W7BR Soluções em Tecnologia

contato@w7br.com

# 1 - PLANEJAMENTO DE EXECUÇÃO LGPD
# CÂMARA MUNICIPAL DE ALTO PARAÍSO

Responsável: W7BR Soluções em Tecnologia LTDA – ME

Projeto: W7BR Soluçõe em Tecnologia LTDA - ME
Tecnologia da Informação: W7BR Soluçõe em Tecnologia LTDA - ME
Jurídico: Adv. Contratado

Início : 24.08.2023
Final: 24.11.2023

Roteiro

# Introdução

A Câmara Municipal de Alto Paraíso (CMAP) inicia seu percurso rumo à implementação do Programa de Proteção de Dados Pessoais a partir de um projeto para cumprimento dos requisitos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), iniciado em julho de 2023, com a contratação de empresa certificada em LGPD para adequação de todo o ambiente de sua dependencia.

Como resultado do trabalho dessa como resultado dessa contrataçao, foram definidos conceitos, critérios e metodologias para possibilitar a realização do diagnóstico inicial da gestão de dados pessoais, a análise das lacunas de conformidade e a análise de risco dos processos. Adicionalmente, também foi apresentada proposta de Política para gestão da LGPD no âmbito da CMAP.

Munido de todo esse material, o Encarregado de Dados conseguirá trilhar o caminho rumo a evolução do nível de maturidade da gestão da LGPD na CMAP. A produção de todo esse conhecimento a auxiliará também na tomada de decisão, na execução dos planos de ações e demais ajustes necessários para assegurar a conformidade requerida pela norma.

A seguir, descrever-se-ão os conceitos, critérios e metodologias utilizadas pela contratada para realização do mapeamento de dados, cujo diagnóstico inicial compõe o Relatório de Análise de Dados Pessoais (RADP) e se constitui na ferramenta inicial para o Programa de Proteção de Dados Pessoais da CMAP, com a nomeação e atividade do Encarregado de Dados.

# Fases do Projeto LGPD

Responsável: Contratada

Objetivo: Preparação (avaliação e desenho) das operações e Organização das estruturas e mecanismos para possibilitar a implementação dos requisitos da LGPD na CMAP pelo Operador de Proteção de Dados (DPO) Registros Dados Pessoais (RDP)

Conscientização

- planejamento inicial (Executado);
- mapeamento do tratamento dos dados (Executado);
- análise de adequação (Execução);
- criação do programa de conformidade (Em Processo);
- assessoria para implantação do programa de conformidade e treinamentos (Em Processo);.

# Adequação

Definição de:

- áreas estratégicas para a adequação;
- papéis das equipes (Negócios, Tecnologia e Jurídico) e suas atribuições;
- conceitos e taxonomias;

Metodologia para:

- Governança de proteção de dados pessoais;
- Inventário de dados pessoais;
- Inventário de serviços e processos que tratam dados pessoais;
- Políticas, normas e procedimentos de Proteção de Dados Pessoais;
- Concientização e treinamento em Proteção de Dados Pessoais;
- Gerenciamento de riscos em Segurança da Informação;
- Gerenciamento de riscos em Segurança Cibernética;
- Gerenciamento de riscos de terceiros;
- Melhores práticas de Proteção de Dados Pessoais;
- Gerenciamento de demandas dos titulares;
- Gerenciamento de Incidentes;
- Aspectos Legais vinculados à Proteção de Dados Pessoais.;

## Governanssa de Proteção de Dados

- Revisões e adequações contratuais - jurídico;
- Identificação e proposta de Framework para acompanhamento da maturidade;
- Elaboração de minuta de Política de Proteção de Dados Pessoais;

- Elaboração de material audiovisual para capacitação de servidores e magistrados quanto a conceitos e importância da LGPD para o CMAP;

Proposta de fases para Programa de Proteção de Dados Pessoais e Privacidade.

- Definição dos agentes de tratamento;

Adequação de hotsite com informações sobre LGPD no âmbito do CMAP.

## Fases para Programa de Proteção de Dados Pessoais e Privacidade

- Responsável: Alta Administraião e Encarregado de Proteção de Dados
- Objetivo: Implementar e monitorar as operações necessárias para a implementaião dos requisitos da LGPD na CMAP

## Plano de Ação e Maturidade da Governança de Proteção de Dados

- Estabelecer a partir do RAD o atual nível de maturidade e governança dos processos de proteção de dados da CMAP;
- Estabelecer, com base nos riscos, o plano de ação necessário, com seus respectivos responsáveis e prazos para migrar os riscos e evoluir para o próximo nível de maturidade desejado;
- Definir com base em riscos a necessidade do DPIA;
- Propor a estrutura de governança de dados.

## Regulamentação e Gestão

- Ações de Regulação - propostas para administração :
- Programa de Proteção de Dados e Privacidade
- Políticas de privacidade da CMAP;
- Plano de comunicação, conscientização e treinamento sobre proteção de dados e privacidade.

## Plano de comunicação para questões Proteção de dados e Privacidade

- Orçamento e estrutura necessária para Gestão de Proteção de Dados;

## Controles de segurança para dados pessoais.

- Informações da coleta, finalidade, política de cookies etc.
- Procedimentos para manutenção de avisos de privacidade de dados;

## Ações de Gerenciamento LGPD

- Plano e registros de direito dos titulares de dados, tratamento de solicitações, reclamações e retificações de dados.
- Procedimentos e periodicidade para avaliação de riscos e gerenciamento;
  - Periodicidade de atualização dos relatórios de análise de dados pessoais;
  - Plano de resposta à violação de privacidade e vazamento de dados pessoais;
- Sistema informatizado para gerenciamento de Proteção de Dados e Privacidade.

# Estratégia de anonimização de dados nas fontes

Para o ordenamento de sua relevância para o projeto foram considerados os seguintes parâmetros: sensibilidade, criticidade e abrangência da atividade quanto a utilização e proteção de dados pessoais e privacidade.

Os parâmetros de avaliação variam de 1- muito baixo a 5 muito alto;

Quadro 1- Atividades de Processamento Estratégicas

| Área | Atividade de Processamento | SENSIBILIDADE | CRITICIDADE | ABRANGÊNCIA | ORDEM |
|---|---|---|---|---|---|
| Administrativo | | | | | |
| Presidente Edmilson | Contração - Manutenção | | | | |
| Secretária Geral | Contratação – Administrativo Estratégico | | | | |
| Juridico | Processo, Parecer e Contrato | | | | |
| Juridico | Lesgislativo, Parecer e Lei. | | | | |
| Contabilidade | Processamento altomatizado | | | | |
| Controladoria | Conferencia de Processo | | | | |
| Tesouraria | Pagamento | | | | |
| Recussos Humanos | Cadastro de Servidor, Estagiário | | | | |
| Chefe de Gabinete | Processo Administrativo | | | | |
| Frotas | Locomoção | | | | |
| Amoxarifado | Equipamento | | | | |
| Recepção | Atendimento e Direcionamento | | | | |
| Ouvidoria | Resposta ao Cidadão | | | | |
| Sala Emprendedor | Serviço a População | | | | |
| Acessora Scretária | Insere Dados no Portal Transparencia | | | | |
| Protocolo | Recebe Documeto | | | | |

| Leslativo | | | | | |
|---|---|---|---|---|---|
| Gab. Ver. Claudio | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Eliseu | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Valmir | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Leandro | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Roberto | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Jerdson Lins | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Elissandra | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Romario | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. Paulo Cesar | Ficalização Geral, Aprovar Lei | | | | |
| Gab. Ver. José Oliveira | Ficalização Geral, Aprovar Lei | | | | |

| Administrativo | Terceirizados | SENSIBILIDADE | CRITICIDADE | ABRANGÊNCIA | ORDEM |
|---|---|---|---|---|---|
| Tecnologia da Informáção | Estrutura e manutenção computacional | | | | |
| Contabilidade | SIAFIC | | | | |
| Comunicação | Som e Projeção Gravação sessão | | | | |

# Conceitos e Taxonomias

Para possibilitar um entendimento comum entre as equipes da CMAP, foram definidos conceitos e classificações para utilização na fase de coleta de dados para diagnóstico.

## Dados Pessoais - Categorias

| |
|---|
| Nome |
| Data Nascimento |
| Filiação |
| Dados de Descendentes |
| Sexo |
| Naturalidade |
| Fotografias / imagens em vídeo |
| Nome usuário nas redes sociais |
| Estado Civil |
| Cônjuge |
| Endereço |
| Telefone |
| e mail |
| Profissão |
| RG |
| CPF |
| PIS |
| CNH |
| Carteira ProfissionaL |
| Título de Eleitor |
| Passaporte |
| Matrícula |

| |
|---|
| Local de Trabalho |
| Salário |
| Cargo |
| Data de Posse |
| Dados Bancários |
| Dado acadêmico |
| Registro Profissional |

| |
|---|
| Titular de Dado |
| Servidor |
| Estagiário |
| Familiares de servidor |
| Terceirizados |
| Licitante |

| |
|---|
| Dados Sensíveis |
| 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 |
| Dado penal, criminal ou tributário |
| Origem dos dados |
| Diretamente do titular |
| Outra área de atividade de tratamento |
| Provedor externo |
| Agentes Responsáveis pelo Tratamento |
| Controlador |
| Operador |
| Encarregado de Dados |

## Métodos de Transferências

- E-mail institucional
- E-mail não institucional
- Aplicativos de mensagens
- Aplicação de Integração - API
- Formulário web
- Formulário em papel
- Cópia eletrônica por e-mail
- Transferência de arquivos
- Telefone
- Serviços web
- Não sabe informar

## Transferência para entidades Privadas

- Execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI;
- Se for indicado um encarregado para as operações de tratamento de dados pessoais;
- Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (que deverão ser comunicados à autoridade nacional);
- Para a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados;
- Nos casos em que os dados forem acessíveis publicamente;
- Outros não relacionados.

## Nível de Interesse na Intrusão

- Baixo, dados públicos facilmente acessíveis;
- Médio, dados que podem possibilitar uso para cadastros ou divulgação externa;
- Alto, dados que podem ser usados para fins de manipulação de comportamento, dados de crédito ou dados sensíveis

## Parâmetros de prazo e forma para tratamento

- Prazo indeterminado para guarda de dados pessoais sensíveis;
- Prazo indeterminado para guarda de dados pessoais em geral;
- Falta de consentimento para dados de menores;
- Transferência de dados por aplicativos de mensagem ou e mail não institucionais;
- Utilização de planilhas pessoais para armazenamento e tratamento de dados pessoais sem proteção da organização;
- Documentos físicos armazenados sem proteção ou procedimento específico;
- Bases de dados pessoais sem proteção para manuseio, download, tratamento;
- Transferência de dados pessoais para terceiros sem proteção direta ou regulação;
- Dados passados para atividades analíticas com acesso a outras áreas na organização;
- Consentimento sem condições do artigo 8º e 9º;

Base legal de legítimo interesse não cobre o disposto no artigo 10.

## Base Legal

- Art. 7º, I - mediante fornecimento de consentimento pelo titular;
- Art 7º II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
- Art 7º III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- Art. 7º V -quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Art. 7º VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- Art. 7º VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Art. 7º VIII -para a tutela da saúde exclusivamente, em

procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

- Art 7º IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;
- Art 7º X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;
- Art. 11 I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- Art. 11 II, a - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para a) cumprimento de obrigação legal ou regulatória pelo controlador;
- Art. 11 II, b - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- Art. 11 II, c - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para c) realização de estudos por órgão de pesquisa, garantida, sempre que possível,a anonimização dos dados pessoais sensíveis;
- Art. 11 II, d - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996
- Art. 11 II, e - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- Art. 11 II, f - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
- Art. 11 II, g - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para g) garantia da

prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

## Compartilhamento dos dados

- Outras entidades externas do Poder Público
- Outras entidades externas privadas
- Contratados privados

## Avaliação do nível de segurança de sistemas

- Não há medidas de segurança ou medidas ad hoc
- Medidas reativas ou apenas políticas organizacionais não institucionalizadas
- Medidas reativas, organizacionais ou preventivas institucionalizadas
- Medidas preventivas, reativas e políticas organizacionais institucionalizadas
- Medidas preventivas, reativas e políticas organizacionais institucionalizadas e gerenciadas

## Finalidade do tratamento dos dados

- Art. 4º - II - realizado para fins exclusivamente:
  - jornalístico e artísticos e /ou
  - acadêmicos;
- Art. 4º -III - Realizado para fins exclusivos de:
  - segurança pública;
- Art. 4º -III - Realizado para fins exclusivos de:
  - defesa nacional;
- Art. 4º Estado; -III - Realizado para fins exclusivos de:
  - segurança do nacional;
- Art. 4º -III - Realizado para fins exclusivos de:
  - atividades de investigação e repressão de infrações penais;
- Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à

Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público,

## Coleta de Dados - Formulário

A coleta de dados foi realizada a partir de formulário próprio apresentado na tabela abaixo:

| **1 - Identificação dos serviços** | | | | | |
|---|---|---|---|---|---|
| 1.1 Nome do serviço | | | | | |
| 1.2 Nº do Serviço | | | | | |
| 1.3 D. Criação do Inventário | | | | | |
| 1.4 D. Atual. do Inventário | | | | | |
| | | | | | |
| **2 - Agente de Tratamento e Ecaregado** | | | | | |
| | Nome | Endereço | CEP | Telefone | E-mail |
| 2.1 Controlador | | | | | |
| 2.2 Encarregado | | | | | |
| 2.3 Operador | | | | | |
| | | | | | |
| **3 - Fases Cliclo V. do Trat. Dados** | | | | | |
| | Coleta | Retenção | Proc. | Compart. | Elimina |
| 3.1 Fase Atuação Operador | | | | | |
| | | | | | |
| **4 - Como os dados são coletados, retidos/amaz., proc./usados, comp** | | | | | |
| 4.1 Descrição do Fluxo de Tratamento dados pessoais | | | | | |

Risco Inerente - é o risco ao qual uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco Residual - é o risco ao qual uma organização está exposta após considerar as ações de mitigação aplicadas para reduzir a probabilidade de sua ocorrência ou seu impacto, ou ambos.

- Apetite a Risco - o nível de risco que a organização está disposta a aceitar enquanto persegue seus objetivos;

- Respostas a Riscos - envolve a escolha de opções de ações para gestão do risco identificado.
  - Pode ser categorizada em: aceitar, mitigar, compartilhar ou evitar.

- Matriz de Riscos - ferramenta de gerenciamento de riscos que permite identificar de forma visual os riscos a que a organização está sujeita.

Parâmetros escalares para avaliação de riscos:

| | |
|---|---|
| 1 | Muito Baixo |
| 2 | Baixo |
| 3 | Médio |
| 4 | Alto |
| 5 | Extremo |

| | Matriz de Portfólio de Risco | | | | |
|---|---|---|---|---|---|
| Extremo | | | | | |
| Alto | | | | | |
| Médio | | | | | |
| Baixo | | | | | |
| Muito Baixo | | | | | |
| | Muito Baixo | Baixo | Médio | Alto | Extremo |

Para mensuração dos conceitos para identificação e análise dos riscos os seguintes atributos foram utilizados:

Objetivo processo de Proteção à Privacidade:

- tratar dados pessoais assegurando a proteção à privacidade do titular, analisando o manuseio destas informações a partir da

ocorrência dos seguintes eventos: mau uso do dado por membro interno, vazamento, captura ou intrusão de sistemas de armazenamento por membro externo.

Probabilidade - é a chance atribuída a ocorrência de evento que possam impactar na proteção à privacidade dos titulares de dados pessoais. Base - Artigo 50 § 2º:

- Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados ……

A mensuração da probabilidade de ocorrência destes eventos foi realizada tendo como parâmetro central o índice de volumetria ajustado pela escala supracitada (mau uso, vazamento, intrusão) operada pelo processo em exame. O cálculo da volumetria considerou como parâmetros para estabelecimento do valor da probabilidade:

- Período de apuração do volume de dados pessoais tratados pelo processo12 meses.

Índice de volumetria ajustada considera em um índice agregado os seguintes fatores: quantidade de titulares de dados x perfis de servidores com acesso aos dados, ponderados pela quantidade de manipulação mensal padrão destes dados (mau uso e vazamento) e pelo nível de interesse de intrusão para captura destes dados (intrusão).

1- Baixo, dados públicos facilmente acessíveis;
2- Médio dados que podem possibilitar uso para cadastros ou divulgação externa;
3- Alto, dados que podem ser usados para fins de manipulação de comportamento,crédito ou sensíveis;

Faixas: mínima = 0; máxima >=ao máximo de dados

| Índice de volumetria ajustado- Faixas | Classificação | Rótulo |
|---|---|---|
| 0-900.000 | 1 | Muito Baixo |
| 900.001 - 1.800.000 | 2 | Baixo |
| 1.800.001 - 2.700.000,00 | 3 | Médio |
| 2.700.001 - 3.599.999 | 4 | Alto |
| >= 3.600.000 | 5 | Extremo |

Impacto é o resultado de um evento que impacta o atingimento do objetivo do processo em exame. O impacto foi estimado a partir da base legal para coleta do dado pessoal.
Base - Artigo 50 § 2º:

- Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados …...

## Tabela de classificação de impacto:

| Impacto na organização Fator base Legal LGPD | Classificação | Rótulo |
|---|---|---|
| Art. 7º, I - mediante fornecimento de consentimento pelo titular | 3 | Médio |
| Art 7º II - para o cumprimento de obrigação legal ou regulatória pelo controlador | 2 | Baixo |
| Art 7º III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; | 1 | Muito Baixo |
| Art. 7º V -quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; | 2 | Baixo |
| Art. 7º VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; | 2 | Baixo |
| Art. 7º VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; | 2 | Baixo |

| | | |
|---|---|---|
| Art 7º IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais | 4 | Alto |
| Art 7º X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. | 1 | Muito Baixo |
| Art. 11 I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; | 5 | Extremo |
| Art. 11 II, a - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para a) cumprimento de obrigação legal ou regulatória pelo controlador; | 3 | Médio |
| Art. 11 II, b - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; | 3 | Médio |
| Art. 11 II, c - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; | 5 | Extremo |
| Art. 7º VIII -para a tutela da saude exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; | 2 | Baixo |

| | | |
|---|---|---|
| Art. 11 II, d - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável parad) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 | 2 | Baixo |
| Art. 11 II, e - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para e) proteção da vida ou da incolumidade física do titular ou de terceiro; | 2 | Baixo |
| Art. 11 II, f - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência | 4 | Médio |
| Art. 11 II, g - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. | 4 | Médio |
| Não se aplica | 1 | Muito Baixo |

# Tabela de Correlação - Probabilidade x Impacto para Risco Inerente

| Probabilidade | Impacto | Classificação Risco Inerente |
|---|---|---|
| 1 | 1 | Muito Baixo |
| 2 | 1 | Muito Baixo |
| 3 | 1 | Baixo |
| 4 | 1 | Médio |
| 5 | 1 | Alto |
| 1 | 2 | Muito Baixo |
| 2 | 2 | Baixo |
| 3 | 2 | Médio |
| 4 | 2 | Alto |
| 5 | 2 | Extremo |
| 1 | 3 | baixo |
| 2 | 3 | Médio |
| 3 | 3 | Alto |
| 4 | 3 | Alto |
| 5 | 3 | Extremo |
| 1 | 4 | Médio |
| 2 | 4 | Muito Baixo |
| 3 | 4 | Muito Baixo |
| 4 | 4 | Extremo |
| 5 | 4 | Extremo |
| 1 | 5 | Médio |
| 2 | 5 | Alto |
| 3 | 5 | extremo |
| 4 | 5 | extremo |
| 5 | 5 | extremo |

Categorização da atividade de controle identificado para mitigar o risco inerente de vazamento, mau uso e intrusão - Níveis de segurança de ativos e sistemas

| | | |
|---|---|---|
| Não há medidas de segurança ou medidas ad hoc | 1 | Muito Baixo |
| Medidas reativas ou apenas políticas organizacionais não institucionalizadas | 2 | Baixo |
| Medidas reativas, organizacionais ou preventivas institucionalizadas | 3 | Médio |
| Medidas preventivas, reativas e políticas organizacionais institucionalizadas | 4 | Alto |
| Medidas preventivas, reativas e políticas organizacionais institucionalizadas e gerenciadas | 5 | Extremo |

Para mensuração das lacunas de procedimentos, governança e obrigações legais que possam impactar a ocorrência dos eventos de risco ( mau uso, vazamento e intrusão) os seguintes atributos foram utilizados:

## Tabela de Classificação de Criticidade – Lacunas de Procedimentos e Governança

| Quantidade de Lacunas | Classificação de Risco |
|---|---|
| 0-1 | Muito Baixo |
| 2-3 | Baixo |
| 4-5 | Médio |
| 6-7 | Alto |
| 8 | Extremo |

## Tabela de Classificação de Criticidade Lacunas de Obrigações Legais LGPD

| Quantidade de Lacunas | Classificação de Risco |
|---|---|
| 0-2 | Muito Baixo |
| 3-5 | Baixo |
| 6-8 | Médio |
| 9-10 | Alto |
| | |
| 11-12 | Extremo |

# Check list

1. Qual o porte da sua empresa?
2. Quantos funcionários sua empresa possui?
3. Qual o seu principal tipo de cliente?
4. Qual a unidade federativa da sede da sua empresa?
5. Qual o setor da sua empresa?
6. A empresa realiza o tratamento de dados pessoais?
7. A empresa realiza o tratamento de dados pessoais sensíveis?
8. O tratamento de dados pessoais é realizado com base na boa-fé e os princípios da LGPD (i.e., finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas)?
9. O tratamento de dados pessoais realizado pela empresa inclui automatização de qualquer tomada de decisão (RPA), criação de perfis com base nos dados pessoais transferidos (profiling) ou utilização analítica (analytics)?
10. O tratamento de dados pessoais realizado pela empresa é fundamentado nas bases legais estipuladas na LGPD?
11. O tratamento de dados pessoais de acesso público é baseado na finalidade, boa-fé e o interesse público que justificaram sua disponibilização?
12. O consentimento para tratamento de dados pessoais é obtido por escrito ou por outro meio que demonstre a manifestação de vontade do titular de dados?
13. Ao obter o consentimento do titular de dados pessoais a empresa deixa de forma clara, precisa e objetiva as finalidades para as quais os dados serão tratados?

**14.** A empresa garante ao titular de dados pessoais o direito de retirar o consentimento para tratamento de dados a qualquer momento (opt-out)?

**15.** O acesso a dados pessoais está restrito somente a funcionários autorizados?

**16.** A empresa possui um Portal de Privacidade para os titulares de dados pessoais nos quais as informações sobre o tratamento de seus dados são disponibilizadas de forma clara, adequada e ostensiva?

**17.** Caso haja alteração na finalidade do tratamento de dado pessoal, a empresa possui um procedimento para informar os titulares dos dados pessoais acerca dessa mudança?

**18.** A empresa realiza o tratamento de dados pessoais sensíveis de acordo com as bases legais específicas previstas na LGPD?

**19.** Os dados pessoais sensíveis tratados pela empresa são compartilhados com terceiros?

**20.** A empresa obtém o consentimento específico e destacado de um dos pais ou responsável legal para tratar dados pessoais de crianças?

**21.** A empresa condiciona a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de dados pessoais?

**22.** A empresa possui uma política periódica para eliminação de dados pessoais?

**23.** Os dados pessoais são tratados por período indeterminado?

**24.** A empresa possui um procedimento para eliminação de dados pessoais?

**25.** A empresa possui um procedimento para atender solicitações para eliminar dados pessoais de seus sistemas, se necessário?

**26.** A empresa anonimiza os dados pessoais que permanecem em seus sistemas após o término do tratamento?

**27.** A empresa possui um procedimento para atender às solicitações de acesso aos dados pessoais realizadas por titulares?

**28.** A empresa possui registros de todos os dados pessoais por ela tratados e seus respectivos titulares?

**29.** A empresa possui procedimento para disponibilização e acesso dos dados pessoais de seus titulares caso venham a ser solicitados em até 15 dias após o requerimento?

**30.** Os dados pessoais tratados são acessados por terceiros?

**31.** A empresa possui a capacidade de indicar para os titulares de dados pessoais em quais processos existe tomada de decisão gerada pelo tratamento automatizado de dados pessoais?

**32.** A empresa realiza transferência internacional de dados pessoais?

**33.** A empresa realiza transferência internacional de dados pessoais de acordo com as bases legais da LGPD?

**34.** Os países para os quais a empresa realiza transferência internacional de dados possuem grau de proteção de dados adequado?

**35.** A empresa possui Record of Processing Activities (Registro das Operações de Tratamento de Dados Pessoais), conforme exigido pelo art. 30 da GDPR e 37 da LGPD?

**36.** Em caso de atividades de tratamento de dados pessoais que resultem em um alto risco para os titulares de dados, você realiza um Relatório de Impacto à Proteção de Dados Pessoais?

**37.** A empresa nomeou um Encarregado (Data Protection Officer - DPO)?

**38.** A empresa limita o tratamento de dados pessoais ao tratamento necessário para os fins específicos que justificam a sua coleta?

**39.** A empresa possui políticas, procedimentos, e medidas protetivas (e.g., controles de acesso, criptografia, modificação de dados, mascaramento de dados) que asseguram a segurança e garantia de conformidade com os regulamentos/leis de privacidade?

**40.** A empresa possui uma política/procedimento de back-up em relação aos dados pessoais?

**41.** A empresa contratou algum serviço de assessoria para implementação da LGPD?

**42.** A empresa possui estratégia e roadmap de implementação para estar em conformidade com as novas regulamentações?

**43.** A empresa possui um programa de governança em privacidade?

**44.** Os dados pessoais são armazenados em um local e ambiente seguros?

**45.** Existe um processo para atualizar políticas, procedimentos, diretrizes de gerenciamento de riscos, procedimentos de violação, etc. para refletir as atualizações / mudanças das expectativas regulatórias ou mudanças internas no programa de privacidade?

**46.** A empresa conduz avaliações de vulnerabilidade e testes de penetração em seus sistemas de tratamento de dados pessoais?

**47.** A empresa é certificada em algum padrão ou framework de segurança?

**48.** A empresa promove treinamentos obrigatórios para os funcionários, conscientizando-os sobre a importância e sobre suas responsabilidades em relação à privacidade e proteção de dados pessoais?

**49.** Existe um processo formal para revisar e atualizar o treinamento periodicamente?

**50.** A empresa oferece orientação aos funcionários de terceiros a respeito das práticas a serem tomadas em relação à proteção de dados pessoais?

**51.** A empresa exige que seus funcionários e prestadores de serviços assinem acordos de confidencialidade e segurança de dados?

**52.** A empresa instrui seus funcionários e contratados a limitar o armazenamento de dados pessoais do cliente em dispositivos de armazenamento móvel ao mínimo exigido para fins comerciais?

**53.** A empresa possui uma política de revisão regular das permissões de acesso aos dados pessoais que garanta o acesso somente aos funcionários e contratados que precisam ter acesso, bem como um procedimento para prevenir prontamente funcionários e contratados desligados de acesso a dados pessoais?

**54.** A empresa possui um processo apropriado para notificar os titulares de dados pessoais sobre uma violação de dados, quando aplicável?

**55.** A empresa é capaz de detectar rapidamente incidentes de segurança (e.g., incluindo acesso não autorizado, destruição, perda, alteração e violações de dados)?

**56.** A empresa possui um procedimento para agir, prontamente, em caso de incidentes de segurança, incluindo notificação aos titulares de dados pessoais afetados?

**57.** A empresa pode fornecer uma lista de todas as notificações de privacidade de dados que possui?

**58.** Sua empresa já passou por algum incidente de violações de segurança da informação nos últimos dois (2) anos?

**59.** Sua empresa está atualmente sujeita a quaisquer ações de execução, investigações ou litígios relacionados à privacidade ou à segurança da informação?

**60.** Os contratos com terceiros da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados, em vigor?

**61.** Os contratos de trabalho da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados, em vigor?

**62.** A empresa possui cláusulas contratuais de privacidade e proteção de dados em seus contratos em casos de transferência internacional de dados pessoais?

**63.** A empresa possui uma metodologia de auditoria prévia de privacidade e proteção de dados para fins de negociação com terceiros?

**64.** A empresa possui políticas de privacidade (interna e externa) e boas práticas com relação a proteção de dados pessoais alinhadas com as regras da LGPD?

**65.** A empresa possui algum tipo de metodologia para fins de acompanhamento das alterações jurídicas, legais e de jurisprudência relacionadas à LGPD e proteção de dados pessoais no Brasil?

Alto Paraíso, 31 de agosto de 2023.

_____

W7BR Soluções em Tecnologia LTDA - ME

Rua Bom Sucesso, n º 1811 Jardim Monte Alegre