	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

POLÍTICA DE TOKENIZAÇÃO E PROTEÇÃO DO PAN (PRIMARY ACCOUNT NUMBER)

Sumário

1. Objetivo

Estabelecer diretrizes, controles e mecanismos para proteção do PAN (Primary Account Number) e demais dados de cartão, por meio de criptografia, tokenização e controles de acesso, assegurando conformidade com o PCI DSS e mitigação de riscos de exposição de dados sensíveis.

2. Abrangência

Esta política aplica-se a:

a. Todos os sistemas que armazenam, processam ou transmitem PAN

b. Ambientes que integram o CDE

c. Sistemas de tokenização

d. APIs, aplicações e integrações

e. Colaboradores e terceiros com acesso a dados de pagamento

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 (Requisitos 3 e 4)

b. PCI SSC Tokenization Guidelines

c. ISO/IEC 27001 e 27002

d. NIST SP 800-57 (gestão de chaves)

4. Definições

PAN (Primary Account Number): número do cartão do portador.

Tokenização: processo de substituição do PAN por um identificador (token) sem valor explorável fora do sistema.

Token: representação não sensível de dados de pagamento.

Vault (cofre de tokenização): ambiente seguro onde o PAN é armazenado e associado ao token.

5. Princípios

A Moneria adota:

a. Minimização do armazenamento de PAN

b. Uso obrigatório de tokenização sempre que possível

c. Criptografia forte de dados sensíveis

d. Redução do escopo do CDE

e. Proteção em camadas (defense in depth)

f. Rastreabilidade e controle rigoroso

6. Proibição de Armazenamento Indevido

É expressamente proibido:

a. Armazenar PAN em texto claro

b. Armazenar dados sensíveis de autenticação (ex: CVV) após autorização

c. Registrar PAN completo em logs

7. Tokenização de Dados de Cartão

A Moneria deve:

a. Implementar tokenização para todos os dados de pagamento

b. Substituir PAN por tokens em sistemas internos

c. Utilizar tokens em integrações e APIs

d. Garantir que tokens não possam ser revertidos sem acesso ao vault

8. Arquitetura de Tokenização

A solução de tokenização deve:

a. Utilizar vault seguro e segregado

b. Isolar o armazenamento de PAN

c. Controlar rigorosamente acesso ao vault

d. Ser auditável e monitorada

9. Proteção do PAN

O PAN deve ser:

a. Criptografado em repouso (ex: AES-256)

b. Criptografado em trânsito (TLS 1.2+)

c. Acessado apenas quando estritamente necessário

d. Protegido contra exposição

10. Mascaramento de PAN

A Moneria deve:

a. Exibir apenas parte do PAN (ex: **** **** **** 1234)

b. Restringir visualização completa a usuários autorizados

c. Aplicar mascaramento em interfaces e relatórios

11. Gestão de Chaves Criptográficas

A Moneria deve:

a. Utilizar KMS/HSM para gestão de chaves

b. Separar chaves dos dados

c. Controlar acesso às chaves

d. Realizar rotação periódica

12. Controle de Acesso ao PAN

O acesso ao PAN deve:

a. Ser restrito ao mínimo necessário

b. Utilizar autenticação forte

c. Ser monitorado continuamente

d. Ser revisado periodicamente

13. Monitoramento e Logs

A Moneria deve:

a. Registrar acessos ao PAN

b. Monitorar uso de tokens

c. Detectar comportamentos anômalos

d. Garantir logs imutáveis

14. Tokenização em APIs e Integrações

As APIs devem:

a. Utilizar tokens ao invés de PAN

b. Evitar exposição de dados sensíveis

c. Implementar autenticação robusta

d. Monitorar requisições

15. Gestão de Vulnerabilidades

A Moneria deve:

a. Avaliar vulnerabilidades no sistema de tokenização

b. Realizar testes periódicos

c. Priorizar correções críticas

d. Monitorar continuamente

16. Testes de Segurança

Devem ser realizados:

a. Testes de intrusão

b. Avaliação de reversibilidade de tokens

c. Testes de exposição de dados

d. Validação de controles criptográficos

17. Gestão de Terceiros

A Moneria deve:

a. Avaliar fornecedores de tokenização

b. Garantir conformidade com PCI DSS

c. Formalizar requisitos contratuais

d. Monitorar continuamente

18. Gestão de Incidentes

Incidentes envolvendo PAN devem:

a. Ser tratados como críticos

b. Ser registrados imediatamente

c. Acionar resposta a incidentes

d. Avaliar necessidade de notificação

19. Redução de Escopo PCI

A Moneria deve:

a. Utilizar tokenização para reduzir escopo do CDE

b. Isolar sistemas que armazenam PAN

c. Minimizar exposição de dados

20. Auditoria e Conformidade

Os controles de tokenização estão sujeitos a:

a. Auditorias PCI DSS

b. Avaliações por QSA

c. Auditorias internas

21. Treinamento e Conscientização

A Moneria promove:

a. Treinamento sobre proteção de dados de cartão

b. Capacitação em PCI DSS

c. Conscientização sobre riscos

22. Integração com Outras Políticas

Esta política se integra com:

a. Política de Gestão de Dados de Pagamento

b. Política de Criptografia

c. Política de Gestão de Chaves

d. Política de IAM

e. Política de Segurança de APIs

23. Responsabilização

O descumprimento desta política pode resultar em:

a. Medidas disciplinares

b. Sanções regulatórias

c. Perda de conformidade PCI DSS

d. Impactos operacionais

24. Revisão e Atualização

Esta política será:

a. Revisada anualmente

b. Atualizada conforme evolução do PCI DSS

25. Aprovação

Aprovada pela Alta Administração da Moneria.

26. Vigência

Esta política entra em vigor na data de sua aprovação.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria