| | 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 | CTO | David Santos | [inserir descrição] |

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 CONFORMIDADE COM PCI DSS

## Sumário

## 1. Objetivo

Estabelecer diretrizes, controles e responsabilidades para assegurar a conformidade da Moneria com o padrão **PCI DSS (Payment Card Industry Data Security Standard)**,

garantindo a proteção de dados de pagamento, a redução de riscos e a manutenção da segurança do ambiente de dados de cartão.

## 2. Abrangência

Esta política aplica-se a:

a. Todos os sistemas que armazenam, processam ou transmitem dados de pagamento

b. Ambiente de dados de cartão (CDE – Cardholder Data Environment)

c. Infraestrutura de TI, redes e aplicações

d. Colaboradores e terceiros com acesso ao CDE

e. Ambientes on-premise e em nuvem

## 3. Referências Normativas

**Regulação**

a. Lei nº 13.709/2018 (LGPD)

b. Resolução CMN nº 4.658/2018

c. Resolução CMN nº 5.274/2025

d. Resolução BCB nº 538/2025

**Padrões Técnicos**

a. PCI DSS v4.0 (e atualizações vigentes)

b. PCI SSC (Security Standards Council) Guidelines

c. ISO/IEC 27001 e 27002

d. NIST Cybersecurity Framework

## 4. Definições

**PCI DSS:** padrão internacional de segurança para proteção de dados de cartão.

**CDE (Cardholder Data Environment):** ambiente que processa, armazena ou transmite dados de cartão.

**PAN:** número do cartão de pagamento.

**QSA (Qualified Security Assessor):** auditor certificado PCI.

## 5. Princípios

A Moneria adota:

a. Proteção integral de dados de pagamento

b. Redução do escopo do CDE

c. Princípio do menor privilégio

d. Segurança em camadas (defense in depth)

e. Monitoramento contínuo

f. Conformidade contínua (não pontual)

## 6. Estrutura de Governança PCI

A Moneria deve:

a. Designar responsável pelo programa PCI DSS

b. Manter governança formal de segurança

c. Definir papéis e responsabilidades

d. Reportar conformidade à alta administração

## 7. Escopo do CDE

A Moneria deve:

a. Identificar e documentar o escopo do CDE

b. Mapear fluxos de dados de pagamento

c. Reduzir o escopo sempre que possível

d. Segregar ambientes críticos

## 8. Requisitos de Segurança (PCI DSS)

A Moneria deve implementar os controles baseados nos **12 requisitos do PCI DSS v4.0.1**:

### 8.1 Construção e Manutenção de Rede Segura

a. Firewalls e segmentação de rede

b. Configuração segura de sistemas

### 8.2 Proteção de Dados de Cartão

a. Criptografia de dados em repouso e trânsito

b. Tokenização e mascaramento

c. Proibição de armazenamento de dados sensíveis

### 8.3 Gestão de Vulnerabilidades

a. Antivírus e proteção contra malware

b. Atualizações e patches

c. Scans regulares

### 8.4 Controle de Acesso

a. Acesso baseado em necessidade

b. Identificação individual

c. MFA para acessos críticos

### 8.5 Monitoramento e Testes

a. Logs e monitoramento contínuo

b. Testes de segurança

c. Pentests periódicos

### 8.6 Política de Segurança da Informação

a. Política formal e atualizada

b. Treinamento de colaboradores

c. Conscientização contínua

## 9. Controle de Acesso ao CDE

A Moneria deve:

a. Restringir acesso ao mínimo necessário

b. Monitorar acessos privilegiados

c. Registrar todas as atividades

d. Revisar acessos periodicamente

## 10. Criptografia e Proteção de Dados

A Moneria deve:

a. Criptografar dados com algoritmos fortes

b. Proteger chaves criptográficas

c. Utilizar tokenização sempre que possível

d. Evitar exposição de dados sensíveis

## 11. Monitoramento e Logs

A Moneria deve:

a. Registrar todas as atividades no CDE

b. Monitorar acessos e eventos

c. Utilizar SIEM

d. Garantir integridade dos logs

## 12. Gestão de Vulnerabilidades

A Moneria deve:

a. Realizar scans trimestrais (ou conforme PCI)

b. Corrigir vulnerabilidades críticas rapidamente

c. Executar testes de intrusão periódicos

d. Monitorar continuamente riscos

## 13. Testes de Segurança

a. Devem ser realizados:

a. Testes de intrusão (pentest)

b. Testes de segmentação

c. Testes de aplicações

d. Validação de controles

## 14. Gestão de Terceiros

A Moneria deve:

a. Avaliar fornecedores que acessam o CDE

b. Exigir conformidade com PCI DSS

c. Formalizar responsabilidades contratuais

d. Monitorar continuamente

## 15. Gestão de Incidentes

Incidentes envolvendo dados de pagamento devem:

a. Ser tratados como críticos

b. Ser registrados imediatamente

c. Acionar resposta a incidentes

d. Seguir requisitos de notificação

## 16. Treinamento e Conscientização

A Moneria promove:

a. Treinamento obrigatório em PCI DSS

b. Conscientização sobre segurança

c. Atualização contínua

## 17. Auditoria e Certificação

A Moneria deve:

a. Realizar auditorias internas

b. Submeter-se a avaliação por QSA quando aplicável

c. Manter evidências de conformidade

d. Produzir relatórios (ROC, SAQ, etc.)

## 18. Gestão de Documentação

A Moneria deve manter:

a. Políticas atualizadas

b. Procedimentos documentados

c. Evidências de controle

d. Registros auditáveis

## 19. Monitoramento Contínuo de Conformidade

A Moneria deve:

a. Monitorar controles continuamente

b. Identificar desvios

c. Implementar ações corretivas

d. Manter conformidade contínua

## 20. Integração com Outras Políticas

Esta política se integra com:

a. Política de Gestão de Dados de Pagamento

b. Política de Criptografia

c. Política de IAM

d. Política de Logs

e. Política de Segurança em Nuvem

f. Política de Vulnerabilidades

## 21. Responsabilização

O descumprimento desta política pode resultar em:

a. Medidas disciplinares

b. Penalidades contratuais

c. Sanções regulatórias

d. Perda de certificação PCI DSS

## 22. Revisão e Atualização

Esta política será:

a. Revisada anualmente

b. Atualizada conforme mudanças no PCI DSS

## 23. Aprovação

Aprovada pela Alta Administração da Moneria.

## 24. Vigência

Esta política entra em vigor na data de sua aprovação.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria