

POLÍTICA DE GERENCIAMENTO DE RISCOS – NOROBANK

1. Objetivo

1.1. Esta Política tem como objetivo estabelecer diretrizes e responsabilidades para a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos que possam impactar os objetivos estratégicos, operacionais, legais, financeiros e reputacionais da Norobank.

Visa garantir a resiliência operacional e a conformidade regulatória, promovendo uma cultura de risco sólida e aderente ao nosso modelo de negócios como subadquirente digital.

2. Abrangência

Aplica-se a todas as áreas, processos, sistemas, colaboradores, parceiros e prestadores de serviço da Norobank, especialmente aqueles que envolvem:

- Processamento e liquidação de transações financeiras
- Tratamento de dados pessoais e sensíveis (LGPD)
- Relacionamento com credenciadoras, bandeiras e instituições financeiras
- Segurança cibernética e continuidade de negócios

3. Princípios Norteadores

- **Proporcionalidade:** O gerenciamento de riscos será compatível com o porte, complexidade e perfil de risco da Norobank.
- **Transparência e Comunicação:** Riscos relevantes devem ser reportados tempestivamente à alta administração.
- **Responsabilização:** A gestão de riscos é responsabilidade de todos, com papéis bem definidos.
- **Segregação de Funções:** A função de gerenciamento de riscos atua de forma independente da primeira linha (operações).

4. Classificação dos Riscos

4.1. Risco Operacional

Riscos decorrentes de falhas em processos, pessoas, sistemas ou eventos externos. Exemplos:

- Fraude interna ou externa
- Erros de processamento de pagamentos
- Indisponibilidade de sistemas

4.2. Risco de Crédito

Riscos relacionados à inadimplência ou falência de clientes ou parceiros envolvidos em transações com responsabilidade solidária.

4.3. Risco de Liquidez

Possibilidade de a Norobank não conseguir honrar suas obrigações financeiras no prazo esperado, especialmente em dias de liquidação de transações.

4.4. Risco de Mercado

Riscos oriundos da variação de taxas, câmbio ou outros indicadores que impactem receitas ou custos financeiros.

4.5. Risco Legal e Regulatórios

Riscos associados a sanções, processos judiciais, autuações de órgãos reguladores, incluindo o Banco Central, ANPD e Receita Federal.

4.6. Risco de Imagem/Reputação

Impactos negativos derivados de falhas operacionais, incidentes de segurança, vazamentos de dados ou má conduta empresarial.

4.7. Risco Cibernético

Ameaças de ataques externos, ransomwares, phishing, vazamento de dados ou exploração de vulnerabilidades.

5. Processo de Gestão de Riscos:

5.1. Identificação

Realizada de forma contínua por meio de entrevistas, checklists, análise de processos, auditorias internas, eventos de perda e indicadores de risco.

5.2. Avaliação e Classificação

Cada risco é classificado segundo:

- Probabilidade de ocorrência (baixa, média, alta)
- Impacto (financeiro, legal, operacional, reputacional)
- Grau de exposição (risco inerente e residual)

5.3. Tratamento

Estratégias adotadas:

- Mitigação (implementação de controles)
- Aceitação (com base no apetite a risco)
- Transferência (seguros, contratos com terceiros)
- Eliminação (revisão ou encerramento do processo)

5.4. Monitoramento Contínuo

Métricas e indicadores-chave de risco (KRIs) são acompanhados mensalmente. Riscos críticos são reportados à diretoria.

5.5. Testes de Estresse e Simulações

Realizados anualmente para avaliar a capacidade de resposta a cenários adversos, incluindo falhas sistêmicas, crises reputacionais e ataques cibernéticos.

6. Penalidades e Responsabilidades

A negligência no reporte ou tratamento de riscos poderá resultar em medidas disciplinares, conforme o Código de Ética e Conduta da Norobank.