	Versão	Data de criação	Data de atualização	Autor	Revisado por	Aprovado por /data	Descrição das alterações
moneria	1.0	24/07/2025		José Souza	Andrey Santos	David Santos	[inserir descrição]
	1.2		16/02/2026	José Souza	Compliance	David Santos	Atualização Padrão

Controle de acesso:

Cargo ou função	Acesso permitido (somente leitura, ler e editar/atualizar)
Diretoria, Andrey, Consultoria JS	Ler e editar/atualizar
Diretoria	Leitura e aprovação
Colaboradores	Leitura

Observações: [inserir quaisquer observações relevantes sobre a política]

FRAMEWORK DE GESTÃO DE RISCOS DE TERCEIROS (TPRM)

Sumário

1. OBJETIVO

Estabelecer a estrutura integrada de gestão de riscos de terceiros da Moneria, abrangendo todo o ciclo de vida de fornecedores e parceiros, assegurando:

1. Conformidade regulatória (BACEN, LGPD, PCI DSS)
2. Mitigação de riscos operacionais, tecnológicos e legais
3. Segurança da informação e proteção de dados
4. Governança contínua e auditável

2. ESCOPO

Aplica-se a:

1. Fornecedores e prestadores de serviço
2. Parceiros tecnológicos
3. Provedores cloud (AWS, SaaS)
4. Integradores e APIs
5. Terceiros com acesso a dados ou sistemas

Inclui terceiros envolvidos em:

1. Pix / SPI / STR
2. CDE (PCI DSS)
3. Dados pessoais (LGPD)

3. MODELO DE GOVERNANÇA TPRM (ESTRUTURA)

O framework é estruturado em **5 pilares**:

PILAR 1 — GOVERNANÇA DE TERCEIROS

(Base: Política de Gestão de Terceiros)

Responsável por:

a. Estrutura organizacional

b. Classificação de fornecedores

c. Definição de papéis e responsabilidades

d. Atribuição de criticidade

Classificação de Risco

Nível	Descrição
Crítico	Impacto direto no negócio ou CDE
Alto	Acesso a dados sensíveis
Médio	Impacto moderado
Baixo	Impacto limitado

PILAR 2 — DUE DILIGENCE (ONBOARDING)

(Base: Política de Due Diligence)

Etapas obrigatórias

1. Coleta de informações
2. Avaliação de segurança
3. Avaliação de LGPD
4. Avaliação técnica
5. Avaliação de continuidade
6. Score de risco

Outputs obrigatórios

a. Classificação de risco

b. Relatório de avaliação

c. Plano de mitigação

d. Aprovação formal

PILAR 3 — CONTRATUALIZAÇÃO SEGURA

(Base: Política de Cláusulas Contratuais)

Todo contrato deve conter:

a. Cláusula de confidencialidade

b. Cláusula LGPD

c. Requisitos de segurança

d. Direito de auditoria

e. SLA

f. Notificação de incidentes

Para fornecedores PCI (CDE)

a. Conformidade PCI DSS v4.0.1

b. Tokenização

c. Logs auditáveis

d. Testes de segurança

PILAR 4 — AVALIAÇÃO CONTÍNUA DE SEGURANÇA

(Base: Política de Avaliação de Segurança)

Tipos de avaliação

a. Documental (ISO, SOC, PCI)

b. Técnica (arquitetura, APIs)

c. Compliance (LGPD, BACEN)

d. Continuidade (PCN/DRP)

Frequência

Nível	Frequência
Crítico	Contínuo
Alto	Anual
Médio	Bienal
Baixo	Sob demanda

PILAR 5 — MONITORAMENTO CONTÍNUO E OFFBOARDING

(Novo — fechamento do ciclo)

Monitoramento contínuo

a. SLA

b. Incidentes

c. Performance

d. Risco dinâmico

Offboarding de fornecedores (CRÍTICO)

Deve incluir:

a. Revogação imediata de acessos

b. Exclusão de dados

c. Desvinculação de sistemas

d. Evidência de descarte

e. Encerramento contratual formal

4. CICLO DE VIDA DE TERCEIROS (END-TO-END)

1. Identificação da necessidade
2. Due diligence
3. Classificação de risco
4. Contratação
5. Integração técnica
6. Monitoramento contínuo
7. Reavaliação periódica
8. Offboarding

5. MATRIZ DE RESPONSABILIDADE (RACI)

Função	Responsabilidade
Segurança	Avaliação técnica
Compliance	Regulação
Jurídico	Contratos
TI	Integração
Negócio	Justificativa

6. GESTÃO DE RISCOS DE TERCEIROS

Inclui:

a. Risco operacional

b. Risco de segurança

c. Risco regulatório

d. Risco de continuidade

e. Risco de dados (LGPD)

7. INTEGRAÇÃO COM REGULAÇÃO

O framework atende:

BACEN

a. CMN 4.658/2018

b. CMN 5.274/2025

c. BCB 538/2025

LGPD

a. Proteção de dados pessoais

b. Controle de terceiros

PCI DSS

a. Gestão de terceiros no CDE

b. Responsabilidade compartilhada

8. INDICADORES (KPIs/KRIs)

a. % fornecedores avaliados

b. % fornecedores críticos monitorados

c. Incidentes por fornecedor

d. Tempo de resposta

e. Score médio de risco

9. AUDITORIA E EVIDÊNCIA

Devem ser mantidos:

a. Questionários de due diligence

b. Relatórios de avaliação

c. Contratos

d. Evidências de auditoria

e. Registros de offboarding

10. GESTÃO DE INCIDENTES DE TERCEIROS

Deve incluir:

a. Notificação imediata

b. Investigação conjunta

c. Plano de resposta

d. Mitigação

11. RESPONSABILIZAÇÃO

O descumprimento pode resultar em:

a. Rescisão contratual

b. Penalidades

c. Sanções regulatórias

d. Impacto operacional

12. REVISÃO E EVOLUÇÃO

O framework deve:

a. Evoluir continuamente

b. Incorporar novas ameaças

c. Ser revisado periodicamente

13. APROVAÇÃO E VIGÊNCIA

Aprovado pela Alta Administração.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria