1. Política Interna de Privacidade e Segurança da Informação

1. Contexto e Finalidade

A Paez Gestão reconhece que o ativo mais valioso da organização é a informação — seja ela de natureza técnica, comercial, estratégica ou pessoal. Em um ambiente empresarial baseado em conhecimento, planejamento e tomada de decisões, a proteção dos dados é condição essencial para manter a confiança dos clientes e a conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Esta política tem por finalidade estabelecer um conjunto estruturado de princípios, diretrizes e controles para garantir a privacidade e a segurança da informação em todas as operações da empresa. O objetivo é criar um ambiente de governança digital responsável, em que o uso de tecnologias, sistemas e processos respeite a confidencialidade, a integridade e a disponibilidade dos dados sob gestão da Paez Gestão.

A aplicação desta política se estende a todas as áreas da empresa e abrange tanto as atividades internas quanto as interações externas — especialmente aquelas realizadas através do **Sistema Web de Mentoria**, plataforma que permite a comunicação entre clientes, compartilhamento de experiências e registro de atividades acompanhadas pelos consultores.

A segurança da informação é tratada como um valor organizacional, integrado à cultura corporativa da Paez Gestão, devendo ser considerada na rotina de cada colaborador e no desenvolvimento de cada serviço digital.

---

2. Âmbito de Aplicação

Esta política aplica-se a todos os colaboradores, mentores, parceiros, fornecedores, prestadores de serviço, estagiários e clientes que, de forma direta ou indireta, acessem, manipulem ou armazenem informações pertencentes à Paez Gestão ou aos seus usuários.

O escopo inclui o tratamento de dados pessoais e corporativos por meio de qualquer meio físico, digital ou remoto, abrangendo:

- Sistema Web da Paez Gestão e suas bases de dados;
- Equipamentos e dispositivos corporativos (computadores, notebooks, celulares, servidores);
- Ferramentas de comunicação (e-mails, chats, plataformas de reunião, grupos e mensagens internas);
- Documentos impressos, planilhas, relatórios e registros administrativos;
- Armazenamentos em nuvem e integrações com sistemas de terceiros.

Todos os agentes de tratamento têm o dever de seguir as práticas de proteção definidas neste documento, sob pena de responsabilização conforme as normas internas e a legislação aplicável.

---

3. Diretrizes Principais

1. **Princípios da LGPD:** todo tratamento de dados deve observar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.
2. **Classificação da Informação:** as informações são categorizadas em públicas, internas, restritas e confidenciais, conforme seu grau de sensibilidade e impacto em caso de vazamento.
3. **Confidencialidade:** é proibido o compartilhamento de dados pessoais ou estratégicos fora dos canais autorizados ou sem consentimento formal.
4. **Integridade:** todos os registros eletrônicos e documentos devem manter-se íntegros, sem adulterações, salvo atualizações devidamente registradas.
5. **Disponibilidade:** a empresa adota medidas para assegurar que as informações estejam acessíveis a quem de direito, quando necessário, mediante autenticação segura.
6. **Gestão de Incidentes:** qualquer evento que possa comprometer a segurança das informações deve ser imediatamente comunicado ao Encarregado de Dados (DPO), que acionará o protocolo de resposta.
7. **Ambiente Tecnológico Seguro:** o sistema web da Paez Gestão utiliza protocolos HTTPS, criptografia de dados, autenticação em múltiplos fatores e logs automáticos de acesso.
8. **Treinamento Contínuo:** todos os colaboradores participam de capacitações sobre boas práticas de segurança da informação e proteção de dados.
9. **Auditoria e Melhoria Contínua:** controles e processos são revisados periodicamente para identificar vulnerabilidades e garantir conformidade regulatória.

---

4. Procedimentos Operacionais

- **Controle de Acesso:** o acesso às informações e sistemas é concedido de acordo com o cargo e a função desempenhada, mediante uso de credenciais individuais e senhas seguras.

- **Gestão de Dispositivos:** equipamentos corporativos devem possuir antivírus atualizado, bloqueio automático de tela e softwares licenciados.
- **Armazenamento Seguro:** documentos eletrônicos sensíveis devem ser armazenados em servidores protegidos por autenticação e monitoramento de integridade.
- **Transmissão de Dados:** a troca de informações via e-mail, grupos ou mensagens deve ocorrer apenas por canais corporativos, com linguagem profissional e respeito à privacidade dos envolvidos.
- **Documentos Físicos:** arquivos impressos contendo informações pessoais devem ser guardados em locais trancados e descartados por fragmentação segura após o período de retenção.
- **Relatórios e Logs:** as operações realizadas nos sistemas são registradas em logs automáticos, garantindo rastreabilidade e responsabilidade de cada ação executada.

---

5. Monitoramento e Conformidade

O cumprimento desta política é responsabilidade de todos os membros da organização, sob supervisão do **Encarregado de Proteção de Dados (DPO)**, que realiza auditorias internas e relatórios de conformidade periódicos.
A empresa adota o princípio da **melhoria contínua**, atualizando as diretrizes conforme avanços tecnológicos e novas determinações legais da Autoridade Nacional de Proteção de Dados (ANPD).

A violação das regras estabelecidas nesta política pode resultar em sanções administrativas internas, suspensão de acessos, desligamento contratual e, quando aplicável, comunicação às autoridades competentes.
A política será revisada anualmente ou sempre que houver mudanças relevantes no ambiente tecnológico ou nas exigências regulatórias.