GUIA ORIENTATIVO DE ADEQUAÇÃO À LGPD NO PODER EXECUTIVO DO ESTADO DE ALAGOAS

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) estabelece normas para a coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais no Brasil.

Sua aplicação nos órgãos e entidades da Administração Pública Direta e Indireta do Estado de Alagoas requer planejamento estratégico e contínuo, envolvendo:

- Conscientização e engajamento da alta gestão;
- Identificação e classificação dos dados pessoais tratados;
- Gestão de riscos e implementação de medidas de segurança;
- Elaboração de políticas e procedimentos de proteção de dados;
- Ajustes administrativos, contratuais e regulatórios;
- Monitoramento e revisão contínua das práticas de proteção de dados.

Este guia está estruturado em sete fases complementares, que orientam o processo de adequação à LGPD no âmbito estadual, fortalecendo a cultura de privacidade e a proteção de dados pessoais.

1ª FASE: PREPARAÇÃO E PLANEJAMENTO

1. DESIGNAÇÃO DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

- [ ] Designar formalmente os DPOs (titular e substituto) por ato publicado no Diário Oficial;
- [ ] Disponibilizar suas informações de contato no site institucional;
- [ ] Divulgar internamente as funções e responsabilidades do DPO;
- [ ] Criar unidade específica no SEI para tramitação de processos relacionados à LGPD.

2. APOIO DA ALTA GESTÃO

- [ ] Garantir comprometimento da alta administração;
- [ ] Participar de eventos, reuniões estratégicas e capacitações sobre a LGPD;
- [ ] Definir papéis e responsabilidades setoriais em conjunto com o DPO;
- [ ] Apoiar a formação continuada do DPO.

3. CRIAÇÃO DE GRUPO DE TRABALHO (GT) DE PRIVACIDADE E PROTEÇÃO DE DADOS

- [ ] Formar equipe multidisciplinar (Jurídico, TI, Segurança da Informação, RH e setores estratégicos);
- [ ] Responsabilizar o GT pelo acompanhamento, monitoramento e execução de adequação à LGPD pelo órgão ou entidade.
- [ ] Realizar reuniões periódicas para avaliar o cumprimento das competências do GT e o progresso das ações de adequação.

4. CULTURA INTERNA DE PROTEÇÃO DE DADOS

- [ ] Elaborar/disponibilizar plano de sensibilização, treinamento e capacitação contínua;
- [ ] Utilizar canais internos (intranet, e-mail, cartilhas, workshops) para disseminação da LGPD;
- [ ] Desenvolver trilhas de aprendizagem por perfil de setor/servidor;
- [ ] Instruir/informar os servidores sobre boas práticas da LGPD.

2ª FASE: MAPEAMENTO E CLASSIFICAÇÃO DOS DADOS PESSOAIS

1. MAPEAMENTO DE DADOS PESSOAIS

- [ ] Capacitar equipes responsáveis sobre métodos de mapeamento de dados pessoais;
- [ ] Identificar todos os setores que tratam dados pessoais;
- [ ] Mapear fluxos de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2. CLASSIFICAÇÃO E CATEGORIZAÇÃO

- [ ] Diferenciar as diversas espécies de dados pessoais previstas na LGPD (dados pessoais, dados pessoais sensíveis e dados pessoais de crianças e de adolescentes);
- [ ] Categorizar dados de acordo com a finalidade específica de tratamento (identificação, financeiros, saúde, hábitos, entre outros);
- [ ] Indicar, em cada setor, equipe responsável por atuar como ponto focal para apoiar a identificação, classificação e categorização dos dados pessoais tratados, em razão de sua experiência e conhecimento sobre os fluxos existentes.

3. INVENTÁRIO DE DADOS E REGISTRO DAS OPERAÇÕES DE TRATAMENTO (ROPA)

- [ ] Registrar detalhadamente todas as operações de tratamento de dados pessoais;
- [ ] Incluir: finalidade, necessidade específica, base legal (arts. 7º e 11 da LGPD), categorias de dados, compartilhamento, prazo de retenção, medidas de segurança adotadas;
- [ ] Atualizar periodicamente o Inventário de Dados e ROPA de acordo com o fluxo de atividade de tratamento do setor.

3ª FASE: GESTÃO DE RISCOS

1. IDENTIFICAÇÃO E ANÁLISE DE RISCOS

- [ ] Mapear vulnerabilidades técnicas, administrativas, físicas e operacionais;
- [ ] Avaliar impactos à privacidade e segurança dos dados;

- [ ] Priorizar riscos críticos e propor medidas mitigadoras.

2. PLANO DE MITIGAÇÃO DE RISCOS

- [ ] Capacitar equipes sobre identificação, prevenção e mitigação de riscos relacionados à proteção de dados pessoais;
- [ ] Definir medidas técnicas (criptografia, controle de acesso), administrativas (políticas, segregação de funções) e físicas (controle de entrada, monitoramento);
- [ ] Registrar ações corretivas e prazos de implementação.

3. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

- [ ] Elaborar RIPD sempre que o tratamento apresentar riscos elevados à privacidade dos titulares;
- [ ] Revisar periodicamente ou sempre que houver alterações significativas nos processos de tratamento.

4ª FASE: POLÍTICAS E PROCEDIMENTOS DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO

1. POLÍTICA DE PRIVACIDADE E USO DE COOKIES

- [ ] Publicar, no sítio eletrônico oficial do órgão ou entidade, Política de Privacidade e banner/aviso de cookies de forma clara, acessível e em linguagem cidadã;
- [ ] Incluir informações sobre cookies, bases legais, hipóteses de tratamento de dados, direitos dos titulares e canais de atendimento;
- [ ] Utilizar elementos visuais para facilitar a compreensão pelos cidadãos.

2. POLÍTICA DE PROTEÇÃO DE DADOS (INTERNA)

- [ ] Estabelecer regras e procedimentos internos para o tratamento de dados pessoais;
- [ ] Definir responsabilidades, bases de tratamento, prazos de retenção e descarte;
- [ ] Incluir diretrizes específicas para servidores, terceirizados e estagiários.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- [ ] Estabelecer controles sobre acessos, uso de dispositivos, senhas, armazenamento e descarte seguro;

- [ ] Integrar boas práticas de segurança digital e física, em alinhamento com normativos estaduais e federais já existentes;
- [ ] Formação continuada em cibersegurança.

4. POLÍTICA DE CONTROLE DE ACESSO

- [ ] Definir critérios para concessão, revisão e revogação de acessos a sistemas e dados;
- [ ] Estabelecer responsabilidades sobre monitoramento de acessos e registro de auditoria;
- [ ] Estabelecer perfis de níveis de acessos.

5. POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

- [ ] Estabelecer rotinas de backup periódico e testes regulares de restauração de dados;
- [ ] Garantir disponibilidade e integridade dos dados em situações de falhas técnicas ou incidentes de segurança;
- [ ] Documentar procedimentos e responsáveis pelo processo de backup e recuperação.

5ª FASE: AJUSTES ADMINISTRATIVOS E CONFIDENCIALIDADE

1. REVISÃO DE NORMAS E ATOS ADMINISTRATIVOS

- [ ] Adequar regulamentos, portarias e procedimentos internos à LGPD;
- [ ] Garantir que práticas administrativas reflitam as políticas institucionais de proteção de dados pessoais.

2. AJUSTES ADMINISTRATIVOS (CONTRATOS, CONVÊNIOS E TERMOS DE COOPERAÇÃO)

- [ ] Inserir cláusulas de privacidade e proteção de dados em todos os instrumentos jurídicos;
- [ ] Especificar responsabilidades, medidas de segurança e obrigações de comuicação de incidentes;

- [ ] Realizar diligência prévia de terceiros que tratem dados pessoais.

3. TERMO DE COMPROMISSO E CONFIDENCIALIDADE DE PROTEÇÃO DE DADOS PESSOAIS

- [ ] Solicitar assinatura do termo a todos os agentes públicos vinculados ao órgão ou entidade (servidores, terceirizados, estagiários, entre outros, com acesso a dados pessoais);
- [ ] Garantir acompanhamento do cumprimento das obrigações de confidencialidade e tratamento adequado dos dados pessoais.

4. CUMPRIMENTO DAS DIRETRIZES DO COMITÊ ESTADUAL DE PROTEÇÃO DE DADOS PESSOAIS (CEPD)

- [ ] Implementar e observar as diretrizes, recomendações e normas emitidas pelo CEPD;
- [ ] Incorporar essas orientações às rotinas administrativas e procedimentos internos do órgão ou entidade;
- [ ] Manter registro das ações realizadas para comprovar conformidade.

6ª FASE: GESTÃO E RESPOSTA A INCIDENTES

1. IDENTIFICAÇÃO E CONTENÇÃO

- [ ] Monitorar sistemas para detecção de incidentes;
- [ ] Contenção imediata de falhas, acessos indevidos ou vazamentos.

2. COMUNICAÇÃO INTERNA E EXTERNA

- [ ] Notificar imediatamente o DPO e a alta administração;
- [ ] Avaliar relevância do incidente;
- [ ] Estabelecer estratégias para manter operações críticas em situações de crise (falhas

- [ ] Comunicar titulares e a ANPD em prazo razoável, em até 2 dias úteis, quando o incidente for relevante.

3. REGISTRO E APRENDIZADO

- [ ] Documentar o incidente, causas, ações corretivas e medidas preventivas;
- [ ] Revisar políticas e procedimentos para evitar recorrência.

4. PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP)

- [ ] Estabelecer estratégias para manter operações críticas em situações de crise (falhas técnicas, indisponibilidade de sistemas ou incidentes de segurança);
- [ ] Integrar o BCP com medidas de proteção de dados e planos de resposta a incidentes;
- [ ] Testar e revisar periodicamente o plano, assegurando sua efetividade em cenários reais.

7ª FASE: MONITORAMENTO E AVALIAÇÃO CONTÍNUA

1. MONITORAMENTO PERMANENTE

- [ ] Revisar periodicamente fluxos de tratamento de dados;
- [ ] Realizar testes de segurança, incluindo simulações de engenharia social;
- [ ] Atualizar indicadores de desempenho em proteção de dados.

2. AUDITORIAS INTERNAS

- [ ] Elaborar plano de auditoria em LGPD com periodicidade definida;
- [ ] Avaliar setores críticos e operações de tratamento;
- [ ] Emitir relatórios de conformidade.

3. REVISÃO DE POLÍTICAS E CONTRATOS

- [ ] Atualizar políticas de privacidade, segurança e cláusulas contratuais sempre que houver mudanças legislativas, tecnológicas ou operacionais;

- [ ] Garantir integração entre auditorias, monitoramento e plano de mitigação de riscos.

CRONOGRAMA DE EXECUÇÃO													
ATIVIDADES	out/25	nov/25	dez/25	jan/26	fev/26	mar/26	abr/26	mai/26	jun/26	jul/26	ago/26	set/26	out/26
Sensibilizações e treinamentos	X	X	X	X	X	X	X	X	X	X	X	X	X
1º Fase: Preparação e Planejamento	X	X											
2º Fase: Mapeamento e Classificação dos Dados Pessoais			X	X	X								
3º Fase: Gestão de Riscos						X	X						
4º Fase: Políticas e Procedimentos de Proteção de Dados e Segurança da Informação								X	X	X			
5ª Fase: Ajustes Administrativos e Confidencialidade									X	X			
6º Fase: Gestão e Resposta a Incidentes										X	X	X	
7º Fase: Monitoramento e Avaliação Contínua												X	X

REFERÊNCIAS BIBLIOGRÁFICAS

VALE, Luís Manoel Borges do; OLIVEIRA, Rafael Carvalho Rezende. LGPD na Administração Pública. 1. ed. Rio de Janeiro: GEN Editora Forense, 2025. ISBN 9788530995737.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 ago. 2024.

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial da União: Brasília, DF, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 ago. 2024.

ALAGOAS. Decreto Estadual n. 91.229, de 18 de maio de 2023. Dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados – LGPD, no âmbito da administração pública direta e indireta do executivo estadual. Diário Oficial do Estado de Alagoas: Maceió, AL, 19 maio 2023. Disponível em: Acesso em: 14 ago. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Política Nacional de Segurança da Informação. Decreto n. 9.637, de 26 de dezembro de 2018. Diário Oficial da União: Brasília, DF, 27 dez. 2018. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-9.637-de-26-de-dezembro-de-2018-71168460. Acesso em: 14 ago. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005: Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 37301: Sistemas de gestão de compliance: requisitos com orientações para uso. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27701: Técnicas de segurança: extensão da ISO/IEC 27001 e da ISO/IEC 27002 para gestão da privacidade da informação: requisitos e diretrizes. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 38505-2: Governança de TI: Governança de dados. Rio de Janeiro: ABNT, 2021.