1. Introdução e Objetivo

O **GRUPOPZM** estabelece, por meio desta política, seu compromisso com a segurança da informação e a privacidade de dados, que constituem pilares essenciais para a relação de confiança com seus clientes, parceiros e colaboradores. O presente documento formaliza a abordagem da organização para a proteção de seus ativos de informação contra ameaças, assegurando sua **confidencialidade**, **integridade** e **disponibilidade**.

O objetivo primordial é a instituição e manutenção de uma cultura de segurança robusta, em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD) e as melhores práticas de mercado.

2. Abrangência

A aplicabilidade desta política estende-se a todos os dados e informações processados, armazenados ou transmitidos no âmbito das operações do **GRUPOPZM**, englobando seus colaboradores, prestadores de serviços, sistemas, plataformas e processos correlatos.

3. Princípios Fundamentais da Segurança da Informação

A estratégia de segurança da informação do **GRUPOPZM** é fundamentada nos seguintes princípios basilares:

- **Confidencialidade:** Assegurar que o acesso à informação seja restrito exclusivamente a indivíduos devidamente autorizados.
- **Integridade:** Garantir a exatidão, completude e ausência de alterações indevidas nos dados e informações.
- **Disponibilidade:** Assegurar que o acesso às informações e aos ativos associados esteja disponível aos usuários autorizados conforme a necessidade.
- **Privacidade e Proteção de Dados:** Realizar o tratamento de dados pessoais para finalidades legítimas, específicas e explícitas, em total aderência à legislação aplicável.

4. Governança e Responsabilidades

A responsabilidade pela segurança da informação é distribuída em toda a estrutura organizacional do **GRUPOPZM**:

- **Alta Gestão:** Promover e patrocinar a cultura de segurança, alocando os recursos necessários para a implementação e manutenção dos controles.
- **Equipe de Segurança e Tecnologia da Informação:** Definir, implementar e gerenciar as ferramentas e os processos de segurança, bem como monitorar o ambiente tecnológico contra ameaças.
- **Colaboradores:** Cumprir as diretrizes desta política e os procedimentos de segurança inerentes às suas atividades diárias.

5. Gestão de Acessos

O controle de acesso aos sistemas, redes e informações corporativas é executado com rigor para mitigar o risco de acesso não autorizado.

- **Menor Privilégio e Necessidade de Conhecer:** A concessão de acesso obedece estritamente aos princípios do menor privilégio e da necessidade de conhecer, garantindo que as permissões dos usuários se limitem ao estritamente necessário para o exercício de suas funções.
- **Controle de Acesso Baseado em Função (RBAC):** A gestão de permissões é estruturada por meio de perfis de acesso associados às responsabilidades de cada cargo, promovendo a segregação de funções.
- **Autenticação Forte:** É mandatório o uso de mecanismos de autenticação robustos, incluindo senhas complexas e a aplicação de Autenticação Multifator (MFA) em sistemas críticos.
- **Revisão Periódica:** Os direitos de acesso são submetidos a revisões e revalidações periódicas. Os acessos de colaboradores desligados são revogados de forma imediata.

6. Segurança de Dados e Ativos

Um conjunto de medidas técnicas e administrativas é implementado para a proteção dos dados em todo o seu ciclo de vida.

- **Classificação da Informação:** As informações são classificadas conforme seu nível de sensibilidade, o que permite a aplicação de controles de proteção proporcionais ao seu valor e risco.
- **Criptografia:** São adotados padrões de criptografia robustos para a proteção de dados.
    - **Dados em Trânsito:** As comunicações em redes públicas são protegidas por protocolos seguros, como TLS 1.2 ou superior. O acesso remoto à rede corporativa é realizado exclusivamente por meio de Redes Privadas Virtuais (VPN) criptografadas.
    - **Dados em Repouso:** Dados sensíveis armazenados em servidores, bancos de dados e dispositivos de usuários são protegidos com criptografia de disco ou volume.
- **Segurança do Ambiente de Trabalho:** É promovida a política de "mesa e tela limpas", que orienta os colaboradores a protegerem informações sensíveis em seus ambientes de trabalho físico e digital.
- **Trabalho Remoto Seguro:** O regime de trabalho remoto é regido por diretrizes de segurança estritas, visando garantir que o ambiente externo não exponha as informações da empresa a riscos.

7. Uso de Dados, Tratamento e Inteligência Artificial

O **GRUPOPZM** reitera seu compromisso com a inovação responsável. O tratamento de dados para quaisquer finalidades, incluindo o desenvolvimento e treinamento de tecnologias de inteligência artificial, é conduzido em estrita observância aos mais elevados padrões éticos e legais.

- **Base Legal para Tratamento:** A utilização de dados pessoais para finalidades secundárias é condicionada à existência de uma base legal apropriada, conforme previsto na legislação, como o consentimento do titular ou a prévia anonimização dos dados.
- **Conformidade Global:** As práticas de tratamento de dados do **GRUPOPZM** estão alinhadas às principais regulamentações de privacidade, incluindo a **Lei Geral de Proteção de Dados (LGPD)**, o **General Data Protection Regulation (GDPR)** e as diretrizes da **Autoridade Nacional de Proteção de Dados (ANPD)**.
- **Anonimização e Minimização:** São aplicadas, sempre que tecnicamente viável, técnicas de anonimização ou pseudonimização em dados utilizados para análises estatísticas ou desenvolvimento tecnológico, em observância ao princípio da minimização de dados.

8. Ciclo de Vida e Compartilhamento de Dados

- **Compartilhamento com Terceiros:** O compartilhamento de dados pessoais com parceiros de negócio, fornecedores e prestadores de serviços (operadores) ocorre de forma restrita, apenas para viabilizar as operações da empresa. Tais transferências são formalizadas por instrumentos contratuais que impõem aos terceiros obrigações de segurança e conformidade equivalentes às praticadas internamente.
- **Transferência Internacional de Dados:** A prestação de nossos serviços pode requerer o uso de uma infraestrutura tecnológica global. Nesses casos, a transferência internacional de dados é realizada em conformidade com a legislação, direcionada a países que ofereçam grau de proteção de dados adequado ou por meio de mecanismos que assegurem os direitos dos titulares.
- **Período de Retenção:** A retenção de dados pessoais é limitada ao período estritamente necessário para o cumprimento das finalidades que motivaram sua coleta, incluindo o atendimento a obrigações legais, regulatórias ou contratuais.

9. Direitos dos Titulares de Dados

Em conformidade com a legislação vigente, o **GRUPOPZM** assegura aos titulares de dados o exercício dos seguintes direitos:

- **Confirmação** da existência de tratamento.
- **Acesso** aos dados.
- **Correção** de dados incompletos, inexatos ou desatualizados.
- **Anonimização, bloqueio ou eliminação** de dados desnecessários ou tratados em desconformidade.
- **Portabilidade** dos dados a outro fornecedor.
- **Eliminação** dos dados pessoais tratados mediante consentimento.
- **Informação** sobre as entidades com as quais os dados foram compartilhados.
- **Revogação do consentimento**.

10. Gestão de Incidentes de Segurança

O **GRUPOPZM** mantém um processo formal para a gestão de incidentes de segurança. Na eventualidade de um incidente que implique risco ou dano relevante aos titulares, serão efetuadas as devidas comunicações aos afetados e à Autoridade Nacional de Proteção de Dados (ANPD), conforme os ditames da LGPD.

11. Conscientização e Treinamento

São mantidos programas contínuos de conscientização e treinamento para todos os colaboradores, com foco em proteção de dados e nas melhores práticas de segurança, visando fortalecer a cultura de proteção da informação.

12. Atualizações desta Política

O presente documento está sujeito a revisões periódicas para refletir a evolução das práticas de segurança e privacidade ou para adequação a novas exigências legais. Recomenda-se a consulta regular deste documento.

13. Contato

O **GRUPOPZM** designou um Encarregado pela Proteção de Dados (DPO) para supervisionar a conformidade com a legislação de privacidade. O exercício dos direitos de titular ou o esclarecimento de dúvidas sobre esta política devem ser encaminhados para os seguintes canais de contato:

- **dpo@grupopzm.com**
- **segurancadainformacao@grupopzm.com**