6. Política de Backup e Restauração de Dados

1. Contexto e Finalidade

A continuidade das operações da Paez Gestão depende da disponibilidade e integridade das informações mantidas em seu sistema web, que concentra cadastros, comunicações, atividades e relatórios das mentorias.
Esta política tem por objetivo estabelecer normas e procedimentos para **criação, armazenamento, verificação e restauração de backups**, garantindo que os dados corporativos e pessoais possam ser recuperados em caso de falhas, ataques cibernéticos, exclusões acidentais ou desastres físicos.

A política busca assegurar que nenhuma perda de dados afete a execução das atividades, a confiança dos clientes ou a conformidade com a LGPD. Assim, define responsabilidades, periodicidade, meios tecnológicos e padrões de segurança para todas as cópias de dados digitais da empresa.

---

2. Âmbito de Aplicação

Aplica-se a todos os sistemas, servidores, bancos de dados, estações de trabalho, arquivos digitais e comunicações corporativas da Paez Gestão.
Inclui dados coletados de clientes, mentores, colaboradores e terceiros, bem como relatórios financeiros, documentos administrativos, mensagens do sistema de mentoria e registros de consentimento.

Todos os colaboradores e prestadores com acesso a sistemas ou informações críticas devem observar as práticas descritas nesta política.

---

3. Diretrizes Principais

1. **Periodicidade:** cópias completas do banco de dados são realizadas diariamente, com versões incrementais a cada 6 horas em ambiente em nuvem.
2. **Redundância:** os backups são armazenados em ao menos dois locais distintos — servidor principal e nuvem criptografada.
3. **Integridade e criptografia:** todos os arquivos de backup devem ser criptografados (AES-256) e protegidos por autenticação multifatorial.
4. **Controle de acesso:** apenas a equipe técnica e o DPO possuem credenciais para acessar ou restaurar backups.
5. **Testes periódicos:** restaurações parciais são realizadas mensalmente para validar a eficiência e integridade das cópias.
6. **Retenção:** as versões de backup são mantidas por 90 dias antes da substituição automática.

7. **Proteção física e lógica:** servidores locais devem permanecer em ambiente seguro, com no-break, firewall e antivírus atualizados.

---

4. Procedimentos Operacionais

- **Planejamento:** o setor de TI mantém um calendário documentado com os horários e tipos de backup (completo, incremental e diferencial).
- **Execução automatizada:** scripts programados executam os backups, reduzindo risco de erro humano.
- **Monitoramento:** alertas automáticos informam falhas ou interrupções no processo de cópia.
- **Restauração:** em caso de incidente, o DPO autoriza o procedimento de recuperação conforme a criticidade do sistema afetado.
- **Registro:** cada operação de backup e restauração é registrada com data, hora, tamanho e status.
- **Descarte:** cópias antigas são eliminadas após o ciclo de retenção, mediante exclusão segura e irrecuperável.

---

5. Monitoramento e Conformidade

A verificação dos backups é feita por meio de auditorias internas mensais, supervisionadas pelo DPO.
O não cumprimento desta política constitui falha grave, podendo gerar sanções administrativas e comunicação à ANPD, em caso de incidente que afete dados pessoais.

Esta política é revisada anualmente ou quando houver mudanças tecnológicas significativas. O compromisso da Paez Gestão é manter a resiliência digital como valor permanente e parte da cultura de governança de dados.