

LEI GERAL DE PROTEÇÃO DE DADOS

LGPD



**GOVERNO
DO ESTADO**
Mato Grosso do Sul

Guia de Boas Práticas para
implementação e adequação à
LGPD na Administração Pública Estadual

Sumário

INTRODUÇÃO

.....	05
-------	----

1 DIREITOS FUNDAMENTAIS DO TITULAR DOS DADOS 07

1.1 Base Legal para Tratamento dos Dados Pessoais	07
---	----

1.2 Direitos do Titular	12
-------------------------------	----

1.3 Exercício dos Direitos dos Titulares perante a Administração	15
--	----

1.3.1 Meios de acesso à informação em transparência passiva	15
---	----

1.3.2 Meios de petição e manifestação à administração pública	16
---	----

1.4 Tipos de dados pessoais	17
-----------------------------------	----

2 O TRATAMENTO DOS DADOS PESSOAIS 18

2.1 Hipóteses de Tratamento de dados pessoais.....	18
--	----

2.1.1 Identificação das hipóteses de tratamento	19
---	----

2.1.2 Conformidade do tratamento de dados quanto aos princípios da LGPD.....	24
--	----

2.1.3 Tratamento de dados de crianças e adolescentes	25
--	----

2.2 Coleta	25
------------------	----

2.3 Anonimização e Pseudonimização	25
--	----

2.4 Publicidade	26
-----------------------	----

2.5 Relatório de Impacto à Proteção de Dados Pessoais	27
---	----

2.5.1 Definição do Relatório de impacto à proteção de dados pessoais	27
--	----

2.5.2 Como elaborar	27
---------------------------	----

2.5.2.1 Identificar os Agentes de Tratamento e o Encarregado	27
--	----

2.5.2.2 Identificar a necessidade de elaborar o Relatório	28
---	----

2.5.2.3 Descrever o tratamento	28
--------------------------------------	----

2.5.2.3.1 Natureza do tratamento	29
--	----

2.5.2.3.2 Escopo do tratamento	29
2.5.2.3.3 Contexto do tratamento	29
2.5.2.3.4 Finalidade do tratamento.....	29
2.5.2.4 Identificar partes interessadas consultadas	30
2.5.2.5 Descrever necessidade e proporcionalidade	30
2.5.2.6 Identificar e avaliar os riscos	31
2.5.2.7 Identificar medidas para tratar os riscos	32
2.5.2.8 Aprovar o Relatório	32
2.5.2.9 Manter Revisão	32
2.6 Término do Tratamento	32
3 O CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS	34
3.1 Fases do Ciclo de Vida	35
3.2 Ativos Organizacionais	37
3.3 Relacionamento do Ciclo de Vida com Ativos Organizacionais.....	38
3.4 Plano de Ação dos Trabalhos de Adequação da LGPD.....	40
4 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO	42
4.1 Privacidade desde a concepção e por padrão (Privacy by Design e by Default).....	42
4.1.1 Privacidade desde a concepção	42
4.1.1.1 Proativo, e não reativo; preventivo, e não corretivo	42
4.1.1.2 Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio	43
4.1.1.3 Privacidade incorporada ao projeto (design)	43
4.1.1.4 Funcionalidade total	43
4.1.1.5 Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados.....	43
4.1.1.6 Visibilidade e Transparência	44

4.1.1.7 Respeito pela privacidade do usuário	45
4.1.2 Privacidade desde a concepção	45
4.2 Padrões, Frameworks e Controles de Segurança da Informação	46
4.2.1 ABNT NBR ISO/IEC 27001:2013. Sistemas de gestão da segurança da informação.....	46
4.2.2 ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de segurança da informação.....	46
4.2.3 ABNT NBR ISO/IEC 27005:2019. Gestão de riscos de segurança da informação.....	47
4.2.4 ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes	47
4.2.5 ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.....	47
4.2.6 Resoluções do CONARQ.....	47
4.2.6.1 Resolução Nº 25, de 27 de abril de 2007.....	48
4.2.6.2 Resolução Nº 39, de 29 de abril de 2014.....	48
ANEXO I	49

INTRODUÇÃO

A publicação da Lei Federal nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados ou simplesmente LGPD, instituiu um novo marco legal de grande impacto, visto que integrou o Brasil ao grupo de países que possuem legislação específica para proteção de dados pessoais.

Ocorre que, com o advento da legislação da União Europeia, a chamada *General Data Protection Regulation* (GDPR), vigente a partir de 25 de maio de 2018, as empresas europeias ficaram impedidas de contratar em países que não procediam ao tratamento dos dados pessoais de forma adequada, o que afetou diretamente o Brasil e, certamente, contribuiu para acelerar a regulamentação da lei no país.

A LGPD disciplina, de maneira pormenorizada, a proteção de dados pessoais em qualquer tipo de relação que abranja o tratamento de informações classificadas como “dados pessoais”, seja por pessoa natural, seja por pessoa jurídica de direito público ou privado. O Estado, para o exercício de suas múltiplas atribuições constitucionais, possui acesso a inúmeros bancos de dados dos cidadãos, uma vez que cada órgão público é custodiante de informações pessoais e sensíveis, tais como número do RG, CPF, endereços, veículos, sociedades empresariais, dados da área da saúde, dados fiscais, para citar apenas alguns.

A essência da LGPD, conforme explicitado em seu artigo 1º, objetiva proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. As informações relacionadas à pessoa são ínsitas aos “direitos da personalidade”, que são direitos fundamentais, expressos e implícitos no art. 5º da Constituição Federal, além de se constituírem em cláusula pétrea da Carta Magna brasileira.

As normas contidas na lei federal devem ser observadas pela União, Estados, Distrito Federal e Municípios, sendo que, neste sentido, o Governo do Estado de Mato Grosso do Sul editou o Decreto nº 15.572, de 28 de dezembro de 2020, atualizado pelo Decreto nº 15.646, de 06 de abril de 2021.

No cumprimento do parágrafo único do art. 5º do Decreto supramencionado, o Presidente do Conselho de Governança publicou a Deliberação “P” nº 1, de 24 de fevereiro de 2021, constituindo o Comitê Encarregado de Editar Diretrizes do Plano de Adequação, composto por representantes da Controladoria-Geral do Estado, Procuradoria-Geral do Estado, Secretaria de Estado de Administração e Desburocratização e Superintendência de Gestão da Informação, cujas diretrizes serão seguidas pelos órgãos do Poder Executivo Estadual, observando-se as deliberações do Comitê Estratégico de Tecnologia da Informação. Oportunamente, houve substituição de representante da Superintendência de Gestão da Informação, por intermédio da Deliberação “P” Conselho de Governança nº 3, de 18 de março de 2021.

Nesse contexto, o Plano de Adequação preconizado pelo art. 2º do Decreto Estadual deve englobar regras de boas práticas e de governança de dados pessoais, visando à implantação da LGPD pelos órgãos da Administração Direta, autarquias e fundações do Poder Executivo Estadual, razão pela qual foram adotados os parâmetros indicados no “**Guia de Boas Práticas para implementação na Administração Pública Federal**”, elaborado pelo Governo Federal, por já ser um produto fruto de estudo aprofundado junto àquela esfera de governo e perfeitamente aplicável ao Estado de Mato Grosso do Sul, com as adaptações cabíveis.

As orientações relativas ao tratamento dos dados pessoais pela Administração Pública foram estruturadas em quatro capítulos:

- ✓ Capítulo 1 – apresenta os direitos do titular dos dados, com respectiva base legal de tratamento e exercício dos direitos dos titulares perante a Administração;
- ✓ Capítulo 2 – demonstra como realizar o tratamento dos dados pessoais e sugestão de modelo de elaboração do Relatório de Impacto à Proteção de Dados Pessoais;
- ✓ Capítulo 3 – detalha o ciclo de vida de tratamento dos dados pessoais;
- ✓ Capítulo 4 – menciona padrões e frameworks de segurança da informação

A LGPD dedicou um capítulo para a Administração Pública, estabelecendo a necessidade de demonstração da finalidade pública no tratamento dos dados pessoais, concretizada no interesse público.

Cabe, ainda, àquela, conferir publicidade às hipóteses de tratamento/compartilhamento, divulgando informações claras e atualizadas em veículo de fácil acesso, preferencialmente nos respectivos sítios eletrônicos, alusivas à previsão legal, procedimentos e práticas utilizadas na execução das atividades, além de publicar os dados do agente público encarregado pela operação de tratamento.

Para fins de compartilhamento de dados com o propósito de execução de políticas públicas, prestação de serviços públicos, descentralização de atividades e disseminação e acesso de informação à população brasileira, a LGPD determina que a Administração Pública mantenha as informações da pessoa natural em formato interoperável e estruturado.

O presente documento tem por objeto indicar as diretrizes que possibilitarão a cada Unidade Gestora a elaboração do Plano de Adequação à Lei Geral de Proteção de Dados Pessoais. Neste momento, não se tem a pretensão de esgotar todos os tópicos abordados pela LGPD, mesmo porque apenas recentemente a Autoridade Nacional de Proteção de Dados publicou sua Agenda Regulatória para o biênio 2021/2022, estabelecendo de que forma serão regulados e qual o prazo previsto para o início da regulamentação de 10 temas prioritários.

Todavia, a época é oportuna para estimular o acultramento do corpo funcional, com vistas à capacitação dos servidores, de forma que o tratamento dos dados pessoais espelhe a proteção dos direitos relacionados à liberdade, intimidade, personalidade, dignidade e privacidade dos cidadãos.

Comitê para implementação de Diretrizes e Plano de Adequação sobre a Lei Geral de Proteção de Dados Pessoais – LGPD, no âmbito do Governo do Estado de Mato Grosso do Sul

- **Controladoria-Geral do Estado**
- **Procuradoria-Geral do Estado**
- **Secretaria de Estado de Administração e Desburocratização**
- **Superintendência de Gestão da Informação**



DIREITOS FUNDAMENTAIS DO TITULAR DOS DADOS

1.1 BASE LEGAL PARA TRATAMENTO DOS DADOS PESSOAIS

A **Lei Geral de Proteção de Dados Pessoais** (LGPD – Lei nº 13.709, de 14 de agosto de 2018) foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo e versa sobre o tratamento de dados pessoais das pessoas naturais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

No âmbito do Poder Executivo Estadual, o Decreto nº 15.572, de 28 de dezembro de 2020, dispõe sobre a adoção de medidas destinadas à aplicação da LGPD, estabelecendo diretrizes, competências, procedimentos e providências correlatas a serem observadas pelos órgãos da Administração Direta, pelas autarquias e pelas fundações, visando garantir a proteção de dados pessoais.

Consoante definição dos incisos VI, VII e VIII do art. 5º da LGPD, na esfera do Decreto Estadual o tratamento dos dados pessoais pode ser realizado por dois “agentes de tratamento”, o Controlador e o Operador:

- O **Controlador** é definido pelo Decreto como pessoa jurídica do órgão da Administração Direta, da autarquia ou da fundação estadual sujeita à LGPD, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de dados. (OBS.: importante destacar que a lei federal define o controlador como pessoa “natural” ou “jurídica”, ao passo que a norma estadual optou por qualificar apenas a pessoa “jurídica”).

- O **Operador**, nos termos do citado Decreto, é o(s) agente(s) público(s), no sentido amplo, que exerça(m) o tratamento de dados, bem como pessoa(s) jurídica(s) diversa(s) daquela representada pelo Controlador, que exerça(m) atividade de tratamento no âmbito de contrato ou de instrumento congênere.

Além dos “agentes de tratamento”, outra figura essencial para o adequado cumprimento da LGPD é o “**Encarregado**”, definido pelo art. 5º, VIII, da LGPD, reiterado pelo art. 3º, III, do Decreto Estadual, como o(s) agente(s) público(s), formalmente designado(s), para o desempenho da comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), bem como das demais funções previstas no art. 41 da LGPD. A designação se dá pelo Controlador.

Outro conceito fundamental estabelecido na LGPD é o de “**tratamento de dados**”, que abrange qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

As operações de tratamento são destacadas a seguir:

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;

ARQUIVAMENTO - ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;

CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;

COLETA - recolhimento de dados com finalidade específica;

COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;

- CONTROLE** - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- DIFUSÃO** - ato ou efeito de divulgação, propagação, multiplicação dos dados;
- DISTRIBUIÇÃO** - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- ELIMINAÇÃO** - ato ou efeito de excluir ou destruir dado do repositório;
- EXTRAÇÃO** - ato de copiar ou retirar dados do repositório em que se encontrava;
- MODIFICAÇÃO** - ato ou efeito de alteração do dado;
- PROCESSAMENTO** - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
- PRODUÇÃO** - criação de bens e de serviços a partir do tratamento de dados;
- RECEPÇÃO** - ato de receber os dados ao final da transmissão;
- REPRODUÇÃO** - cópia de dado preexistente obtido por meio de qualquer processo;
- TRANSFERÊNCIA** - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- TRANSMISSÃO** - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;
- UTILIZAÇÃO** - ato ou efeito do aproveitamento dos dados.

Em razão de taxativa previsão (Art. 4º) da LGPD, a lei não se aplica ao tratamento de dados pessoais nas seguintes situações:

- I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- II - realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);
- III- realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou;
- IV- provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Os casos de tratamento de dados que estão previstos e permitidos pela LGPD serão explicados a seguir. Mas é muito importante destacar que eles não são amplos e absolutos; ao contrário, existem limites para essa operação que estão dados pela boa-fé e demais princípios previstos no Art. 6º da mesma norma.

Antes de iniciar alguma espécie de tratamento de dados pessoais, o agente deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Tais políticas públicas, vale destacar, devem estar inseridas nas atribuições legais do órgão ou da entidade da administração pública que efetuar o referido tratamento. Outra finalidade corriqueira para o tratamento de dados no serviço público é o cumprimento de obrigação legal ou regulatória pelo controlador. Nessas duas situações, o consentimento do titular de dados é dispensado.

Além disso, no tratamento feito pelo poder público, as regras previstas nos artigos 23 (procedimentos de atuação) e 30 (regulamentos da ANPD) da LGPD sempre devem ser seguidas de forma complementar.

Em seu artigo 7º, a LGPD previu expressamente dez hipóteses que autorizam o tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais.

Nos casos de tratamento de dados em que a base legal não é o consentimento, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados, garantindo-lhes o exercício aos direitos previstos no art. 18 da LGPD, com destaque aos direitos de acesso, retificação, oposição, eliminação e informação das entidades públicas e privadas com as quais o controlador irá realizar o uso compartilhado de dados .

A comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência. Além disso, é necessário que a cada tratamento de dados seja feita uma análise de se os princípios da necessidade e adequação também estão sendo cumpridos pelo controlador.

Nos casos de tratamento de dados feitos com base no consentimento, cada nova operação realizada com os dados pessoais deve ser objeto de nova requisição de consentimento, inclusive para o compartilhamento dos dados com outras entidades, de dentro ou fora da administração pública.

O compartilhamento dentro da administração pública no âmbito da execução de políticas públicas é previsto na lei e dispensa o consentimento específico. Contudo, o órgão que coleta deve informar claramente que o dado será compartilhado e com quem. Do outro lado, o órgão que solicita acesso a dado colhido por outro, isto é, solicita receber o compartilhamento, precisa justificar esse acesso com base na execução de uma política pública específica e claramente determinada, descrevendo o motivo da solicitação de acesso e o uso que será feito com os dados. Informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas.

São hipóteses legais previstas na LGPD de tratamento de dados pessoais:

I - Mediante o fornecimento de consentimento pelo titular

Hipótese que exige consentimento do titular do dado. Trata-se da regra da autonomia da vontade. É a manifestação livre e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. É a regra da lei.

O ônus da prova do consentimento cabe ao controlador, sendo proibido o tratamento de dados pessoais mediante vício de consentimento.

O titular dos dados tem liberdade para autorizar, negar ou revogar (reconsiderar) autorização anteriormente concedida para tratamento de seus dados pessoais.

O consentimento autoriza tão somente o agente que o obteve, não se estendendo a outras pessoas. Daí que o controlador, quando compartilhar os dados pessoais obtidos com outros controladores, deve obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa de consentimento previstas em lei.

Frise-se que a obtenção de consentimento específico do titular não é exigida da Administração Pública, quando ela efetuar o tratamento de dados com base nos incisos II, III, IV, VI, VII, VIII, IX e X do art 7º da LGPD ou mesmo quando compartilhar os dados pessoais obtidos com outros órgãos ou entidades públicas para atender as exigências de determinada política pública ou para cumprir atribuição legal do órgão ou entidade.

Por outro lado, a dispensa do consentimento não desobriga a Administração das demais obrigações previstas na LGPD, especialmente da observância dos princípios gerais de proteção e da garantia dos direitos do titular.

II - Para o cumprimento de obrigação legal ou regulatória pelo controlador

Hipótese que dispensa o consentimento do titular do dado. É a regra da legalidade ampla e da preservação do interesse público sobre o particular.

Esse é um autorizador da LGPD que possibilita que a lei não entre em conflito com outras legislações ou regulamentos vigentes. Há previsões normativas que autorizam tratamento de dados extra LGPD; entre elas, a Lei de Acesso à Informação (Lei nº 12.527/2011 - LAI), a do processo administrativo na administração pública federal (Lei nº 9.784/1999) e o Marco Civil da Internet (Lei nº 12.965/2014).

Um exemplo típico de aplicação dessa hipótese é o cumprimento pelo Poder Público de requisições oriundas dos órgãos de controle, solicitando a ficha funcional de determinado servidor público para fins de investigação de eventual irregularidade administrativa. A Administração não precisará do consentimento do servidor titular para realizar o tratamento e o compartilhamento de seus dados, pois estará cumprindo obrigação legal.

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 da Lei

É o tratamento de dados feito com a finalidade específica da execução de política pública formalmente instituída por Lei ou Ato administrativo. O instrumento que fixa a política pública que autoriza o tratamento do dado pessoal pode ser desde uma norma formal (ex.: lei ou decreto) até um contrato ou instrumento congêneres. É importante ressaltar que este tipo de tratamento independe de consentimento do titular e deve respeitar as regras previstas pelos artigos 23 a 30 da LGPD.

Sempre que a administração pública efetuar o tratamento de dados pessoais no exercício de suas competências legais vinculadas a políticas públicas e entrega de serviços públicos, não precisará colher o consentimento; mas, necessariamente, será obrigada a informar a finalidade e a forma como o dado será tratado.

Todas as regras descritas pelos Artigos 23 a 30 da LGPD devem ser observadas pelos órgãos e entidades públicas. As ações destacadas a seguir são de especial importância para viabilizar o tratamento dos dados pelo poder público:

- informar as hipóteses em que, no exercício de suas competências, o órgão respalda o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (Art. 23, I);
- indicar encarregado quando realizar operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD (Art. 23, II);
- observar as formas de publicidade das operações de tratamento que poderão ser estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD, Art. 23, § 1º);
- manter os dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. (Art. 25); e
- realizar o uso compartilhado de dados pessoais de acordo com as finalidades específicas de execução de políticas públicas e atribuição legal do órgão ou entidade, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD (Art. 26).

IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais

Hipótese que dispensa o consentimento do titular do dado. Utilização estrita para realização de estudos por órgão de pesquisa público ou privado.

Observações:

- a) a divulgação dos resultados ou excertos do estudo ou pesquisa não poderá revelar dados pessoais;

b) o órgão de pesquisa será responsável pela segurança da informação e não poderá transferir os dados obtidos a terceiros;

c) na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas; e

d) o acesso a dados pessoais pelos órgãos de pesquisa para fins de realização de estudos em saúde pública será objeto de regulamentação pela ANPD (Autoridade Nacional de Proteção de Dados) e das autoridades da área de saúde e sanitárias no âmbito de suas competências

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

Hipótese que dispensa novo consentimento do titular, desde que: (a) o tratamento de dados em questão seja imprescindível para o devido cumprimento do contrato; e (b) o titular dos dados tenha previamente manifestado consentimento, na celebração do contrato.

São exemplos de tratamento sem previsão expressa: enviar comunicado ou notificação; processar pagamentos.

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)

Hipótese que dispensa o consentimento do titular do dado. Previsão para exercício regular de direito, incluindo contraditório, ampla defesa e devido processo legal. Trata-se de ressalva para esclarecer que a proteção aos dados pessoais não compromete o direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário; ou seja, que não cabe oposição ao tratamento de dados pessoais no contexto dos processos judiciais, administrativos e arbitrais.

Nessa linha, é viável o tratamento de dados pessoais de servidores ou empregados públicos para fins de defesa dos interesses da Administração Pública em processos judiciais, arbitrais ou administrativos

VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiro

Hipótese que dispensa o consentimento do titular do dado nos casos de necessidade de tutela do bem maior da pessoa natural, a vida e sua incolumidade, ambos inseridos no conceito de dignidade da pessoa humana como fundamento da República.

VIII - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

Hipótese que dispensa o consentimento do titular do dado nos casos de estrita necessidade de tutela da saúde do titular, de terceiro ou pública. É a única hipótese de tratamento de dado manejado por agente exclusivo: profissionais de saúde, serviços de saúde ou autoridade sanitária. (ex. prontuários médicos)

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

Hipótese que dispensa o consentimento do titular do dado. É uma previsão geral e subsidiária, mediante prévia e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento, ou seja, somente se não houver o enquadramento da situação fática nos incisos II e III do art.

7º, ou seja, se a hipótese de tratamento não disser respeito à consecução de políticas públicas ou competências legais do controlador.

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I – apoio e promoção de atividades do controlador; II – 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, nos termos da LGPD.

Em tais circunstâncias, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo o controlador adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Convém salientar que o tratamento autorizado por esta hipótese traz consigo conjunto adicional de medidas de salvaguarda dos dados, inclusive com a possibilidade de a ANPD solicitar ao controlador relatórios de impacto à proteção de dados pessoais, justamente pelo risco de violação que tal hipótese acarreta, em particular, para entidades privadas.

X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

Hipótese que dispensa o consentimento do titular do dado. Previsão para os casos estritos de tutela do crédito. Há expressa necessidade de observância simultânea da legislação pertinente.

1.2 DIREITOS DO TITULAR

A LGPD visa assegurar a titularidade de dados pessoais e proteger os direitos fundamentais de privacidade, liberdade e intimidade. Assim, estabeleceu direitos aos titulares de dados pessoais que devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade. Desta forma, toda atividade de tratamento de dados pessoais deverá observar a boa-fé e os seguintes princípios (art. 6º):

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	PRINCÍPIO CORRESPONDENTE	REFERÊNCIA LEGISLATIVA (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	Princípio da finalidade	Art. 6º, I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6º, II
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento	Princípio da necessidade	Art. 6º, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	Princípio do livre acesso	Art. 6º, IV

Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	Princípio da qualidade dos dados	Art. 6º, V
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial	Princípio da transparência	Art. 6º, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas 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 difusão	Princípio da segurança	Art. 6º, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Princípio da prevenção	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio da não discriminação	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	Princípio da responsabilização e prestação de contas	Art. 6º, X

Além dos direitos dos titulares de dados que são decorrentes do art. 6º da LGPD, a Lei apresenta direitos específicos dos titulares de dados, que são destacados na tabela abaixo.

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIA LEGISLATIVA (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca	Art. 9º, § 1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	Art. 8º, § 5º

Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento	Arts. 8º, § 6º e 9º, § 2º
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização	Art. 7º, § 3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da Administração Pública, em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento	Art. 7º, § 5º
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa	Art. 11, II, c
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, § 2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular)	Art. 11, § 4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas	Art. 13

Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa	Art. 13, § 2º
Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Lei	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais	Art. 16

1.3 EXERCÍCIO DOS DIREITOS DOS TITULARES PERANTE A ADMINISTRAÇÃO

Para o exercício dos direitos dos titulares, a Lei prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva, bem como criam meios processuais para provocar a Administração Pública.

Essas obrigações são : (i) obrigações de transparência ativa (Publicidade, que será tratada em tópico próprio mais abaixo); (ii) meios de acesso à informação em transparência passiva; e (iii) meios de petição e manifestação à administração pública.

Em todos os casos, o titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

1.3.1 Meios de acesso à informação em transparência passiva

A LGPD estabelece que, no âmbito público, os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, citando (mas sem se ater exclusivamente) a Lei de Acesso à Informação, a Lei do Processo Administrativo e a Lei do Habeas data (essa última no âmbito judicial).

Observação a ser feita é que no Estado de Mato Grosso do Sul não existe ainda regramento específico tratando de Processo Administrativo.

Desta forma, considerando que a Lei 12.527/2011 -LAI, já previa, em seu art. 31, procedimentos e diretrizes básicas para o tratamento de dados pessoais no âmbito público, entre eles: o tratamento transparente, a garantia expressa aos direitos de personalidade e o consentimento do titular para a disponibilização de suas informações àqueles que não possuíssem a necessidade de conhecê-la no exercício de sua função pública, submetem-se aos prazos e procedimentos já estabelecidos- inclusive com o recebimento dos requerimentos junto ao Serviço de Informação ao Cidadão - o exercício dos seguintes direitos expressamente previstos na Lei Geral de Proteção de Dados Pessoais:

- a. acesso à informação sobre a confirmação da existência de tratamento (art. 18, I);
- b. acesso aos dados pessoais de que é titular e que são objeto de tratamento pela Administração Pública (art. 18, II);
- c. acesso à informação sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII);
- d. nos casos em que o tratamento tiver origem no consentimento do titular ou em contrato, o acesso à cópia eletrônica integral de seus dados pessoais. Devem ser observados os segredos comercial e

industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente inclusive em outras operações de tratamento (art. 19, §3º); e

e. acesso às informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º).

Em Mato Grosso do Sul, sobre acesso à informação, temos a Lei Estadual nº 4.416, de 16/10/2013, regulamentada pelo Decreto Estadual nº 14.471, de 12/05/2016. Portanto, é importante atentar a estes normativos locais.

1.3.2 Meios de petição e manifestação à administração pública

Como a LGPD não estabelece a observância exclusiva somente da Lei de Acesso à Informação e a Lei do Processo Administrativo ainda não existe em Mato Grosso do Sul, e considerando a existência de procedimentos mais benéficos ao titular para o exercício de seus direitos no que se refere a esse último conjunto apresentado, existe o mecanismo mais célere estabelecido pelo Código de Defesa dos Usuários de Serviços Públicos (Lei Federal nº 13.460/2017), regulamentado em âmbito estadual pelo Decreto nº 14.904, de 27 de dezembro de 2017, que poderiam ser adotados como padrão para o recebimento de solicitações de providências e reclamações relativas ao tratamento de dados.

Além da vantagem em termos de prazo e procedimentos padronizados, com unidades de recebimento de petições e reclamações padronizadas e coordenadas, a Lei 13.460/2017 tem abrangência nacional, permitindo melhor coordenação entre instituições públicas na defesa dos direitos dos titulares de dados.

O titular do dado tem o direito, mediante requerimento expresso seu ou de representante legalmente constituído, sem custos, nos prazos e nos termos previstos em regulamento, de requisitar manifestação conclusiva do controlador ou agente responsável pelo tratamento sobre os seguintes itens:

- a. correção de dados incompletos, inexatos ou desatualizados (art. 18, III);
- b. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);
- c. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (art. 18, VI); e
- d. revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).

A resposta deve ser providenciada de imediato e em formato simplificado; ou por declaração clara e completa, fornecida no prazo previsto em Lei e que indique: origem dos dados, a inexistência de registro, critérios utilizados, finalidade do tratamento (observados os segredos comercial e industrial).

O titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

A petição deve ser respondida com agilidade, clareza e completude, sob pena de o titular dos dados ter a prerrogativa de representar contra o responsável na ANPD, organismos de defesa do consumidor ou ajuizar pretensão com tal causa de pedir.

Na impossibilidade de atendimento imediato do requerimento do titular do dado pessoal, o controlador poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Por último, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Nas hipóteses acima, o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Quando tais segredos impossibilitarem o oferecimento de informações,

a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Os dados pessoais referentes ao exercício regular de direitos pelo titular, previstos no Art. 18 da LGPD (Capítulo III), não podem ser utilizados em seu prejuízo. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

1.4 TIPOS DE DADOS PESSOAIS

A LGPD manteve o conceito de dado pessoal trazido pela Lei 12.527/2011 que, de acordo com o inciso IV, artigo 4º, “é aquela relacionada à pessoa natural identificada ou identificável”. Entende-se por pessoa natural a pessoa física, ou seja, o indivíduo.

A novidade é que a LGPD evoluiu sobre o conceito de informação sensível que passa a ser: **“dado pessoal 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”** (Art. 5º, II). São informações que podem ser utilizadas de forma discriminatória e carecem de proteção especial.

Diferentemente da LAI, no entanto, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

No caso de dados sensíveis, em se tratando de Poder Público, algumas regras precisam ser observadas:

a) é exigência da LGPD de que os órgãos e entidades públicas que realizarem o tratamento de dados sensíveis para o cumprimento de obrigação legal ou regulatória pelo controlador ou para o tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos, deem a devida publicidade da dispensa de consentimento do titular, preferencialmente em seus sítios eletrônicos (art. 23, I);

b) o tratamento de dados pessoais sensíveis pelo Poder Público com base nas alíneas “c”, “d”, “e”, “f” e “g” do inciso II do art. 11 da LGPD, não exige o consentimento do titular, bem como dispensa a Administração de garantir a publicidade; e

c) o controlador, antes de efetuar o tratamento de um dado sensível, deverá demonstrar que a situação fática posta enquadra-se em uma das alíneas do inciso II, do art. 11 da LGPD, bem como justificar, de forma fundamentada, que o tratamento do dado sensível é indispensável para a Administração.



O TRATAMENTO DOS DADOS PESSOAIS

2.1 HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

A LGPD autoriza, em seu art. 23, os órgãos e entidades da administração pública a realizar o tratamento de dados pessoais 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, desde que as hipóteses de tratamento sejam informadas ao titular, dispositivo este reiterado pelo art. 12 do Decreto Estadual nº 15.572/2020, atualizado pelo Decreto Estadual nº 15.646/2021.

Na Seção 1 deste Guia, consta que o tratamento de dados pessoais poderá ser realizado desde que enquadrado em uma das hipóteses elencadas na Lei. Tais hipóteses se consubstanciam em condições necessárias para analisar se o tratamento de dados pelo controlador ou operador é permitido. As hipóteses de tratamento de dados pessoais são enumeradas no Art. 7º da Lei Federal nº 13.709/2018.

Também são destacadas nesta seção, as previsões expressas no Art. 11 da Lei Federal nº 13.709/2018, que trata das hipóteses autorizativas para o tratamento de informações pessoais sensíveis.

O inciso II do art. 5º da LGPD dispõe que os dados pessoais sensíveis de pessoas naturais são aqueles 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. Oportuno destacar que a lei autoriza o tratamento de dados sensíveis apenas em situações imprescindíveis.

Primeiramente, é importante que os órgãos e entidades da Administração Pública Estadual conheçam as hipóteses, a fim de que seja possível analisar os casos de tratamento de dados pessoais já realizados, para verificar se dispõem de hipótese legal autorizativa; e avaliar previamente cada novo caso de tratamento que seja realizado, aplicando a hipótese legal correspondente.

A tabela a seguir demonstra, de forma resumida, as hipóteses de tratamento estabelecidas pela LGPD, informando, em cada caso, a base legal equivalente ao tratamento de dados pessoais, bem como dos dados pessoais sensíveis, todos contidos nos Artigos 7º e 11 da Lei Federal nº 13.709/2018.

HIPÓTESES DE TRATAMENTO AUTORIZATIVAS		FUNDAMENTO LEGAL	
		TRATAMENTO DE DADOS PESSOAIS	TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1	Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art.11, I
Hipótese 2	Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, “a”
Hipótese 3	Para a execução de políticas públicas	LGPD, art. 7º, III	LGPD, art. 11, II, “b”
Hipótese 4	Para a realização de estudos por órgão de pesquisa	LGPD, art. 7º, IV	LGPD, art. 11, II, “c”
Hipótese 5	Para a execução ou preparação de contrato	LGPD, art. 7º, V	Não se aplica
Hipótese 6	Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, VI	LGPD, art. 11, II, “d”
Hipótese 7	Para a proteção da vida ou da incolumidade física do titular ou terceiro	LGPD, art. 7º, VII	LGPD, art. 11, II, “e”
Hipótese 8	Para a tutela da saúde do titular	LGPD, art. 7º, VIII	LGPD, art. 11, II, “f”
Hipótese 9	Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, IX	Não se aplica
Hipótese 10	Para proteção do crédito	LGPD, art. 7º, X	Não se aplica
Hipótese 11	Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, “g”

A base principiológica da LGPD é de grande relevância e se encontra estabelecida no art. 6º, sendo que as atividades de tratamento de dados pessoais devem observar a boa-fé e respeitar os seguintes princípios:

PRINCÍPIOS	DESCRIÇÃO
FINALIDADE	realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
ADEQUAÇÃO	compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento
NECESSIDADE	limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados
LIVRE ACESSO	garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais
QUALIDADE DOS DADOS	garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
TRANSPARÊNCIA	garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial
SEGURANÇA	utilização de medidas 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 difusão
PREVENÇÃO	adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
NÃO DISCRIMINAÇÃO	impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS	demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

2.1.1 Identificação das hipóteses de tratamento

A identificação de uma ou mais hipóteses legais aplicáveis a cada caso depende das finalidades específicas da situação, lembrando ser necessário que o titular conheça a hipótese autorizativa do processamento de seus dados pessoais.

É de fundamental importância que o órgão ou entidade pública avalie corretamente a hipótese de tratamento aplicável, uma vez que o princípio da responsabilização e prestação de contas demanda que a realização do tratamento de dados pessoais demonstre estar plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia.

Objetivando auxiliar os órgãos e entidades no processo de adequação à LGPD, o **Guia de Boas Práticas do Governo Federal** elaborou checklists que destacam questões fundamentais a serem verificadas para garantir a conformidade do tratamento de dados pessoais às disposições da Lei, sendo que são perfeitamente aplicáveis à Administração Pública Estadual.

Os checklists poderão ser utilizados tanto no início de novos tratamentos, quanto na avaliação da conformidade de tratamentos principiados antes da vigência da LGPD e foram **transcritos abaixo, juntamente com a verificação da conformidade quanto aos princípios**, no intuito de facilitar a definição da hipótese mais apropriada:

HIPÓTESE 1: Tratamento mediante consentimento do titular

Essa é uma hipótese em que o titular tem chance real de escolha sobre o tratamento de seus dados. Trata-se de hipótese possível quando as demais do art. 7º da Lei Federal nº 13.709/2018 forem descartadas.

Uma vez descartadas as demais hipóteses, o órgão/entidade deve avaliar:

1. Serão viáveis a coleta e o armazenamento da opção de consentimento do titular de modo a poder comprovar posteriormente a sua expressa manifestação de vontade?
2. Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado?
3. O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento?

Observações:

- a) É vedado o tratamento de dados pessoais mediante vício de consentimento.
 - b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
 - c) Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.
 - d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.
4. Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado?
 5. No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal?
 6. No caso do tratamento de dados pessoais sensíveis, será registrada a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento?

Ressalta-se que todas as questões acima, se aplicáveis, devem ser respondidas positivamente para que a hipótese de tratamento do dado por consentimento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 2: Tratamento para o cumprimento de obrigação legal ou regulatória

Essa hipótese é aplicável quando é necessário processar dados pessoais para o cumprimento de obrigações legais ou regulatórias específicas. Não se enquadram nessa hipótese as obrigações estabelecidas por contrato.

Para enquadramento nessa hipótese, deve-se avaliar:

1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?
2. É possível identificar a competência legal do órgão que dará cumprimento à obrigação legal ou regulatória?
3. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?
4. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 3: Tratamento para a execução de políticas públicas

Essa hipótese é aplicável 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. Trata-se de uma hipótese que dispensa o consentimento do titular e que deve ser realizada por controladores que sejam pessoas jurídicas de direito público e que podem envolver operadores para a realização do tratamento de dados pessoais necessários à consecução de políticas públicas.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O controlador é pessoa jurídica de direito público?
2. Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência?
3. O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?
4. É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais?
5. É possível identificar a competência legal que autoriza o órgão à execução da política pública?
6. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?
7. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei, inclusive quando da necessidade de compartilhamento de dados?
8. Será indicado um Encarregado (Art. 5º, inciso VIII da Lei Federal nº 13.709/2018; **Art 3º, inciso III do Decreto Estadual nº 15.572/2020**) para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a Autoridade Nacional de Proteção de Dados, que verificará a observância das instruções e normas sobre a política pública em questão?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Segundo o Art. 23 da LGPD, **reiterado pelo art.12 do Decreto Estadual nº 15.572**, os órgãos e entidades públicas deverão realizar o tratamento de dados apenas para o atendimento de sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Não havendo delimitação inequívoca das atribuições legais que poderiam ser diretamente relacionadas à execução de políticas públicas, cabe aos órgãos e entidades analisar, em cada caso concreto, a possibilidade de enquadrar o tratamento do dado na hipótese prevista no Art. 7º, inciso III, combinada com o disposto no Art. 23, ambos da LGPD.

HIPÓTESE 4: Tratamento para a realização de estudos e pesquisas

Essa hipótese é aplicável para o tratamento de dados para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Para enquadramento nesta hipótese, deve-se avaliar:

1. O controlador ou operador é órgão de pesquisa?
2. Os dados pessoais serão utilizados dentro do órgão estritamente para a finalidade estabelecida para o estudo ou pesquisa?
3. Em se tratando de estudos em saúde pública, os dados serão mantidos em ambiente seguro e controlado, e será garantida, sempre que viável, a anonimização ou pseudonimização dos dados?
4. O órgão de pesquisa garante que não serão revelados dados pessoais, em caso de divulgação dos resultados ou de qualquer trecho do estudo ou da pesquisa realizada?

5. O órgão de pesquisa que tiver acesso aos dados pessoais assume a responsabilidade pela segurança da informação e se compromete a não transferir os dados a terceiros em circunstância alguma?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Especificamente no que tange à realização de estudos em saúde pública, o art. 13 da LGPD possibilita que os órgãos tenham acesso a bases de dados pessoais, inclusive os atributos sensíveis, que serão tratados exclusivamente dentro do referido órgão e estritamente para a finalidade de realização de estudos e pesquisas. Nessa hipótese, o órgão ou entidade deverá garantir que os dados sejam mantidos em ambiente controlado e seguro, e que, sempre que possível, sejam anonimizados ou pseudonimizados (vide Seção 2.3).

HIPÓTESE 5: Tratamento para a execução de contrato ou de procedimentos preliminares relacionados a contrato

Essa hipótese é aplicável para o tratamento de dados necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular. As hipóteses de tratamento de dados estarão previstas no contrato. O consentimento é fornecido no ato de formalização do termo ou decorrente do mesmo.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para a consecução dos termos do contrato ou para a realização de procedimentos preliminares relacionados ao contrato?

Essa pergunta deve ser respondida positivamente para que tal hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 6: Tratamento para o exercício de direitos em processo judicial, administrativo ou arbitral

Essa hipótese é aplicável para o tratamento de dados necessários ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?

2. O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 7: Tratamento para a proteção da vida ou da incolumidade física do titular ou de terceiro

Essa hipótese é aplicável para o tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros?

2. O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 8: Tratamento para a tutela da saúde do titular

Essa hipótese é aplicável para o tratamento de dados para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais será realizado por profissional de saúde, serviço de saúde ou autoridade sanitária?

2. O tratamento de dados pessoais se faz necessário para a tutela da saúde do titular?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 9: Tratamento para atender interesses legítimos do controlador ou de terceiro

Essa hipótese é aplicável para o tratamento de dados quando necessário atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Órgãos e entidades públicas não devem recorrer a essa hipótese se o tratamento de dados ocorre para a consecução de políticas públicas ou de suas próprias competências legais. No entanto, em caso de finalidade diversa, essa opção poderá ser aplicável.

Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificado interesse legítimo do controlador, considerado a partir de situações concretas, que respeite as legítimas expectativas do titular em relação ao tratamento de seus dados?
2. O controlador se responsabiliza por garantir a proteção do exercício regular dos direitos do titular ou a prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?
3. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?
4. Serão adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 10: Tratamento para proteção do crédito

Essa hipótese é aplicável para o tratamento de dados para proteção do crédito do titular.

Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificada necessidade de tratamento de dados pessoais para a proteção do crédito do titular?
2. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 11: Tratamento para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos

Essa hipótese é aplicável para o tratamento de dados pessoais sensíveis para assegurar a identificação e autenticação de cadastro em sistemas eletrônicos, visando à prevenção de fraudes e à garantia da segurança do titular.

Para enquadramento nessa hipótese, deve-se avaliar se não há outro meio para a identificação do titular sem a necessidade do tratamento de dados sensíveis.

Esta hipótese refere-se, por exemplo, à possibilidade de uso de biometria para identificação e autenticação em sistemas eletrônicos.

Destaca-se que essa hipótese não pode ser utilizada no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

2.1.2 Conformidade do tratamento de dados quanto aos princípios da LGPD

Realizada a identificação da(s) hipótese(s) de tratamento aplicável(is) às situações específicas de processamento de dados por órgãos e entidades da Administração Pública, deve-se proceder à verificação da conformidade quanto aos princípios da LGPD, efetuando o que se segue:

1. Identificação da finalidade para a qual o tratamento de dado é necessário, sendo que os propósitos devem ser legítimos, específicos e explícitos (princípio da finalidade).
2. Definição de como a finalidade do tratamento será informada ao titular, o que deve ser realizado antes do início do tratamento do dado (princípio da finalidade).
3. No caso de tratamento de dados que tenha sido iniciado antes da vigência da LGPD, indicação de que providências serão tomadas para comunicar o titular sobre o tratamento realizado e a finalidade a qual se destina (princípio da finalidade).
4. Garantia de que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação).
5. Atentar para a limitação do tratamento ao mínimo de informações necessárias, de forma a garantir abrangência pertinente e proporcional à consecução das finalidades informadas ao titular (princípio da necessidade).
6. Definir, antecipadamente, os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (princípio do livre acesso).
7. Garantia de que quaisquer alterações quanto à finalidade especificada para o tratamento do dado; à forma ou à duração do tratamento; ao controlador responsável pelo dado; ou, ainda, à abrangência de compartilhamento sejam comunicadas ao titular (princípio do livre acesso).
8. Definição de procedimento de verificação quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular (princípio da qualidade do dado).
9. Observar a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).
10. Definir e documentar as medidas 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 difusão (princípio da segurança).
11. Identificação e registro de medidas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção).
12. Comprometimento em não realizar o tratamento do dado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).
13. Comprometimento em adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas).

Para iniciar novos tratamentos de dados, é fundamental que os órgãos e entidades da Administração Pública analisem todas as questões citadas acima e documentem a forma de aplicação de cada um dos princípios da LGPD. O **Relatório de Impacto à Proteção de Dados Pessoais – RIPD**, tratado na seção 2.5, representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição.

O exame das questões acima deve também ser realizado para os casos de tratamento de dados anteriores à vigência da Lei. É importante verificar os pontos de não conformidade com a LGPD, para os quais deverão ser elaborados planos para adaptação à Lei.

2.1.3 Tratamento de dados de crianças e adolescentes

A LGPD dedica especial atenção ao tratamento de dados de crianças e adolescentes, determinando, no art. 14, que seja realizado em seu melhor interesse. A Lei requer **consentimento específico e em destaque**, dado por, pelo menos, um dos pais ou pelo responsável legal, caso em que os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para acesso às informações tratadas.

É também dever do controlador realizar todos os esforços razoáveis para verificar se o consentimento foi dado realmente pelo responsável pela criança ou adolescente, consideradas as tecnologias disponíveis.

No desenvolvimento, por órgãos e entidades públicas, de jogos, aplicações de internet ou outras atividades semelhantes, direcionadas ao público infante-juvenil, a coleta dos dados pessoais desses deverá restringir-se ao estritamente necessário à atividade proposta.

As hipóteses que **dispensam o consentimento** acima ocorrem quando:

- a) A coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente. Os dados deverão ser utilizados uma única vez, vedados o armazenamento e o repasse a terceiros;
- b) O Tratamento de dados for imprescindível para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.

2.2 COLETA

A coleta mencionada no art. 5º, inciso X da LGPD é a etapa inicial do ciclo de tratamento dos dados pessoais e somente deve ser realizada mediante o atendimento das hipóteses de tratamento, dos direitos do titular, dos princípios e demais regras estabelecidas pela Lei (capítulo 3).

O presente conteúdo visa justamente orientar o Poder Público no cuidado necessário para coletar e tratar os dados pessoais dos cidadãos de forma a assegurar a privacidade dos titulares de dados.

2.3 ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Dado anonimizado, no conceito adotado pelo art. 5º da LGPD, é o dado alusivo a titular que não possa ser identificado, considerados os meios técnicos razoáveis no momento do tratamento. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, que impossibilita a associação entre estes, de forma direta ou indireta. A partir do momento em que o dado é considerado anonimizado, e não permite mais qualquer identificação do seu titular, esse dado não será mais considerado pessoal, conforme previsto no art. 12 da LGPD.

Cabe destacar que, ainda que o dado seja considerado anonimizado pelo controlador, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, permitindo a reidentificação do titular de dados, se está diante de um dado potencialmente pseudonimizado.

Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

De acordo com a legislação em vigor, esses processos devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis, na ocasião do tratamento dos dados.

A seguir, algumas recomendações elaboradas pelo **Guia de Boas Práticas do Governo Federal** para subsidiar a escolha da técnica a ser utilizada, as quais replicamos no presente Guia, por serem aplicáveis à Administração Pública Estadual :

- Elencar os principais processos de trabalho que realizam tratamento de dados pessoais para a realização de estudos, especialmente em órgão de pesquisa, conforme Art. 7º, IV, da Lei 13.709/2018.
- Identificar os dados pessoais a que se referem os processos de trabalho listados, que não podem ter os titulares relacionados.
- Analisar o ciclo de vida de tratamento do dado a fim de mitigar riscos de violação de dados que não são mais de uso corrente e, ainda, propor arquivamento ou eliminação dos dados, visto que a gestão de dados desnecessários causa aumento do quantitativo de dados a serem geridos e da manutenção do custo operacional relacionado a este processo .
- Avaliar o risco de identificação do titular dos dados listados. Deve-se levar em consideração que, quanto maior o uso de tecnologias de análise de dados, quanto maior o volume de dados processados e quanto mais significativos forem estes dados, maior será o risco de violação.
- Quando houver a obrigatoriedade de proteção de dados pessoais, sem a necessidade de guarda dos dados que associam estes aos titulares, pode-se optar pelo processo de anonimização, sem prejuízo de atividades do órgão ou entidade. Caso contrário, pode-se optar pela técnica de pseudonimização.
- Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.
- Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.
- Promover a conscientização contínua acerca da importância da proteção de dados no órgão ou entidade.

2.4 PUBLICIDADE

O inciso I do art. 23 da LGPD impõe às pessoas jurídicas de direito público a **publicação de informações sobre os tratamentos de dados pessoais por elas realizados em seus sítios eletrônicos** de forma clara e atualizada, especificando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos. Este dispositivo da LGPD foi reiterado pelo parágrafo único do art. 12 do Decreto Estadual nº 15.572/2020.

Quando o tratamento de dados envolver **dados pessoais sensíveis**, na hipótese de dispensa do consentimento do titular, tanto para cumprimento de obrigação legal ou regulatória, quanto para compartilhamento de dados necessários para a execução de políticas públicas previstas em leis ou regulamentos, também deve ser dada publicidade, consoante previsão do §2º do art. 11 da LGPD.

O art. 25 da LGPD prescreve que, com vistas à execução de políticas públicas, prestação de serviços públicos, descentralização da atividade pública e disseminação e acesso das informações pelo público em geral, os dados deverão ser mantidos em **formato interoperável e estruturado** para o uso compartilhado.

O §1º do art.3º do Decreto Estadual nº 15.572/2020, ratificado pelo art. 41,§1º da LGPD, determina, ainda, publicação da **identidade e informações de contato do Encarregado**.

Quanto à publicação das informações, deve se localizar nas páginas dos órgãos da Administração Direta, das autarquias e das fundações do Poder Executivo Estadual na internet, bem como no Portal da Transparência do Governo de Mato Grosso do Sul, disponível em www.transparencia.ms.gov.br.

Neste endereço eletrônico deve ser publicado, ainda, banner para o **Fala.BR**, que será o canal para endereçamento de petições e reclamações do titular de dados, previstas nos artigos 18 e 20 da LGPD.

2.5 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

2.5.1 Definição de Relatório de Impacto à Proteção de Dados Pessoais

A LGPD considera o **Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)** como documentação do controlador apta a descrever os 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 (art. 5º, inciso XVII).

O conteúdo mínimo do RIPD consta no parágrafo único do art. 38 da LGPD, abrangendo descrição dos tipos de dados coletados, metodologia utilizada para a coleta e garantia das informações, bem como análise do controlador com relação a mecanismos de mitigação de riscos adotados.

O **Guia de Boas Práticas do Governo Federal** disponibilizou modelo do RIPD, contido no Anexo I, cujos aspectos foram abaixo reproduzidos, visto que se aplicam à Administração Pública Estadual:

2.5.2 Como Elaborar

A elaboração do RIPD contempla as etapas destacadas pela figura a seguir.

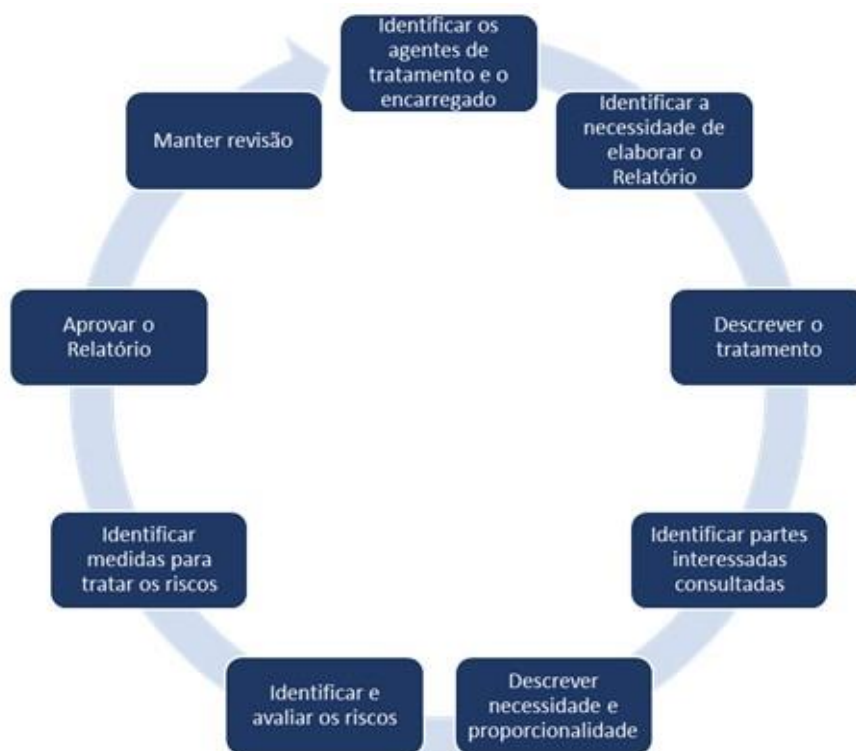


Figura 1 Etapas da Fase de Elaboração do RIPD

2.5.2.1 Identificar os Agentes de Tratamento e o Encarregado

Esta etapa consiste em identificar os agentes de tratamento (Controlador e Operador) e o Encarregado no RIPD, conforme estabelecido no **art. 3º do Decreto Estadual nº 15.572/2020**:

“Art. 3º No âmbito do Poder Executivo Estadual e, consoante definição dos incisos VI, VII e VIII do art. 5º da LGPD, consideram-se:

I- Controlador: pessoa jurídica do órgão da Administração Direta, da autarquia ou da fundação estadual sujeita à LGPD, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de dados;

II- Operador: o(s) agente público(s), no sentido amplo, que exerça(m) o tratamento de dados, bem como pessoa(s) jurídica(s) diversa(s) daquela representada pelo Controlador, que exerça(m) atividade de tratamento no âmbito de contrato ou de instrumento congênere;

III- Encarregado: o(s) agente(s) público(s), formalmente designado(s), para o desempenho da comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), bem como das demais funções previstas no art.41 da LGPD.”

2.5.2.2 Identificar a necessidade de elaborar o Relatório

O Decreto Estadual nº 15.572/2020, no inciso IV do art. 5º, determina que o RIPD deve ser realizado e continuamente atualizado pelos órgãos da Administração Direta, as autarquias e as fundações do Poder Executivo Estadual, quando solicitado.

No mesmo sentido, o RIPD deve ser elaborado pelo Controlador, quando determinado pela Autoridade Nacional de Proteção de Dados, consoante art. 7º, inciso III do Decreto.

O art. 7º, inciso VIII do Decreto Estadual estabelece, ainda, que o Controlador de dados pessoais deve encaminhar ao encarregado, em prazo fixado, relatórios de impacto à proteção de dados pessoais, ou informações necessárias à elaboração de tais relatórios, nos termos do art. 32 da Lei Federal nº 13.709, de 2018.

Da mesma forma, quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, consoante arts. 31 e 32 da Lei Federal nº 13.709/2018.

A elaboração de um único **RIPD** para todas as operações de tratamento de dados pessoais ou de um **RIPD** para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um **RIPD** único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único **RIPD** não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o **RIPD** ser elaborado ou atualizado pela instituição.

2.5.2.3 Descrever o tratamento

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

Lembrando que a LGPD (art. 5º, X) considera tratamento “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

2.5.2.3.1 Natureza do tratamento

A **natureza** representa como a instituição pretende tratar ou trata o dado pessoal.

Importante descrever, por exemplo:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
- com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados;
- quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;
- se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
- medidas de segurança atualmente adotadas.

2.5.2.3.2 Escopo do tratamento

O **escopo** representa a abrangência do tratamento de dados. Nesse sentido, considerar destacar:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis;
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- o número de titulares de dados afetados pelo tratamento; e
- a abrangência da área geográfica do tratamento.

2.5.2.3.3 Contexto do tratamento

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos;
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

2.5.2.3.4 Finalidade do tratamento

A **finalidade** é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- alguma espécie de estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde;
- atender aos interesses legítimos do controlador ou de terceiro;
- proteção do crédito; e
- garantia da prevenção à fraude e à segurança do titular.

Cumpra-se destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

2.5.2.4 Identificar partes interessadas consultadas

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Nessa etapa, é importante identificar:

- quais partes foram consultadas, como, por exemplo: operador, encarregado, gestores, especialistas em segurança da informação, consultores jurídicos, etc.; e

- o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.

2.5.2.5 Descrever necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III).

Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:
 - esse tratamento de dados pessoais é indispensável;
 - não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e esse processamento de fato auxilia no propósito almejado.
- Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.

- Quais medidas são adotadas a fim de assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador.
- Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
- Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.

2.5.2.6 Identificar e avaliar os riscos

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever “medidas, salvaguardas e mecanismos de mitigação de risco”.

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário **identificar os riscos** que geram impacto potencial sobre o titular dos dados pessoais.

De antemão, cabe registrar a importância de que seja editada **Política de Gestão de Riscos**, a nível estadual, de forma a possibilitar a identificação, avaliação, bem como posterior mitigação dos riscos.

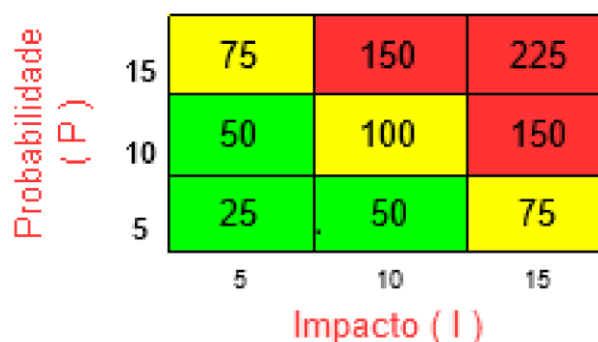
A título de sugestão, o **Guia de Boas Práticas do Governo Federal** leciona o que se segue:

Para cada risco identificado, define-se a **probabilidade** de ocorrência do evento de risco, bem como o possível **impacto** caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.



Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
		Impacto (I)		

Matriz Probabilidade x Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada.

Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

Lembrando que deve ser identificado qualquer risco que afete o tratamento de dados pessoais, independentemente de sua natureza (técnica, administrativa, de segurança da informação ou de privacidade).

2.5.2.7 Identificar medidas para tratar os riscos

Os agentes de tratamento 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 (LGPD, art. 46). Este dispositivo foi reiterado pelo art. 7º, inciso V do Decreto Estadual nº 15.572/2020.

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas.

No modelo sugerido pelo **Guia de Boas Práticas do Governo Federal, no Anexo I**, a coluna “Medida(s)” pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento de cada risco identificado na etapa “Identificar e avaliar riscos”.

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto -, devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

2.5.2.8 Aprovar o Relatório

Esta etapa visa formalizar a aprovação do **RIPD** por meio da obtenção das assinaturas do responsável pela elaboração do **RIPD**, pelo encarregado e pelas autoridades que representam o controlador e operador.

2.5.2.9 Manter Revisão

O **RIPD** deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizado pela instituição.

A instituição deve manter revisão do **RIPD** a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

2.6 TÉRMINO DO TRATAMENTO

Nos termos do art. 15 da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

- I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- II - fim do período de tratamento;
- III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
- IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Na incidência de qualquer uma das hipóteses acima, o art. 16 da LGPD determina que os dados sejam eliminados, autorizada a conservação para as seguintes finalidades:

- I-cumprimento de obrigação legal ou regulatória pelo controlador;
- II-estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;

- III-transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em Lei;
- IV-uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados.

No âmbito da Administração Pública, é importante que este dispositivo seja harmonizado com a legislação de arquivos, em especial com o que preceituam o Decreto Estadual nº 13.664, de 25 de junho de 2013, e o Decreto Estadual nº 15.168, de 25 de fevereiro de 2019, haja vista que os dados pessoais coletados pelo poder público passam a constituir o que se denomina arquivo público, sendo que a sua eliminação deverá obedecer aos procedimentos de gestão de documentos.

3

O CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS

O ponto de partida, no caso de tratamento de dados pessoais pelo Poder Público, é verificar, no caso concreto, qual a base legal será utilizada para a operação. E isso porque a Administração encontra-se jungida ao princípio constitucional da legalidade, necessitando, sempre, estar amparada em lei para as suas ações, o que inclui o tratamento de dados pessoais. Nesse sentido, o art. 23 da LGPD preconiza que o tratamento de dados pessoais pelo Poder Público deverá ser realizado, independentemente do consentimento do titular (art. 11, II) 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.

Tratamento é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Assim, a LGPD não adota qualquer tipo de segregação, considerando como tratamento, por exemplo, tanto a coleta quanto o armazenamento de dados pessoais, mesmo essas operações tratando de propósitos diferentes.

Ao aplicar os dispositivos da disciplina da Lei Geral de Proteção de Dados, entenda que o legislador quer que você: respeite a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Autodeterminação informativa é saber quais dados pessoais estão sendo coletados e qual a finalidade. A Lei Geral de Proteção de Dados aplica-se a qualquer operação de tratamento: realizada no território nacional; que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que tenham sido coletados no território nacional, considerando-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

O dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados¹ (LGPD, art. 18, IV), ao cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (LGPD, art. 52, VI) ou ao término de seu tratamento (LGPD, art. 16). Dessa forma, percebemos a configuração de um ciclo que se inicia com a coleta e que determina a “vida” (existência) do dado pessoal durante um período de tempo, de acordo com certos critérios de eliminação.

Para orientar a prática do tratamento e apresentar os ativos institucionais envolvidos, divide-se o ciclo de vida do tratamento dos dados pessoais em cinco fases: coleta, retenção, processamento, compartilhamento e eliminação.

Nesta seção, abordaremos o que é cada fase do ciclo de vida, a relação das fases do ciclo com as operações de tratamento da LGPD, os tipos de ativos organizacionais e o relacionamento desses ativos com as fases do ciclo de tratamento, destacando as ações a serem executadas em tais fases.

¹ Ressalte-se que no caso de cumprimento de obrigação legal, como ocorre com a administração pública na maior parte dos casos, é autorizada a conservação do dado (LGPD, art. 16, I). Isso significa que, da mesma forma que o titular dos dados não precisa consentir o tratamento dos dados pessoais pela administração pública em casos determinados, também não é possível ao titular do dado solicitar a eliminação.

3.1 FASES DO CICLO DE VIDA

Para implementar o correto tratamento dos dados pessoais e as medidas correlatas, o órgão precisa conhecer os dados pessoais que gerencia e quais processos, projetos, serviços e ativos perpassam o ciclo de vida do tratamento dos dados pessoais.

A LGPD considera como tratamento toda operação realizada com os dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Para além da legislação de proteção de dados pessoais, é preciso também observar a legislação de arquivos que deve ser considerada conjuntamente na realização das operações com os dados pessoais contidos em documentos arquivísticos², ainda que estes sejam mantidos em sistemas informatizados e bases de dados. Do mesmo modo, vale lembrar, a Lei de Acesso à Informação - LAI (Lei nº 12.527, de 18 de novembro de 2018) e o seu regulamento (Decreto Estadual nº 14.471, de 12 de maio de 2016) igualmente apresentam regras específicas para o acesso a documentos que, embora apresentem dados pessoais, possuem valor permanente e foram recolhidos a instituições arquivísticas públicas. A LGPD e a LAI também devem, portanto, ser interpretadas sistematicamente.

Nesse cenário, o ciclo de vida do tratamento tem início com a coleta do dado e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento definidas na LGPD. A fase coleta refere-se à coleta, produção e recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.). A retenção corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.). O processamento é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador. O compartilhamento, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais. Por fim, a eliminação é qualquer operação que visa excluir ou eliminar um dado ou conjunto de dados pessoais armazenados em banco de dados, em virtude do tratamento da LGPD. Quando se tratar da eliminação de documentos arquivísticos, devem ser levadas em consideração as legislações Estaduais.

A figura a seguir sintetiza as fases do ciclo de vida do tratamento de dados pessoais:



FASES DO CICLO DE VIDA DO TRATAMENTO DE DADOS PESSOAIS	
COLETA	obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação, etc.).
RETENÇÃO	arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço, etc.).
PROCESSAMENTO	qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.
COMPARTILHAMENTO	qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.
ELIMINAÇÃO	qualquer operação que visa apagar, excluir ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

² Documento Arquivístico: documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência.

A tabela abaixo ilustra a relação entre as fases do ciclo de vida descrito nesta seção e as operações consideradas como tratamento pela LGPD:

DADOS PESSOAIS	
FASE DO CICLO DE TRATAMENTO	OPERAÇÕES DE TRATAMENTO - LGPD, ART. 5º, X
Coleta	Coleta, produção, recepção e acesso
Retenção	Arquivamento, armazenamento e acesso
Processamento	Classificação, utilização, reprodução, processamento, avaliação, controle da informação, extração, modificação e acesso
Compartilhamento	Transmissão, distribuição, comunicação, interconexão, transferência, difusão e acesso
Eliminação	Eliminação e acesso.

A operação de tratamento “acesso” (LGPD, art. 5º, X) está presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma temos que realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação.

Essas operações de tratamento de dados pessoais se cruzam com os procedimentos e operações da gestão de documentos, nas diversas fases do ciclo de vida do documento. Quando os dados pessoais integrarem documentos arquivísticos, os procedimentos e operações da gestão de documentos também precisam ser efetivados conjuntamente, como por exemplo, produção, recebimento, tramitação, arquivamento, classificação, indexação, atribuição de restrição de acesso, avaliação, transferência, acesso e eliminação. Alguns desses procedimentos e operações da gestão de documentos, apesar de serem referidos pelo mesmo termo, têm entendimento distinto daquele utilizado no contexto do tratamento de dados pessoais, e cada um deve ser entendido e realizado em conformidade com seu contexto.

Em se tratando de gestão documental, a classificação e avaliação dos documentos (Decreto Estadual nº 13.664, de 25 de junho de 2013; Decreto Estadual nº 13.881, de 04 de fevereiro de 2014; Decreto Estadual nº 15.168, de 25 de fevereiro de 2019) são instrumentos que auxiliam na execução das atividades, sendo a base para a elaboração do Plano de Classificação e das Tabelas de Temporalidade de Documentos de Arquivo.

A Tabela de Temporalidade de Documentos de Arquivo é o instrumento resultante da atividade de avaliação dos documentos produzidos e recebidos dos órgãos e entidades do Poder Executivo do Estado de Mato Grosso do Sul, definindo os prazos de guarda e destinação final desses documentos.

Nas Tabelas de Temporalidade de Documentos de Arquivo relativos à administração pública estadual, são definidos quais documentos serão preservados para fins administrativos ou de pesquisa e em que momento poderão ser eliminados ou destinados aos arquivos intermediários e permanente, segundo o valor e o potencial de uso que apresentam para a administração que os gerou e para a sociedade.

No contexto da gestão de documentos, o ciclo de vida dos documentos de arquivo compreende três fases, a saber: produção, utilização e destinação final (eliminação ou guarda permanente). Em cada uma dessas fases são realizados os procedimentos e operações de gestão de documentos, conforme figura e tabela, a seguir.



Produção: operações referentes à elaboração de documentos em razão da execução das atividades de um órgão ou entidade.

Utilização (uso e manutenção): operações referentes ao fluxo percorrido pelos documentos para o cumprimento de sua função administrativa, assim como de sua guarda, após cessar o seu trâmite.

Destinação final: operações referentes ao ato de decidir quais documentos devem ser eliminados (mediante autorização, conforme legislação vigente), bem como quais documentos devem ser mantidos por razões administrativas, legais ou fiscais. Para tal, envolve as atividades de análise, seleção e fixação de prazos de guarda dos documentos.

DOCUMENTOS DE ARQUIVO	
DOCUMENTOS DE ARQUIVO FASE DO CICLO DE VIDA DOS DOCUMENTOS DE ARQUIVO	OPERAÇÕES DE TRATAMENTO NA GESTÃO DE DOCUMENTOS (INDEPENDENTEMENTE DO SUPORTE MATERIAL E DA ENTIDADE PRODUTORA) LEI Nº 8.159/1991 E NORMA ABNT NBR ISO 15489:2018
Produção	Elaboração, recebimento, registro, classificação, indexação e atribuição de restrição de acesso
Utilização(uso e manutenção)	Tramitação, controle, arquivamento, transferência para guarda intermediária, acesso e empréstimo.
Destinação final	Avaliação, seleção, eliminação e recolhimento para guarda Permanente.

3.2 ATIVOS ORGANIZACIONAIS

É importante identificar quais ativos organizacionais estão envolvidos em cada fase do ciclo de vida do tratamento dos dados pessoais. Os **principais ativos** são: **bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais**. A figura apresenta os principais ativos envolvidos no ciclo de vida do tratamento dos dados.



A seguir, são apresentadas definições para os ativos envolvidos no ciclo de vida do tratamento dos dados pessoais.

DEFINIÇÕES DOS ATIVOS
Base de dados é uma coleção de dados logicamente relacionados, com algum significado. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico.
Documento unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005).
Equipamento objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.
Local físico determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal. Por exemplo, uma sala, um arquivo, um prédio, uma mesa, etc.
Pessoa qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais, como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
Sistema qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais.
Unidade organizacional órgãos e entidades da Administração Pública

3.3 RELACIONAMENTO DO CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS COM ATIVOS ORGANIZACIONAIS

Para cada fase do ciclo de tratamento de dados é importante identificar os ativos organizacionais que estarão envolvidos.

Na fase de **Coleta** deve-se identificar os ativos envolvidos na coleta de dados pessoais. Esses dados podem entrar na organização por algum **documento**, algum **sistema** hospedado em algum **equipamento** localizado em **local físico** do órgão público. Podem ser coletados pela prestação de algum serviço externo ou serviço prestado pelo próprio órgão público por meio de alguma de suas **unidades organizacionais**.

Na fase de **Retenção**, deve-se avaliar os ativos utilizados para armazenar os dados pessoais. Esses dados podem estar armazenados em **bases de dados**, **documentos**, **equipamentos** ou **sistemas**. É preciso considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados, bem como os **locais físicos** onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em “nuvem”, por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado.

A fase de **Processamento** segue a mesma linha de raciocínio das anteriores. Identifica-se os ativos onde são realizados os tratamentos dos dados. O tratamento pode ser realizado em **documento**, pode ser feito por um **sistema** interno ou contratado pelo órgão. É preciso identificar as **pessoas** (papeis organizacionais), **unidade organizacionais e equipamentos** envolvidos nesse tratamento. Onde estão **localizadas fisicamente** essas unidades organizacionais e os equipamentos envolvidos nesse tratamento também são importantes.

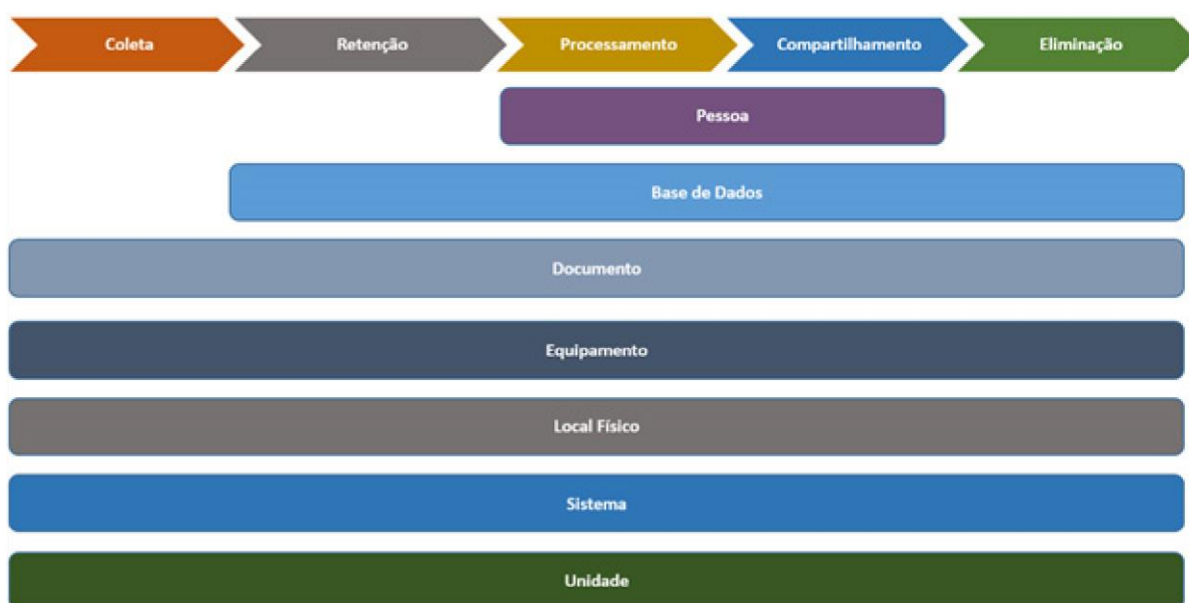
Na fase de **Compartilhamento** é preciso mapear os ativos envolvidos na distribuição ou divulgação dos dados pessoais para dentro e para fora do órgão público. Quais **sistemas** são usados para transmitir, exibir ou divulgar dados pessoais? Quais **pessoas** são destinatárias dessas informações? Quais **unidades organizacionais**, quais **equipamentos** são usados para tal?

No que se refere à fase de **Eliminação**, deve-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de: solicitação de eliminação de dados a pedido do titular dos dados pessoais; ou descarte nos casos necessários ao negócio da instituição. Os dados pessoais a serem eliminados podem estar armazenados em ativos relacionados com **bases de dados, documentos, equipamentos ou sistemas**. É necessário considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados que possam ser objeto de eliminação ou descarte, bem como os **locais físicos** onde estão localizados os ativos que contenham dados a serem eliminados ou descartados. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em “nuvem”, por exemplo, é preciso considerar o serviço de armazenamento contratado ou utilizado.

Quando os dados pessoais estiverem contidos em documentos arquivísticos, qualquer que seja o suporte ou formato, esses dados poderão ser tratados no contexto da LGPD, mas os documentos arquivísticos propriamente ditos, deverão seguir os procedimentos definidos pela gestão de documentos.

Esse processo demanda esforço considerável, principalmente para grandes organizações. O ideal é que se estabeleçam ações de **mapeamento e análise dos processos organizacionais**, tendo em vista que, desta forma, o órgão conseguirá identificar de maneira mais eficaz os ativos descritos anteriormente.

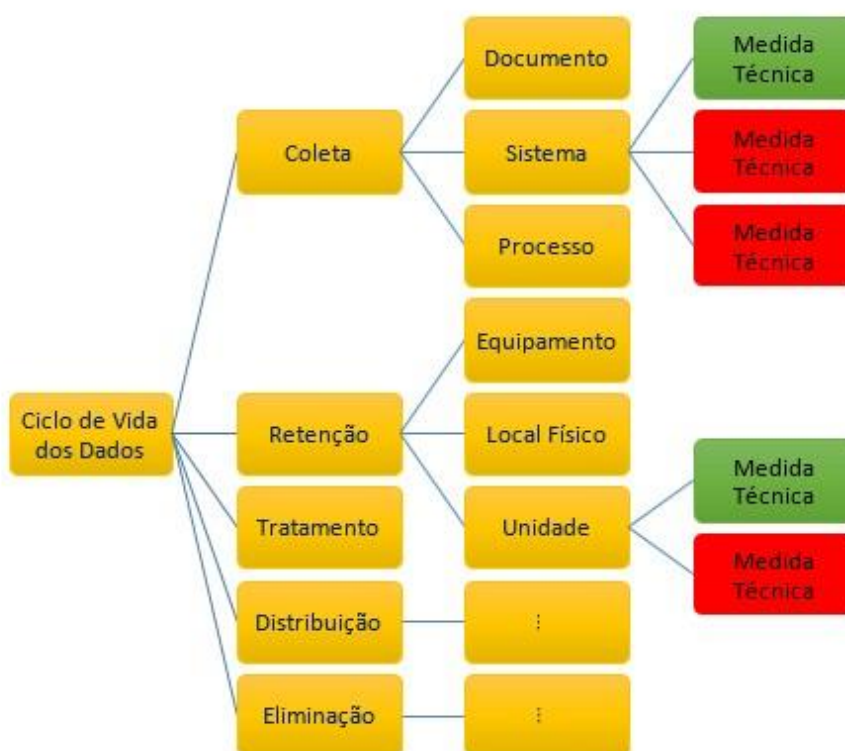
Por exemplo, a figura abaixo apresenta o relacionamento entre as fases do ciclo de tratamento de dados pessoais e os ativos que podem ser utilizados em cada etapa. É importante registrar, assim, que existem ativos presentes em todas as fases do ciclo (ex: Documento) e outros que estarão em apenas algumas delas (ex: Pessoa).



Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD. Recomenda-se a utilização de algum framework, boa prática ou norma

técnica aplicável como a **ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos**; **ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação**; **ABNT NBR ISO/IEC 27701 Técnicas de segurança – Extensão da ABNT NBR ISO/ IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes**; **ISO/IEC 29151 – Code of practice for personally identifiable information protection**; **CIS® (Center for Internet Security, Inc.®) Controls™** e **ISO/IEC 29134 - Guidelines for privacy impact assessment**.

O resultado dessa análise vai determinar quais medidas de segurança devem ser implementadas em cada ativo e quais devem ser ajustadas para que o órgão público possua o adequado grau de proteção de dados exigido pela LGPD. A figura a seguir apresenta esquema de mapeamento dos ativos e suas respectivas **medidas de segurança** implementadas (destacadas em verde) e não implementadas (destacadas em vermelho).



3.4 PLANO DE AÇÃO DOS TRABALHOS DE ADEQUAÇÃO DA LEI GERAL DE PROTEÇÃO DOS DADOS PESSOAIS

Objetivando auxiliar na implementação e adequação à LGPD na Administração Pública Estadual, apresentamos, a título de sugestão, roteiro contendo 5 fases, caracterizadas por atividades e ações relevantes. A aplicabilidade da proposta, a critério do gestor público, pode servir de base para os trabalhos a serem desenvolvidos, respeitadas as limitações. O prazo poderá ser estabelecido de acordo com a conveniência, necessidade e oportunidade de cada órgão e entidade.

FASE	ATIVIDADE	AÇÃO
1	LEVANTAMENTO DE PROCESSOS, CONTRATOS E INVENTÁRIO DE DADOS PESSOAIS	Realizar levantamento dos processos do órgão
		Realizar levantamento de documentos e normativos, administrativos que tenham relação com a proteção de dados pessoais
		Calibrar/validar instrumento para realizar inventário de dados pessoais
		Realizar inventário de dados pessoais no órgão
		Levantamento de contratos relacionados a dados pessoais
		Definir plano de divulgação e treinamento sobre LGPD e implantação da conformidade

FASE	ATIVIDADE	AÇÃO
2	FALHAS, RISCOS E TRATAMENTO	Realizar análise de riscos diante das informações do inventário
		Elaborar relatório de impacto de proteção de dados - RIPD
		Identificar pontos falhos na proteção aos dados pessoais (<i>gap analysis</i>)
		Propor medidas para sanar as falhas referentes à proteção de dados pessoais
		Propor ações corretivas/ mitigadoras dos riscos apontados
		Elaborar e publicar política e diretrizes de privacidade e proteção de dados pessoais no site institucional (versão interna) – Decreto Estadual n. 15.572/2020
		Aprimorar política de segurança da informação
		Realizar adequação de contratos
		Cultura interna de proteção de dados pessoais e segurança da informação: comunicação, treinamento, sensibilização dos servidores

FASE	ATIVIDADE	AÇÃO
3	IMPLEMENTAÇÃO DAS MEDIDAS DE CONFORMIDADE	Propor cronograma de trabalho de implementação das medidas de conformidade
		Atribuir responsáveis pelas ações (matriz de responsabilidade)

FASE	ATIVIDADE	AÇÃO
4	ATENDIMENTO E PLANO DE CONTINGENCIAMENTO	Estabelecer plano de respostas para as solicitações dos titulares (definir processos, destacar prazos, padronizar práticas)
		Definir funcionamento de canal de comunicação com os titulares
		Elaborar plano de resposta e divulgação para o caso de incidentes (vazamento ou uso irregular) de dados pessoais

FASE	ATIVIDADE	AÇÃO
5	MONITORAMENTO	Indicadores de desempenho
		Diagnóstico de maturidade e análise de resultados
		Reporte de resultados à alta administração
		Gestão de incidentes

4

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

4.1 PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO (PRIVACY BY DESIGN E BY DEFAULT)

4.1.1 Privacidade desde a concepção

Os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, pois ambas estão relacionadas.

Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de **medidas de segurança, técnicas e administrativas**.

Art. 46. Os agentes de tratamento 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

O art. 46, § 2º menciona que as **medidas de segurança**, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Isso apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais denominado **Privacidade desde a Concepção** (do inglês *Privacy by Design*).

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009) destacados nas próximas subseções deste tópico.

4.1.1.1 Proativo, e não reativo; preventivo, e não corretivo

A abordagem de Privacidade desde a Concepção (PdC) é caracterizada por medidas proativas e não reativas. Ou seja, essa abordagem antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem nem ofereçam soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram. Em resumo, a Privacidade desde a Concepção vem antes do fato, não depois.

Se aplicada a tecnologias da informação, práticas organizacionais, projeto físico ou em rede de ecossistemas de informação, a PdC começa com um reconhecimento explícito do valor e dos benefícios de adoção de práticas de privacidade fortes, de forma precoce e consistente. Por exemplo, prevenindo a ocorrência de violações de dados, internas ou externas. Isso implica:

- um compromisso claro da alta administração em definir e fazer cumprir altos padrões de privacidade;
- um compromisso de privacidade comprovadamente compartilhado pelas comunidades de usuários e pelas partes interessadas e inserido em uma cultura de melhoria contínua; e
- métodos estabelecidos para reconhecer projetos de privacidade inadequados, antecipar práticas inadequadas de privacidade e corrigir quaisquer impactos negativos, muito antes de ocorrerem.

4.1.1.2 Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio

A privacidade por padrão procura oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

Com relação aos documentos arquivísticos, a privacidade precisa ser resguardada de acordo com legislação vigente, seguindo os procedimentos de gestão de documentos. Os sistemas que mantêm e gerenciam documentos arquivísticos devem ter controles para garantir esse resguardo, conforme descrito nos instrumentos aprovados pelo CONARQ, por meio da Resolução nº 25, de 27 de abril de 2007, que aprova o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil, e da Resolução nº 39, de 29 de abril de 2014, que aprova as diretrizes para Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq).

4.1.1.3 Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios. Isto significa que não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

A privacidade deve ser incorporada às tecnologias, operações e arquiteturas de informação de maneira holística, integrativa e criativa:

- holística significa que contextos adicionais mais amplos devem sempre ser considerados;
- integrativa indica que todas as partes interessadas devem ser consultadas; e
- criativa, pois incorporar privacidade às vezes significa reinventar as escolhas atuais quando as alternativas forem inaceitáveis.

Para alcançar esse objetivo, deve-se adotar uma abordagem sistemática apoiada em padrões e frameworks reconhecidos, os quais necessitam ser revistos e passíveis de auditorias externas. Todas as práticas de informação equitativa precisam ser aplicadas com igual rigor a cada etapa do projeto e da operação.

O impacto do uso, configuração incorreta ou erros relativos à tecnologia, à operação ou à arquitetura de informações sobre a privacidade devem ser comprovadamente minimizados. Por isso, avaliações de impacto e risco na privacidade devem ser realizadas e publicadas, documentando claramente os riscos à privacidade e todas as medidas tomadas para mitigá-los. A seção 2.5 deste documento apresenta orientações referentes à elaboração de Relatório de Impacto à Proteção dos Dados Pessoais.

4.1.1.4 Funcionalidade total

A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade. A PdC é habilitadora duplamente em natureza, permitindo funcionalidade total com resultados reais e práticos.

Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.

A questão da privacidade é frequentemente vista como de nenhuma ou baixa relevância e que compete com a objetividade do projeto, com as capacidades técnicas de um produto ou serviço e com outros interesses das partes envolvidas. A PdC visa justamente contrapor essa visão, pois objetiva satisfazer todos os objetivos da instituição, e não somente os de privacidade. Evitando a pretensão de dicotomias falsas, como privacidade X segurança, o PdC demonstra que é possível — e mais desejável — ter ambos.

4.1.1.5 Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados

Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. Não deve haver lacunas na proteção ou na prestação de contas. O princípio “Segurança” tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade.

As instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões.

Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo art. 6º, inciso VII.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII - segurança: utilização de medidas 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 difusão;

4.1.1.6 Visibilidade e Transparência

A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Esse cenário pode ser sintetizado pelo seguinte lema: confie, mas verifique!

Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança. A avaliação independente deste princípio fundamental deve concentrar-se, especialmente, sobre os seguintes aspectos:

● **Responsabilização** - A coleta de dados pessoais implica um dever de cuidar de sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuído a um indivíduo especificado. E ao transferir dados pessoais para terceiros, medidas equivalentes de proteção à privacidade devem ser asseguradas por contratos ou outros tipos de acordos formais.

● **Abertura** - Abertura e transparência são fundamentais para a prestação de contas. Informações sobre as políticas e práticas relacionadas ao gerenciamento de dados pessoais devem estar prontamente disponíveis para consulta dos titulares de dados. Mecanismos de reclamação e reparação dos dados pessoais devem ser estabelecidos e comunicados para os titulares dos dados.

● **Conformidade** - As etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade devem ser estabelecidas.

A responsabilização, abertura e transparência estão expressas na LGPD pelos seguintes princípios destacados no art. 6º:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; e

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4.1.1.7 Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados.

Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

Empoderar os titulares de dados a desempenhar um papel ativo no gerenciamento de seus próprios dados pessoais pode ser o meio mais eficaz de verificação contra abusos de e uso indevido. O respeito à privacidade do titular dos dados pessoais é suportado pelos seguintes aspectos:

- **Consentimento ou hipótese de tratamento prevista em lei** - é necessário o consentimento livre e específico do titular dos dados para a coleta, uso ou divulgação de dados pessoais, exceto onde permitido por lei. As hipóteses de tratamento de dados pessoais e dados pessoais sensíveis estão preconizadas pelos arts. 7º e 11 da LGPD.
- **Precisão** - os dados pessoais devem ser precisos, completos e atualizados, conforme necessário para cumprir finalidades especificadas.
- **Acesso** - os titulares devem ter acesso aos seus dados pessoais e ser informados do uso e divulgação de tais dados. Os mencionados titulares devem ser capazes de contestar a precisão e integridade dos dados e alterá-los conforme apropriado.
- **Conformidade** - as instituições devem estabelecer mecanismos de reclamação e reparação e comunicar informações sobre eles ao público.

4.1.2 Privacidade desde a concepção

Os agentes de tratamento devem implementar medidas adequadas para garantir que, por padrão, apenas serão processados os dados pessoais necessários para cumprimento da(s) finalidade(s) específica(s) definida(s) pela instituição que desempenha o papel de controlador dos dados pessoais.

Essa obrigação de implementação significa que a instituição deve limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Essa medida deve garantir, por exemplo, que nem todos os usuários dos agentes de tratamento tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pela instituição.

Na LGPD, a **Privacidade por Padrão** (do inglês Privacy by Default) está diretamente relacionada ao princípio da necessidade, expresso pelo art. 6º, inciso III.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

A privacidade por padrão é obtida por meio da adoção das seguintes práticas:

- **Especificação da finalidade** - os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados antes ou no momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.
- **Limitação da coleta** - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.
- **Minimização dos dados** - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser

minimizada. A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada.

● **Limitação de uso, retenção e divulgação** - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Dessa forma, as configurações padrão devem ser as de maior proteção à privacidade.

4.2 PADRÕES FRAMEWORKS E CONTROLES DE SEGURANÇA DA INFORMAÇÃO

É importante ter e seguir um conjunto de documentos para melhorar o gerenciamento de riscos de segurança cibernética. Um framework, por exemplo, apresenta condutas e recomendações para que sejam aplicados princípios e práticas recomendadas de gerenciamento de riscos para melhorar a segurança e a resiliência.

4.2.1 ABNT NBR ISO/IEC 27001:2013. Sistemas de gestão da segurança da informação

É uma norma do comitê técnico formado pela ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), aprovada e traduzida pela Associação Brasileira de Normas Técnicas (ABNT) - e transformada em uma Norma Brasileira (NBR) - de gestão de segurança da informação. São apresentados os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gestão da Segurança da Informação (SGSI), bem como os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização.

A ABNT NBR ISO/IEC 27001:2013 é dividida em 11 seções e Anexo A, sendo que as seções de 0 a 3 são introdutórias (não obrigatórias), e as seções de 4 a 10 são obrigatórias. Controles do Anexo A devem ser implementados apenas se declarados como apropriados e aplicáveis na Declaração de Aplicabilidade.

4.2.2 ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de segurança da informação

Estipula melhores práticas para apoiar a implantação do SGSI, com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Esta norma contém 14 seções de controles de segurança da informação, de um total de 35 objetivos de controles e 114 controles. A parte principal da norma se encontra distribuída nas seguintes seções:

- Seção 5 – Política de Segurança da Informação;
- Seção 6 – Organização da Segurança da Informação;
- Seção 7 – Gestão de ativos;
- Seção 8 – Segurança em recursos humanos;
- Seção 9 – Segurança física e do ambiente;
- Seção 10 – Segurança das operações e comunicações;
- Seção 11 – Controle de acesso;
- Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas;
- Seção 13 – Gestão de incidentes de segurança da informação;
- Seção 14 – Gestão da continuidade do negócio; e

- Seção 15 – Conformidade.

4.2.3 ABNT NBR ISO/IEC 27005:2019. Gestão de riscos de segurança da informação.

Esta norma apresenta diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um SGSI, conforme a NBR ISO/IEC 27001.

As atividades do processo de gestão de riscos de segurança da informação, apresentadas na Seção 6, são detalhadas nas seguintes seções:

- Seção 7 - definição do contexto;
- Seção 8 - processo de avaliação de riscos;
- Seção 9 - tratamento do risco de segurança da informação;
- Seção 10 - aceitação do risco de segurança da informação;
- Seção 11 - comunicação e consulta do risco de segurança da informação; e
- Seção 12 - monitoramento e análise crítica de riscos de segurança da informação.

Os anexos apresentam informações adicionais para as atividades de gestão de riscos de segurança da informação:

- Anexo A - Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação;
- Anexo B - Identificação e valoração dos ativos e a avaliação do impacto são discutidas;
- Anexo C - Exemplos de ameaças comuns;
- Anexo D - Vulnerabilidades e métodos para avaliação de vulnerabilidades;
- Anexo E - Exemplos de abordagens para o processo de avaliação de riscos de segurança da informação;
- Anexo F - Restrições relativas à modificação do risco; e
- Anexo G - Diferenças nas definições entre a NBR ISO/IEC 27005:2011 e a NBR ISO/IEC 27005:2019.

4.2.4 ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes.

É um documento com recomendações para gerenciar riscos enfrentados pelas organizações, podendo ser personalizado para qualquer contexto. A versão do ano de 2018 apresenta um guia mais claro e conciso, com o intuito de ajudar as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

4.2.5 ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/ IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Visa a gestão da privacidade no contexto da organização.

4.2.6 Resoluções do CONARQ.

O Conselho Nacional de Arquivos - CONARQ é um órgão colegiado, vinculado ao Arquivo Nacional do Ministério da Justiça e Segurança Pública, que tem por finalidade definir a política nacional de arquivos públicos e privados, como órgão central de um Sistema Nacional de Arquivos, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo.

No que se refere aos aspectos tecnológicos de gestão arquivísticas de documentos, o CONARQ editou as resoluções indicadas a seguir:

4.2.6.1 Resolução Nº 25, de 27 de abril de 2007.

Resolução que dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

4.2.6.2 Resolução Nº 39, de 29 de abril de 2014.

Resolução que estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR). [Redação dada pela Resolução nº 43 de 04 de setembro de 2015].

Anexo I

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

<Local>, <dia> de <mês> de <ano>

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os 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 risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

Operador

Encarregado

E-mail Encarregado

Telefone Encarregado

2. NECESSIDADE DE ELABORAR O RELATÓRIO

3. DESCRIÇÃO DO TRATAMENTO

3.1 NATUREZA DO TRATAMENTO

3.2 ESCOPO DO TRATAMENTO

3.3 CONTEXTO DO TRATAMENTO

3.4 FINALIDADE DO TRATAMENTO

4. PARTES INTERESSADAS CONSULTADAS

5. NECESSIDADE E PROPORCIONALIDADE

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P1	I2	NÍVEL DE RISCO (P X I) ³

Legenda: P – Probabilidade; I – Impacto.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

7. MEDIDAS PARA TRATAR OS RISCOS

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO ¹	RISCO RESIDUAL ²			MEDIDA(S) ³ APROVADA(S)
			P	I	(P X I)	

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.
3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8. APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<hr/> <p><Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano></p>	<hr/> <p><Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano></p>
AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
<hr/> <p><Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano></p>	<hr/> <p><Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano></p>