| | 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 SEGMENTAÇÃO DE REDE

## Sumário

## 1. Objetivo

Estabelecer diretrizes, controles e padrões para a segmentação de redes da Moneria, assegurando isolamento adequado de ambientes, proteção de ativos críticos e redução da superfície de ataque, em conformidade com requisitos regulatórios e boas práticas de segurança.

## 2. Abrangência

Esta política aplica-se a:

a. Infraestrutura de rede on-premise e em nuvem

b. Ambientes de produção, homologação e desenvolvimento

c. Sistemas críticos (CDE, Pix, SPI, STR)

d. Dispositivos de rede (firewalls, switches, routers)

e. Colaboradores e terceiros envolvidos

## 3. Referências Normativas

**Regulação**

a. Resolução CMN nº 4.658/2018

b. Resolução CMN nº 5.274/2025

c. Resolução BCB nº 538/2025

**Padrões Técnicos**

a. PCI DSS v4.0.1 (segmentação de rede e isolamento do CDE)

b. ISO/IEC 27001 e 27002

c. NIST SP 800-53 (Network Security Controls)

d. CIS Controls

## 4. Definições

**Segmentação de rede:** divisão da rede em zonas isoladas para controle de tráfego e segurança.

**Zona de rede:** agrupamento lógico de ativos com níveis similares de risco.

**CDE:** ambiente de dados de cartão que requer isolamento rigoroso.

**Microsegmentação:** segmentação granular baseada em aplicações ou workloads.

## 5. Princípios

A Moneria adota:

a. Isolamento de ambientes críticos
b. Princípio do menor privilégio de rede
c. Controle rigoroso de tráfego
d. Defesa em profundidade
e. Monitoramento contínuo
f. Segmentação baseada em risco

## 6. Modelo de Segmentação

A Moneria deve estruturar sua rede em zonas, no mínimo:

a. Zona pública (internet / DMZ)
b. Zona de aplicação
c. Zona de banco de dados
d. Zona administrativa
e. Zona de ambientes críticos (CDE, Pix, SPI, STR)
f. Zona de desenvolvimento/teste

Cada zona deve possuir controles específicos.

## 7. Segmentação do CDE

O CDE deve:

a. Ser isolado de outras redes

b. Permitir apenas tráfego estritamente necessário

c. Ser protegido por firewalls dedicados

d. Ser validado por testes de segmentação

## 8. Segmentação de Ambientes

A Moneria deve garantir:

a. Separação entre produção, homologação e desenvolvimento

b. Proibição de acesso direto entre ambientes sem controle

c. Restrição de dados sensíveis em ambientes não produtivos

## 9. Controle de Tráfego de Rede

A Moneria deve:

a. Implementar regras de firewall restritivas

b. Permitir apenas tráfego necessário (whitelisting)

c. Bloquear tráfego não autorizado por padrão

d. Monitorar fluxos de rede

## 10. Firewalls e Controles de Perímetro

Devem ser utilizados:

a. Firewalls de borda

b. Firewalls internos entre zonas

c. WAF para aplicações web

d. IDS/IPS quando aplicável

## 11. Segmentação em Nuvem

A Moneria deve:

a. Utilizar VPCs e subnets segregadas

b. Separar workloads por ambiente

c. Controlar tráfego com security groups e NACLs

d. Evitar exposição pública indevida

## 12. Microsegmentação (quando aplicável)

A Moneria deve:

a. Implementar controle granular entre serviços

b. Restringir comunicação entre aplicações

c. Aplicar políticas baseadas em identidade

## 13. Controle de Acesso de Rede

O acesso à rede deve:

a. Ser autenticado e autorizado

b. Ser restrito por perfil

c. Ser monitorado

d. Seguir o princípio do menor privilégio

## 14. Monitoramento de Rede

A Moneria deve:

a. Monitorar tráfego entre zonas

b. Detectar atividades anômalas

c. Integrar logs com SIEM

d. Gerar alertas em tempo real

## 15. Testes de Segmentação

Devem ser realizados:

a. Testes de validação de segmentação (PCI DSS)

b. Pentests internos

c. Verificação de isolamento entre zonas

## 16. Gestão de Mudanças de Rede

Alterações na segmentação devem:

a. Seguir processo formal de mudança

b. Ser testadas antes da implementação

c. Ser aprovadas previamente

d. Ser documentadas

## 17. Gestão de Vulnerabilidades de Rede

A Moneria deve:

a. Monitorar vulnerabilidades em dispositivos de rede

b. Aplicar patches

c. Avaliar configurações

d. Corrigir falhas rapidamente

## 18. Gestão de Terceiros

A Moneria deve:

a. Controlar acesso de terceiros à rede

b. Segmentar acessos externos

c. Monitorar conexões

d. Formalizar controles de segurança

## 19. Gestão de Incidentes de Rede

Eventos como:

a. Acesso não autorizado

b. Tráfego suspeito

c. Violação de segmentação

Devem:

a. Ser registrados

b. Ser tratados imediatamente

c. Acionar resposta a incidentes

## 20. Continuidade e Resiliência

A Moneria deve:

a. Garantir redundância de rede

b. Evitar pontos únicos de falha

c. Planejar contingência

d. Testar resiliência

## 21. Auditoria e Conformidade

A segmentação de rede está sujeita a:

a. Auditorias internas

b. Auditorias PCI DSS

c. Avaliações do BACEN

## 22. Documentação de Rede

A Moneria deve manter:

a. Diagramas atualizados de rede

b. Mapeamento de zonas

c. Regras de firewall documentadas

d. Inventário de dispositivos

## 23. Treinamento e Conscientização

A Moneria promove:

a. Capacitação em segurança de redes

b. Treinamento em arquitetura segura

c. Atualização contínua

## 24. Integração com Outras Políticas

Esta política se integra com:

a. Política de Segurança da Informação

b. Política de Gestão de CDE

c. Política de Segurança em Nuvem

d. Política de Controle de Acesso

e. Política de Gestão de Vulnerabilidades

## 25. Responsabilização

O descumprimento desta política pode resultar em:

a. Medidas disciplinares

b. Revisão de acessos

c. Ações corretivas

## 26. Revisão e Atualização

Esta política será:

a. Revisada anualmente

b. Atualizada conforme evolução tecnológica e regulatória

## 27. Aprovação

Aprovada pela Alta Administração da Moneria.

## 28. Vigência

Esta política entra em vigor na data de sua aprovação.

Aracaju/SE, 16 de fevereiro de 2026

David dos Santos
Diretoria