

NOTA TÉCNICA Nº 01 BANCO DE CURRÍCULOS COMPARTILHADOS

O Sistema FIEMG, com foco no apoio às indústrias mineiras, vem orientar quanto à prática de criação de bancos de currículos unificados para cadastro de mão de obra por grupos de empresas e organizações.

Iniciativas que buscam aprimorar processos e promover ganhos de eficiência operacional, tais como a centralização de etapas relacionadas à contratação de pessoas, devem estar alinhadas às exigências da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

Isso significa que qualquer iniciativa dessa natureza deve respeitar rigorosamente os direitos dos titulares dos dados pessoais, desde a coleta até a eliminação das informações. A legislação exige a adoção de procedimentos e salvaguardas que garantam a segurança dos dados e o monitoramento contínuo dos fluxos de tratamento.

Nesse contexto, para assegurar a conformidade com a LGPD, recomenda-se que, **antes da implementação de qualquer banco de currículos, a empresa adote, no mínimo**, as seguintes medidas:

1. **Indicar o Encarregado** pelo Tratamento de Dados Pessoais (DPO);
2. Mapear e **registrar o fluxo de tratamento de dados pessoais** da atividade, evidenciando: i) os tipos de dados pessoais ; ii) a finalidade do tratamento; iii) a base legal que o sustenta; iv) as partes envolvidas (controlador, operadores, encarregado); v) as empresas que utilizam a base; vi) sistemas utilizados; vii) o responsável pelo processo;
3. **Adequar o processo**, com base nos princípios e obrigações da LGPD;
4. Realizar análise de risco aos titulares de dados e, quando aplicável, **elaborar o Relatório de Impacto à Proteção de Dados (RIPD)**;
5. **Implementar medidas técnicas e administrativas** para garantir a confidencialidade, integridade e disponibilidade dos dados;
6. Assegurar mecanismos que permitam o **exercício dos direitos pelo titular dos dados**, como acesso, retificação, exclusão, informação sobre compartilhamento e portabilidade;
7. Estabelecer um **Programa de Privacidade** com práticas de proteção de dados, planos de resposta a incidentes, monitoramento contínuo e avaliação de riscos;
8. Formalizar e divulgar **documentos normativos** que regulamentem as práticas relacionadas à proteção de dados, tais como a Política de Privacidade, a Política de Descarte e a Política de Segurança da Informação.

A realização dessas medidas, além de assegurar a conformidade com a legislação, fortalece a transparência no tratamento de dados pessoais e reforça o compromisso com a privacidade dos titulares.

Gerência de Governança, Riscos, Compliance e Privacidade (GRC&P)

Belo Horizonte, 11 de março de 2021.