Política Gestão de Riscos

Sumário

Introdução e Objetivo 3
Escopo 3
Detalhamento 3
Definições 3
Declarações 3
Estrutura de Governança 3
Gerenciamento de Riscos 4
Registrando Eventos de Risco 6
Aprovando Planos de Ação 7
Monitorando Planos de Ação 7
Responsabilidades 7
Governança 8
Histórico de Versões 8

Versão 1.0 | Data de publicação: 25/06/2026

I. INTRODUÇÃO E OBJETIVO

A Leto Capital, através de suas empresas, mantém linhas de negócios de Gestão de Recursos de Terceiros, *Merge & Acquisition* (M&A), *Debt Capital Markets* (DCM) e Provedor de Índice. Essas linhas de negócios, no desempenho de suas atividades estão expostas a riscos que podem impactar o Grupo Econômico.

Esta Política tem por objetivo estabelecer o framework de governança de riscos para o Grupo Econômico.

II. ESCOPO

Esta Política aplica-se a todos os sócios, diretores, funcionários e estagiários ("Colaboradores") do Grupo Econômico da Leto Capital ("Leto Capital" ou "Grupo Econômico"), composta pela Leto Asset Management Ltda. ("Gestora"), Leto Financial Advisory Ltda. e IDEX Analytics Ltda. (todas, individualmente ou em conjunto, referenciadas como "Empresa").

Os Colaboradores devem respeitar as regras estabelecidas por esta Política. A não observância destas regras pode causar danos à Empresa e sujeita o infrator à aplicação de medidas disciplinares que pode incluir encerramento de relacionamento com a Empresa.

III. DETALHAMENTO

DEFINIÇÕES

TERMO	DEFINIÇÃO
Evento de Risco	É a materialização do risco.
Risco	É a possibilidade de ocorrência de um evento que tenha um efeito negativo nos objetivos de negócio da Empresa.
Risco Inerente	Risco Inerente é o nível de risco bruto existente antes da aplicação de controles para responder ao risco.
Risco Residual	Risco Residual é o nível de risco que permanece após a aplicação de controles para responder ao risco.
Taxonomia	É o sistema de classificação padronizado utilizado para identificar, categorizar e agrupar todos os riscos.

DECLARAÇÕES

ESTRUTURA DE GOVERNANÇA

A Empresa adota modelo de governança de Três Linhas de Defesa.

- A Primeira Linha de Defesa ("1ª Linha") é responsável por identificar e gerenciar os riscos em suas atividades diárias. Ela é composta por todas as áreas da Empresa que não sejam de 2ª e 3ª Linha de Defesa.

- A Segunda Linha de Defesa é responsável por estabelecer o framework de gerenciamento de riscos, monitorar a gestão de riscos realizada pela 1ª. Linha e reportar riscos à Diretoria Estatutária. A Área de Compliance e Controles Internos ("Compliance") compõe a Segunda Linha de Defesa. Para a Gestora, a Área de Riscos também integra esta Linha de Defesa.

- A Terceira Linha de Defesa é responsável pela realização de avaliação independente da eficácia da governança e dos controles internos. A Empresa contrata Auditoria Externa com o objetivo de auditar as suas demonstrações financeiras.

GERENCIAMENTO DE RISCOS

- Para o gerenciamento de riscos as unidades organizacionais devem implementar controles de acordo com o tipo de resposta a risco a ser adotado, objetivando a manutenção dos níveis dos riscos dentro do apetite a riscos da Empresa.
  - Os controles devem ser implementados de acordo com a legislação em vigor e as políticas internas.
  - Todos os Colaboradores devem:
    - Estar atentos para os riscos aos quais as suas atividades rotineiras estão expostas e
    - Proativamente implementar ou reforçar controles adicionais, visando evitar a materialização de riscos.
  - A área de Compliance deve verificar a efetividade do funcionamento de controles através de um programa de testes.

- Os riscos aos quais a Empresa está exposta são categorizados conforme quadro de taxonomia abaixo.

TAXONOMIA	**DEFINIÇÃO**
Cibernético	Risco operacional específico de ataques maliciosos digitais que comprometam sistema de informação da Empresa e a confidencialidade, integridade ou disponibilidade das informações.
Financeiro	Risco de perda financeira resultante da materialização de risco Operacional, Legal, Regulatório ou Reputacional.
Legal	Risco de penalidades decorrentes de processos judiciais de qualquer natureza ou extrajudiciais.
Operacional	Risco Operacional é risco de materialização de falhas, deficiências ou inadequação de processos, controles, pessoas e sistemas, que pode adicionalmente resultar na materialização de Risco i) Financeiro, ii) Legal, iii) Regulatório e/ou iv) Reputacional.
Proteção de dados	Risco operacional específico de vazamento de dados de clientes, cotistas, colaboradores, parceiros de negócios e contrapartes de operações protegidos por lei/regulação.
Regulatório	Risco de sanções administrativas, multas e suspensão de atividades decorrentes do não cumprimento de leis e regulações emitidas por órgãos reguladores e autorreguladores.
Reputacional	Risco de percepção negativa da imagem da Empresa diante de clientes, cotistas, órgãos reguladores e autorreguladores, colaboradores, parceiros de negócio e do público em geral, podendo resultar em perdas de credibilidade, de participação de mercado ("*market share*") com perda de negócios e de não concretização de novos negócios.
Tecnológico	Risco Operacional específico de interrupção dos serviços devido a falhas, obsolescência ou indisponibilidade de hardware, software e infraestrutura de rede.

- As ações de resposta aos riscos inerentes são:
  - **Mitigar**
    Resposta que envolve adotar controles para diminuir a probabilidade de o evento se materializar e/ou o seu impacto. Esse tipo de resposta ao risco visa reduzir o nível de risco inerente a nível de risco residual dentro do apetite de risco da Empresa.
  - **Evitar**
    Resposta que envolve não realizar a atividade que gera o risco, evitando a exposição ao risco. Esse tipo de resposta visa zerar o nível de risco inerente.
  - **Transferir**
    Resposta que envolve reduzir a severidade do risco transferindo uma parcela do impacto financeiro para um terceiro. Esse tipo de resposta ao risco visa reduzir o nível de risco inerente a nível de risco residual dentro do apetite de risco da Empresa.
  - **Aceitar**
    Resposta que envolve não tomar nenhuma ação ativa para mitigar, evitar ou transferir o risco. Esse tipo de resposta ao risco não reduz o nível de risco inerente e só deve ser empregado quando o nível e risco for baixo e o custo de controle for maior do que o prejuízo que ele causaria.

- A decisão de Evitar, Transferir ou Aceitar determinado risco compete ao Comitê de Risco e Compliance.
  - As unidades de negócio, mediante identificação de risco, antes de adotar uma destas respostas ao risco devem consultar a área de Compliance.

- Na gestão de riscos, a Empresa deve implementar controles de forma que eles autem nas seguintes três dimensões: i) cronologia, ii) execução e iii) estratégia.

  Cronologia
  - Preventivo
    É o controle cujo objetivo é impedir que o evento ocorra.
  - Detectivo
    É o controle cujo objetivo é identificar eventual falha após o evento ocorrer e impedir que o dano se propague.
  - Corretivo
    É o controle cujo objetivo é remediar a situação, após o impacto do evento ter ocorrido, restaurar a operação e mitigar os prejuízos.

  Execução
  - Automatizado
    É o controle executado integralmente por softwares.
  - Manual
    É o controle executado inteiramente por pessoas.
  - Semiautomatizado
    É o controle que é executado parcialmente de forma manual e parcialmente de forma automatizada.

  Estratégia
  - Administrativo
    É o controle cujo objetivo é orientar o comportamento corporativo e é implementado através de políticas, normas e treinamentos.
  - Diretivo

É o controle que orienta e determina explicitamente como realizar uma atividade em conformidade com as normas internas é implementado através de manuais de procedimentos operacionais.

- Técnico
  É a salvaguarda lógica implementada via hardware ou software para proteger os ativos da Empresa.
- Físico
  É a barreira física que tem por objetivo proteger o perímetro e a integridade física dos colaboradores, das instalações e dos equipamentos.
- Dissuasivo
  É o controle que visa desencorajar potenciais infratores (internos ou externos) ao deixar claras as consequências da violação e que é implementado através de avisos e cláusulas contratuais.
- Compensatório
  É uma solução temporária utilizada quando o controle ideal não pode ser implementado por limitações financeiras ou operacionais ou quando a implementação do controle ideal levará mais tempo do que o aceito de acordo com o apetite a riscos da Empresa.

IDENTIFICANDO EVENTOS DE RISCOS

- Eventos de riscos podem ser identificados: i) pela própria área onde o evento de risco tenha se materializado, ii) em atividades de monitoramento de Compliance, iii) em revisões de auditoria externa ou iv) por exames de reguladores e autorreguladores.

- Todos os Colaboradores devem:
  - Reportar à área de Compliance e ao Head da unidade organizacional onde atuam, em no máximo 2 (dois) dias úteis a partir da data de identificação do evento de risco do qual tome conhecimento.
    - O reporte do evento deve ser realizado, independentemente de ter causado perda ou não, de acordo com procedimento específico estabelecido.

REGISTRANDO EVENTOS DE RISCOS

- O reporte do evento de risco operacional para a área de Compliance deve incluir, no mínimo:
  - Taxonomia do Risco
  - Data de ocorrência

    Data em que o evento de risco ocorreu de fato
  - Data de identificação

    Data em que o evento de risco foi identificado
  - Unidade organizacional onde o evento de risco se materializou
  - Título

    Curta descrição que identifique o evento ocorrido
  - Descrição detalhada do evento de risco

    Descrição do que ocorreu, de como o evento foi detectado, dos impactos internos e externos detectados
  - Identificação da causa raiz

    Descrição do fato gerador que deu causa ao evento de risco

- Plano de Ações a ser executado para remediar evento de risco e para evitar que novos eventos similares ocorram a partir do conhecimento da causa raiz.
  - O plano de ação deve conter as ações a serem executadas, os responsáveis pela execução de cada ação, data prevista de início e fim.

- A unidade organizacional onde o evento de risco se materializou é responsável por prover todas as informações necessárias para o registro do evento.
  - O Head da unidade organizacional deve revisar e aprovar o plano de ação.

- Os eventos de risco devem ser classificados, pela área de Compliance, em nível de severidade quanto ao seu possível ou real impacto, seguindo a Metodologia de Classificação de Evento de Risco.

APROVANDO PLANOS DE AÇÃO

- A área de Compliance deve avaliar e aprovar a adequação do plano de ação.
  - Plano de ações de eventos classificados como de severidade média ou alta deve dever ser levado pela área de Compliance para aprovação do Comitê de Risco e Compliance.

MONITORANDO PLANOS DE AÇÃO

- A área de Compliance deve monitorar o progresso do plano de ações até a sua conclusão.
  - Esse monitoramento deve incluir métricas a serem reportadas mensalmente ao Comitê de Risco e Compliance e à Diretoria Estatutária que permitam o devido acompanhamento do gerenciamento do risco.

- A área de Compliance deve implementar procedimento que assegure o reporte dos eventos de risco ao Comitê de Risco e Compliance com o objetivo de manter a Diretoria Estatutária atualizada.

- O prazo para remediação das falhas identificadas que causaram a materialização do evento de risco deve observar a tabela abaixo, conforme o nível de severidade do evento.
  - Exceções aos limites estabelecidos por esta Política devem ser aprovadas pelo Comitê de Risco e Compliance.

SEVERIDADE DO EVENTO	PRAZO MÁXIMO
ALTA	90 dias
MÉDIA	180 dias
BAIXA	360 dias

IV. RESPONSABILIDADES

Colaboradores

- Implementar controles em observância às normas nas suas atividades rotineiras objetivando a mitigação dos riscos relacionados
- Reportar à área de Compliance e ao Head da unidade organizacional onde atuam evento de risco.

Head de Unidade Organizacional

- Avaliar e aprovar a adequação de plano de ação para endereçar evento de risco que tenha ocorrido em sua unidade.

Compliance e Controles Internos

- Verificar a efetividade do funcionamento de controles.
- Implementar procedimento de registro de eventos de risco.
- Manter registro de eventos de risco.
- Classificar os eventos de risco quanto à severidade.
- Avaliar e aprovar a adequação de plano de ação para endereçar evento de risco.
- Submeter à aprovação do Comitê de Risco e Compliance plano de ações referente a evento classificado como de severidade média ou alta.
- Monitorar o progresso do plano de ações até a sua conclusão.
- Reportar mensalmente o progresso do plano de ações ao Comitê de Risco e Compliance.

Área de Risco

- Monitorar os eventos de riscos operacionais que tenham impacto nos fundos geridos pela Leto Asset Management.

Comitê de Risco e Compliance

- Revisar e aprovar plano de ações referente a evento classificado como de severidade média ou alta.
- Supervisionar o progresso do plano de ações.

V. PROPRIEDADE & GOVERNANÇA

Esta Política é de responsabilidade da Área de Compliance. Ela deve ser revisada pelo menos a cada 24 meses e deve ser aprovada pela Diretoria Estatutária.

VI. HISTÓRICO DE VERSÕES

25/06/2026	Versão 1.0	Criação de documento específico para a gestão de riscos corporativos.