RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Este documento contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de redução de riscos.

Três Barras-SC 2025

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

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador	
Dr. Gilmar Luis Mazurkievicz	
Operadores	
O(s) agente(s) publico(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; contidos nos anexos deste documento.	
Comitê Interdisciplinar de Proteção de Dados Pessoais (CIPDP)	
PORTARIA Nº xxx, DE xxxxxxx. a) representante da Controladoria Municipal; b) representante da área de Tecnologia da Informação; c) representante da Secretaria de Educação; d) representante da Secretaria de saúde; e) representante da Procuradoria Jurídica;	
Encarregado Geral de Proteção de Dados Pessoais	
GILMAR LUIS Mazurkievicz CPF 703.02774904 , nomeado através da PORTARIA Nº **PORTARIA Nº 40, DE 20 DE JANEIRO DE 2025,**. controlador interno e operador para atuar como canal de comunicação entre os tutelares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (LGPD, art. 5º, VIII).	
Legislação Vigente	**Ato Formal**
Regulamentação Designação Encarregado de Dados Pessoais Designação do CIPDP – Comitê Interdisciplinar de Proteção de Dados	
E-mail Encarregado	**Telefone Encarregado**
controleinterno@tresbarras.sc.gov.br	47 3623-0121

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Nos termos do art. 4 º, § 4 º, deste Decreto, e, art. 38 da LGPD, a elaboração dos **Relatórios de Impacto a Proteção de Dados Pessoais – RIPD** é de responsabilidade do Controlador, e deverão considerar os resultados apurados no mapeamento do tratamento de dados pessoais de que trata deste Decreto, e conter ainda, no mínimo:

I. a descrição dos tipos de dados coletados;

II. a metodologia utilizada para a coleta e para a garantia da segurança das informações

III. A análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Parágrafo único. O Relatório de Impacto a Proteção de Dados - RIPD visa a identificação das necessidades de adequação no tratamento de dados pessoais, apontando se há desvios entre o cenário atual e as exigências da Lei Federal nº 13.709/2018 , como identificação de eventuais dados pessoais que não atendam aos critérios de finalidade de processamento ou do mínimo necessário, necessidades de alteração de processos dentro de cada estrutura organizacional, entre outros, e deverá ser divulgado no sítio oficial do Município.

Os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são:

- *para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);*
- *quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e*
- *a qualquer momento sob determinação da ANPD (art. 38).*

Quando for necessária a elaboração do RIPD, a Administração Municipal poderá avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, afim de decidir sobre a elaboração ou atualização do RIPD.

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 secretaria de acordo com os processos internos de trabalho. **Sendo assim a Administração Municipal de nosso município devido a quantidade reduzida de dados pessoais, com poucos processos e serviços, optou por um RIPD único, segmentado por setores.**

Além dos casos específicos previstos pela LGPD no início desta seção relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- *Uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;*
- *Rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 § 2º);*
- *Tratamento de 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" (LGPD, art. 5º, II);*
- *Processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);*
- *Tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);*
- *Tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou*
- *coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);*
- *Tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);*
- *Tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);*
- *Alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, _luxos de dados novos ou alterados, etc.; e*

- *Reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.*

3 – DESCRIÇÃO DO TRATAMENTO

A Prefeitura Municipal de Três Barras empenha-se em adotar as melhores práticas de tratamento e Segurança da Informação, priorizando a proteção e inviolabilidade dos dados pessoais de seus clientes, colaboradores e demais titulares, além de adotar todas as medidas preventivas administrativas, técnicas e físicas, para manutenção da integridade desses dados, de modo a evitar a ocorrência de eventuais danos.

Conforme permitido do pela Lei Geral de Proteção de Dados Pessoais (LGPD), a Administração poderá recorrer à subcontratação de empresas para a realização do tratamento total ou parcial dos dados pessoais. Nessas hipóteses, as organizações se comprometem, nos termos dos contratos celebrados, a guardarem sigilo e a garanti r a privacidade e a segurança dos dados a que tenham acesso, não podendo utilizá-los para quaisquer outros fins, nem os relacionar com outros dados que possuam.

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.

A LGPD (art. 5 º, 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".

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

3.1 – NATUREZA DO TRATAMENTO

A Prefeitura Municipal de Três Barras se preocupa com a segurança da informação, principalmente no que diz respeito à privacidade e proteção de dados

pessoais a que venha a ter acesso em razão das aplicações das suas políticas públicas. Por isso, em observância à Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018) , esta Política descreve as práticas por ela adotadas para coleta, tratamento e armazenamento de seus dados e informações.

Compreendemos nossas atividades de coleta de dados tanto on-line quanto off-line, abrangendo os dados pessoais que coletamos por meio de nossos vários canais, incluindo – mas não limitado ao nosso site na web e nosso serviço presencial de atendimento ao público e sistemas de gestão da Saúde, Educação, Serviço Social, etc. Quando o usuário interage e utiliza os serviços oferecidos pela administração, confere sua livre e expressa ciência e concordância com os termos es pulados nesta Política de Privacidade.

O tratamento dos dados pessoais seguirá os preceitos previstos no ar go 7 º da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018), lembrando da não necessidade de consentimento do titular dos dados pessoais para práticas dos atos ligados a aplicação de políticas públicas, e outras situações previstas no Ar go 7º, incisos: II, III, IV, V, VI, VII, VIII, IX (Bases legais para o tratamento de dados) da Lei Geral de Proteção de dados.

3.2 – ESCOPO DO TRATAMENTO

A legislação vigente prevê os direitos especificados abaixo para atendimento aos titulares de dados pessoais. Esta serven a sempre jus ficará e responderá as solicitações realizadas, sendo que tais direitos somente serão atendidos quando cabível, reforça o compromisso dessa serven a de respeito aos direitos dos titulares.

- Confirmação da existência de tratamento: o titular de dados pessoais poderá ques onar se há realização de operações de tratamento relativas a seus dados pessoais, por meio do endereço eletrônico.

- Acesso aos dados: Este direito será exercido mediante requerimento expresso do titular ou de representante legalmente constituído, ao agente de tratamento (Ar go 18, § 3º da LGPD).
- Correção de dados incompletos, inexatos ou desatualizados: há procedimento específico para a retificação do registro, pois os dados constantes na Prefeitura Municipal de Três Barras possuem caráter para aplicações de políticas públicas e transferências para órgãos estaduais e Federais para validação, esta s cas, repasses de verbas públicas, etc, assim estas revisões devem ser solicitadas nas respec vas Secretarias para evitar prejuízos à administração ou algum benéfico ao titular.
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial (Lei Federal 13.853/2019). A portabilidade dos dados pessoais a que se refere o inciso V do caput deste ar go não inclui dados que já tenham sido anonimizados pelo controlador(Lei 13.709/2018, ar go 18, inciso V, 7º .
- A própria LGPD prevê em seu art. 40 que a Autoridade Nacional de Proteção de dados irá indicar e regulamentar os padrões para a interoperabilidade dos dados, justamente visando garantir o direito à operabilidade. Para, além disso, a Autoridade irá indicar o tempo de guarda dos registros de dados que foram transferidos de uma controladora a outra, levando-se em conta a transparência e a necessidade de manutenção desses dados pela controladora inicial.
- Informação das entidades públicas e privadas com as quais a Administração Municipal realizou o Uso Compartilhado de dados: O titular de dados pessoais possui o direito de saber com quais entidades públicas e privadas está serventia pode realizar o compartilhamento de dados, e poderá obter as devidas informações a partir desta Política de Privacidade ou por solicitação ao nosso encarregado, por meio das informações constantes no item “CONTATO”.
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou desconformes com a LGPD: os dados do Registro na Prefeitura não

podem ser anonimizados, bloqueados ou eliminados, sob pena de comprometer o arquivo público, obrigações e direitos.

- Eliminação dos dados pessoais tratados com o consentimento do titular: o titular de dados pessoais poderá requisitar a exclusão de dados pessoais tratados nesta serven a, que não procederá com a eliminação apenas se houver um motivo legítimo para a sua manutenção (Art. 16 LGPD), como eventual obrigação legal de retenção de dados. Na hipótese de eliminação, a serventia se reserva o direito de escolher o procedimento de eliminação empregado, comprometendo-se a u lizar mecanismo que evite a recuperação dos dados.

- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa: Sempre que a coleta de dados de determinado serviço esteja amparada no consentimento, o titular de dados pessoais será informado sobre a possibilidade de não fornecer consen mento. Em determinados casos, a negativa do consentimento poderá implicar na impossibilidade de prestação de determinados serviços, e a serventia indicará tais casos e suas consequências.

- Revogação do consentimento: Dados do existente na Prefeitura Municipal de Três Barras tornados manifestamente públicos pelo titular, considerando a própria publicidade que se espera dos serviços notariais e registrais para a constituição de direitos, aos quais se dispensa a coleta de consentimento (art. 7 º, §4º da Lei Geral de Proteção de Dados). O titular de dados pessoais poderá revogar o consentimento concedido a determinadas operações de tratamento, hipótese que não afetará a legalidade de qualquer tratamento realizado antes da revogação do consentimento. Em determinados casos, a revogação poderá implicar na impossibilidade de prestação de determinados serviços, nos quais a Prefeitura Municipal de Trê Barras indicará quais serviços podem ser descontinuados. A Prefeitura Municipal de Trê Barras se resguarda no direito de divulgar ou fornecer os dados dos usuários para cumprimento legal e/ou processual, se necessário, e se assim lhe for exigido por autoridades fiscais, judiciais ou administrativas, mediante conhecimento dos respectivos titulares, salvo disposição legal ou judicial em contrário. Estes direitos podem ser exercidos

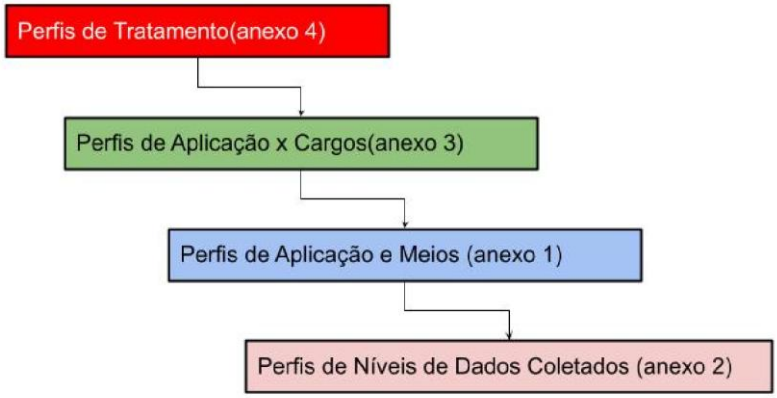
através dos canais de comunicação detalhados no CONTATO" nesta Política, sendo necessária a validação da sua identidade através do fornecimento de uma cópia de RG ou meios equivalentes de identificação, em conformidade com a legislação vigente, os quais serão eliminados tão logo o motivo que levou a solicitação se encerre.

3.3 – CONTEXTO DO TRATAMENTO

Seguindo os preceitos anteriormente citados o Relatório de Impacto à Proteção de Dados Pessoais será focado na divisão atual de Secretarias e Diretorias da Administração Pública (divididos por perfis vinculados aos cargos existentes) conforme organograma abaixo:

Os perfis de Tratamento estão con dos no anexo 3 deste documento.

Formato de Organização do mapeamento das aplicações e meios utilizados pela administração.



3.4 – FINALIDADE DO TRATAMENTO

A administração municipal não solicita, coleta, processa, armazena ou compartilha dados pessoais de crianças e adolescentes menores de idade, excetuando-se casos onde há uma previsão legal, ou consentimento explícito de seus pais ou responsáveis legais, conforme a legislação vigente. Se descobrirmos a ocorrência de qualquer po de tratamento deste tipo de dado pessoal, de forma não-intencional, removeremos os dados pessoais daquela criança ou adolescente de nossos registros, se existir viabilidade legal para as especificidades relacionadas e Setor correspondente.

O tratamento dos dados pessoais seguirá os preceitos previstos no ar go 7 º da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018), lembrando da não necessidade de consentimento do titular dos dados pessoais para práticas dos atos ligados a aplicação de políticas públicas, e outras situações previstas no Artigo 7 º, incisos: II, III, IV, V, VI, VII, VIII, IX (Bases legais para o tratamento de dados) da Lei Geral de Proteção de dados.

Seguindo os princípios legais previstos pela LGPD para o tratamento de dados pessoais descritos abaixo:

I – Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento de forma incompatível com essas finalidades;

II – Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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

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

V – Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados e acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

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

VII – Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações a ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. O cumprimento desses princípios deve ser considerado quando do tratamento dos dados dos titulares.

4 – PARTES INTERESSADAS CONSULTADAS

É importante destacar neste ponto o empenho do encarregado de dados que consultou e informou os setores municipais, utilizando como ferramenta de trabalho formulário próprio sobre as questões relativas a LGPD, trazendo à tona os registros dos sistemas(operadores), agentes de tratamento, especialmente em relação aos riscos que serão expostos mais adiante.

5 – NECESSIDADE E PROPORCIONALIDADE

No Art. 7 º, a LGPD determina 10 hipóteses ou bases legais que devem justificar o tratamento de dados pessoais. Estas bases são fundamentais para garantir que a administração pública esteja em conformidade e adequada à lei.

1 . Consentimento

O **consentimento** é uma das bases legais mais comentadas e conhecidas da LGPD. Basicamente, permite que as empresas tratem dados pessoais para fins específicos mediante a autorização do titular dos dados. A lei prevê que o consentimento deve incluir finalidades específicas para o uso dos dados e que autorizações genéricas serão consideradas nulas.

2 . Cumprimento de obrigação legal ou regulatória

Outra hipótese para tratar legalmente dados pessoais é no caso de cumprimento de obrigação legal ou regulatória. Ou seja, quando lidar com dados pessoais é necessário para poder garantir o cumprimento de outras leis ou normativas. Um exemplo comum são obrigações relacionadas aos dados de funcionários. Neste caso, as leis trabalhistas impactam diretamente o tratamento de dados pessoais, exigindo desde o envio de informações até o armazenamento de determinados dados por longos períodos de tempo.

3 . Execução de políticas públicas

Esta é uma base legal muito específica da LGPD, pois se aplica somente à administração pública , e não a empresas. Ela garante que o poder público

poderá tratar e fazer uso compartilhado de dados pessoais se eles forem necessários para colocar em prática políticas públicas previstas em leis e regulamentos ou respaldadas em contratos e convênios. É o caso de dados necessários para implementar programas de assistência social e de transferência de renda, dentre muitos outros exemplos possíveis.

4 . Realização de estudos por órgão de pesquisa

A realização de estudos por órgãos de pesquisa, como IBGE e IPEA, também está prevista como base legal na LGPD. O detalhe é que a lei coloca que, sempre que possível, deve ser feita a **anonimização** dos dados. Ou seja, preferencialmente deve-se adotar procedimentos que impossibilitem a associação direta ou indireta entre um dado e um indivíduo.

5 . Execução ou criação de contrato

A LGPD também prevê que os dados pessoais podem ser u lizados para executar ou preparar um contrato do qual o titular seja parte, a pedido do Titular É o caso, por exemplo, de dados que precisam ser fornecidos para formalizar a contratação de um funcionário ou o aluguel de um imóvel; ou de dados que precisam ser usados para garantir o cumprimento do contrato em si. Vale ressaltar, inclusive, que as hipóteses de tratamento de dados estejam previstas no contrato.

6 . Exercício regular de direitos

O uso de dados pessoais para o exercício regular de direitos é garantido pela LGPD. A sexta base legal prevê a hipótese de tratamento de dados para exercer direitos em processos judiciais, administrativos e arbitrais. Ou seja, a proteção de dados não impede o uso de dados dentro da legalidade para produzir provas e se defender em processos, garantindo o direito ao contraditório e à ampla defesa.

7 . Proteção da vida

Uma base legal bastante específica da LGPD é o tratamento de dados pessoais para a proteção da vida ou da integridade física do titular ou de terceiro. Como exemplo, podemos citar o acesso a documentos de uma pessoa caso ela sofra um acidente e esteja impossibilitada de chamar uma ambulância ou de se comunicar com a família. Se o uso desses dados

pessoais for realizado para garantir a vida e a integridade física da pessoa, então, está respaldado pela lei.

8 . Tutela da saúde

Profissionais da saúde, serviços de saúde ou autoridade sanitária têm o respaldo legal da LGPD para tratar dados pessoais que sejam necessários para a realização de suas a vidades. É o caso, por exemplo, da análise de dados necessária para uma campanha de vacinação ou para no ficar um paciente sobre o resultado de um exame.

9 . Legítimo interesse

O legítimo interesse é uma das bases legais mais genéricas e flexíveis previstas na LGPD. A lei diz que dados pessoais podem ser tratados "quando necessário para atender aos interesses legítimos do controlador ou de terceiro", desde que isso não se sobreponha a direitos e liberdades fundamentais do titular. No Art. 10º, a lei esclarece um pouco mais a respeito dos limites do legítimo interesse. Ela determina, por exemplo, que o tratamento deve ser feito para finalidades legítimas, consideradas a partir de situações concretas. Como exemplo, a lei cita o apoio e promoção de atividades do controlador e a proteção do exercício de direitos e da prestação de serviços que beneficiem o titular.

10 . Proteção do crédito

A décima e última hipótese para o tratamento de dados pessoais é a proteção do crédito. Ela é, basicamente, uma garantia aos órgãos de proteção ao crédito, como a Serasa, para que possam continuar incluindo dados de consumidores em cadastros positivos. E, também, para que as empresas com as quais o titular tenha pendências financeiras possam comunicar aos órgãos competentes que existe essa dívida.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Conforme o art. 5 º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever **"medidas, salvaguardas e mecanismos de mitigação de risco"** . Para obtermos tais medidas, salvaguardas e

mecanismos, é necessário iden ficar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Desta forma para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, 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

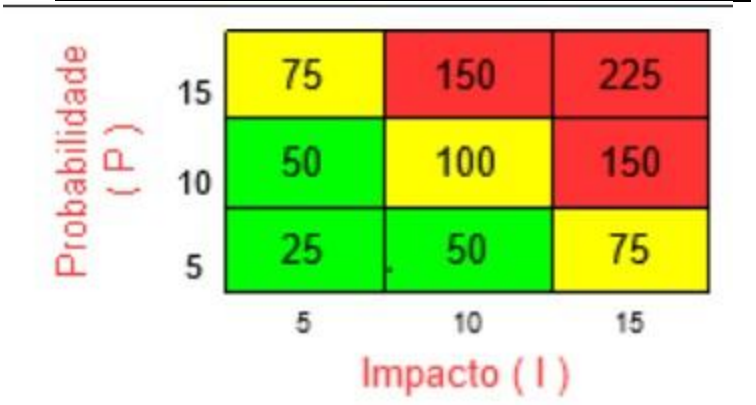


Figura 1: Matriz Probabilidade x Impacto

A figura acima apresenta a Matriz **Probabilidade x Impacto**, instrumento de apoio para a definição dos critérios de classificação do nível de risco. O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

- **Verde** , é entendido como baixo;
- **Amarelo**, representa risco moderado;
- **Vermelho** , indica risco alto.

A titulo de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os riscos elencados no RIPD (CCGD, 2020) foram influenciados e adaptados da norma ISO/IEC 29134:2017 que trata de técnicas de segurança para a avaliação de impacto à privacidade.

Abaixo são descritos os 14 riscos utilizados na avaliação e seus respectivos escopos.

Tabela 6. Os 14 riscos propostos no guia de boas práticas da LGPD (CCGD, 2020) e o escopo de atuação

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50

R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

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 u lizando-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. 2 º, inciso XIII).

7 – MEDIDAS PARA TRATAR OS RISCOS

Esta seção descreve as medidas de segurança e privacidade e o objetivo dos controles presentes nelas. Ao todo são 23 medidas de segurança e privacidade divididas em 12 medidas de segurança e 11 medidas de privacidade. A divisão organiza os controles e facilita a compreensão do leitor. Ressalta-se que o avaliador pode adaptar os controles ou incluir novos controles para que a avaliação reflita a realidade do sistema.

As medidas utilizadas têm como referência as normas ABNT NBR ISO/IEC 27002:2013 (escopo de segurança da informação) e ISO/IEC 29100:2011 (escopo de privacidade).

Medidas de Segurança (12)	Descrição (Objetivo dos controles presentes na medida de segurança)
1 . Continuidade de Negócio	Manter a operação da atividade, apesar das adversidades enfrentadas.
2 . Controles Criptográficos	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).
3 . Controles de Acesso Lógico	Limitar os acessos indevidos ao sistema.

4 . Controles de Segurança em Redes, Proteção Física e do Ambiente	Evitar acessos indevidos às estruturas internas.
5 . Cópia de Segurança	Realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.
6 . Desenvolvimento Seguro	Atender critérios de segurança da informação, desde a concepção do produto.
7 . Gestão de Capacidade e Redundância	Manter a disponibilidade do serviço.
8 . Gestão de Mudanças	Acompanhar as mudanças, comunicar aos interessados e iden ficar potenciais riscos.
9 . Gestão de Riscos	Iden ficar, avaliar, gerenciar e monitorar os riscos iden ficados.
10 . Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos.
11 . Resposta a Incidente	Realizar a coleta, a preservação de evidências, o tratamento e a resposta à incidentes de segurança.
12 . Segurança Web	Elevar os níveis de segurança (da camada de front-end) nos serviços de acessos eletrônicos.

Medidas de Privacidade (11)	**Descrição (Objetivo dos controles presentes na medida de privacidade)**
13 . Abertura, Transparência e Notificação	Atender o princípio de transparência da LGPD (art. 6º, inciso VI11).
14 . Compliance com a Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade.
15 . Consentimento e Escolha	Obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD.
16 . Controles de Acesso e Privacidade	Limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6 º, Incisos VII12 e VIII13).
17 . Legitimidade e Especificação de Propósito	informados ao titular (LGPD, art. 6º, I14).

18 . Limitação da Coleta	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6 º, III15).
19 . Minimização dos Dados	Minimizar os dados u lizados no processamento (LGPD, art. 6º, III).
20 . Participação Individual e Acesso	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6 º, IV16).
21 . Precisão e qualidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento (LGPD, art. 6º, V17)
22 . Responsabilização	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (LGPD, art. 6º, X18).
23 . Uso, Retenção e Limitação de Divulgação	Assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD ao realizar o tratamento de dados pessoais.

Metodologia

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.).

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas. A coluna “Medida(s)” pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório.

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 - , devidos aos benefícios do processamento dos dados pessoais e as 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.

Procedimento a ser seguindo:

Perfil/Setor:						
Risco	**Medida(s)**	**Efeito sobre o Risco [1]**	**Risco Residual [2]**			**Medida(s) Aprovada(s) [3]**
			P	**I**	**Nível (P x I)**	
< Risco 1>	Medida 1; Medida 2, Medida N					
< Risco 2>	Medida 1; Medida 2, Medida N					
< Risco N>	Medida 1; Medida 2, Medida N					

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

A seguir são apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior.

Modelo Exemplo:

Risco	**Medida(s)**	**Efeito sobre o Risco**	**Risco Residual**			**Medida(s) Aprovada(s)**
			P	**I**	**Nível (P x I)**	
R01 Acesso não autorizado.	1 . CONTROLE DE ACESSO LÓGICO 2 . DESENVOLVIMENTO SEGURO 3 . SEGURANÇA EM REDES	Reduzir	5	10	50	Sim
R04 Roubo.	1 . CONTROLE DE ACESSO LÓGICO 2 .CONTROLES CRIPTOGRÁFICOS	Reduzir	5	5	25	Sim

[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, Compar lhar e Aceitar.**

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

	3 . PROTEÇÃO FÍSICA E DO AMBIENTE					
1 . Limitação da coleta.	Reduzir	5	10	50	Sim	

8 – APROVAÇÃO

Esta seção **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. O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

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

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	**ENCARREGADO DE DADOS**
AUTORIDADE REPRESENTANTE DO CONTROLADOR	

Anexo 1

Perfis de Aplica vos e Meios que utilizam dados pessoais:

Aplicativo	
Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Tipo de Banco de Dados	
Licitação	
Volume	
Retenção	
Fonte dos Dados	
Dados Coletados	Nível 1
Aplica vo	
Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Tipo de Banco de Dados	
Licitação	
Volume	
Retenção	
Fonte dos Dados	
Dados Coletados	Nível 2
Aplicativo	

Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Tipo de Banco de Dados	

Dados Coletados	Nível 4
Aplicativo	
Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Tipo de Banco de Dados	
Licitação	
Volume	
Retenção	
Fonte dos Dados	Cidadãos Municipais
Volume	Semanal
Retenção	Indefinida (Registro Histórico)
Fonte dos Dados	Cidadãos Municipais

Outros Meios que u lizam dados pessoais:

Aplica vo	
Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Aplica vo	
Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Aplica vo	
Link de acesso	
Empresa Proprietária	
CNPJ	
Endereço	
Cidade	
Estado	
Telefone	
E-mail	
Tipo de Banco de Dados	
Licitação	
Aplica vo	
Link de acesso	
Empresa Proprietária	

Anexo 2

Perfis de Níveis de Dados Coletados

A Controladora fica autorizada a tomar decisões referentes ao tratamento dos seguintes níveis de dados pessoais do Titular, de acordo com os **preceitos previstos no ar go 7 º da Lei** Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018) , lembrando da não necessidade de consentimento do titular dos dados pessoais para prá cas dos atos ligados a aplicação de polí cas públicas, e outras situações previstas no Ar go 7 º, incisos: II, III, IV, V, VI, VII, VIII, IX (Bases legais para o tratamento de dados) da Lei Geral de Proteção de dados.

Nível 1

- Nome completo;
- Data de nascimento;
- Número e imagem da Carteira de Iden dade (RG);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número e imagem da Carteira Nacional de Habilitação (CNH);
- Número e imagem da Cer dão de Nascimento/Casamento/União Estável;
- Número e imagem da Carteira de Trabalho;
- Número e imagem da Carteira de Reservista;
- Número e imagem da PIS/PASEP;
- Número e imagem do Título do Eleitor;
- Número e imagem do comprovante de inscrição e regularidade para com o órgão fiscalizados;
- Número e imagem do Carteira de Vacinação;
- Fotografia 3x4;
- Estado civil;
- Tipagem Sanguínea;
- Nível de instrução ou escolaridade;
- Endereço completo;
- Números de telefone, WhatsApp e endereços de e-mail;
- Banco, agência e número de contas bancárias;

- Nome de usuário e senha específicos para uso dos serviços do Controlador;
- Comunicação, verbal e escrita, man da entre o Titular e o Controlador;
- Geoprocessamento (coordenadas geográficas);
- CTPS sica e/ou digital;
- Exames e atestados médicos, especialmente admissionais, periódicos, incluídos de retorno por afastamento superior a 30 dias em caso de doença, acidente ou parto, de mudança de função, demissionais e ainda aqueles que atestem doença ou acidente; • Cer dão de nascimento dos filhos menores de 14 anos, Carteira de vacinação dos menores de 7 anos, e atestado de matrícula e frequência escolar semestral dos maiores de 4 anos;
- (relacionar outros documentos específicos para a função, por exemplo: Documento de filiação a Sindicato; Número e Imagem da Carteira Profissional, etc.).

Nível 2

- Nome completo;
- Data de nascimento;
- Número e imagem da Carteira de Iden dade (RG);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número e imagem da Cer dão de Nascimento/Casamento/União Estável;
- Número e imagem do Carteira de Vacinação;
- Fotografia 3x4;
- Estado civil;
- Tipagem Sanguínea;
- Nível de instrução ou escolaridade;
- Endereço completo;
- Números de telefone, WhatsApp e endereços de e-mail;
- Geoprocessamento (coordenadas geográficas);
- Cer dão de nascimento dos filhos menores de 14 anos, Carteira de vacinação dos menores de 7 anos, e atestado de matrícula e frequência escolar semestral dos maiores de 4 anos;

Nível 3

- Nome completo;
- Data de nascimento;
- Número e imagem da Carteira de Iden dade (RG);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número e imagem da Cer dão de Nascimento/Casamento/União Estável;
- Número e imagem do Carteira de Vacinação;
- Número e imagem do Carteira SUS;
- Fotografia 3x4;
- Estado civil;
- Tipagem Sanguínea;
- Nível de instrução ou escolaridade;
- Endereço completo;
- Números de telefone, WhatsApp e endereços de e-mail;
- Geoprocessamento (coordenadas geográficas);
- Prontuários Médicos;

Nível 4

- Nome completo;
- Data de nascimento;
- Número e imagem da Carteira de Iden dade (RG);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número e imagem da Cer dão de Nascimento/Casamento/União Estável;
- Estado civil;
- Nível de instrução ou escolaridade;
- Endereço completo;
- Números de telefone, WhatsApp e endereços de e-mail;
- Geoprocessamento (coordenadas geográficas);
- Cópia de escrituras de terreno;

Anexo 3

Perfis de Aplicação x Cargos Estão abaixo relacionados os perfis versus aplicação acima relacionada como exemplo.

Perfil de Aplicação	Cargos
Professor	PROFESSOR
Secretario Escola	SECRETARIO DE ESCOLA
Secretaria de Educação	ASSESSOR DE EDUCAÇÃO, TECNOLOGO EDUCACIONAL, SECRETARIO DE EDUCAÇÃO, DIRETOR DE ESCOLA, COORDENADOR PEDAGOGICO, NUTRICIONISTA, PSICOLOGO
Secretaria de Planejamento	ARQUITETO, ENGENHEIRO CIVIL, ENGENHEIRO FLORESTAL, COORDENADOR DE PLANEJAMENTO
Assistência Social	MEMBROS CONSELHO TUTELAR, COORDENADOR DA CIDADANIA, ASSISTENTE SOCIAL
Administração/ TI	OPERADOR DE COMPUTADOR, COORDENADOR DE PROCESSAMENTO DE DADOS
Secretaria de Infraestrutura	SECRETARIO DE INFRAESTRUTURA , COORDENADOR DO CONTROLE DE GASTOS, COORDENADOR DO CONTROLE DE GASTOS, DIRETOR DE INFRAESTRUTURA DE OBRAS, , DIRETOR DE INFRAESTRUTURA RODOVIÁRIA, DIRETOR DE INFRAESTRUTURA URBANA
Secretaria de Saúde	SECRETÁRIO DE SAÚDE , COORDENADOR DE ASSISTÊNCIA E VIGILÂNCIA À SAUDE, AGENTE COMUNITARIO DE SAUDE, AGENTE DE COMBATE A ENDEMIAS, AUXILIAR DE ENFERMAGEM, AUXILIAR DE ENFERMAGEM – PSF, DENTISTA – PSF, ENFERMEIRO, ENFERMEIRO PSF, FARMACÊUTICO, FISCAL DE VIGILÂNCIA SANITÁRIA, MEDICO, MEDICO PSF, PSICOLOGO
Secretaria de Fazenda	SECRETARIO DA FAZENDA , CONTADOR, DIRETOR DE ADMINISTRAÇÃO E DESENVOLVIMENTO ECONÔMICO
Administração/Agricultura	TECNICO EM AGROPECUARIA, DIRETOR DE AGRICULTURA FOMENTO AGROPECUÁRIO E MEIO AMBIENTE, MEDICO VETERINARIO
Administração	AGENTE ADMINISTRATIVO, AGENTE DE CONTROLE INTERNO, AGENTE DE DEFESA CIVIL, AGENTE DE ORGANIZAÇÃO, AGENTE DE SERVIÇOS CONTABEIS, ASSESSOR ADMINISTRATIVO, AUXILIAR ADMINISTRATIVO, AUXILIAR DE CONTABILIDADE,

	AUXILIAR DE SERVIÇOS ADMINISTRATIVOS, AUXILIAR DE SERVIÇOS CONTABEIS, DIRETOR DE ADMINISTRAÇÃO E DESENVOLVIMENTO ECONÔMICO, DIRETOR DE ESPORTES, DIRETOR DE GABINETE, ESTAGIARIO, OUVIDOR GERAL, PREFEITO E VICE-PREFEITO
Administração/RH	DIRETOR DE RECURSOS HUMANOS, AGENTE DE RECURSOS HUMANOS,
	DIRETOR DO SERVIÇO DE COMPRAS
Administração/Tributação	DIRETOR DO SERVIÇO DE TRIBUTAÇÃO, , FISCAL DE TRIBUTOS
Jurídico	ADVOGADO e ASSESSOR JURÍDICO

Anexo 4

Perfis de Tratamento

Estão abaixo relacionados os perfis de aplicações/sistema versus setor relacionado.

Perfil	Secretaria de Educação
Aplicações	Ipm, SGE, SAE, SETE, CONVIVA EDUCAÇÃO, BUSCA ATIVA ESCOLAR, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, E-mail Corporativo, E-mail Pessoal, Meios Físicos, Meios Digitais, Drives Virtuais.
Perfil	Professor
Aplicações	SGE, SAE, Meios Físicos, Meios Digitais, Drives Virtuais, E-mail Corporativo, E-mail Pessoal, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz.
Perfil	Secretario Escola
Aplicações	SGE, SAE, Meios Físicos, Drives Virtuais, Meios Digitais, E-mail Corporativo, E-mail Pessoal, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz.
Perfil	Administração/ Compras
Aplicações	Ipm, Comprasbr, TCESC, Dom, Doe, Dou, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Meios Físicos, Meios Digitais, Drives Virtuais, E-mail Corpora vo, E-mail Pessoal,.
Perfil	Administração/ Agricultura
Aplicações	SEFSC - SAT, IPM, SISRURAL WEB FECAM , INCRA , Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Meios Físicos, Meios Digitais, Drives Virtuais, E-mail Corpora vo, E-mail Pessoal,
Perfil	Administração/ Tributos

Aplicações	IPM, TCESC, REGIN, TJ (Jurídico papel) Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz., Redes Sociais, Meios Físicos, Meios Digitais, Drives Virtuais, E-mail Corporativo, E-mail Pessoal,
Perfil	Administração/ RH
Aplicações	IPM, TCESC, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz., Meios Físicos, Meios Digitais, Drives Virtuais, E-mail Corporativo, E-mail Pessoal,

Perfil	Administração
Aplicações	IPM, REGIN, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz., Redes Sociais, E-mail, Meios Físicos, Meios Digitais, Drives Virtuais, E-mail Corporativo, E-mail Pessoal.
Perfil	Secretaria de Planejamento
Aplicações	IPM, REGIN, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz., Redes Sociais, E-mail Corpora vo, E-mail Pessoal.
Perfil	Secretaria de Meio Ambiente
Aplicações	IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.
Perfil	Secretaria de Infraestrutura
Aplicações	IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.
Perfil	Administração/ Controle Interno
Aplicações	IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.
Perfil	Administração/ TI
Aplicações	IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.
Perfil	Secretaria de Saúde
Aplicações	IDS, E-mail, , IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.
Perfil	Assistência Social
Aplicações	IDS, E-mail, , IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.
Perfil	Jurídico
Aplicações	IPM, E-mail , Meios Físicos, Meios Digitais, Drives Virtuais, Aplicativo multiplataforma de mensagens instantâneas e chamadas de voz, Redes Sociais E-mail Corporativo, E-mail Pessoal.

ID	Medidas	Tipo	Descrição
M01	Continuidade de Negócio	Segurança	Manter a operação da atividade, apesar das adversidades enfrentadas.
M02	Controles Criptográficos	Segurança	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).
M03	Controles de Acesso Lógico	Segurança	Limitar os acessos indevidos ao sistema.
M04	Controles de Segurança em Redes, Proteção Física e do Ambiente	Segurança	Evitar acessos indevidos às estruturas internas.
M05	Cópia de Segurança	Segurança	Realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.
M06	Desenvolvimento Seguro	Segurança	Atender critérios de segurança da informação, desde a concepção do produto.
M07	Gestão de Capacidade e Redundância	Segurança	Manter a disponibilidade do serviço.
M08	Gestão de Mudanças	Segurança	Acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos.
M09	Gestão de Riscos	Segurança	Identificar, avaliar, gerenciar e monitorar os riscos identificados.
M10	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Segurança	Registrar eventos com atributos derastreabilidade e proteger de alteração e acessos indevidos.
M11	Resposta a Incidente	Segurança	Realizar a coleta, a preservação de evidências, o tratamento e a resposta à incidentes de segurança.
M12	Segurança Web	Segurança	Elevar os níveis de segurança (da camada de front-end) nos serviços de acessos eletrônicos.
M13	Abertura, Transparência e Notificação	Privacidade	Atender o princípio de transparência da LGPD (art. 6º, inciso VI11).
M14	Compliance com a Privacidade	Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade.
M15	Consentimento e Escolha	Privacidade	Obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 daLGPD.
M16	Controles de Acesso e Privacidade	Privacidade	Limitar acessos indevidos às operações detratamento de dados pessoais (LGPD, art. 6º, Incisos VII12 e VIII13).
M17	Legitimidade e Especificação de Propósito	Privacidade	informados ao titular (LGPD, art. 6º, I14).
M18	Limitação da Coleta	Privacidade	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6º, III15).
M19	Minimização dos Dados	Privacidade	Minimizar os dados utilizados no processamento (LGPD, art. 6º, III).
M20	Participação Individual e Acesso	Privacidade	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6º, IV16).
M21	Precisão e qualidade	Privacidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento (LGPD, art. 6º, V17)
M22	Responsabilização	Privacidade	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (LGPD, art. 6º, X18).
M23	Uso, Retenção e Limitação de Divulgação	Privacidade	Assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD ao realizar o tratamento de dados pessoais.

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

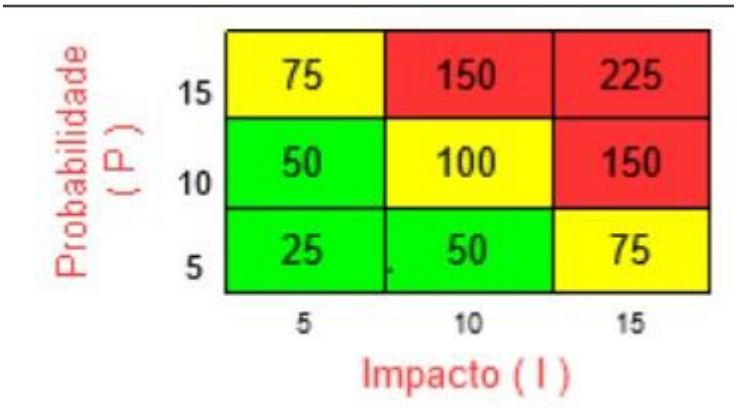


Figura 1: Matriz Probabilidade x Impacto

- **Verde**, é entendido como baixo;
- **Amarelo**, representa risco moderado;
- **Vermelho**, indica risco alto.