POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Código	MGDATA-POL-PSI-001
Versão	1.0
Data de aprovação	12/2025
Próxima revisão	12/2026
Elaboração	Gerência de Tecnologia + Área de Compliance
Aprovação	Diretoria
Monitoramento	CTO e Área de Compliance
Público	Externo

1. Introdução

A MGDATA Tecnologia Ltda. ("MGDATA") opera datacenter próprio, serviços de hospedagem, backup como serviço, cibersegurança e correlatos. A informação é o ativo estratégico central: da MGDATA, de seus clientes contratantes e dos usuários finais destes. A presente Política de Segurança da Informação (PSI) estabelece os princípios, papéis e diretrizes para preservar a confidencialidade, integridade e disponibilidade — tríade CID — desses ativos, acrescida das dimensões complementares de autenticidade, não repúdio e privacidade.

Esta PSI se articula com o CODEC MGDATA, com a Política de Compliance e com a Política de Melhoria Contínua.

2. Objetivo e Escopo

Estabelecer as diretrizes gerais de segurança da informação aplicáveis a todos os ativos informacionais sob custódia ou operação da MGDATA, em qualquer forma (eletrônica, física, verbal), em todos os ambientes (datacenter próprio, nuvem contratada, escritório, home office, deslocamento) e em todas as fases do ciclo de vida (criação, armazenamento, processamento, transmissão, descarte).

Alcança todos os colaboradores, estagiários, prestadores de serviço, terceirizados, clientes contratantes (no âmbito das suas obrigações contratuais) e visitantes.

3. Fundamentação Normativa

A PSI se alicerça em:

- Lei nº 13.709/2018 (LGPD) e regulamentação da ANPD;
- Marco Civil da Internet (Lei nº 12.965/2014);
- Decreto nº 9.637/2018 e demais dispositivos aplicáveis à segurança da informação em relacionamento com a Administração Pública;
- ISO/IEC 27001 — sistema de gestão de segurança da informação (SGSI), como marco filosófico do sistema;
- ISO/IEC 27002 — catálogo de controles (organizacionais, pessoais, físicos e tecnológicos);
- ISO/IEC 27017 — controles específicos para serviços em nuvem, aplicável ao portfólio Cloud da MGDATA;
- ISO/IEC 27018 — proteção de dados pessoais em nuvem, articulada com a LGPD;

- ISO/IEC 27701 — sistema de gestão de privacidade da informação (SGPI);
- ISO/IEC 22301 — gestão de continuidade de negócio, aplicável ao BaaS/DRaaS;
- NIST Cybersecurity Framework 2.0 — funções Govern, Identify, Protect, Detect, Respond, Recover;
- NIST SP 800-207 — arquitetura Zero Trust, para acessos privilegiados;
- CIS Controls v8 — controles prioritários baseados em evidência empírica.

4. Princípios Filosóficos

a) Segurança como sistema de gestão, não como produto. Ferramentas (firewall, EDR, backup) são meios; o SGSI é o fim. Adota-se o ciclo PDCA — Planejar, Executar, Verificar, Agir — como espinha dorsal.

b) Abordagem baseada em risco. Nem toda informação exige o mesmo controle. Ativos são classificados por criticidade (pública, interna, restrita, confidencial) e protegidos proporcionalmente.

c) Defesa em profundidade. Múltiplas camadas independentes de controle (perímetro, rede, host, aplicação, dado, identidade). Falha em uma camada não implica falha do sistema.

d) Zero Trust — "nunca confie, sempre verifique". O acesso é concedido de forma dinâmica, autenticada, autorizada e minimamente privilegiada, independentemente da localização do requisitante.

e) Privacidade desde a concepção (privacy by design). Todo novo serviço, integração ou processo é avaliado quanto ao impacto sobre dados pessoais antes de sua implementação, conforme princípios da LGPD.

f) Resiliência e recuperação. Não basta prevenir; é preciso detectar rapidamente, responder com efetividade e recuperar com o menor impacto possível — as três últimas funções do NIST CSF 2.0.

g) Melhoria contínua. O SGSI é revisado à luz de incidentes, testes de intrusão, auditorias externas e evolução do cenário de ameaças.

5. Responsabilidades

Da Diretoria: aprovar a PSI; deliberar sobre riscos residuais aceitáveis; assegurar recursos.

Do CTO: dirigir tecnicamente o SGSI; aprovar padrões técnicos e baselines de configuração.

Da Gerência de Tecnologia: implementar controles técnicos; conduzir gestão de vulnerabilidades; operar hardening (Linux, Windows, VMware, Microsoft) conforme benchmarks reconhecidos (CIS, fabricantes); manter runbooks de resposta.

Da Central de Serviços: operar controle de acesso, gestão de identidades, atendimento a incidentes de segurança em primeiro nível.

Da Área de Compliance: monitorar aderência; conduzir auditorias internas; interface com a ANPD e clientes contratantes.

De todos os colaboradores: proteger credenciais; não compartilhar acessos; reportar incidentes imediatamente; usar recursos exclusivamente para fins profissionais.

6. Diretrizes Operacionais

6.1 Classificação e Tratamento da Informação. Ativos são classificados em quatro níveis. O manuseio, armazenamento, transmissão e descarte seguem regra específica por nível.

6.2 Controle de Acesso. Identidade individual, intransferível, com autenticação forte (MFA) para todos os acessos privilegiados. Revisão trimestral de acessos privilegiados; imediata em desligamentos.

6.3 Criptografia. Dados em repouso e em trânsito são cifrados por padrões de mercado (AES-256, TLS 1.3 ou superior, quando aplicável).

6.4 Backup e Continuidade. Todo dado sob custódia produtiva é objeto de backup conforme política específica de BaaS, com regra 3-2-1-1-0 (três cópias, dois meios, uma off-site, uma imutável, zero erros na verificação). Testes de restauração periódicos.

6.5 Gestão de Vulnerabilidades e Patching. Ciclo mensal de patching regular; ciclo emergencial para vulnerabilidades críticas (score CVSS ≥ 9,0 ou exploração ativa detectada). Testes de intrusão anuais em sistemas expostos à internet.

6.6 Resposta a Incidentes. Playbook formal com quatro fases: detecção, contenção, erradicação, recuperação, seguidas de análise pós-incidente (post-mortem) para aprendizado.

6.7 Trabalho Remoto. Aplicam-se as regras do CODEC. Acesso via VPN corporativa com MFA; câmera obrigatória em reuniões com clientes; vedado uso de dispositivo pessoal para tratamento de dado classificado como confidencial.

6.8 LGPD. A MGDATA atua como controladora em relação aos dados de seus colaboradores e prospects, e como operadora em relação aos dados que trata por conta de clientes contratantes, na forma dos contratos firmados.

7. Monitoramento

Painel de indicadores mantido pela Gerência de Tecnologia: MTTR de incidentes, taxa de patches em dia, cobertura de MFA, sucesso de restauração de backups em testes, número de acessos privilegiados ativos.

8. Sanções e Vigência

Aplicam-se as sanções previstas no CODEC e na CLT. Terceiros ficam sujeitos às cláusulas contratuais específicas. Esta PSI entra em vigor na publicação e é revisada anualmente.