

Política de Segurança da Informação (PSI)

Gestor Shop — GESTOR SHOP TECNOLOGIA DA INFORMAÇÃO LTDA, CNPJ 55.434.374/0001-07
· www.gestorshop.com.br

Versão 3.0 · Vigência a partir de 02/07/2026 · Revisão anual

1. Introdução

Esta Política de Segurança da Informação (PSI) estabelece os princípios, responsabilidades e controles adotados pela Gestor Shop para proteger seus ativos informacionais e os dados de seus clientes. Alinha-se à norma ISO/IEC 27002:2022, à Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018) e às políticas de proteção de dados dos marketplaces integrados à plataforma.

2. Objetivos

- Proteger a confidencialidade, integridade e disponibilidade da informação.
- Prevenir acessos não autorizados, vazamentos e perdas de dados.
- Garantir transparência, conformidade legal e ética profissional.

3. Aplicabilidade

Aplica-se a todos os colaboradores, prestadores de serviços, fornecedores e parceiros que tenham acesso a dados, sistemas ou recursos da Gestor Shop; o acesso de prestadores de serviços é regido por contrato com obrigações de confidencialidade e proteção de dados equivalentes.

4. Princípios

- Toda informação produzida, tratada ou armazenada sob responsabilidade da Gestor Shop é protegida por esta política.
- Recursos tecnológicos devem ser usados para fins profissionais, com uso pessoal tolerado de forma controlada.
- A proteção da privacidade e dos dados pessoais é prioridade, no princípio da minimização: coletamos e retemos apenas o necessário.

5. Governança e estrutura de segurança

- **Direção Executiva:** aprova esta PSI, suas revisões e os investimentos em segurança.
- **Responsável pela Segurança da Informação (IMPOC):** coordena os controles, o tratamento de incidentes e é o ponto de contato de segurança perante parceiros e marketplaces.
- **Encarregado de Dados (LGPD):** assegura a conformidade com a LGPD e atende titulares e a ANPD.

Esta PSI é revisada **anualmente** ou após incidentes relevantes, com registro de versão e aprovação.

6. Controles de acesso

O acesso aos sistemas segue o princípio do menor privilégio, com credenciais individuais e intransferíveis — o compartilhamento de senhas é expressamente proibido. A atribuição de permissões ocorre por perfil de acesso (RBAC) e é revisada periodicamente.

Controles vigentes:

- Senhas com no mínimo 12 caracteres (máximo 64), exigindo maiúsculas, minúsculas, números e símbolos; bloqueio de reutilização de senhas anteriores e de senhas que contenham o nome do usuário; armazenamento exclusivamente sob hash criptográfico.
- **Bloqueio automático de conta após 10 tentativas de login malsucedidas.**
- Autenticação multifator (MFA) disponível para todos os usuários e exigida para acessos administrativos.
- Acessos à infraestrutura registrados em trilha de auditoria.

7. Proteção de dados pessoais

Cumprimos a LGPD, garantindo os direitos dos titulares conforme nossa Política de Privacidade.

Controles técnicos vigentes:

- Criptografia em trânsito (TLS 1.2+) e em repouso (AES-256) nos bancos de dados e no armazenamento de arquivos.
- **Isolamento por cliente: cada cliente possui base de dados própria**, impedindo por construção o acesso ou a agregação de dados entre contas.
- **Anonimização automática de dados pessoais de compradores 30 dias após a conclusão dos pedidos.**
- Sanitização de dados sensíveis e credenciais nos registros técnicos (logs).
- Ambientes de produção e testes segregados; somente pessoal autorizado acessa dados pessoais.
- A retenção segue base legal e critérios mínimos de necessidade, com eliminação segura ao término (procedimento interno alinhado ao NIST SP 800-88).

8. Segurança de sistemas e infraestrutura

A plataforma opera em nuvem (AWS) com:

- Firewall de aplicação web (WAF) na borda e grupos de segurança de rede restritivos.
- Varredura contínua de vulnerabilidades nas imagens de aplicação (Amazon Inspector) e avaliação automatizada de postura de segurança da conta (benchmark CIS).
- Atualizações e correções de segurança aplicadas regularmente por meio do ciclo de build e implantação.
- Softwares licenciados e homologados antes do uso.

Estações de trabalho com acesso a sistemas devem manter disco criptografado, bloqueio de tela automático, sistema operacional e proteções atualizados; perda ou roubo de dispositivo deve ser comunicado imediatamente ao Responsável pela Segurança.

9. Backup e continuidade

Backups automáticos diários são realizados para os sistemas críticos, com retenção definida e armazenamento versionado. O plano de continuidade de negócios (BCP) e a recuperação de desastres (DRP) estão em desenvolvimento contínuo.

10. Gestão de incidentes

A Gestor Shop mantém um **Plano de Resposta a Incidentes** formal, com responsável designado, passos de contenção e registro dos incidentes. Incidentes devem ser reportados imediatamente ao Responsável pela Segurança (IMPOC). Notificações a autoridades (ANPD) e titulares seguem a LGPD; incidentes envolvendo dados de marketplaces são comunicados aos parceiros nos prazos contratuais.

11. Monitoramento e auditoria

Os sistemas são monitorados continuamente por ferramentas de observabilidade e alertas. A trilha de auditoria da infraestrutura (AWS CloudTrail, multi-região) é retida por no mínimo **12 meses**. Os registros de aplicação possuem retenção definida por categoria, com dados sensíveis sanitizados na origem.

12. Treinamento e conscientização

Todo colaborador assina termo de confidencialidade e proteção de dados antes de receber acesso e recebe orientações de segurança da informação. O descumprimento desta PSI sujeita o colaborador a medidas disciplinares.

13. Conformidade

Esta PSI está alinhada à ISO/IEC 27002:2022, à LGPD e às políticas de proteção de dados dos marketplaces integrados. Evidências de controles podem ser fornecidas a parceiros comerciais mediante solicitação, sob acordo de confidencialidade (NDA).

Histórico de versões

Versão	Data	Alteração
3.0	02/07/2026	Revisão geral: governança adequada à estrutura real, controles de acesso e monitoramento atualizados, isolamento por cliente, anonimização, gestão de incidentes com prazos de parceiros, ciclo anual formalizado
2.0	—	Versão publicada anteriormente

Aprovação: Diretoria Executiva da Gestor Shop · www.gestorshop.com.br