MÓDULO 04
LGPD & SEGURANÇA DA INFORMAÇÃO

Adequação legal obrigatória e proteção da infraestrutura digital do DAE-VG

Inventário de dados · Política de Segurança · Resposta a incidentes · Treinamento

Parceria Estratégica | DAE de Várzea Grande-MT

Target Tecnologia e Inovação + IFMT (ICT Pública Federal) | Contratação via Dispensa de Licitação – Lei 14.133/2021

POR QUE O DAE-VG PRECISA SE ADEQUAR AGORA

A Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018) é obrigatória para entidades públicas. O DAE-VG, como autarquia municipal que processa dados pessoais de mais de 320 mil habitantes, está sujeito a sanções da ANPD.

Sanções da ANPD

Advertências, multas de até 2% do faturamento (máximo R$ 50 milhões por infração) e bloqueio de atividades de tratamento.

Vazamento de dados

O DAE-VG possui dados de endereço, CPF, consumo e inadimplência de +320 mil pessoas. Um vazamento gera dano reputacional severo.

Responsabilidade do Gestor

O titular do tratamento de dados pode responder pessoalmente por violações. Diretores e servidores estão expostos.

Processo de Concessão

A adequação à LGPD é critério avaliado em due diligence de concessões. A não conformidade reduz o valor percebido pelo concessionário.

PASSO 1 — INVENTÁRIO E MAPEAMENTO DE DADOS

Antes de qualquer medida técnica, é necessário mapear TODOS os dados pessoais tratados pelo DAE-VG — quais são, onde estão, quem acessa, por quanto tempo são retidos.

Dados de Clientes

Nome, CPF, endereço, consumo mensal, histórico de pagamentos, inadimplência, documentos de matrícula.

Dados Operacionais Sensíveis

Localização de infraestrutura crítica, senhas de sistemas, configurações de automação e SCADA.

Dados de Funcionários

CPF, endereço, informações bancárias, exames médicos, controle de ponto, benefícios.

Dados de Fornecedores

CNPJ, dados bancários para pagamento, contratos e representantes legais.

Entregável:

Relatório ROPA (Registro das Operações de Processamento) — documento exigido pelo art. 37 da LGPD e pela ANPD.

PASSO 2 — POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação (PSI) é o documento mestre que orienta COMO o DAE-VG protege seus dados e sistemas. Alinhada à ISO 27001 e à LGPD.

01 Controle de Acesso

Autenticação em dois fatores · Gestão de senhas · Princípio do mínimo privilégio · Logs de acesso

02 Segmentação de Rede

Rede OT (SCADA/automação) isolada da rede TI · Firewall industrial · DMZ para serviços externos

03 Backup e Recuperação

Backup diário criptografado · Teste mensal de restauração · Retenção mínima de 90 dias · Cópia offsite

04 Gestão de Incidentes

Plano de Resposta a Incidentes (PRI) · Notificação em 72h à ANPD · Comunicação aos titulares afetados

05 Treinamento Contínuo

Módulo de conscientização para TODOS os servidores · Teste de phishing periódico · Atualização semestral

06 Auditoria e Monitoramento

SIEM (log de eventos) · Relatório trimestral ao Encarregado de Dados (DPO) · Revisão anual da PSI

PASSO 3 — GOVERNANÇA: DPO E ESTRUTURA DE CONFORMIDADE

A LGPD exige a indicação de um Encarregado de Dados (DPO — Data Protection Officer). A Target estrutura esse papel e os processos de conformidade para o DAE-VG.

Indicação do DPO

Formalização do Encarregado de Dados conforme art. 41 da LGPD. Pode ser servidor interno capacitado pela Target ou terceirizado.

DPIA — Avaliação de Impacto

Para processos de alto risco: macromedição com dados de consumo, cadastro de vulnerabilidade social e geolocalização de ligações.

Canal de Atendimento ao Titular

Formulário de solicitação de direitos do titular: acesso, correção, exclusão, portabilidade e oposição. SLA de 15 dias.

Gestão de Consentimento

Adequação dos contratos, termos de serviço e formulários para coleta de consentimento explícito onde exigido pela LGPD.

ROTEIRO DE ADEQUAÇÃO – 12 MESES

Mês 1-2

Diagnóstico

- ✓ Entrevistas com áreas do DAE-VG
- ✓ Inventário de sistemas e banco de dados
- ✓ Mapeamento de fluxos de dados pessoais
- ✓ Avaliação do nível de maturidade de segurança

Mês 3-4

Política e Normas

- ✓ Redação da PSI e procedimentos
- ✓ Definição e indicação do DPO
- ✓ Modelo de inventário ROPA
- ✓ Atualização de contratos e termos

Mês 5-8

Implementação

- ✓ Implantação dos controles técnicos
- ✓ Segmentação de rede OT/TI
- ✓ Configuração de backup e monitoramento
- ✓ Canal de atendimento ao titular live

Mês 9-12

Capacitação e Auditoria

- ✓ Treinamento de todos os servidores
- ✓ Simulação de incidente (exercício de crise)
- ✓ Auditoria de conformidade LGPD
- ✓ Relatório final e plano de melhoria contínua

ESTIMATIVA DE INVESTIMENTO – LGPD & SEGURANÇA

ITEM	ESTIMATIVA
Diagnóstico e inventário de dados (ROPA)	**R$ 20.000 – R$ 30.000**
Elaboração da PSI e documentação de conformidade	**R$ 25.000 – R$ 40.000**
DPO as-a-Service (1º ano — acompanhamento mensal)	**R$ 24.000 – R$ 36.000 /ano**
Ferramentas de segurança (SIEM, backup, firewall)	**R$ 40.000 – R$ 70.000**
Implementação técnica dos controles de segurança	**R$ 35.000 – R$ 55.000**
Treinamento de equipes e capacitação via IFMT	**R$ 15.000 – R$ 25.000**
Auditoria de conformidade (12 meses)	**R$ 20.000 – R$ 30.000**
TOTAL ESTIMADO (1º ano de conformidade)	**R$ 179.000 – R$ 286.000**

A adequação à LGPD não é custo — é proteção patrimonial e requisito de governança para qualquer processo de concessão ou financiamento público (BNDES, PAC, CEF).