	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 AVALIAÇÃO DE SEGURANÇA DE PARCEIROS E FORNECEDORES

Sumário

1. OBJETIVO 3
2. ABRANGÊNCIA 3
3. REFERÊNCIAS NORMATIVAS 3
4. DEFINIÇÕES 4
5. PRINCÍPIOS 4
6. CLASSIFICAÇÃO PARA AVALIAÇÃO DE SEGURANÇA 4
7. TIPOS DE AVALIAÇÃO DE SEGURANÇA 4
   7.1 Avaliação Documental 4
   7.2 Avaliação Técnica 5
   7.3 Avaliação de Conformidade 5
   7.4 Avaliação de Continuidade 5
8. VALIDAÇÃO DE CONTROLES 5
9. AVALIAÇÃO DE SEGURANÇA EM CLOUD 6
10. AVALIAÇÃO DE SEGURANÇA DE APIs 6
11. TESTES DE SEGURANÇA 6
12. FREQUÊNCIA DE AVALIAÇÃO 6
13. MONITORAMENTO CONTÍNUO 7
14. EVENTOS DE REAVALIAÇÃO OBRIGATÓRIA 7
15. GESTÃO DE NÃO CONFORMIDADES 7
16. PLANOS DE MITIGAÇÃO 7
17. DIREITO DE AUDITORIA 8
18. INTEGRAÇÃO COM DUE DILIGENCE 8
19. DOCUMENTAÇÃO E EVIDÊNCIA 8
20. RESPONSABILIDADES 8

21. RESPONSABILIZAÇÃO 9
22. REVISÃO E ATUALIZAÇÃO 9
23. APROVAÇÃO E VIGÊNCIA 9

1. OBJETIVO

Estabelecer diretrizes, critérios e processos para avaliação contínua da postura de segurança da informação de parceiros e fornecedores, assegurando que os controles implementados sejam adequados, eficazes e compatíveis com os requisitos da Moneria e obrigações regulatórias.

2. ABRANGÊNCIA

Esta política aplica-se a:

a. Fornecedores e parceiros tecnológicos
b. Prestadores de serviços com acesso a sistemas ou dados
c. Provedores de cloud e SaaS
d. Terceiros integrados via APIs
e. Parceiros envolvidos em Pix, SPI, STR e CDE

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 SP 800-53 / 800-161

4. DEFINIÇÕES

Avaliação de segurança: processo de validação técnica e documental dos controles de segurança de um parceiro.

Security assurance: garantia contínua de que controles permanecem eficazes.

Parceiro crítico: parceiro com impacto direto em operações essenciais ou dados sensíveis.

5. PRINCÍPIOS

A Moneria adota:

a. Avaliação contínua (não pontual)

b. Validação baseada em evidências

c. Abordagem baseada em risco

d. Verificação independente sempre que necessário

e. Segurança por padrão

f. Responsabilidade indelegável

6. CLASSIFICAÇÃO PARA AVALIAÇÃO DE SEGURANÇA

Os parceiros devem ser classificados conforme:

a. Acesso a dados sensíveis

b. Integração com sistemas críticos

c. Impacto operacional

d. Dependência tecnológica

7. TIPOS DE AVALIAÇÃO DE SEGURANÇA

A Moneria deve realizar:

7.1 Avaliação Documental

a. Políticas de segurança

b. Certificações (ISO, SOC 2, PCI)

c. Relatórios de auditoria

7.2 Avaliação Técnica

a. Arquitetura de segurança

b. Controles de acesso

c. Criptografia

d. Logs e monitoramento

e. Segurança de APIs

7.3 Avaliação de Conformidade

a. LGPD

b. BACEN

c. PCI DSS

7.4 Avaliação de Continuidade

a. PCN/DRP

b. Testes de recuperação

c. Redundância

8. VALIDAÇÃO DE CONTROLES

A Moneria deve validar, quando aplicável:

a. Configuração de segurança

b. Segregação de ambientes

c. Gestão de acessos

d. Proteção de dados

e. Monitoramento ativo

9. AVALIAÇÃO DE SEGURANÇA EM CLOUD

Para parceiros cloud:

a. Avaliar responsabilidade compartilhada

b. Verificar configurações seguras

c. Validar logs (CloudTrail, etc.)

d. Avaliar exposição pública

10. AVALIAÇÃO DE SEGURANÇA DE APIs

Para integrações:

a. Autenticação forte (mTLS, OAuth)

b. Criptografia de dados

c. Controle de acesso

d. Proteção contra ataques (OWASP API Top 10)

11. TESTES DE SEGURANÇA

Quando necessário, a Moneria pode exigir:

a. Pentests independentes

b. Testes de vulnerabilidade

c. Testes de segmentação (PCI)

12. FREQUÊNCIA DE AVALIAÇÃO

Nível	Frequência
Crítico	Contínua + revisão anual
Alto	Anual
Médio	Bienal
Baixo	Sob demanda

13. MONITORAMENTO CONTÍNUO

Inclui:

a. Monitoramento de incidentes

b. Revisão de logs (quando aplicável)

c. Avaliação de performance

d. Reavaliação de risco

14. EVENTOS DE REAVALIAÇÃO OBRIGATÓRIA

Deve ocorrer nova avaliação em caso de:

a. Incidente de segurança

b. Mudança tecnológica relevante

c. Alteração contratual

d. Integração com novos sistemas

e. Mudança de controle societário

15. GESTÃO DE NÃO CONFORMIDADES

Quando identificadas falhas:

a. Registrar não conformidades

b. Classificar criticidade

c. Definir plano de ação

d. Acompanhar correção

16. PLANOS DE MITIGAÇÃO

Devem incluir:

a. Ações corretivas

b. Prazos definidos

c. Responsáveis claros

d. Monitoramento de implementação

17. DIREITO DE AUDITORIA

A Moneria reserva-se o direito de:

a. Auditar parceiros críticos

b. Solicitar evidências

c. Realizar avaliações independentes

18. INTEGRAÇÃO COM DUE DILIGENCE

A avaliação de segurança deve:

- Complementar a due diligence inicial
- Atualizar classificação de risco
- Apoiar decisões de continuidade contratual

19. DOCUMENTAÇÃO E EVIDÊNCIA

Devem ser mantidos:

a. Relatórios de avaliação

b. Evidências técnicas

c. Registros de auditoria

d. Planos de mitigação

20. RESPONSABILIDADES

Segurança da Informação

a. Conduzir avaliações técnicas

Compliance

a. Avaliar conformidade regulatória

TI

a. Apoiar validações técnicas

Jurídico

a. Garantir aderência contratual

21. RESPONSABILIZAÇÃO

A ausência de avaliação adequada pode resultar em:

a. Exposição a riscos críticos

b. Incidentes de segurança

c. Não conformidade regulatória

d. Sanções do BACEN

22. REVISÃO E ATUALIZAÇÃO

Esta política será:

a. Revisada periodicamente

b. Atualizada conforme evolução tecnológica

23. APROVAÇÃO E VIGÊNCIA

Aprovada pela Alta Administração da Moneria.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria