## 17. Política de Gerenciamento de Incidentes de Segurança da Informação

### 1. Contexto e Finalidade

Mesmo com controles técnicos e administrativos robustos, nenhum sistema é imune a falhas.
A Paez Gestão adota abordagem proativa para identificação, resposta e mitigação de **incidentes de segurança da informação**, compreendidos como qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade dos dados tratados pela empresa.

Esta política define o processo formal de detecção, registro, tratamento, comunicação e correção de incidentes, garantindo que as medidas sejam tomadas de forma rápida, coordenada e transparente.
A finalidade é reduzir impactos operacionais, financeiros e reputacionais, além de assegurar cumprimento dos deveres legais perante titulares e autoridades competentes.

---

### 2. Âmbito de Aplicação

Aplica-se a todos os incidentes relacionados a sistemas, redes, dispositivos, aplicativos, comunicações eletrônicas, documentos físicos e processos que envolvam informações sob responsabilidade da Paez Gestão.
Inclui eventos como: acesso não autorizado, perda de dados, falhas em backup, phishing, malware, vazamento de informações, uso indevido de credenciais e violações de confidencialidade.

---

### 3. Diretrizes Principais

1. **Princípio da resposta imediata:** qualquer suspeita de incidente deve ser comunicada imediatamente ao DPO.
2. **Classificação do incidente:** os eventos são categorizados por nível de gravidade (baixo, médio, alto e crítico).
3. **Equipe de resposta:** composta pelo DPO, TI e gestor da área afetada, responsável por investigação e mitigação.
4. **Registro obrigatório:** todos os incidentes devem ser documentados em formulário interno de registro.
5. **Preservação de evidências:** logs, e-mails e arquivos envolvidos devem ser preservados sem alteração.
6. **Notificação de titulares:** quando houver risco relevante, os afetados devem ser informados sobre o ocorrido e as medidas adotadas.
7. **Relato à ANPD:** incidentes de alto impacto devem ser reportados à Autoridade Nacional de Proteção de Dados em até 48 horas após confirmação.

8. **Aprendizado organizacional:** cada incidente gera relatório com recomendações preventivas.

---

**4. Procedimentos Operacionais**

- **Identificação:** o colaborador que detectar falha comunica o DPO via canal exclusivo.
- **Análise:** a equipe técnica avalia extensão, causas e possíveis danos.
- **Resposta:** medidas emergenciais são adotadas (bloqueio de acesso, restauração de backup, aviso aos usuários).
- **Comunicação:** os envolvidos e a direção são informados do andamento e conclusão.
- **Documentação:** todas as etapas são registradas em planilha de incidentes.
- **Revisão:** após a contenção, são revisadas políticas e controles relacionados.

---

**5. Monitoramento e Conformidade**

O DPO realiza auditorias trimestrais sobre os registros de incidentes e elabora relatórios de conformidade.
A reincidência ou a negligência no reporte constitui infração disciplinar.
A empresa reforça que o aprendizado com incidentes é oportunidade de fortalecimento da segurança organizacional.
A política é revisada anualmente, com base nas melhores práticas ISO/IEC 27035 e orientações da ANPD.