	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]

POLÍTICA DE GESTÃO DE TERCEIROS

Sumário

1. OBJETIVO

Estabelecer diretrizes, critérios e controles para a gestão de terceiros e fornecedores, assegurando que a contratação, o monitoramento e a supervisão de serviços externos sejam realizados de forma segura, controlada e em conformidade com requisitos regulatórios e de segurança da informação.

2. ABRANGÊNCIA

a. Esta política aplica-se a:

b. Todos os fornecedores e prestadores de serviço

c. Parceiros tecnológicos e operacionais

d. Provedores de serviços em nuvem (cloud)

e. Terceiros com acesso a dados, sistemas ou infraestrutura da Moneria

3. REFERÊNCIAS NORMATIVAS

Regulação

a. Resolução CMN nº 4.658/2018

b. Resolução CMN nº 5.274/2025

c. Resolução BCB nº 538/2025

d. Lei nº 13.709/2018 (LGPD)

Padrões Técnicos

a. ISO/IEC 27001 e 27002

b. ISO/IEC 27701

c. PCI DSS v4.0.1

d. NIST Cybersecurity Framework

4. DEFINIÇÕES

Terceiro/Fornecedor: entidade externa que presta serviços à Moneria.

Fornecedor crítico: aquele cuja indisponibilidade ou falha impacta significativamente as operações.

Outsourcing: terceirização de atividades operacionais ou tecnológicas.

5. PRINCÍPIOS

A Moneria adota:

a. Responsabilidade indelegável sobre serviços terceirizados

b. Gestão baseada em risco

c. Due diligence obrigatória

d. Monitoramento contínuo

e. Segurança por padrão

f. Conformidade regulatória

6. CLASSIFICAÇÃO DE FORNECEDORES

Os fornecedores devem ser classificados conforme risco:

6.1 Crítico

- Impacto direto no negócio (ex: cloud, core financeiro, Pix)

6.2 Alto

- Acesso a dados sensíveis ou sistemas críticos

6.3 Médio

- Impacto operacional moderado

6.4 Baixo

- Baixo impacto e sem acesso a dados críticos

7. PROCESSO DE CONTRATAÇÃO

Antes da contratação, deve ser realizada:

7.1 Due Diligence

a. Avaliação de segurança da informação

b. Avaliação de conformidade regulatória

c. Verificação de histórico e reputação

7.2 Avaliação de Risco

a. Classificação do fornecedor

b. Identificação de riscos operacionais e tecnológicos

c. Definição de controles necessários

7.3 Aprovação Formal

a. Aprovação por áreas responsáveis

b. Registro documental

8. REQUISITOS CONTRATUAIS OBRIGATÓRIOS

Os contratos com terceiros devem incluir, no mínimo:

a. Cláusula de confidencialidade (NDA)

b. Requisitos de segurança da informação

c. Obrigações de conformidade com LGPD

d. Requisitos de continuidade de negócios

e. SLA (nível de serviço)

f. Direito de auditoria pela Moneria

g. Notificação obrigatória de incidentes

h. Responsabilidades e penalidades

9. SEGURANÇA DA INFORMAÇÃO

Os terceiros devem:

a. Implementar controles de segurança compatíveis

b. Proteger dados e sistemas

c. Utilizar acessos restritos

d. Seguir políticas da Moneria

10. CONTROLE DE ACESSO DE TERCEIROS

O acesso deve:

a. Ser limitado ao mínimo necessário

b. Ser autorizado formalmente

c. Ser monitorado continuamente

d. Ser revogado ao término do contrato

11. PROTEÇÃO DE DADOS (LGPD)

Os terceiros devem:

a. Tratar dados pessoais conforme LGPD

b. Garantir confidencialidade

c. Não utilizar dados para fins não autorizados

d. Adotar medidas de segurança adequadas

12. MONITORAMENTO CONTÍNUO

A Moneria deve:

a. Monitorar desempenho do fornecedor

b. Avaliar cumprimento de SLAs

c. Revisar riscos periodicamente

d. Identificar desvios

13. GESTÃO DE INCIDENTES

Os terceiros devem:

a. Notificar incidentes imediatamente

b. Cooperar com investigações

c. Adotar medidas corretivas

14. CONTINUIDADE DE NEGÓCIOS

A Moneria deve:

a. Avaliar planos de continuidade dos fornecedores

b. Garantir redundância quando necessário

c. Monitorar disponibilidade

15. TERCEIRIZAÇÃO EM NUVEM (CLOUD)

Para serviços cloud, a Moneria deve:

a. Avaliar modelo de responsabilidade compartilhada

b. Garantir conformidade regulatória

c. Monitorar segurança do ambiente

d. Formalizar requisitos contratuais

16. AUDITORIA E DIREITO DE VERIFICAÇÃO

A Moneria reserva-se o direito de:

a. Auditar fornecedores

b. Solicitar evidências de controle

c. Avaliar conformidade

17. REAVALIAÇÃO PERIÓDICA

Os fornecedores devem ser:

a. Reavaliados periodicamente

b. Reclassificados conforme risco

c. Submetidos a revisões contratuais

18. ENCERRAMENTO DE CONTRATO

Ao término da relação:

a. Acessos devem ser revogados

b. Dados devem ser devolvidos ou eliminados

c. Deve haver confirmação formal de exclusão

19. GESTÃO DE TERCEIROS CRÍTICOS

Para fornecedores críticos:

a. Monitoramento reforçado

b. Avaliação contínua

c. Controles adicionais

d. Testes de continuidade

20. RESPONSABILIZAÇÃO

O descumprimento desta política pode resultar em:

a. Rescisão contratual

b. Aplicação de penalidades

c. Responsabilização legal

d. Sanções regulatórias

21. INTEGRAÇÃO COM OUTRAS POLÍTICAS

Esta política se integra com:

a. Política de Segurança da Informação

b. Política de Gestão de Riscos

c. Política de Continuidade de Negócios

d. Política de LGPD

e. Política de Segurança em Nuvem

22. REVISÃO E ATUALIZAÇÃO

Esta política será:

a. Revisada periodicamente

b. Atualizada conforme requisitos regulatórios

23. APROVAÇÃO E VIGÊNCIA

Aprovada pela Alta Administração da Moneria, entrando em vigor na data de sua publicação.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria