	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 GESTÃO DO AMBIENTE DE DADOS DE CARTÃO (CDE)

Sumário

1. Objetivo

Estabelecer diretrizes, controles e responsabilidades para a gestão segura do Ambiente de Dados de Cartão (CDE), assegurando a proteção, segregação, monitoramento e conformidade com o PCI DSS e demais requisitos regulatórios aplicáveis.

2. Abrangência

Esta política aplica-se a:

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

b. Infraestrutura, redes e aplicações que compõem ou suportam o CDE

c. Ambientes on-premise e em nuvem

d. Colaboradores e terceiros com acesso ao CDE

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 v4.0.1

b. PCI SSC Guidelines (CDE Scoping e Segmentation)

c. ISO/IEC 27001 e 27002

d. NIST Cybersecurity Framework

4. Definições

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

Dados de cartão: PAN, dados de autenticação e informações relacionadas.

Segmentação: isolamento lógico ou físico do CDE.

5. Princípios

A Moneria adota:

a. Redução do escopo do CDE

b. Segregação rigorosa de ambientes

c. Controle de acesso restrito

d. Monitoramento contínuo

e. Segurança em camadas (defense in depth)

f. Conformidade contínua com PCI DSS

6. Definição e Escopo do CDE

A Moneria deve:

a. Identificar todos os ativos que compõem o CDE

b. Mapear fluxos de dados de pagamento (data flow)

c. Documentar conexões com outros ambientes

d. Revisar periodicamente o escopo

7. Segmentação do CDE

O CDE deve:

a. Ser isolado de outros ambientes

b. Utilizar segmentação de rede (firewalls, VLANs, VPCs)

c. Restringir tráfego apenas ao necessário

d. Ser validado por testes de segmentação

8. Arquitetura Segura do CDE

A Moneria deve garantir:

a. Arquitetura dedicada ou segregada

b. Redundância de componentes críticos

c. Proteção contra acesso externo não autorizado

d. Controle rigoroso de comunicação entre sistemas

9. Controle de Acesso ao CDE

O acesso ao CDE deve:

a. Ser baseado no princípio do menor privilégio

b. Utilizar autenticação forte (MFA obrigatório)

c. Ser individual e rastreável

d. Ser revisado periodicamente

10. Gestão de Identidade no CDE

A Moneria deve:

a. Proibir contas genéricas

b. Monitorar acessos privilegiados

c. Controlar sessões administrativas

d. Registrar todas as atividades

11. Proteção de Dados no CDE

A Moneria deve:

a. Evitar armazenamento de dados sensíveis quando possível

b. Utilizar tokenização

c. Implementar mascaramento de dados

d. Proibir armazenamento de dados em texto claro

12. Criptografia no CDE

A Moneria deve:

a. Criptografar dados em repouso e em trânsito

b. Utilizar algoritmos fortes (AES-256, TLS 1.2+)

c. Gerenciar chaves de forma segura

d. Rotacionar chaves periodicamente

13. Monitoramento e Logs do CDE

A Moneria deve:

a. Registrar todas as atividades no CDE

b. Monitorar acessos e eventos críticos

c. Integrar logs com SIEM

d. Garantir integridade e imutabilidade dos logs

14. Gestão de Vulnerabilidades no CDE

A Moneria deve:

a. Realizar scans regulares

b. Priorizar correções críticas

c. Executar pentests periódicos

d. Monitorar continuamente o ambiente

15. Hardening do CDE

Os sistemas do CDE devem:

a. Seguir baselines de segurança

b. Desativar serviços desnecessários

c. Restringir portas e protocolos

d. Ser continuamente monitorados

16. Gestão de Mudanças no CDE

Mudanças devem:

a. Seguir processo formal

b. Ser testadas antes da produção

c. Ser aprovadas previamente

d. Ser rastreáveis

Mudanças emergenciais devem ser justificadas e revisadas posteriormente.

17. Gestão de Terceiros no CDE

A Moneria deve:

a. Avaliar fornecedores com acesso ao CDE

b. Garantir conformidade PCI DSS

c. Formalizar responsabilidades contratuais

d. Monitorar continuamente acessos

18. Testes de Segurança no CDE

Devem ser realizados:

a. Testes de intrusão (pentest)

b. Testes de segmentação

c. Avaliações de vulnerabilidade

d. Validação de controles

19. Monitoramento Contínuo do CDE

A Moneria deve:

a. Monitorar eventos em tempo real

b. Detectar comportamentos anômalos

c. Gerar alertas automáticos

d. Integrar com resposta a incidentes

20. Gestão de Incidentes no CDE

Incidentes devem:

a. Ser tratados como críticos

b. Ser registrados imediatamente

c. Acionar resposta a incidentes

d. Avaliar necessidade de notificação regulatória

21. Continuidade de Negócios

O CDE deve:

a. Estar incluído no PCN

b. Possuir alta disponibilidade

c. Ter mecanismos de recuperação

d. Ser testado periodicamente

22. Auditoria e Conformidade

O CDE está sujeito a:

a. Auditorias PCI DSS

b. Avaliações por QSA

c. Auditorias internas

d. Avaliações regulatórias

23. Documentação do CDE

A Moneria deve manter:

a. Inventário de ativos do CDE

b. Diagramas de arquitetura

c. Fluxos de dados

d. Evidências de controle

24. Treinamento e Conscientização

A Moneria promove:

a. Treinamento específico sobre CDE

b. Capacitação em PCI DSS

c. Conscientização sobre riscos

25. Integração com Outras Políticas

Esta política se integra com:

a. Política de Conformidade PCI DSS

b. Política de Gestão de Dados de Pagamento

c. Política de Criptografia

d. Política de IAM

e. Política de Logs

f. Política de Segurança em Nuvem

26. Responsabilização

O descumprimento desta política pode resultar em:

a. Medidas disciplinares

b. Sanções regulatórias

c. Perda de conformidade PCI DSS

d. Impactos operacionais

27. Revisão e Atualização

Esta política será:

a. Revisada anualmente

b. Atualizada conforme PCI DSS e regulamentação

28. Aprovação

Aprovada pela Alta Administração da Moneria.

29. Vigência

Esta política entra em vigor na data de sua aprovação.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria