



MPS

Manual de Procedimento de Segurança

MANUAL DE PROCEDIMENTO DE SEGURANÇA DA INFORMAÇÃO PARA SOFTWARE E SERVIÇOS

Este documento apresenta a estrutura técnica de Segurança da Informação adotada pela Cingo em suas ofertas de Sistemas de Gestão e Serviços Cloud, detalhando os mecanismos de defesa, processos de gestão e monitoramento contínuo. Nossa abordagem é dividida em três pilares fundamentais: Servidores e Conectividade, Gerenciamento de Software e Monitoramento e Proteção, garantindo integridade, confidencialidade e disponibilidade dos dados.

O objetivo é evidenciar o cumprimento de requisitos de Segurança da Informação (SI) exigidos pelo mercado, garantindo a confidencialidade, integridade e disponibilidade dos dados processados, e as informações aqui contidas refletem o estado atual da nossa infraestrutura tecnológica e processos de governança.



1) Servidores e Conectividade

A segurança em infraestrutura de servidores e conectividade constitui o primeiro pilar para garantir a proteção dos ativos de informação. Este grupo abrange desde a segregação de ambientes até os mecanismos de controle de acesso e criptografia.

Visão Geral



Segregação de Ambientes

Existe uma rigorosa segregação física e lógica entre ambientes. As máquinas virtuais (VMs) de produção residem em compartimentos específicos, isolados das VMs de homologação.

Para clientes com infraestrutura dedicada, criamos sistemas completamente isolados desde a VCN (Virtual Cloud Network) e subnets até as instâncias, garantindo privacidade total.

Arquitetura de Firewall em Múltiplas Camadas

Utilizamos dois níveis de controle de tráfego, além da proteção de aplicação:

- Camada de Rede: OCI Network Security (Security Rules).
- Camada de Host: Firewalls locais (Firewalld/iptables e kernel security modules) em cada VM.
- Camada de Aplicação: NGINX atuando como Reverse Proxy para controlar acessos nas portas 80/443.

Princípio de Menor Privilégio

Todos os acessos a máquinas e serviços são configurados concedendo apenas o menor nível de acesso possível necessário para a operação, minimizando a superfície de ataque.

Criptografia de Comunicações

Toda a comunicação entre sistemas é realizada via protocolo HTTPS, utilizando exclusivamente versões seguras do TLS (1.2 e 1.3). Os servidores aceitam apenas cifras fortes.

Autenticação Multifator (Acesso Administrativo)

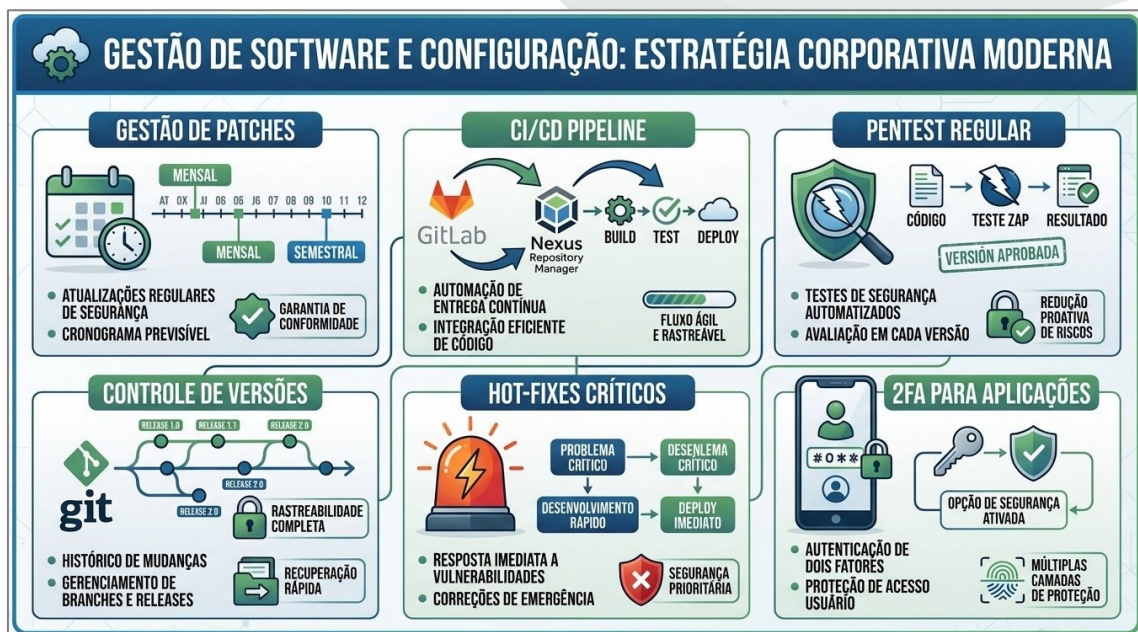
O acesso administrativo aos servidores é restrito a usuários pré-definidos e protegido obrigatoriamente por autenticação de dois fatores (2FA) e certificado digital individual por servidor.



2) Gerenciamento de Software e Configuração

Este grupo assegura que o ciclo de vida do desenvolvimento e a manutenção dos softwares sigam padrões rigorosos de segurança, desde a escrita do código até a aplicação de correções.

Visão Geral



Processo de Gestão de Patches e Releases

Seguimos um calendário rigoroso: liberações mensais para correções e semestrais para novas releases. Para vulnerabilidades críticas de segurança, utilizamos o conceito de hot-fixes para aplicação imediata.

CI/CD e Controle de Versões

Utilizamos automação via pipelines no GitLab (CI/CD) e gestão de artefatos através do Nexus (Sonatype), garantindo rastreabilidade, controle de versões e integridade do código implantado.

Desenvolvimento Seguro e PenTests

A cada nova versão liberada, executamos ciclos de testes de penetração (PenTest) utilizando ferramentas como ZAP (Zed Attack Proxy). Vulnerabilidades de nível médio, alto ou crítico são corrigidas antes da entrada em produção.

Autenticação Multifator em Aplicações

As aplicações desenvolvidas suportam e incentivam a ativação de Autenticação de 2 Fatores (2FA) para os usuários finais, elevando a segurança no acesso aos dados.

Rastreabilidade e Controle

Os sistemas possuem logs detalhados de auditoria que permitem monitorar inserção, eliminação e consulta de dados, garantindo total rastreabilidade das ações dos usuários.



3) Monitoramento e Proteção

A vigilância constante e a capacidade de resposta a incidentes compõem o terceiro pilar, garantindo a disponibilidade e a recuperação em caso de falhas.

Visão Geral



Proteção Antivírus e Integridade

Todos os servidores possuem soluções de antivírus instaladas e atualizadas. As atualizações de sistema operacional são planejadas e controladas para evitar comprometimento da integridade do ambiente.

Firewall de Aplicação Web (WAF)

Além dos firewalls de rede, as aplicações são protegidas por WAF (Web Application Firewall) baseado em Nginx, que filtra tráfego malicioso específico da camada de aplicação.

Monitoramento Contínuo

Ambientes são monitorados em tempo real (24/7) utilizando ferramentas como Grafana e Zabbix. Monitoramos infraestrutura, serviços e disponibilidade da aplicação de forma conjunta.

Política de Backups

Os backups são realizados diariamente com retenção padrão de 30 dias (personalizável conforme contrato). Para garantir a recuperação de desastres, os backups são armazenados fisicamente em local separado do ambiente produtivo.



4) Melhoria Contínua

Na Cingo, conduzimos nossa atuação com foco estratégico na criação e entrega de soluções cada vez mais relevantes, competitivas e alinhadas às demandas de um mercado em constante transformação. Rompemos com modelos tradicionais, superamos práticas obsoletas e aprimoramos processos com base em inovação, eficiência e visão de futuro, consolidando uma cultura orientada à melhoria contínua e à geração de valor para nossos clientes.

Nesse contexto de evolução permanente, a segurança da informação ocupa papel central em nossa estratégia. Tratamos a proteção de dados e das operações como um processo dinâmico e estruturado, sustentado por políticas robustas, governança ativa e tecnologias atualizadas. Assim, reforçamos nosso compromisso técnico em oferecer um ambiente seguro, resiliente e confiável, garantindo a integridade, a confidencialidade e a disponibilidade que sustentam o crescimento e a continuidade dos negócios de nossos clientes.

Para maiores detalhes sobre procedimentos específicos, consulte também o documento "Política de Segurança da Informação (PSI)".

