a probabilidade de ocorrência, conforme detalhado a seguir: - **Impacto:** deve ser analisado em relação a cinco aspectos: (i) Financeiros; (ii) Clientes; (iii) Pessoas; (iv) Reputação; e (v) Sanção Legal/Regulatória. O valor do impacto final será sempre o maior nível obtido entre esses aspectos. - **Probabilidade:** deve ser quantificada considerando a frequência de ocorrência do risco, e aplicando a metodologia mais adequada à avaliação de cada macroprocesso. **Importante:** Nesta etapa também são identificados os controles existentes, e avaliado se o desenho dos controles é adequado para mitigar os riscos identificados.
3ª	**Avaliação e Priorização**	• Consiste na avaliação da necessidade e da prioridade de tratamento do risco, com a finalidade de auxiliar na tomada de decisões. O processo compara o nível de exposição ao risco com as diretrizes de apetite a riscos determinadas pela Alta Direção; • Com base nesta avaliação, define-se a escala de priorização para o tratamento, utilizando a Matriz GUT (Gravidade, Urgência e Tendência), para facilitar a alocação de recursos. Os riscos devem ser reavaliados periodicamente, para garantir que a análise reflita a realidade do processo/área.

4ª	**Tratamento**	• O tratamento de riscos consiste na tomada de decisões e na seleção e implantação de uma ou mais respostas aos riscos, com base na matriz de avaliação e nos limites preestabelecidos no Apetite a Riscos; • As alternativas para tratamento classificam-se da seguinte forma: a) **Eliminar:** Eliminar as atividades que geram o evento de risco; b) **Mitigar:** Diminuir a probabilidade e/ou a magnitude do impacto do evento de risco; c) **Transferir/Compartilhar:** Transferir ou compartilhar o todo ou parte do evento de risco; d) **Aceitar:** Aceitar o evento de risco de forma consciente. • As respostas são implantadas por meio de planos de ação específicos e factíveis, que podem contemplar desde a revisão de processos e a implantação de novos controles até a alteração de instrumentos de governança. Podem incluir, também, a eliminação da atividade geradora do risco. **Importante:** A assunção de riscos que permaneçam fora do Apetite a Riscos da Companhia requer a aprovação formal da Alta Direção.
5ª	**Monitoramento**	Processo contínuo e dinâmico, essencial para a boa governança corporativa, o monitoramento deve contemplar integralmente todas as etapas da gestão de riscos, de forma a: • Garantir que os controles adotados sejam eficazes e eficientes para os processos definidos e a suas situações de riscos residuais; • Acompanhar e analisar "quase incidentes", eventuais concretizações dos riscos identificados e dos emergentes, identificando mudanças, tendências, sucessos e fracassos que gerem aprendizado com sua ocorrência; • Acompanhar KRIs dos riscos estratégicos; • Obter informações adicionais de outras linhas de defesa, para melhorar o processo de mapeamento e avaliação dos riscos; • Assegurar que eventuais alterações circunstanciais nos contextos interno e/ou externo, que ensejem na alteração do risco e/ou demandem a revisão dos controles aplicados, sejam devidamente endereçadas; • Garantir que o modelo de Gestão de Riscos está aderente aos objetivos do Conglomerado MagaluPay ao longo do tempo; • Manter a matriz de riscos de cada processo/área devidamente atualizada.

4.5 Matriz de avaliação e níveis de severidade

Para melhor visualização e gestão dos riscos de cada processo/área, após a conclusão da etapa de Avaliação e Priorização, os riscos devem ser plotados em uma Matriz de Avaliação de Riscos, que estabelece os níveis de severidade com base na combinação entre o impacto e a probabilidade de ocorrência.

Figura 2: Matriz de Avaliação de Riscos



Fonte: elaboração própria.

4.5.1 Características dos Riscos

I. RISCO ALTO e MUITO ALTO: Representam ameaça potencial aos negócios do Conglomerado MagaluPay. Demandam ação gerencial prioritária para eliminar o componente de risco ou ao menos reduzir sua severidade e/ou frequência.

II. RISCO MÉDIO: Refere-se a riscos que podem ter impacto baixo, moderado ou alto no valor do negócio, entretanto, pela combinação com sua probabilidade, resultam em severidade média. Manifestam-se de duas formas: (i) riscos com probabilidade alta, porém com impacto reduzido, exigindo definição de níveis aceitáveis de perda e limites de competência para evitar escalonamento do impacto ao longo do tempo; e (ii) riscos inesperados, com alto impacto e baixa probabilidade, incluindo eventos extremos e raros ("cisnes negros"), que demandam quantificação, monitoramento contínuo e planos de contingência. O tratamento pode incluir, quando viável, a contratação de seguros como resposta de tratamento.

III. RISCO BAIXO: Abrange perdas de menor relevância, podendo o custo do impacto ser menor

do que o custo de tratá-los. Riscos de baixo impacto e frequência, não havendo necessidade de monitoramento contínuo.

5. APETITE A RISCOS

O Conglomerado MagaluPay deve elaborar e manter atualizada sua Declaração de Apetite a Riscos, a qual deverá orientar o processo de aceitação de riscos, prevendo, como instrumento de governança, a formalização da decisão de aceite de riscos pela alçada competente. Adicionalmente, os riscos aceitos devem ser monitorados com base em critérios previamente definidos.

6. DISPOSIÇÕES GERAIS

6.1 Aplicabilidade

Esta Política se aplica, a todos os administradores e colaboradores do Conglomerado MagaluPay.

6.2 Vigência e aprovação

Esta Política tem vigência a partir da data de sua aprovação e divulgação, podendo ser revisada sempre que necessário.

6.3 Política de Consequências e Violações

Qualquer violação a presente política será passível de penalização, que poderá ser desde advertência verbal até demissão por justa causa e, no caso de ocorrência de danos, reparação do eventual dano causado.

As medidas de consequências adotadas pelo Grupo Magalu, seja no âmbito interno ou por meio de adoção de medida judicial cabível, serão aplicadas após a avaliação da gravidade do caso concreto e dos impactos causados pela violação.

Compete à área de *Compliance*, Integridade e PLD apurar os casos relatados, submeter ao Comitê Disciplinar e reportar os incidentes relacionados a esta matéria ao Comitê de Integridade e ao Comitê de Auditoria, Riscos e *Compliance*. As medidas de consequências deverão ser aplicadas pelo Comitê Disciplinar, em conformidade com as diretrizes da Política de Consequências.

7. REFERÊNCIAS

- Circular BCB n° 3.681/13;

- Código de Ética e Conduta;
- COSO - *Committee of Sponsoring Organizations of the Treadway Commission;*
- ISO 31.000/2018;
- Política de Conformidade;
- Política de Consequências;
- Política de Práticas Contábeis;
- Política de Segurança Cibernética;
- Resolução BCB n° 25 de 22/10/2020;
- Resolução BCB n° 65, de 26/01/2021;
- Resolução BCB nº 85, de 08/04/2021;
- Resolução BCB nº 201/2022;
- Resolução BCB n° 260, de 22/11/2022;
- Resolução CMN nº 4.557/2017;
- Resolução CMN nº 4.595/2017.