Gestor Shop

Política de Segurança da Informação (PSI)

Versão 2.0 – Junho/2025

1. Introdução

Esta Política de Segurança da Informação (PSI) estabelece as diretrizes para proteger as informações da Gestor Shop, seguindo as recomendações da norma ISO/IEC 27002:2022 e a legislação brasileira, especialmente a Lei Geral de Proteção de Dados (LGPD).

2. Objetivos

- Preservar a confidencialidade, integridade e disponibilidade das informações.
- Prevenir incidentes e responsabilidades legais associadas à segurança da informação.
- Garantir o comportamento ético e profissional dos usuários.

3. Aplicação

Esta política aplica-se a todos os funcionários, prestadores de serviços, parceiros e fornecedores da Gestor Shop, independentemente do vínculo empregatício ou contratual.

4. Princípios

- Informações produzidas ou recebidas no exercício profissional são propriedade exclusiva da Gestor Shop, exceto se formalizado em contrato.
- Recursos tecnológicos são disponibilizados para atividades profissionais. O uso pessoal é permitido com moderação, sem prejudicar o desempenho dos sistemas.

5. Estrutura de Governança

- Comitê de Segurança da Informação (CSI): Responsável pela gestão e revisão periódica desta PSI.
- Gerência de Tecnologia da Informação (GTI): Executa e monitora controles técnicos.
- Encarregado de Proteção de Dados (DPO): Responsável pela conformidade com a LGPD.

6. Responsabilidades

6.1 Funcionários e Prestadores de Serviços

- Assumir a responsabilidade pela segurança das informações acessadas.
- Comunicar imediatamente incidentes ou suspeitas ao gestor ou GTI.

6.2 Gestores

- Garantir adesão à PSI por parte de seus subordinados.
- Exigir assinatura dos termos de responsabilidade e confidencialidade.

6.3 GTI

- Implementar controles técnicos eficazes e manter registro auditável de atividades.
- Garantir atualizações regulares de segurança e backups de sistemas críticos.

6.4 DPO

- Assegurar a conformidade com a LGPD e gerenciar incidentes envolvendo dados pessoais.
- Promover treinamentos periódicos sobre segurança da informação e proteção de dados.

7. Uso de Recursos

7.1 Correio Eletrônico

- Uso corporativo preferencial. Uso pessoal moderado permitido.
- Proibido enviar spam, arquivos maliciosos ou conteúdo inadequado.
- Incluir assinatura institucional padronizada.

7.2 Internet

- Acesso monitorado e registrado, podendo ocorrer bloqueios preventivos.
- Downloads apenas autorizados e ligados às atividades profissionais.
- Proibidos softwares não autorizados e atividades ilegais.

7.3 Dispositivos Móveis

- Permitidos somente equipamentos autorizados e configurados pela GTI.
- Uso de senhas obrigatórias e criptografia de dados sensíveis.
- Perda ou roubo devem ser imediatamente reportados à GTI.

7.4 Identificação e Senhas

- Proibido compartilhamento de senhas ou dispositivos identificadores.

- Senhas devem ter complexidade adequada (mínimo 8 caracteres alfanuméricos e especiais).
- Trocas obrigatórias periódicas (a cada 45 dias, 30 para administradores).

8. Gestão de Backup

- Backups automatizados diariamente para sistemas críticos.
- Testes periódicos de restauração conforme criticidade dos sistemas.
- Registros detalhados e auditoria periódica das rotinas executadas.

9. Gestão de Incidentes

- Todos os incidentes devem ser comunicados imediatamente à GTI e ao DPO.
- Comitê de Segurança avaliará incidentes graves e adotará medidas corretivas.

10. Auditoria e Monitoramento

- Sistemas de monitoramento contínuo implantados para prevenir incidentes.
- Auditorias periódicas de conformidade técnica e legal realizadas pela GTI.

11. Conformidade com LGPD

- Garantia dos direitos dos titulares dos dados conforme legislação vigente.
- Implementação de controles adequados para proteção e privacidade dos dados pessoais.

12. Histórico de Revisões

- Versão 2.0 – Junho/2025: Atualização conforme ISO/IEC 27002:2022 e LGPD.

Diretoria Executiva