SANTA MARCELINA SAÚDE

Treinamento de LGPD

NOVEMBRO - 2025

Orientações Gerais sobre a Lei nº 13.709/2018 (LGPD)

Introdução

Qual o objetivo da LGPD?

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi criada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

A quem se aplica?

- ❑ Pessoas físicas ou naturais;
- ❑ Pessoas jurídicas de direito público;
- ❑ Pessoas jurídicas de direito privado.

Os Hospitais e Serviços de Saúde estão sujeitos à LGPD?

Sim. A LGPD dispõe acerca do tratamento dos dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado (art. 1º da Lei 13.709/2018), sendo que na esfera da Saúde, possui considerável relevância, tendo em vista as importantes informações transacionadas nesta área, principalmente ao se considerar que os dados de Saúde alcançam o íntimo do paciente e das relações estabelecidas pelas instituições

Fonte: LGPD na Saúde – OAB Distrito Federal

Fundamentos da Proteção de Dados

I Respeito à privacidade

II Autodeterminação informativa

III Liberdade de expressão, de informação, de comunicação e de opinião

IV Inviolabilidade da intimidade, da honra e da imagem

V Desenvolvimento econômico e tecnológico e a inovação

VI Livre iniciativa, a livre concorrência e a defesa do consumidor

VII Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais

Conceitos Importantes e Agentes de acordo com a LGPD

Dado Pessoal

Informação relacionada à pessoa natural identificada ou identificável;

Dado Pessoal Sensível

Origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;

Dado anonimizado

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Conceitos Importantes e Agentes de acordo com a LGPD

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Controlador

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD);

Encarregado

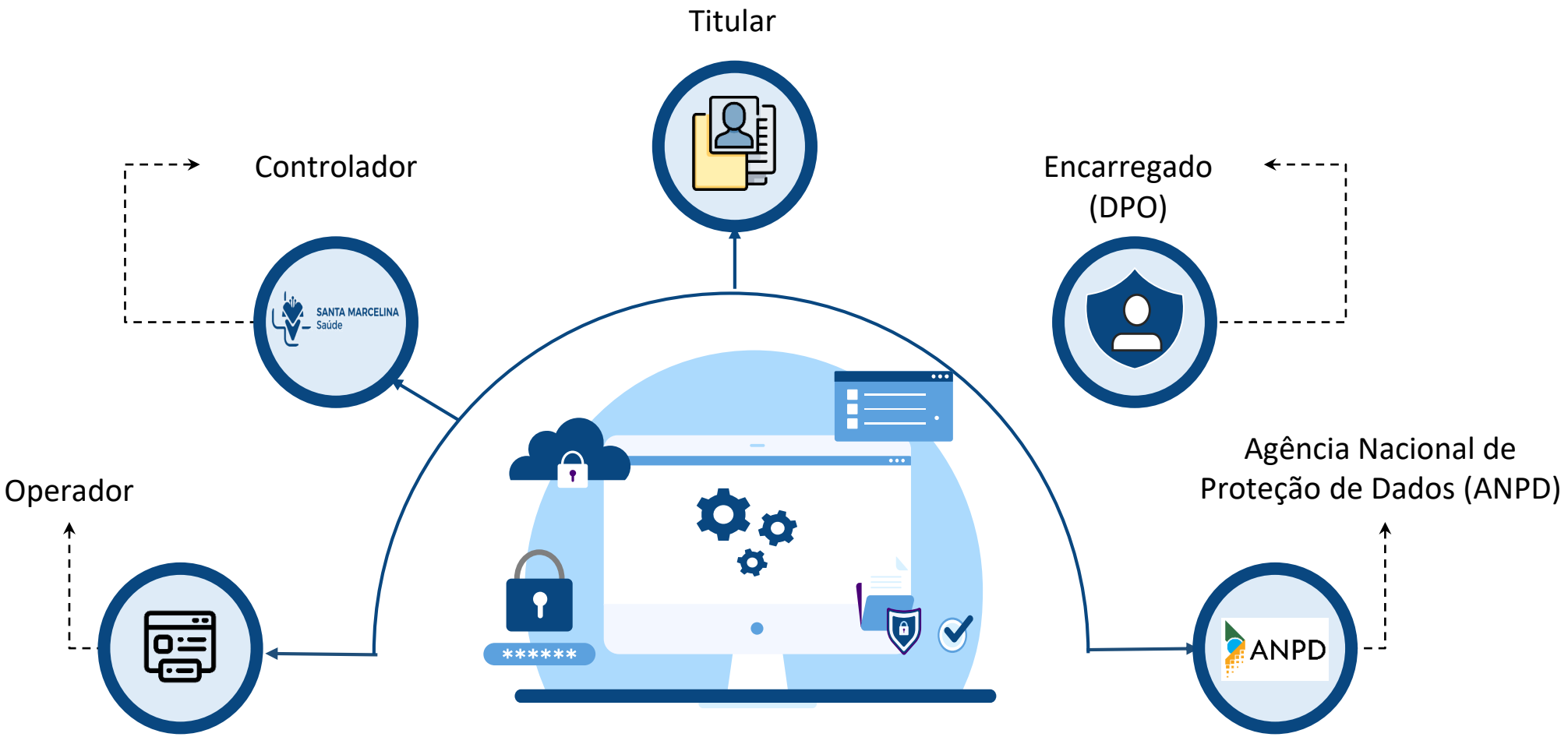
DPO

Tratamento

Coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Principais Atores da LGPD

Quem são as partes envolvidas na LGPD?



Papéis e Responsabilidades

Responsabilidades do Titular de Dados

- Seguir todas as normas de privacidade e proteção dos dados pessoais;
- Seguir e acompanhar os treinamentos;
- Cuidar com zelo dos dados pessoais dos titulares, dentre outras normas contidas nas Políticas da Organização.

Responsabilidades do Controlador

SANTA MARCELINA Saúde

- Controlar como os dados serão coletados e usados;
- Definir quais dados serão coletados;
- Define por quanto tempo esses dados serão retidos;
- Definir com quem os dados serão compartilhados;
- Definir as medidas de seguranças que serão aplicadas;
- Realizar auditoria nos Operadores dos Dados;
- Determina quem tem o acesso a esses dados.

Responsabilidades do Operador

- Seguir as instruções do controlador;
- Firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;
- Dar ciência ao controlador em caso de contrato com suboperador.

Fonte: Cartilha - Lei Geral de Proteção de Dados Pessoais da OAB Minas Gerais

Qual a responsabilidade dos colaboradores(as) da Santa Marcelina Saúde em relação à LGPD?

Não realizar o tratamento do dado para fins discriminatórios, ilícitos ou abusivos (Princípio da Não Discriminação)

Prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção)

Garantir que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação)

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)

Fonte: Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

Responsabilidade do Encarregado de Dados (DPO)

I – Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;

II – Receber comunicações da ANPD e adotar providências;

III – Orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – Executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Atenção

Cabe, ao Encarregado, nos termos do art. 10, inciso II, da Resolução CD/ANPD nº 18, de 16 de julho de 2024 , prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação.

Fonte: Art. 15, incisos I a IV e o parágrafo único da Resolução CD/ANPD nº 18, de 16 de julho de 2024

Quadro Comparativo das Obrigações do Controlador e do Operador segundo a LGPD

Obrigação	Previsão Legal	Aplicável ao Controlador	Aplicável ao Operador
Definir as bases legais para o tratamento de dados pessoais	Art. 7º e incisos da Lei nº 13.709/2018	✓	✗
Fornecer informação para os titulares de dados sobre as atividades de tratamento de dados pessoais	Art. 7º, Art. 8º, § 6º, Art. 9º e Art. 14, §2º, todos da Lei nº 13.709/2018	✓	✗
Assegurar a transparência do tratamento de dados pessoais quando baseado no legítimo interesse do controlador	Art. 10, §2º da Lei nº 13.709/2018	✓	✗
Fornecer Relatório de Impacto à Proteção de Dados (RIPD) para a ANPD, se solicitado, quando o tratamento tiver base no legítimo interesse	Art. 10, §3º da Lei nº 13.709/2018	✓	✗
Verificar se o consentimento foi dado pelo responsável legal da criança ou do adolescente	Art. 14, §5º da Lei nº 13.709/2018	✓	✗

Quadro Comparativo das Obrigações do Controlador e do Operador segundo a LGPD

Obrigação	Previsão Legal	Aplicável ao Controlador	Aplicável ao Operador
Eliminar os dados pessoais após o término de seu tratamento atividade de tratamento	Art. 16 da Lei nº 13.709/2018	✓	✓
Receber e responder requisições relacionadas aos direitos dos titulares de dados pessoais e informar outros controladores e operadores das ações necessárias para cumprir tais requisições	Art. 18 e §6º da Lei nº 13.709/2018	✓	✗
Cooperar com o controlador para responder em tempo hábil as requisições feitas pelos titulares de dados pessoais	Implícito	✗	✓
Estabelecer mecanismos e salvaguardas apropriadas para a transferência de dados	Art. 33, inciso II, da Lei nº 13.709/2018	✓	✗
Manter registro das operações de tratamento de dados	Art. 37 da Lei nº 13.709/2018	✓	✓

Quadro Comparativo das Obrigações do Controlador e do Operador segundo a LGPD

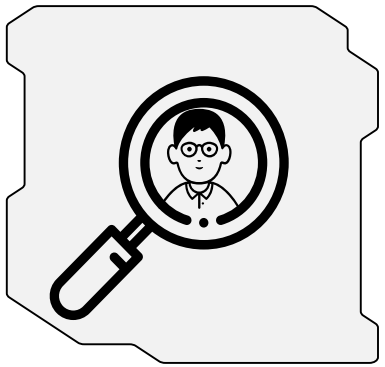
Obrigação	Previsão Legal	Aplicável ao Controlador	Aplicável ao Operador
Fornecer Relatório de Impacto à Proteção de Dados Pessoais à ANPD, inclusive de dados sensíveis, quando solicitado.	Art. 38 da Lei nº 13.709/2018	✓	✗
Tratar dados pessoais seguindo as instruções dos controladores	Art. 39 da Lei nº 13.709/2018	✗	✓
Indicar um Encarregado de Dados ou DPO	Art. 41 da Lei nº 13.709/2018	✓	✗
Adotar medidas técnicas e organizacionais para a assegurar a segurança dos dados pessoais	Art. 46 e art. 47 da Lei nº 13.709/2018	✓	✓
Estar sujeito à sanções administrativas aplicáveis pela ANPD	Art. 52 Lei nº 13.709/2018	✓	✓

Dado Pessoal X Dado Pessoal Sensível - Exemplos

Dado Pessoal

Cookie/ Log (endereço IP + Hora de acesso)

Endereço residencial, comercial ou eletrônico



E-mail Corporativo

Nome, sobrenome; data de nascimento; CPF, RG, CNH; CTPS; passaporte; título de eleitor; matrícula

Número de Telefone

Dado Pessoal Sensível

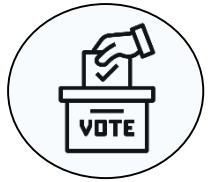
Convicção Religiosa

Referente à saúde ou à vida sexual

Dado genético ou biométrico

Origem racial ou étnica

Filiação a sindicato ou a organização de caráter religioso ou filosófico



Opinião Política

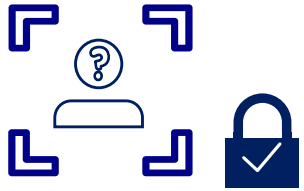
Fonte: Cartilha - Lei Geral de Proteção de Dados – Tribunal Regional do Trabalho da 15ª Região

Dado Anonimizado X Dado Pseudoanonimizado

Dado Anonimizado

Os dados anonimizados, segundo a LGPD, não serão considerados dados pessoais, salvo, quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Dado Pseudoanonimizado



É o dado pessoal sem associação direta ou indireta ao titular, senão pelo uso de informação adicional mantida separadamente em ambiente controlado e seguro. A pseudonimização é reversível, pois existem informações adicionais que reestabelecem a ligação entre os dados pseudonimizados e a identidade do titular.

Fonte: Cartilha LGPD – Lei Geral de Proteção de Dados Pessoais - Portos Rio

Princípios Norteadores da Lei nº 13.709/2018 (LGPD)

Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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;

Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

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;

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

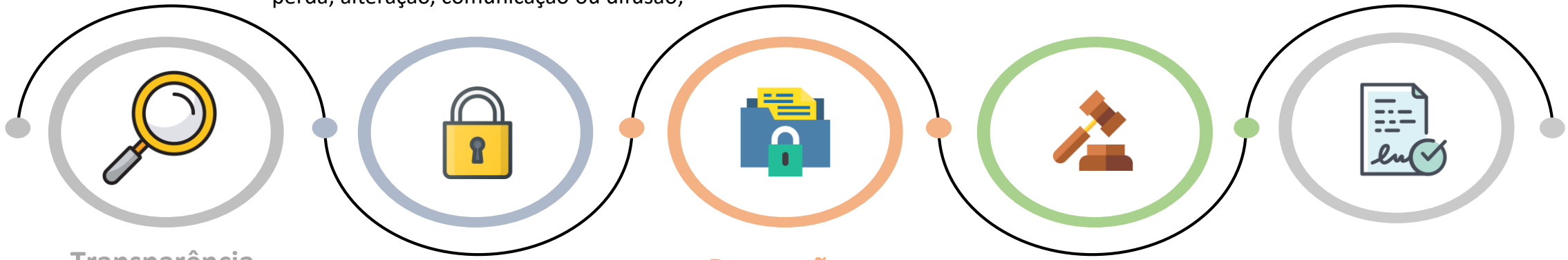
Fonte: Art. 6º da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

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;

Não Discriminação

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;



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;

Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

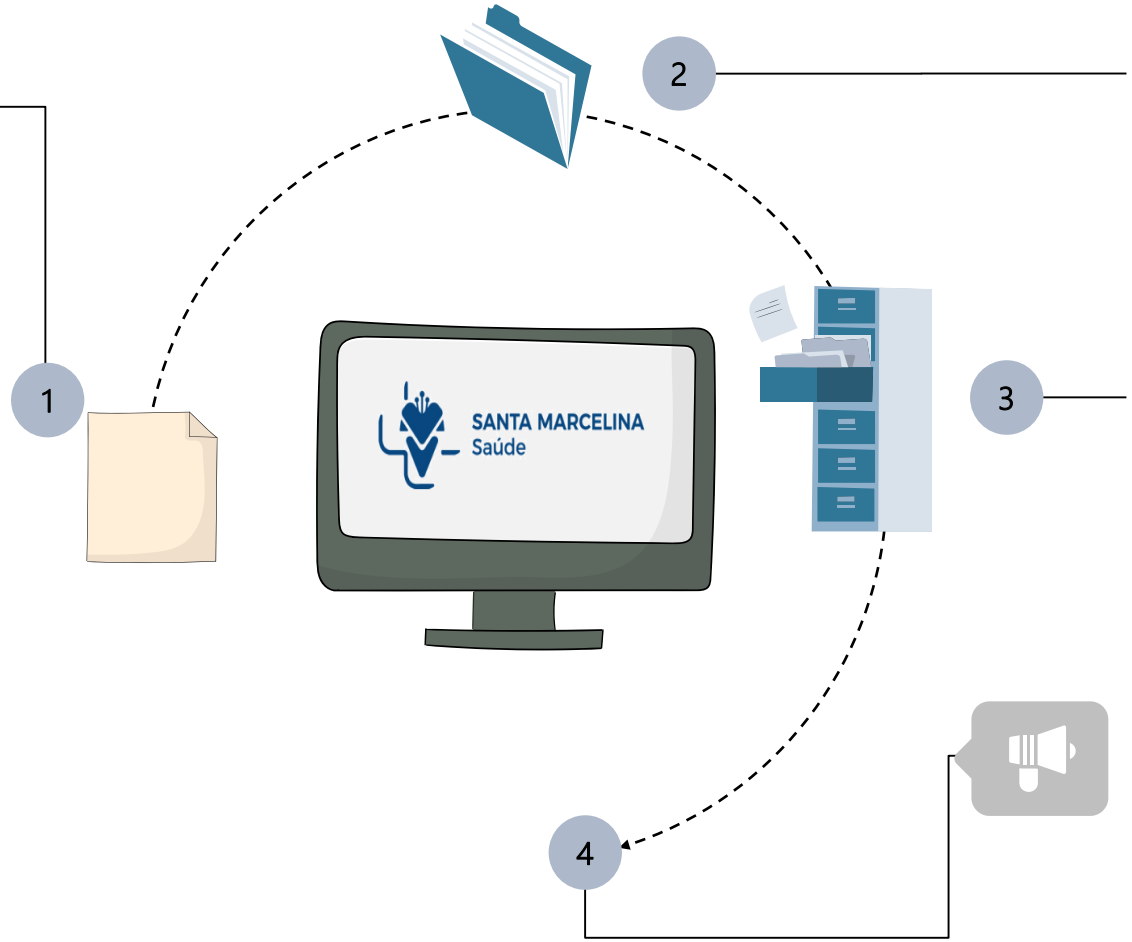
Accountability

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.

Fonte: Art. 6º da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

O cenário abaixo está em conformidade com a LGPD?

Recebi um documento, seja ele um contrato, formulário ou qualquer outro tipo de papel, de forma física (em papel) ou digital (em formato eletrônico).



Armazenei na pasta física ou digital para utilizar em determinada finalidade.

Uma outra área solicitou o documento para uma finalidade diferente daquela para a qual os dados foram coletados.

Posso encaminhar o documento à área?

Direitos do Titular de Dados

Direitos do Titular

A propriedade do dado pessoal é garantida a seu titular, ao qual também são outorgados os direitos fundamentais à liberdade, privacidade e intimidade, além de todos os direitos estabelecidos na LGPD

- Confirmação da existência de tratamento;
- Acesso ao dado pessoal;
- Retificação de dados pessoais incompletos;
- Exclusão de dados pessoais;
- Anonimização, bloqueio ou exclusão de dados desnecessários ou excessivos;
- Portabilidade dos dados a outro fornecedor de serviço ou provedor de serviço;
- Informação das entidades públicas e privadas com as quais o Controlador dividiu os dados;
- Informar acerca da possibilidade de não consentir;
- Oposição ao tratamento de dado, se irregular;
- Reclamação à Agência Nacional de Proteção de Dados (ANPD);
- Revogação do Consentimento.

Fonte: Orientações Institucionais – LGPD – Santa Marcelina Saúde

Gestão do Consentimento

A LGPD (Lei Geral de Proteção de Dados) estabelece, em seus artigos 5º e 7º, que o consentimento deve ser livre, informado e inequívoco, com manifestação de vontade clara do titular para o tratamento de seus dados pessoais, para uma finalidade específica.

Consentimento

É a manifestação clara e direta da vontade do titular, geralmente por escrito ou por meio eletrônico, indicando que ele concorda com o tratamento de seus dados para uma finalidade específica.

Exemplo

CONTRATO DE PRESTAÇÃO DE SERVIÇOS MÉDICOS

Contrato que entre si fazem, na melhor forma de direito, de um lado(nome da operadora), com sede na rua ....., nº.....,bairro....., em(nome da cidade), (Estado), inscrita no CNPJ nº.....e registrada na ANS nº....., representada neste ato por seus executivos legalmente constituídos, doravante denominada simplesmente **CONTRATANTE** de outro lado o Dr(a).....,CPFnº....., inscrito no (CRM) sob nº.....,com consultório (ou clínica) na rua.....,nº.....bairro,(cidade), (Estado), doravante denominado simplesmente **CONTRATADO**, os quais livremente e de comum acordo firmam o presente contrato de prestação de serviços médicos que reger-se-á pelas seguintes cláusulas e condições, atendendo ao que dispõe as Leis 9.656/98 e 13.003/14, bem como a Resolução C.F.M. 1.931/09(Código de Ética Médica)

Consentimento sobre Dados Pessoais Sensíveis

O tratamento de dados pessoais sensíveis, conforme a LGPD, exige o consentimento explícito do titular ou de seu responsável legal, e este consentimento deve ser específico e para uma finalidade previamente determinada.

Exemplo

Prontuário/Paciente:
Data Nasc./Idade:
Registro de Atendimento:
Profissional do Atendimento:
Convênio/Plano: **Nr. Carteira:**
Acomodação/Leito: **Data/Hora:** 23/08/2019 - 15:59:03

AVALIAÇÃO MÉDICA DA URGÊNCIA

QUEIXA PRINCIPAL / HISTÓRIA DA DOENÇA ATUAL
teste

ANTECEDENTES PESSOAIS
ASMA: Sim | DIABETES: Sim | HIPERTENSÃO: Sim | CARDIOPATIA: Nao
TVP/TEP: Sim | DPOC: N.A. | TABAGISMO: Nao | ETILISMO: Nao
DOENÇA INFECTO CONTAGIOSA: Nao | OUTRAS DOENÇAS: Sim

EXAME FÍSICO
teset

PLANO TERAPÊUTICO
etset

HIPÓTESES DIAGNÓSTICAS INICIAIS

CONDIÇÃO FÍSICA NA AVALIAÇÃO INICIAL
Deambula

Penalidades

Sanções Administrativas

- I — Advertência
- II — Obrigação de divulgação do incidente
- III — Eliminação de dados pessoais
- IV — Bloqueio, suspensão e/ou proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais
- V — Multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil e no seu último exercício, limitada a 50 MM

Agência deve levar as seguintes questões em consideração:

- Reincidência
- Boa-fé
- Capacidade Financeira
- Proporcionalidade
- Ação Imediata de Medidas Preventivas
- Procedimentos e ferramentas relativas à proteção de dados
- Política de boas práticas de Governança
- Cooperação
- Grau de Dano/Seriedade
- Vantagem obtida ou intencionada

Fonte: Orientações Institucionais – LGPD – Santa Marcelina Saúde

Tratamento de Dados Pessoais

O tratamento de dados pessoais deve pautar-se pela boa-fé, além de observância aos seguintes princípios:

01 Finalidade

Especificada e informada expicitamente ao titular do dado pessoal.

02 Adequação

Á finalidade previamente acordada e divulgada.

03 Necessidade

Do tratamento, limitado ao mínimo necessário para sua finalidade.

04 Livre Acesso

Aos dados, com garantia aos titulares, de consulta facilitada e gratuita

05 Qualidade dos Dados

Garantindo sua exatidão, clareza e atualização.

06 Transparência

Ao titular, com informações claras e acessíveis sobre o tratamento.

07 Segurança

Medidas técnicas e administrativas para proteção dos dados pessoais.

08 Prevenção

Da ocorrência de dados ao titular em virtude do tratamento de dados.

09 Não Discriminação

Impossibilitando o tratamento discriminatório, ilícito ou abusivo.

10 Responsabilidade

Do agente, devendo demonstrar a eficácia das medidas de proteção de dados adotadas.

Fonte: Comitê de Segurança da Informação e Comunicação – Tribunal de Contas do Estado de Rondônia

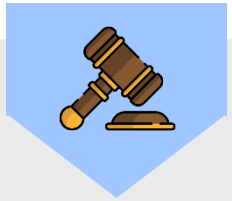
Hipóteses de Coleta de Dados Pessoais

- Mediante o fornecimento de consentimento pelo titular;
- Para cumprimento de obrigação legal ou regulatória;
- Pela administração pública para execução de políticas previstas em leis;
- Para estudos por órgão de pesquisa, desde que mantido o anonimato;
- Para o exercício de contrato do qual é parte o titular dos dados;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiro;
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Fonte: Art. 7º da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

Justificativa para a Coleta de Dados na Saúde

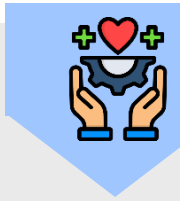
No caso da Santa Marcelina Saúde, a coleta de dados é justificável perante a LGPD quando atende, em geral, a:



Obrigações legais: Conforme exigido pela LGPD.

Obrigações contratuais: Necessário para a execução de um contrato.

Melhora da Assistência ao Paciente, desde da qualificação do atendimento quanto do histórico de consultas.



Gestão e Eficiência dos Serviços de Saúde, incluindo adoção de políticas e pesquisas.

O tratamento de dados pessoais se torna um ponto de atenção e inadequado perante a LGPD quando:

É excessivo em relação à finalidade da atividade

1

Coleta-se mais dados do que o estritamente necessário para o objetivo declarado.

Envolve dados sensíveis sem base legal robusta

2

A coleta de dados sensíveis uma base legal ainda mais específica e justificável, além de cuidados redobrados.

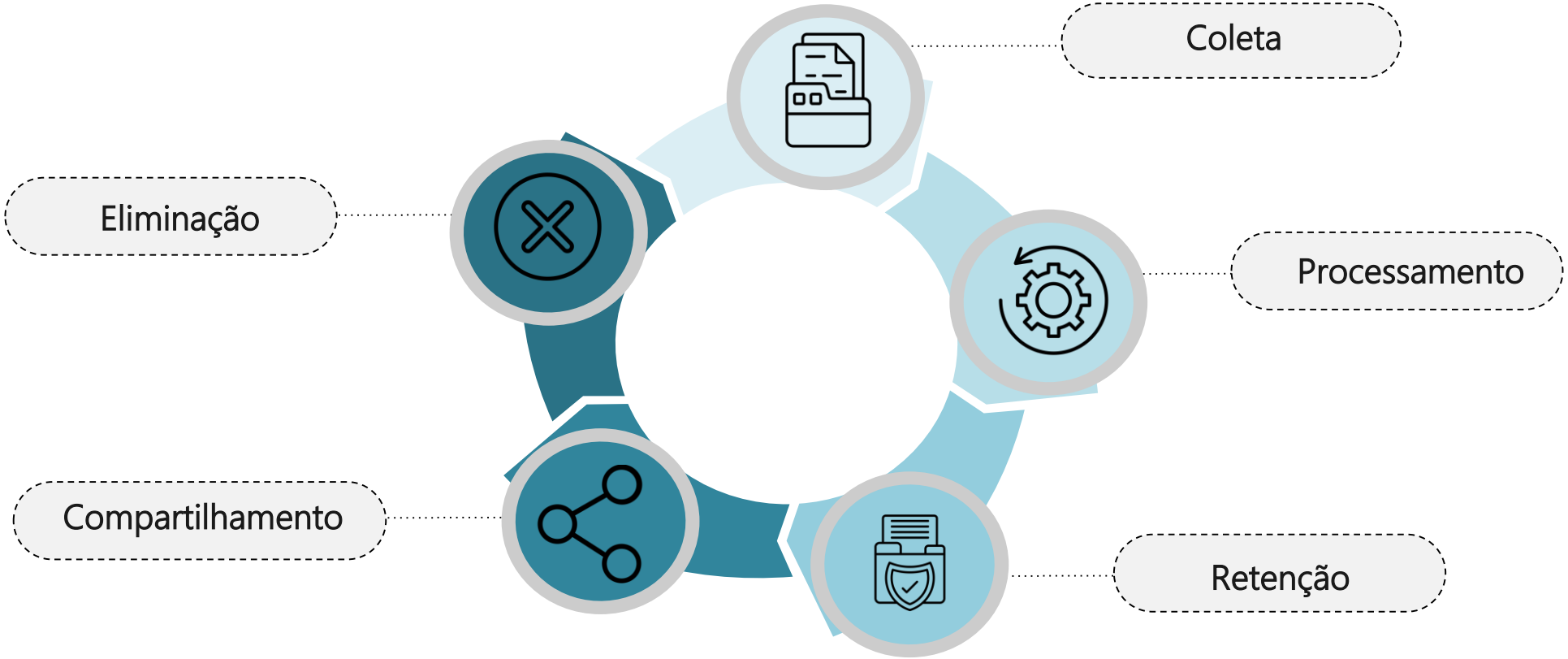
Compromete os direitos e liberdades fundamentais do titular de dados

3

A coleta excessiva ou desnecessária, especialmente de dados sensíveis, pode expor os titulares a riscos.

Ciclo de vida do Tratamento dos Dados Pessoais

O ciclo de vida do tratamento de dados pessoais, segundo a LGPD, pode ser dividido em 05 (cinco) fases principais, a saber:



Fonte: Cartilha LGPD MPRS - Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018

Tratamento de Dados Pessoais - Crianças e Adolescentes

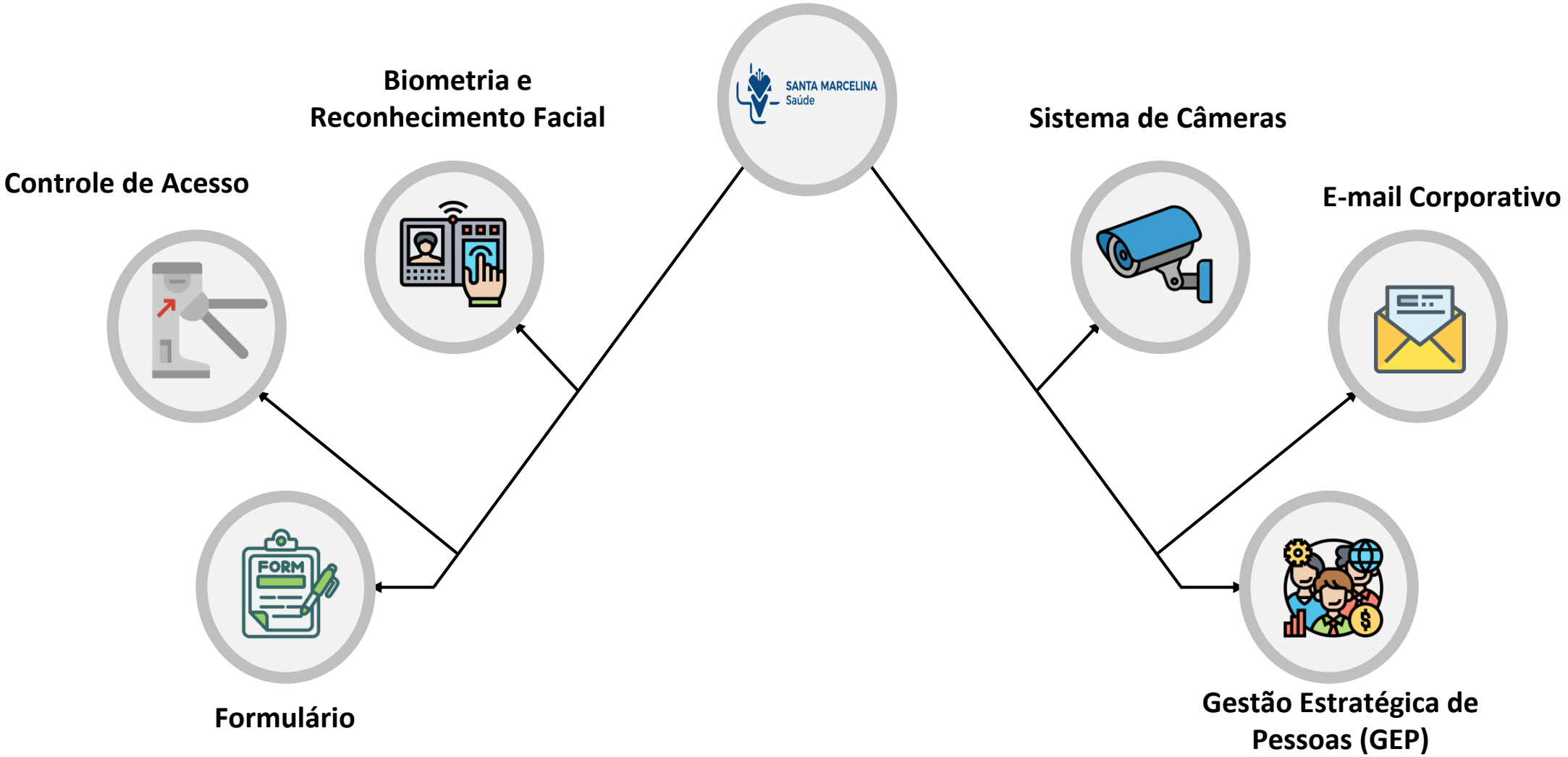
O artigo 2º do Estatuto da Criança e do Adolescente (ECA) estabelece a diferença entre as definições de criança e adolescente da seguinte forma:

- ❑ Criança: 0 à 12 anos incompletos;
- ❑ Adolescente: 12 à 18 anos.

A LGPD estabeleceu, em harmonia com a ordem jurídica brasileira, que todo tratamento de dados pessoais de crianças e adolescentes deve ser realizado **observando o melhor interesse do menor, devendo haver o consentimento específico e destacado de um dos pais ou responsável legal da criança para autorizar o tratamento**, salvo quando for **necessário coletar dados para contatar os pais ou responsável legal ou para a proteção da criança**. Atender ao melhor interesse é refletir sobre a vulnerabilidade e a necessidade de cuidado pelo Estado, família e sociedade.

Fonte: Guia Orientativo – Tratamento de Dados Pessoais de Crianças e Adolescentes - MPCE

Exemplos de Tratamento de Dados Pessoais – Colaboradores(as)



Fonte: Cartilha Lei Geral de Proteção de Dados Pessoais 2021 - LGPD

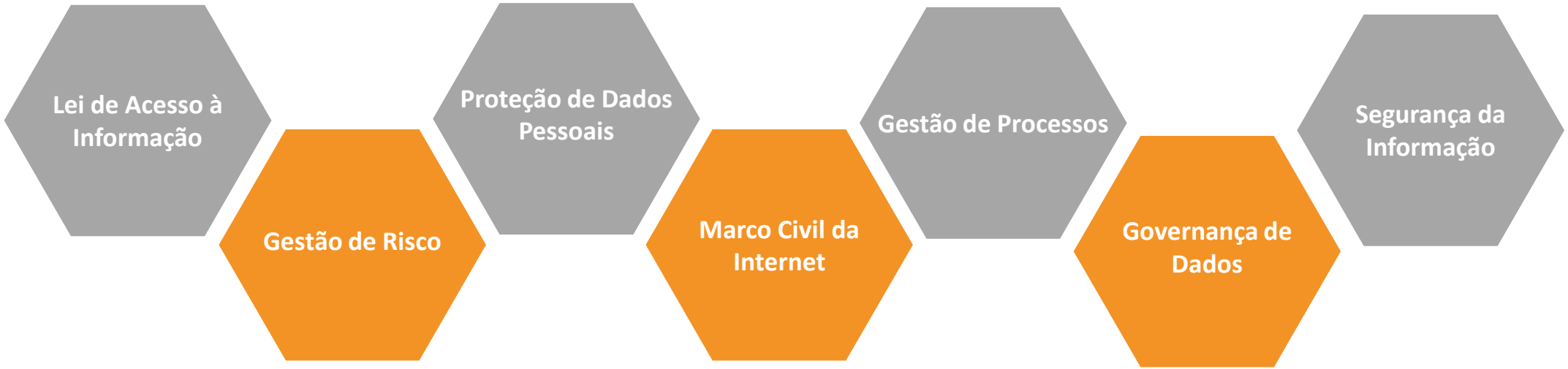
Em quais hipóteses não será exigido o consentimento para o tratamento de dados?

- Para cumprimento de obrigação legal ou regulatória;
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- Para estudos por órgão de pesquisa, desde que mantido o anonimato;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos

Fonte: Art. 7º da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

Requisitos e Conhecimentos

Alinhamento da proteção de dados, conformidade, governança e segurança da informação



GOVERNO DIGITAL E TRANSPARÊNCIA

Introdução à Lei Brasileira de Proteção de Dados Pessoais

GOVERNO DIGITAL E TRANSPARÊNCIA

Proteção de Dados no Setor Público

Fonte: Orientações Institucionais – LGPD – Santa Marcelina Saúde

Fluxograma do Time de Privacidade da Santa Marcelina Saúde

Comitê LGPD da Santa Marcelina Saúde

Monitorar e apoiar o projeto de implantação execução da LGPD.

CONTROLADOR

Representante Legal

Definir prioridades, indicar o Encarregado de Dados, emitir instruções e prestar contas.

ENCARREGADO

Conformidade

Área de Compliance & LGPD da Santa Marcelina Saúde.

OPERADOR

Operações

Órgãos, entidades, pessoas físicas e demais contratadas.

Apoio Técnico

Ouvidoria e Controle Técnico

- Transparência Ativa e Passiva;
- Gestão de Risco;
- Accountability (Prestação de Contas).

Apoio do Jurídico

Jurídico

- Consulta e Pareceres de LGPD;
- Gestão do Risco Jurídico;
- Proposições Normativas.

Apoio da área de Tecnologia da Informação

Área de Tecnologia da Informação

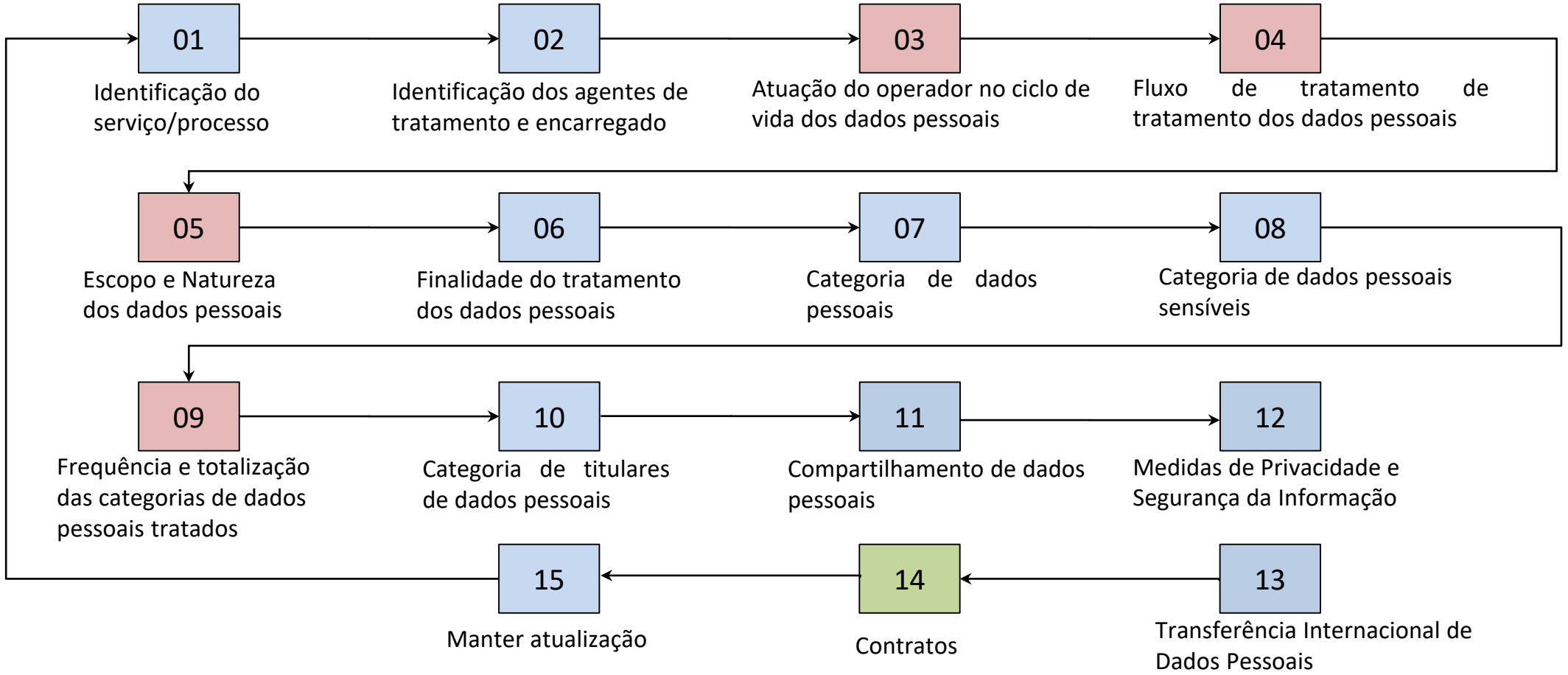
- Gestão de aplicações;
- Gestão da Segurança da Informação;
- Proposições técnicas.

Etapas do Planejamento Estratégico – Adequação à LGPD


SANTA MARCELINA
Saúde
LGPD
1 Alinhamento Estratégico
2 Diagnóstico Preliminar
3 Avaliação de Controles
4 Plano de Implantação de Controles
5 Inventário de Dados Pessoais
6 Política de Privacidade e Termo de Uso
7 Adequação dos Instrumentos Contratuais
8 Sensibilidade Institucional
9 Relatório de Impacto à Proteção de Dados
10 Plano de Gestão de Resposta a Incidentes
11 Transparência da Proteção de Dados Pessoais
12 Tabela de Retenção de Dados Pessoais

Etapas do Planejamento Estratégico - Mapeamento ou Inventário de Dados

O mapeamento de dados, também conhecido como inventário de dados ou *data mapping*, é o processo de identificar, analisar e documentar o fluxo de dados dentro da Santa Marcelina Saúde. O presente documento servirá de subsídio para criação do Relatório de Impacto à Proteção de Dados Pessoais – RIPD da Organização. O fluxograma a seguir destaca as fases de elaboração do inventário.



Fonte: Guia de Elaboração de Inventário de Dados Pessoais - Programa de Privacidade e Segurança da Informação (PPSI)

Relatório de Impacto à Proteção de Dados (RIPD)

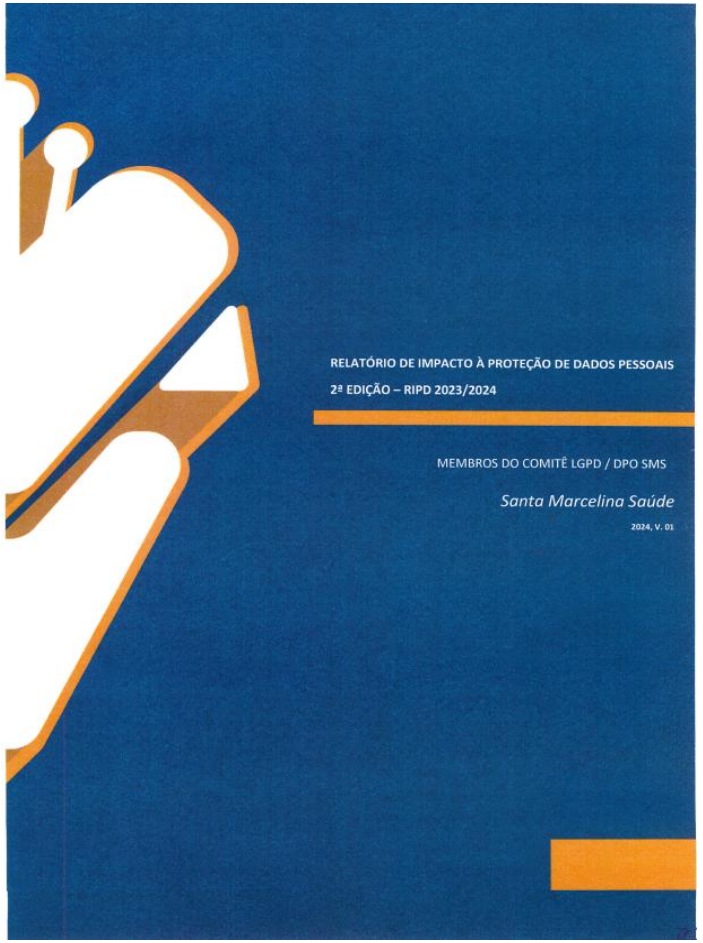
Qual é o objetivo do Relatório de Impacto à Proteção de Dados (RIPD)?

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.

Quais são as etapas do Relatório de Impacto à Proteção de Dados (RIPD)?

1. Identificação dos Agentes de Tratamento e do Encarregado;
2. Necessidade de Elaborar o Relatório;
3. Descrição do Tratamento;
4. Partes Interessadas Consultadas;
5. Necessidade e Proporcionalidade;
6. Identificação e Avaliação de Riscos;
7. Medidas para tratar os riscos;
8. Conclusão.

Exemplo



Acesse o site da Santa Marcelina Saúde, vide: https://santamarcelina.org/, para conferir o documento na íntegra.

Etapas do Planejamento Estratégico – Gestão de Risco

Identificar

Nesta primeira etapa, é importante enumerar todos os riscos encontrados no processo e que possam impactar de forma negativa, no contexto da Lei Geral de Proteção de Dados (LGPD), para a criação de um diagnóstico.

- Mapeamento de Ativos
- Identificação de Ameaças e Vulnerabilidades
- Entrevistas e Análise dos Processos das Áreas
- Mapeamento de Dados Pessoais Coletados

Avaliar

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.

Exemplo de Matriz Probabilidade x Impacto

Classificação	Valor
Baixo	05
Moderado	10
Alto	15

15	75	150	225
10	50	100	150
5	25	50	75
	5	10	15

Mitigar

A partir da avaliação dos riscos, a Organização tomará ações sobre os riscos classificados, propondo controles para tratamento. As medidas recomendadas pelo Subcomitê deverão ser acompanhadas e atualizadas, em intervalos regulares.

- Controle de Processos (Segurança em Redes, Acesso Lógico, Proteção Física do ambiente, entre outros).
- Criação de Documentos
- Campanha de conscientização
- Treinamentos Regulares

Fonte: Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD)

O que é um incidente de Segurança com Dados Pessoais?

Um incidente é uma ocorrência comprovada de divulgação, alteração, perda de dados pessoais ou acesso não autorizado a eles, que impacta a confidencialidade, a integridade ou a disponibilidade das informações.

Exemplos de Incidente de Segurança:

- Violações de Dados
- Vazamento de Dados Pessoais
- Erros Humanos
- Ataques Cibernéticos
- Intrusões de rede
- Acesso não autorizado
- Uso inapropriado
- Exploração de Vulnerabilidade

Etapas do Planejamento Estratégico – Plano de Gestão de Resposta a Incidentes

Comunicar o Encarregado de Dados

01

O conhecimento da ocorrência de incidente de segurança deve motivar uma comunicação ao Encarregado de Dados, o mais rápido possível, a fim de que avalie o conteúdo e adote os mecanismos cabíveis.

Comunicar ao Controlador dos Dados

02

Na sequência, o Encarregado de Dados cientifica a Controladora de Dados, visto que esta detém o poder de decisão sobre o tratamento de dados da Organização.

Caso o Subcomitê de LGPD e o Comitê Institucional concluam que o incidente acarretou risco ou danos relevantes aos titulares de dados, deverão ser realizadas as comunicações obrigatórias previstas na Lei.

Comunicar à Agência Nacional de Proteção de Dados (ANPD)

03

A ANPD deve ser comunicada em prazo razoável, considerando o prazo de 03 (três) dias úteis a partir do momento em que o controlador toma conhecimento do incidente que afetou dados pessoais.

Comunicar ao Titular dos Dados Pessoais

04

O titular dos dados pessoais deverá ser notificado, sendo recomendado pela ANPD que a Notificação seja feita de forma individual e direta. Exemplos: E-mail, Carta, SMS ou mensagem.

Fonte: Plano de Resposta - A Incidente de Segurança com Dados Pessoais - CGE

Etapas do Planejamento Estratégico – Plano de Gestão de Resposta a Incidentes

Identificação do Incidente

Um novo incidente é notificado por colaborador, terceiro ou por alarme de monitoramento.

Notificação

Ao se registrar uma notificação de incidente de segurança da informação e privacidade, é importante inserir informações como: origem, contato, registro, local, recursos utilizados, endereço do alvo, protocolos, servidos envolvidos, descrição do incidente e evidências.

Registro

Nesta etapa, o incidente deverá ser documentado em base de conhecimento apropriada, detalhando as informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Triagem

A etapa de triagem tem como objetivo reunir informações sobre o evento, avaliar a sua natureza, e classificá-lo como incidente para que, adiante, se inicie o processo de tratamento.

Classificação

É importante classificar o incidente a fim de esclarecer e auxiliar no tipo de atendimento a ser realizado e também na definição da sua criticidade, como por exemplo: Conteúdo abusivo, Código malicioso, Prospecção por informações, Tentativa de intrusão e Intrusão entre outros.

Criticidade

Esta etapa tem como objetivo definir uma ordem de atendimento dos incidentes e um SLA de acordo com a urgência de tratamento e o impacto nas áreas Administrativas, Artísticas e Pedagógicas da Santa Marcelina Saúde. Classificação do nível de criticidade: Alto, Médio e Baixo,

Fonte: Plano de Resposta a Incidentes de Segurança do Tribunal Regional do Trabalho da 15ª Região

Etapas do Planejamento Estratégico – Plano de Gestão de Resposta a Incidentes

Situação

Definir uma situação para cada incidente, a qual tem como escopo acompanhar o andamento de tal evento dentro do processo de tratamento. Exemplos: Aberto, Processamento, Pendente, Transferido (quando está pendente pelo Terceiro, Solucionado e Fechado.

Preservação das Evidências

Antes de se iniciar as ações para restaurar as operações do ambiente, é necessária a preservação de provas para a identificação correta da causa raiz do incidente e, posteriormente, para a recuperação dos sistemas afetados.

Processo de Mitigação

O processo de mitigação do incidente envolve as etapas de: preparação, detecção, contenção, erradicação, recuperação e avaliação.

Fonte: Plano de Resposta a Incidentes de Segurança do Tribunal Regional do Trabalho da 15ª Região

Preparação

Prevenir contra incidentes

- Implementar mecanismos de defesa e controle de ameaças.
- Desenvolver procedimentos para lidar com incidentes de forma eficiente.
- Obter recursos e equipe necessária para lidar com os problemas.
- Estabelecer infraestrutura de suporte à atividade de resposta a incidentes.

Detecção

Detectar o incidente

- Identificar todos os sistemas e serviços afetados relacionados com o incidente.
- Avaliar o impacto do incidente e os potenciais riscos dos sistemas afetados (dados vazados).
- Informações de instituições parceiras, impacto na própria organização e na reputação).
- Identificar que tipo de informação e processos podem ter sido afetados.

Contenção

Conter o incidente

- Desconectar o sistema comprometido ou isolar a rede afetada.
- Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque.
- Bloquear padrões de tráfego, interrompendo o fluxo malicioso.
- Desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas.

Erradicação

Eliminar as causas Incidente

- Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente.
- Assegurar a remoção de todos os métodos de acesso utilizados pelo invasor: novas contas de acessos; *backdoors* e, se aplicável, acesso físico ao sistema comprometido.

Recuperação

Restaurar o Sistema

- Restaurar a integridade do sistema.
- Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas.
- Implementar medidas de segurança para evitar novos comprometimentos.
- Restauração do último e íntegro backup completo armazenado.

Avaliação

Avaliar as ações realizadas

- Aprimorar os procedimentos e processos existentes.
- Identificar características de incidentes que podem ser utilizadas para treinar novos membros da equipe.
- Criar métricas relativas ao processo de resposta a incidentes.
- Obter informações que podem ser utilizadas em processos legais.

Fonte: Plano de Resposta a Incidentes de Segurança do Tribunal Regional do Trabalho da 15ª Região

Etapas do Planejamento Estratégico – Estudo de Caso

Recentemente, saiu na mídia uma notícia sobre uma empresa pública federal que identificou um vazamento de dados pessoais que afetou cerca de 2% de sua base de cadastro. O incidente envolveu o acesso indevido ao número de celular vinculado ao CPF de alguns clientes do aplicativo da Estatal.

Chegou a hora! Vamos avaliar juntos o passo a passo das medidas adotadas pela Estatal, desde a avaliação do incidente, notificação para a Agência Nacional de Proteção de Dados (ANPD) e o comunicado aos Titulares de Dados Pessoais.

01. A Estatal teve ciência de um possível incidente de segurança em seu sistema.

02. Assim que a vulnerabilidade foi identificada no sistema, a Estatal agiu imediatamente, implementando medidas protetivas adicionais para proteger as informações.

03. Notificou a Agência Nacional de Proteção de Dados (ANPD), conforme exige a Lei Geral de Proteção de Dados (LGPD).

04. Emitiu um comunicado a diferentes clientes para alertar sobre um vazamento de dados ocorrido no sistema da Estatal.

Lições Aprendidas

- Ao identificar uma vulnerabilidade, comunique imediatamente ao Encarregado de Dados pelo Canal Oficial;
- Adote práticas como: alterar sua senha periodicamente, ativar as verificações em duas etapas e fique atento a mensagens pedindo seus dados.

Tráfego e Transferência Internacional de Dados

A Santa Marcelina Saúde veda a comercialização de quaisquer informações, portanto não aluga, vende e tampouco libera, sob qualquer justificativa, dados a terceiros com a finalidade de permitir qualquer vantagem de seus serviços.

Além disso, é possível que os dados pessoais sejam transferidos e mantidos em ambiente fora do município, estado ou país, regendo-se nestes casos por leis de proteção de dados diferentes, mas com grau de proteção similar ao previsto na LGPD.

Você sabe quais são os mecanismos de Transferência Internacional?

- ❑ Cláusulas-padrão contratuais;
- ❑ Cláusulas-padrão contratuais equivalentes;
- ❑ Cláusulas contratuais específicas;
- ❑ Normas corporativas globais;
- ❑ Decisões de adequação.

Boas práticas de Privacidade e Proteção de Dados

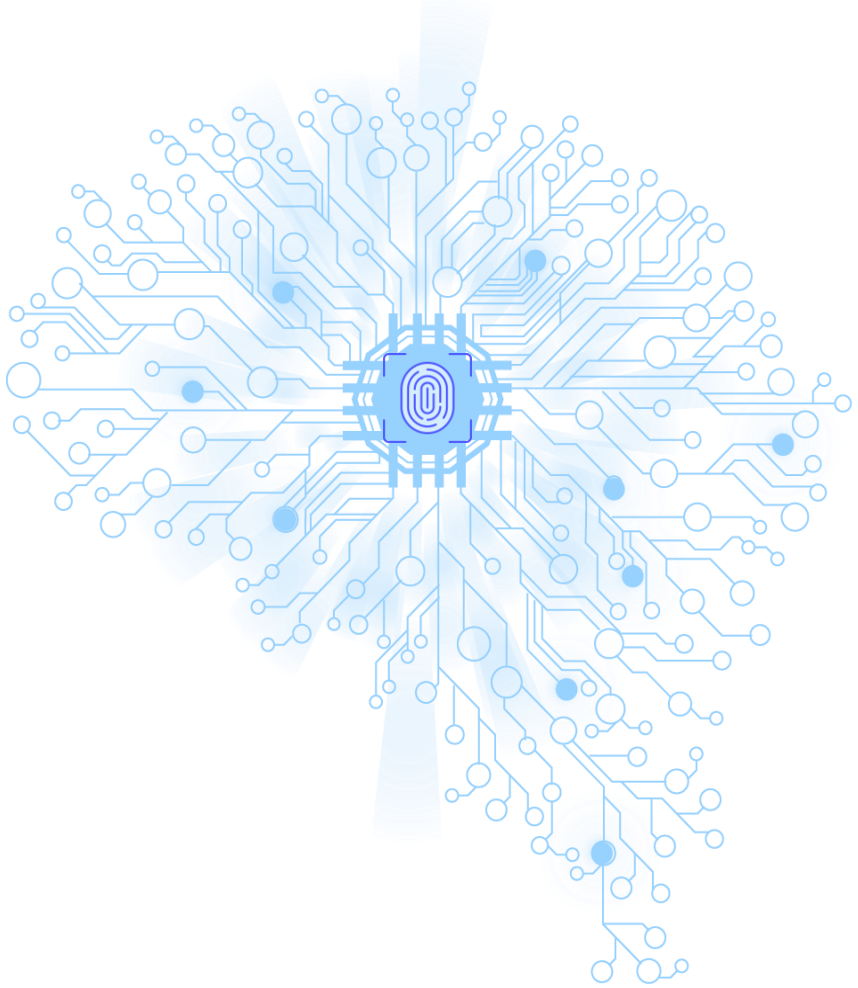
Quadro Comparativo de Boas Práticas (O que fazer e O que Evitar) para contribuir com a Adequação:

O que Fazer	O que Evitar
✓ Realizar a troca periódica de senha;	X Compartilhar senha;
✓ Descartar papéis/documentos que contenham dados pessoais da forma correta;	X Deixar papéis/documentos que contenham dados pessoais à vista de outras pessoas;
✓ Utilizar a função de bloqueio quando se ausentar da estação de trabalho;	X Deixar a tela do computador aberta/exposta quando ausente da estação de trabalho;
✓ Armazenar dados pessoais ou documentos na pasta de rede da Santa Marcelina Saúde;	X Coletar informações desnecessárias para o exercício da atividade;
✓ Ao tomar ciência de um e-mail desconhecido ou suspeito, reportar imediatamente à área de Tecnologia da Informação;	X Abrir e-mail suspeitos, quando houver dúvida quanto à origem;
✓ Realizar a coleta de dados de forma proporcional e limitada à finalidade explícita da atividade.	X Realizar coleta redundante de dados.

Fonte: Cartilha LGPD MPRS Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018

Caso prático

Uma rede de farmácias foi notificada pelo Instituto Brasileiro de Defesa do Consumidor (Idec) para prestar esclarecimentos sobre a coleta e uso de biometria (dado sensível) para identificação e liberação de descontos em suas lojas.



Neste caso prático foi observado o Princípio da Necessidade. Este princípio, fundamental na proteção de dados, estabelece que o tratamento de informações pessoais deve ser limitado ao mínimo indispensável para a realização da finalidade pretendida, evitando a coleta excessiva ou irrelevante de dados.

Lição Aprendida

- ❑ Observar a real necessidade da coleta de dados;
- ❑ Coletar os dados indispensáveis para a finalidade pretendida;
- ❑ Garantir a segurança das informações.

Conteúdo/Situação Fática

Paciente dá entrada na emergência após acidente de trânsito, sem condições de dar consentimento imediato. A equipe médica precisa coletar dados sensíveis como identificação, histórico de saúde, exames e diagnóstico para realizar o atendimento e preservar a vida.

Pergunta

No caso acima, informe quem são os agentes de tratamento?

Resposta

Controlador: O hospital, que decide sobre o tratamento dos dados do paciente.

Operador: A equipe médica e de enfermagem que lida diretamente com as informações do paciente.

Titular dos Dados: O próprio paciente.

Pergunta

Neste caso, quais são os fundamentos legais previstos na LGPD?

Resposta

Artigo 7º, inciso VIII: Tratamento de dados pessoais para a tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Artigo 11, inciso II, alínea "f": Tratamento de dados pessoais sensíveis (saúde) indispensável para a tutela da saúde, quando realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Lição Aprendida

Não compartilhar informações com terceiros sem a devida autorização e manter a guarda do prontuário em local com acesso restrito e monitorado.

Conteúdo/Situação Fática

Equipe de saúde da família realiza o acompanhamento periódico de pacientes com diabetes e hipertensão. Para monitoramento, são coletados dados sensíveis como glicemia, pressão arterial, peso e medicação.

Pergunta

No caso acima, informe quem são os agentes de tratamento?

Resposta

Controlador: A Unidade Básica de Saúde (UBS), que define como os dados serão coletados e usados.

Operador: Profissionais de saúde (médicos, enfermeiros, agentes comunitários de saúde) que realizam as coletas e inserem os dados no sistema.

O Titular dos Dados: Os pacientes acompanhados.

Pergunta

Neste caso, quais são os fundamentos legais previstos na LGPD?

Resposta

Artigo 7º, inciso III: Tratamento para a execução de políticas públicas pela administração pública.

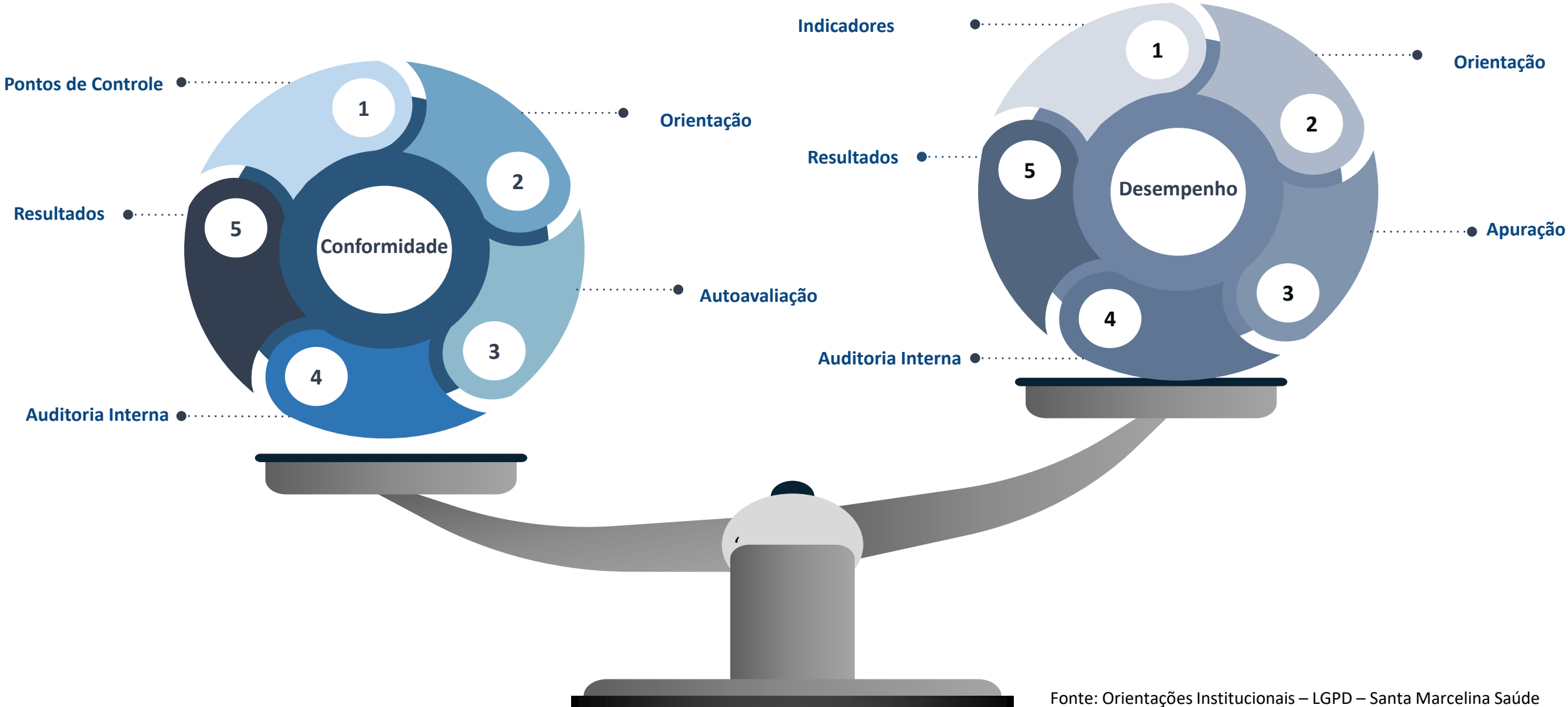
Artigo 11, inciso II, alínea "f": Tratamento de dados pessoais sensíveis indispensável para a tutela da saúde, com foco no acompanhamento e prevenção.

Princípio: Transparência no uso dos dados e finalidade específica para o cuidado em saúde.

Lição Aprendida

O agente comunitário de saúde, conforme o referido caso, não deve compartilhar informações de saúde com terceiros, bem como manter a guarda do prontuário eletrônico em local seguro e restrito.

Atualização e Monitoramento Contínuo



Fonte: Orientações Institucionais – LGPD – Santa Marcelina Saúde

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.mprs.mp.br/media/areas/lgpd/arquivos/cartilha_lgpd.pdf. Acesso em: 29 ago 2025.

BRASIL. Tribunal de Contas do Estado de Rondônia. Comitê de Segurança da Informação e Comunicação. Disponível em: https://lgpd.tcero.tc.br/principios-da-lgpd/ . Acesso em: 29 ago 2025.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO. Princípios da LGPD. Disponível em: https://lgpd.tcero.tc.br/principios-da-lgpd/. Acesso em: 29 ago 2025.

GUIA ORIENTATIVO. Tratamento de Dados de Pessoais Criança e Adolescentes. MPCE Ministério Público do Ceará. Versão 1.0. Disponível em: https://www.mpce.mp.br/wp-content/uploads/2023/10/Guia-orientativo-de-tratamento-de-dados-pessoais-de-criancas-e-adolescentes.pdf. Acesso em: 29 ago 2025.

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI). Guia de Elaboração de Inventário de Dados Pessoais. Versão 2.0. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf Acesso em: 29 ago 2025.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Cartilha - Lei Geral de Proteção de Dados - MPRS. Disponível em: https://www.mprs.mp.br/media/areas/lgpd/arquivos/cartilha_lgpd.pdf. Acesso em: 29 ago 2025.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 2021 - LGPD. Disponível em: https://www.gov.br/dnit/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/cartilha_lgpd_2021.pdf .Acesso em: 29 ago 2025.

GUIAS DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Governo. Comitê Central de Governança de Dados. Edição: Agosto/2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 29 ago 2025.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Cartilha - Lei Geral de Proteção de Dados - OAB Minas Gerais. Disponível em: https://www.oabmg.org.br/DocPublicacoes/Cartilha_LGDP_Protecao_dados_OABMG_491.pdf. Acesso em: 05 ago 2025.
. Acesso em: 29 ago 2025.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Cartilha - Lei Geral de Proteção de Dados -Tribunal Regional do Trabalho da 15ª Região. Disponível em: https://trt15.jus.br/sites/portal/files/roles/institucional/gestao-estrategica/lgpd/Cartilha%20-%20LGPD.pdf. Acesso em: 29 ago 2025.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Cartilha LGPD - Portos Rio Autoridade Portuária. Disponível em: https://portosrio.gov.br/sites/default/files/2025-files/cartilha_lgpd_2025_rev2.pdf. Acesso em: 29 ago 2025.

ORDEM DOS ADVOGADOS DO BRASIL. Cartilha LGPD na Saúde. Disponível em: https://oabdf.org.br/wp-content/uploads/2022/01/Cartilha-LGPD-na-Saude.pdf. Acesso em: 29 ago 2025.

PLANO DE RESPOSTA A INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS. Controladoria Geral do Estado do Mato Grosso do Sul. Disponível em: https://www.cge.ms.gov.br/wp-content/uploads/2024/10/Plano-de-Resposta.pdf . Acesso em: 29 ago 2025.

REDE DE SAÚDE SANTA MARCELINA. Orientações Institucionais – LGPD – Santa Marcelina Saúde. 1. ed. São Paulo. Acesso em: 29 ago 2025.

REDE DE SAÚDE SANTA MARCELINA. Relatório de Impacto à Proteção de Dados Pessoais. 2ª Edição – RIPD 2023/2024. Disponível em: https://santamarcelina.org/wp-content/uploads/2024/05/RELATORIO-DE-IMPACTO_2023_2024_2a.-Edicao-RIPD.pdf . Acesso em: 29 ago 2025.

Missão que vem do coração!

Integrar para evoluir