MANUAL DE IMPLEMENTAÇÃO

LEI GERAL DE PROTEÇÃO DE DADOS

Ouvidoria Geral do Sistema de Segurança Pública

Secretaria de **Segurança Pública**

AMAZONAS
GOVERNO DO ESTADO
TRABALHO QUE TRANSFORMA

Governador do Estado
Wilson Miranda Lima

Secretário de Estado de Segurança Pública
Cel. Marcus Vinícius Oliveira de Almeida

Secretário Executivo de Segurança Pública
Cel. QOPM Anézio Brito de Paiva

Secretário Executivo Adjunto de Operação – SEAOP
Cel. QOPM Algenor Maria da Costa Teixeira Filho

Secretário Executivo Adjunto de Planejamento e Gestão Integrada de Segurança – SEAGI
Cel. QOPM José Almir Cavalcante Rodrigues

Secretário Executivo Adjunto de Inteligência – SEAI
José Divanilson Cavalcanti Júnior

Corregedor-Geral do Sistema de Segurança Pública
Cel. QOPM Franciney Machado Bó

Diretora do Departamento de Polícia Técnico Científica-DPTC
Sanmya Beatriz Tiradentes Leite

Ouvidor-Geral do Sistema de Segurança Pública
Sérgio Augusto Costa da Silva

SUMÁRIO

APRESENTAÇÃO

O presente manual tem o objetivo de orientar os servidores quanto aos procedimentos para a implementação da LGPD no âmbito da Secretaria de Segurança Pública do Estado do Amazonas – SSP/AM.
Tais orientações são fundamentais não só para garantir a correta aplicabilidade da lei, mas também para evitar a violação dos direitos do titular de dados em relação ao tratamento de dados pessoais efetuado pela SSP/AM.

As recomendações para a implementação da LGPD estão baseadas no conjunto de normas legais relacionadas ao tema, bem como nos materiais disponibilizados pela ANPD e CGE.

1. LEI GERAL DE PROTEÇÃO DE DADOS - LEI 13.709/2018

Afinal que lei é essa?

Vigência:
27/08/2010

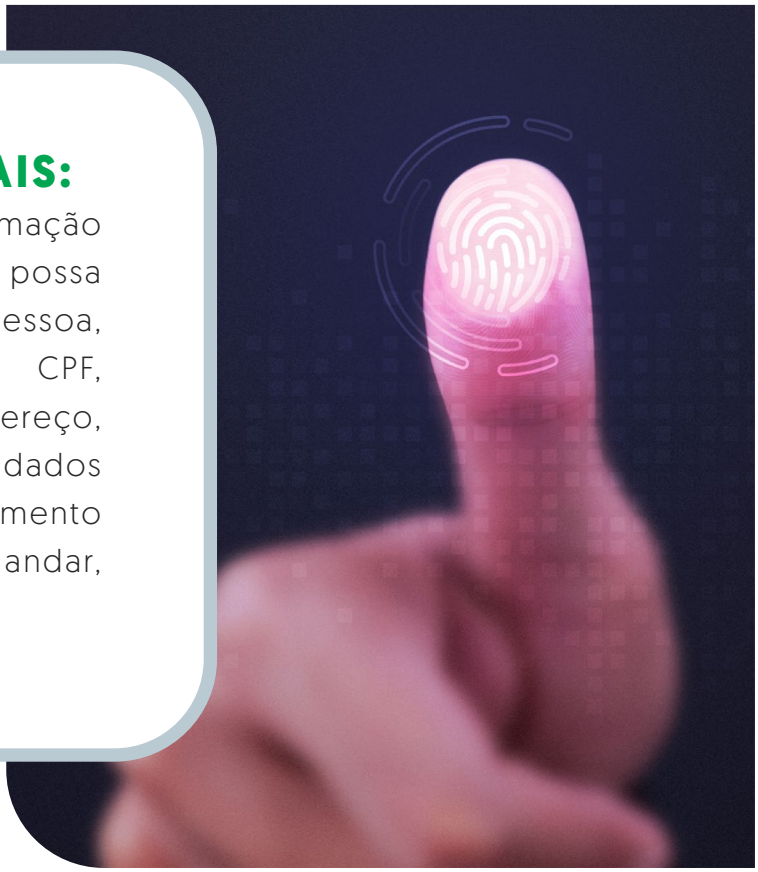
Vigente desde 27 de agosto de 2020, a LGPD tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Isso significa que a LGPD protege a forma como os dados pessoais são utilizados.

Estamos vivendo a era da economia orientada a dados, a ausência de uma adequada regulação para o tratamento de dados pessoais, gera uma coleta desenfreada e utilização descomedida de dados dos titulares.

Diante deste cenário, muito além de um problema de privacidade, a proteção de dados revela-se como um verdadeiro fundamento para a preservação da individualidade, da liberdade e da própria democracia.

Lembre-se sempre, os dados são dos titulares

2. O QUE SÃO DADOS PESSOAIS E DADOS SENSÍVEIS



- **DADOS PESSOAIS:**
Qualquer informação que identifique ou possa identificar uma pessoa, por exemplo: nome, CPF, RG, e-mail, endereço, fotografia, biometria, dados de localização, batimento cardíaco, forma de andar, entre outros.

- **DADO SENSÍVEL:**
Dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

3. AGENTES DE TRATAMENTO DE DADOS

3.1 CONTROLADOR E OPERADOR:

CONTROLADOR:

Empresa / parte(s) interessada(s) na privacidade que determina (m) os objetivos e os meios para o tratamento dos dados pessoais e que não é (são) pessoa (s) natural (is) que usa (m) os dados para objetivos pessoais.

OPERADOR:

Empresa / parte interessada na privacidade, que realiza o tratamento dos dados pessoais em benefício e de acordo com as instruções de um controlador de DP.

Devem manter registro das operações de tratamento de dados que realizarem.

A Autoridade Nacional de Proteção de Dados (ANPD), bem como o Ministério Público poderá determinar ao controlador que elabore relatório de impacto à proteção de dados, contendo a descrição detalhada dos tipos de dados coletados, a metodologia que é utilizada para garantir a segurança dos dados e informações e também sobre os mecanismos utilizados para a mitigação dos riscos adotados.

• 3.2 ENCARREGADO PELO TRATAMENTO DE DADOS:

Deve o controlador indicar um profissional encarregado, seja pessoa física ou jurídica, para que fique responsável pelo tratamento de dados pessoais, o qual deverá conhecer em detalhes todas as operações da empresa.

Caberá a este encarregado atender as reclamações e comunicações dos titulares e adotar providências, receber comunicações da ANPD e tomar as medidas determinadas por esta, também deve orientar demais funcionários e contratados sobre as práticas adequadas a serem tomadas em relação ao tratamento e proteção dos dados.

4. COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS - CGPDP

O Comitê Gestor de Proteção de Dados Pessoais - CGPDP tem a finalidade de dar auxílio no cumprimento da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), este Comitê é formado por equipe multidisciplinar, composta de servidores da alta gestão, tecnologia da informação, setor jurídico, encarregado de dados, entre outras áreas afins que possam contribuir para o desenvolvimento de um plano de ação adequado e eficiente para implementação da LGPD.

É recomendável que CGPDP esteja sujeito, ao menos, às seguintes atribuições:

• Avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade da SSP/AM com as disposições da Lei n. 13.709, de 14 de agosto de 2018;

- Formular princípios e diretrizes para a gestão de dados pessoais;
- Supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei n. 13.709, de 14 de agosto de 2018;
- Prestar orientações sobre o tratamento e a proteção de dados pessoais, de acordo com as diretrizes estabelecidas na Lei n. 13.709, de 14 de agosto de 2018 e nas normas internas;
- Propor e monitorar a adoção de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
- Promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos.

5. PLANO DE AÇÃO PROCESSOS E DETALHAMENTOS DA IMPLEMENTAÇÃO

O Plano de Ação elenca as principais atividades que deverão ser executadas pela SSP/AM para o cumprimento das exigências da Lei Geral de Proteção de Dados, bem como quanto a implementação da LGPD, sugere-se o modelo a seguir, que poderá sofrer adequações, conforme especificidades:

PROCESSO	DETALHAMENTO
1. Diagnósticos: 1.1. Da cultura organizacional;	Aplicação de questionário aos servidores para verificar a percepção e o conhecimento dos mesmos a respeito da LGPD;
1.2.Da governança de dados	Aplicação de questionário ao gestor da pasta para verificar quais as práticas atuais aplicadas e em qual estágio o órgão se encontra.
2. Mapeamento de Dados Pessoais	Catalogar todo o fluxo de dados pessoais, objeto das operações de tratamento
3. Levantamento de Riscos	Procedimento para ajudar a planejar as ações preventivas tomadas por parte do órgão; Deverá abranger todos os envolvidos no processo de tratamento de dados (controlador e operador). *ISO 27001 *Necessidade de atualização periódica

4. Criação de Política de Privacidade de Dados	A Política de Privacidade de Dados é um documento informativo que descreve ao titular a forma, os processos e os procedimentos adotados no tratamento dos dados pessoais e as medidas de privacidade empregadas.
5. Adaptação de documentos	Revisão de contratos e demais documentos (impressos e digitais) para atender ao disposto nas normas pertinentes à LGPD.
6. Termo de Compromisso e Confidencialidade	Termo de Compromisso e Confidencialidade a ser exigido daqueles que tenham acesso a dados pessoais no âmbito do órgão ou entidade.
7. Política de Segurança da Informação	A Política de Segurança da Informação é o conjunto de princípios e diretrizes que têm a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação do órgão ou entidade.
8. Plano de Resposta a Incidentes e Privacidade	a.conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes; b. preservar a reputação e imagem do órgão ou entidade; c. assegurar respostas rápidas, efetivas e coordenadas; d. quantificar e monitorar desempenho; e. evoluir continuamente com as lições aprendidas.

5.1. DIAGNÓSTICOS

5.1.1 DA CULTURA ORGANIZACIONAL

A adequação da Secretária de Segurança Pública do Estado do Amazonas em relação à Lei Geral de Proteção de Dados está diretamente relacionada a uma transformação cultural da instituição de modo que sejam atingidos todos os níveis, desde o estratégico até o operacional.

Essa mudança cultural envolve: (i) refletir sobre a privacidade dos dados pessoais do cidadão em todas as fases que envolvem o tratamento; e (ii) desenvolver ações de conscientização dos servidores, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Nesse contexto, o diagnóstico da cultura organizacional tem como principal objetivo, identificar o nível de percepção dos servidores em relação à LGPD, orientar a gestão superior e os agentes de tratamento, conforme as suas necessidades específicas, e promover melhoramentos em relação ao tratamento de dados.

É relevante que essa pesquisa seja feita de forma ampla, de modo a atingir um número expressivo de agentes públicos, para que a partir da análise sobre a percepção e o conhecimento dessas pessoas sobre a proteção de dados pessoais, seja possível identificar a necessidade de ampliação da conscientização em relação ao assunto, a referida avaliação poderá ser realizada por meio do questionário sugerido que está inserido no QR CODE, o qual deverá ser encaminhado a todos os servidores e colaboradores da SSP/AM.

5.1.2 DA GOVERNANÇA DE DADOS

Tão importante quanto a conscientização dos servidores em relação à proteção de dados, é a governança desses, realizada mediante a análise do planejamento, gestão e controle do uso dos mesmos.

A avaliação desses aspectos pode ser efetuada por meio de questionário próprio (Anexo I), a ser preenchido pelos gestores, com o objetivo de mensurar quais são as práticas atuais, determinando em qual estágio a SSP/AM se encontra, antes de avançar nas mudanças necessárias para adequação à LGPD, por intermédio de estratégias futuras.

Ressalta-se a importância da realização periódica dessa avaliação, com a finalidade de acompanhar a evolução e a necessidade de eventuais melhorias, fundamentais à governança do tratamento.

5.2 MAPEAMENTO DE DADOS PESSOAIS

Mapeamento de dados pessoais é uma atividade de catalogação de todo o fluxo de dados pessoais, que são objeto das operações de tratamento. Recomenda-se que as informações obtidas sejam mantidas em sistemas eletrônicos, facilitando a tomada de decisões e a manutenção de registros. Esse levantamento pode ser realizado mediante o preenchimento de planilhas, conforme modelo sugerido: **Planilha para Mapeamento de Dados** (ANEXO II).

Em paralelo ao mapeamento, é importante manter o inventário de dados pessoais, que visa entender, de forma detalhada, a variedade dos dados tratados nos órgãos ou entidades públicos e categorizá-los, mensurando os riscos existentes e seus impactos, servindo como base para elaboração de planos de ação mais direcionados e efetivos.

5.3 LEVANTAMENTO DE RISCOS

O levantamento de riscos tem como objetivo mitigá-los, por meio do controle e da redução desses, até que, em algum momento, eles sejam extintos. Trata-se de um procedimento que ajuda a planejar as ações preventivas tomadas por parte da SSP/AM.

Para que essa análise ocorra de forma satisfatória, todos os envolvidos no processo de tratamento de dados devem participar desse levantamento. Considerando que o resultado é utilizado como um indicador que informa o nível dos riscos, a fim de obter um diagnóstico da situação, deve ser periodicamente revisitado e atualizado.

5.4 ELABORAÇÃO DE RELATÓRIO DE IMPACTO DE PROTEÇÃO À DADOS - RIPD

De acordo com o art. 5º, XVII da LGPD, relatório de impacto à proteção de dados pessoais é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

O conteúdo mínimo do RIPD está previsto no parágrafo único, do art. 38 da LGPD, devendo conter a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O Relatório de Impacto de Proteção de Dados (RIPD) deve ser elaborado, tanto na fase inicial do programa que inclui o tratamento de dados, quanto nas operações de tratamento que estão em andamento.

5.5 A ELABORAÇÃO DO RIPD DEVE CONTEMPLAR AS SEGUINTES ETAPAS:

A. Identificar os agentes de tratamento de dados: controlador, operador, encarregado;

B. Reconhecer a necessidade de elaborar o relatório:

• Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
• Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
• A qualquer momento sob determinação da ANPD (art. 38).
• Descrever o tratamento: especificação da natureza, escopo, contexto e finalidade do tratamento que podem gerar riscos às liberdades civis e aos direitos fundamentais.

É importante que o RIPD seja revisto e atualizado anualmente ou quando houver mudança que atinja o tratamento dos dados pessoais realizados SSP/AM.

5.6 POLÍTICA DE PRIVACIDADE DE DADOS

Criar Políticas de Privacidade de Dados e Tratamento de Incidentes é um dos passos mais importantes para adequação à LGPD, que visa atender o princípio da transparência previsto na lei.

A Política de Privacidade de Dados é um documento informativo que descreve ao usuário a forma, os processos e os procedimentos adotados no tratamento dos dados pessoais e as medidas de privacidade empregadas.

Com relação ao conteúdo, recomenda-se que contenham as seguintes informações:

• Informação sobre o órgão ou entidade pelo tratamento;
• Quais os dados pessoais tratados e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, etc.);

- Fundamento legal do tratamento;
- Prazo de retenção dos dados pessoais;
- Informações de contato do encarregado de proteção de dados;
- Como são atendidos os direitos do titular, informando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento. No caso da inviabilidade de alguma operação, é necessário deixar claro o motivo. Entretanto, aconselhase que esses casos sejam avaliados e autorizados pela área jurídica, sendo justificados por algum outro requisito legal.
- Se há o compartilhamento de dados com terceiros e qual a finalidade;
- Se há transferência internacional de dados;
- Proteção de dados de menores de idade, se for o caso;
- Proteção de dados sensíveis.

5.7 ADAPTAÇÃO DE DOCUMENTOS

Esta etapa do processo de implementação se refere a revisão de contratos, termos de cooperação, convênios e outros instrumentos congêneres, físicos ou digitais, a fim de incluir deveres e obrigações às partes contratantes, pertinentes ao direito constitucional à proteção de dados pessoais. Neste contexto, a Procuradoria-Geral do Estado-PGE e a Controladoria Geral do Estado – CGE deverão elaborar minutas padrões para os contratos com Administração Pública, para Implementação do Direito Constitucional à Proteção dos Dados nos contratos firmados com a Administração Pública.

Todos os documentos oficiais as SSP/AM devem atender ao disposto nas normas pertinentes à LGPD. Assim, deve ser feita a revisão de contratos e demais documentos (impressos e digitais) para a realização de uma atualização e padronização.

5.8 TERMO DE COMPROMISSO E CONFIDENCIALIDADE

É um documento aplicável àqueles que tenham acesso a dados pessoais no âmbito da SSP/AM. Tem como escopo efetuar o tratamento de dados pessoais confidencialmente, não podendo ser divulgados a terceiros não autorizados, salvo quando explicitamente forem classificados como públicos, sendo disponíveis, conforme as regras de sigilo.

5.9 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é um documento que tem por objetivo promover o gerenciamento da segurança da informação, estabelecendo regras e padrões de proteção. Busca ainda manter a confidencialidade e o sigilo das informações classificadas como tal, e evitar incidentes de segurança, como vazamentos, perdas, alterações ou acessos indevidos.

Para a criação de uma política adequada é recomendável que sejam observadas as seguintes etapas:
a) Compreenda as necessidades de segurança da informação do órgão ou entidade: a primeira etapa é entender as necessidades de segurança da informação do órgão ou entidade, incluindo os dados e informações sensíveis que precisam ser protegidos.
b) Identifique as ameaças: é essencial identificar as ameaças mais comuns que podem afetar a segurança da informação, como vírus, invasões de hackers e erros humanos.
c) Elabore sua política de segurança da informação: com base nas necessidades de segurança e nas ameaças identificadas, é hora de elaborar sua PSI. A política deve incluir medidas para garantir a confidencialidade, integridade e disponibilidade das informações.
d) Implemente as medidas de segurança: após a elaboração da política, é hora de implementar as medidas de segurança, incluindo a autenticação de usuários, criptografia de dados, controle de acesso a sistemas e dados, backups regulares, verificações de integridade de arquivos, proteção contra vírus, alta disponibilidade, entre outras medidas.
e) Treinamento: é imprescindível que todos os agentes públicos estejam cientes da política de segurança da informação e saibam como aplicá-la.

5.10 PLANO DE RESPOSTA A INCIDENTES E PRIVACIDADE

De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

A LGPD determina que os agentes de tratamento de dados pessoais (Controlador e Operador) devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Diversas ferramentas e técnicas podem ser utilizadas para mitigar os riscos e efeitos de incidentes de segurança, como por exemplo, senhas fortes, anonimização ou pseudonimização dos dados, criptografia, minimização dos dados coletados, atualização constante dos aplicativos, ferramentas técnicas de segurança, dentre outros.

O vazamento de dados pessoais, um dos mais conhecidos incidentes de segurança, ocorre quando dados são indevidamente acessados, coletados e divulgados ou repassados a terceiros. O dano ao titular pode ser das mais diversas naturezas, como fraudes, tentativas de golpes, uso indevido dos dados, venda dos dados, etc.

O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo que descreve a forma como o órgão ou entidade vai responder às situações de emergência e exceção.

Pela potencial gravidade, a resposta deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência. Para o processo funcionar e ser estabelecido é pré-requisito a preparação prévia e contínua, atendendo os seguintes itens:

a) conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
b) preservar a reputação e imagem da SSP/AM;
c) assegurar respostas rápidas, efetivas e coordenadas;
d) quantificar e monitorar desempenho; e
e) evoluir continuamente com as lições aprendidas.

ANEXO I

Participe do **QUESTIONÁRIO DE GOVERNANÇA DA DADOS**

Acesse o QR CODE abaixo e colabore com a pesquisa

ANEXO II

MAPEAMENTO DE DADOS LGPD													
ÁREA	PROCESSO/ ATIVIDADE	FINALIDADE DO TRATAMENTO	AÇÕES DE TRATAMENTO	DADOS PESSOAIS	BASE LEGAL P/ TRATAMENTO DE DADOS PESSOAIS	DADOS PESSOAIS SENSÍVEIS	BASE LEGAL P/ TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS	CATEGORIA DO TITULAR DO DADOS SENSÍVEIS	COMPARTILHAMENTO DE DADOS (Sim ou não)	COM QUEM OS DADOS SÃO COMPARTILHADOS	PERÍODO DE RETENÇÃO DOS DADOS	RISCOS (Incidentes de Segurança)	SUGESTÕES DE MEDIDAS DE MITIGAÇÃO DE RISCOS

ÁREA: Gabinete/Coordenadorias/Grupos/Núcleos

PROCESSO/ATIVIDADE: Atividades desenvolvidas com os dados pessoais
FINALIDADE DO TRATAMENTO: motivo pelo qual os dados são tratados (Ex: formalização de contrato, registro de um novo servidor, etc.)

AÇÕES DE TRATAMENTO (Vide Glossário): Coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

DADOS PESSOAIS: Nome, endereço, CPF, RG, estado civil, dados bancários, vídeos, fotos, dados de gps, endereço de IP etc.

DADOS PESSOAIS SENSÍVEIS: dados de saúde ou vida sexual, origem racial, étinca, convicção religiosa, opinião política, filiação a sindicato, dado genético, dado biométrico

BASE LEGAL PARA O TRATAMENTO DE DADOS: Arts. 7º e 23 da LGPD

BASE LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: Art. 11 e 23 da LGPD

CATEGORIA DO TITULAR DE DADOS: servidor público, usuário do serviço público, criança, adolescente, outros

RISCOS: Acesso Indevido/Perda dos dados Pessoais/Armazenamento Inseguro/Vazamento de Dados.

6. REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: Acesso em: 14 de maio de 2021. GOVERNO FEDERAL. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD).

GOVERNO FEDERAL. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). 10 abr. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd.

GOVERNO FEDERAL. gov.br. Guias operacionais para adequação à LGPD. 11 abr. 2019. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd.

AMAZONAS

GOVERNO DO ESTADO

TRABALHO QUE TRANSFORMA