	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 TESTES DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. Objetivo

Estabelecer diretrizes, processos e controles para realização de testes de segurança da informação, visando identificar vulnerabilidades, validar controles de segurança e fortalecer a resiliência dos sistemas, aplicações e infraestruturas da Moneria.

2. Abrangência

Esta política aplica-se a:

a. Sistemas, aplicações e APIs

b. Infraestrutura de TI (on-premise e nuvem)

c. Ambientes de desenvolvimento, teste e produção

d. Ambientes críticos (Pix, CDE, SPI, STR)

e. Colaboradores e terceiros envolvidos em testes

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 27005 (Gestão de Riscos)

c. ISO/IEC 27035 (Incidentes)

d. PCI DSS v4.0.1 (Requisitos 11.x)

e. NIST SP 800-115 (Technical Guide to Information Security Testing)

f. OWASP Testing Guide

4. Definições

Teste de segurança: avaliação técnica para identificar vulnerabilidades e falhas de controle.

Pentest (teste de intrusão): simulação controlada de ataque.

SAST/DAST: testes estáticos e dinâmicos de aplicações.

Red Team: simulação avançada de ataque realista.

5. Princípios

A Moneria adota:

a. Testes contínuos e baseados em risco

b. Validação independente de controles

c. Abordagem preventiva e proativa

d. Rastreabilidade e evidência

e. Integração com gestão de vulnerabilidades

f. Melhoria contínua

6. Tipos de Testes de Segurança

A Moneria deve realizar, no mínimo:

6.1 Testes de Vulnerabilidade (Vulnerability Scans)

a. Scans automatizados

b. Identificação de falhas conhecidas

6.2 Testes de Intrusão (Pentest)

a. Simulação de ataques externos e internos

b. Avaliação de exploração real

6.3 Testes de Aplicação

a. SAST (análise estática)

b. DAST (análise dinâmica)

c. Testes de APIs

6.4 Testes de Infraestrutura

a. Redes, servidores e cloud

b. Avaliação de configuração

6.5 Testes de Segmentação (PCI DSS)

a. Validação de isolamento do CDE

b. Verificação de controles de rede

6.6 Testes de Engenharia Social (quando aplicável)

a. Simulações de phishing

b. Avaliação de comportamento humano

6.7 Red Team / Purple Team (quando aplicável)

a. Simulação avançada de ataques

b. Avaliação de detecção e resposta

7. Frequência dos Testes

A Moneria deve realizar:

a. Scans de vulnerabilidade: periódicos (ex: mensais/trimestrais)

b. Pentest: no mínimo anual ou após mudanças relevantes

c. Testes de aplicação: contínuos (DevSecOps)

d. Testes de segmentação: conforme PCI DSS

e. Testes adicionais conforme risco

8. Planejamento de Testes

Os testes devem:

a. Ser formalmente planejados

b. Definir escopo, objetivos e metodologia

c. Considerar criticidade dos ativos

d. Ser aprovados previamente

9. Execução de Testes

Os testes devem:

a. Ser realizados por profissionais qualificados

b. Seguir metodologias reconhecidas (OWASP, NIST, etc.)

c. Evitar impacto indevido em produção

d. Ser devidamente monitorados

10. Gestão de Resultados

Os resultados devem:

a. Ser documentados formalmente

b. Classificar vulnerabilidades por criticidade

c. Incluir evidências técnicas

d. Ser compartilhados com áreas responsáveis

11. Tratamento de Vulnerabilidades

As vulnerabilidades identificadas devem:

a. Ser registradas

b. Ser priorizadas

c. Ser corrigidas conforme SLA

d. Ser revalidadas após correção

12. Integração com Gestão de Vulnerabilidades

Os testes devem:

a. Alimentar o processo de gestão de vulnerabilidades

b. Priorizar riscos críticos

c. Apoiar decisões de segurança

13. Testes em Ambientes Críticos

Ambientes como:

a. Pix/SPI/STR

b. CDE (dados de cartão)

c. Infraestrutura crítica

Devem:

a. Ter testes reforçados

b. Seguir requisitos regulatórios

c. Ter validação adicional

14. Testes em Produção

Testes em produção devem:

a. Ser controlados e autorizados

b. Minimizar impacto operacional

c. Possuir plano de contingência

15. Gestão de Terceiros

A Moneria deve:

a. Avaliar fornecedores de testes

b. Garantir qualificação técnica

c. Formalizar escopo e responsabilidades

d. Proteger informações sensíveis

16. Monitoramento e Evidências

A Moneria deve manter:

a. Registros de testes realizados

b. Evidências de execução

c. Histórico de vulnerabilidades

d. Relatórios auditáveis

17. Auditoria e Conformidade

Os testes de segurança estão sujeitos a:

a. Auditorias internas

b. Auditorias externas (PCI DSS, BACEN)

c. Avaliações regulatórias

18. Integração com Outras Políticas

Esta política se integra com:

a. Política de Gestão de Vulnerabilidades

b. Política de Gestão de Incidentes

c. Política de DevSecOps

d. Política de Segurança da Informação

e. Política de Hardening

19. Treinamento e Conscientização

A Moneria promove:

a. Capacitação em testes de segurança

b. Treinamento em ferramentas e metodologias

c. Atualização contínua

20. Indicadores de Segurança

A Moneria acompanha:

a. Número de vulnerabilidades identificadas

b. Tempo de correção

c. Taxa de reincidência

d. Efetividade dos testes

21. Responsabilização

O descumprimento desta política pode resultar em:

a. Medidas disciplinares

b. Ações corretivas

c. Revisão de processos

22. Revisão e Atualização

Esta política será:

a. Revisada anualmente

b. Atualizada conforme evolução tecnológica e regulatória

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

David dos Santos
Diretoria