# Política de Segurança da Informação e da Prestação de Serviços

| | |
|---|---|
| Código do Documento: PSI-SER-001 | Versão: 1.0 |
| Data de Emissão: Janeiro de 2026 | Classificação de Informação: Uso Interno / Clientes / Fornecedores |
| Área Responsável: Governança de TI e Segurança da Informação | Aplica-se a: Todos os Serviços, Sistemas e Colaboradores |

## 1. OBJETIVO

Esta Política de Segurança da Informação (PSI) visa estabelecer os requisitos, diretrizes e padrões de segurança aplicáveis à prestação de serviços, manutenção de sistemas e gestão de infraestrutura de tecnologia. O objetivo principal é garantir a proteção contra acessos não autorizados, indisponibilidade, alterações indevidas ou vazamentos de dados, assegurando a conformidade com as melhores práticas do mercado e exigências regulatórias (incluindo LGPD).

## 2. ALCANCE E ESCOPO

As diretrizes estipuladas nesta norma aplicam-se integralmente a:

- Todos os serviços prestados, mantidos ou operados pela organização;
- Ambientes de produção, homologação e desenvolvimento (nuvem e on-premises);
- Bancos de dados, APIs, micros serviços, integrações e pipelines de implantação;
- Colaboradores, terceiros, fornecedores e prestadores de serviços que tenham acesso aos ambientes operacionais.

## 3. PILARES DA SEGURANÇA DA INFORMAÇÃO

A prestação e operação dos serviços são regidas por quatro pilares essenciais:

| **Pilar** | **Descrição Técnica e Operacional** |
|---|---|

| | |
|---|---|
| Confidencialidade | Garantia de que os dados transacionados e armazenados no serviço estejam acessíveis exclusivamente por sistemas e pessoas formalmente autorizados. |
| Integridade | Salvaguarda da exatidão e do estado completo das informações e sistemas, protegendo-os contra modificações não autorizadas ou acidentais. |
| Disponibilidade | Garantia de que os serviços e dados permaneçam operacionais e acessíveis para os usuários autorizados sempre que necessário. |
| Rastreabilidade (Auditabilidade) | Capacidade de registrar, monitorar e auditar todas as ações, acessos e alterações realizadas no ambiente do serviço. |

# 4. DIRETRIZES DE SEGURANÇA APLICÁVEIS AO SERVIÇO

## 4.1. Controle de Acesso e Gestão de Identidade

- Autenticação Forte: Obrigatoriedade do uso de Autenticação Multi-Fator (MFA) para todas as conexões administrativas e acesso aos ambientes de infraestrutura.
- Princípio do Menor Privilégio: Acesso a servidores, bancos de dados e ferramentas concedido estritamente com base na necessidade funcional (Need-to-Know).
- Contas de Serviço: Credenciais de integrações, APIs e processos automatizados devem utilizar chaves temporárias ou ser mantidas em cofres de segredos (*secret managers*) protegidos.

## 4.2. Segurança em Redes e Infraestrutura

- Segregação de Ambientes: Isolação lógica rigorosa entre ambientes de Desenvolvimento, Testes/Homologação e Produção.
- Proteção de Perímetro: Uso de firewalls de aplicação (WAF), restrições de redes privadas (VPC/Subnets) e proteção contra ataques de negação de serviço (DDoS).
- Criptografia: Criptografia obrigatória de dados em trânsito (HTTPS/TLS 1.2+) e de dados em repouso (*Data at Rest*) utilizando algoritmos consolidados.

## 4.3. Desenvolvimento Seguro e Gestão de Mudanças

- Práticas de DevSecOps: Análise estática de código (SAST) e varreduras de vulnerabilidades automatizadas durante a esteira de build e deploy.
- Gestão de Dependências: Revisão e atualização contínua de bibliotecas e pacotes para prevenir vulnerabilidades conhecidas (CVEs).
- Versionamento e Revisão de Código: Nenhuma alteração pode ir para produção sem revisão por pares (*Peer Review*) e validação dos testes automatizados.

# 5. CONTINUIDADE DE NEGÓCIOS E BACKUP

Para assegurar a resiliência dos serviços, a infraestrutura deve seguir as diretrizes de backup e recuperação estipuladas:

- Rotina de Backups: Realização de backups diários incrementais e snapshots periódicos automatizados.
- Testes de Restauração: Execução regular de simulações de restauração para validar a integridade das cópias de segurança.
- Planos de RPO e RTO: Manutenção de metas de RPO (Objetivo de Ponto de Recuperação) e RTO (Objetivo de Tempo de Recuperação) compatíveis com o Acordo de Nível de Serviço (SLA) estabelecido.

# 6. GESTÃO DE INCIDENTES DE SEGURANÇA

Em caso de suspeita ou confirmação de incidente de segurança afetando o serviço:

- A equipe técnica deve conter imediatamente a ameaça, isolando os componentes afetados;
- Os registros e evidências devem ser preservados para análise forense e causa-raiz;
- Notificação formal aos gestores e partes interessadas conforme prazos legais e regimentais estabelecidos.

# 7. CONFORMIDADE E AUDITORIA

Esta política é revisada periodicamente para assegurar sua eficácia e adequação aos avanços tecnológicos e legais. O descumprimento destas diretrizes pode acarretar sanções contratuais e disciplinares cabíveis.

---

Revisão #5
Criado 2026-09-03 18:12:37 UTC por Marcio Klitzke
Atualizado: 2026-09-04 18:02:20 UTC por Marcio Klitzke