SECOVIMED

SERVIÇO SOCIAL DA HABITAÇÃO DO RIO GRANDE DO SUL

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Porto Alegre/RS, 18 de dezembro de 2024.

E	ACTIVITY
E1 – MAPEAMENTO	1.1 Levantamento de Informações Legais, Societárias e Técnicas do PEA (Planejamento Estratégico de Adequação). Plano de Ação. Reuniões kickoff;
	Montagem das Equipes, definição de escopos e apresentação do PEA;
	Reuniões semanais e internas finalizadas. Definido Sr. Jorge Dani como Ponto Focal e acionamento por demanda além da evolução dos itens das Etapas;
	1.2 Mapeamento da coleta, armazenamento, compartilhamento e eliminação de dados;
	Verificação de todos os sistemas e canais de entrada de dados pessoais, considerando: locais físicos, uso de cookies ou outras tecnologias, políticas existentes sobre segurança da informação, análise do ciclo de vida dos dados, mídia programática, geolocalização, recursos humanos, aplicativos, marketing, sistemas de videovigilância, coleta de dados biométricos, dados dos Síndicos, Subsíndicos, Conselheiros, visitantes, locatários, proprietários, prestadores de serviços, cessionários e parceiros, dados contidos em documentos físicos e eletrônicos, sites e outros. Realização de inventário de cada processo e análise dos riscos e vulnerabilidade jurídica, técnica e operacional da Entidade. Fase entrevistas, reuniões, contatos, tantas quanto forem necessárias;
	Mapeamento da documentação disponibilizada no drive: Relação de Funcionários, Relação de Contratos/Fornecedores, Ata Assembleia, Proposta de Sócio Efetivo, Proposta de Sócio Condomínio, Proposta de Sócio Colaborador, Organograma, Formulário de Inscrição em Evento, Ficha de Atendimento Jurídico-Recepção, Estatuto e Atualização de Cadastro de Associada. A princípio dados suficientes apurados em reunião e site do SECOVIMED/RS para gerar o presente RIPD nos termos do artigo 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018 (“LGPD”);
	1.3 Elaboração de mapeamento e o levantamento dos gaps com identificação de não-conformidade e análise de riscos jurídicos e regulatórios no tratamento de dados pessoais e sistemas. Alocação de recursos tecnológicos, governança e cultura;
	Análise das informações dos controles internos e governança de dados pessoais. Análise da documentação que legitima o tratamento de dados pessoais de Fornecedores (Fornecedor, Objeto, Dados Pessoais, Dados Sensíveis, Observações, Contatos) e Templates (Documento, Dados Pessoais, Dados Sensíveis, Aplicação LGPD, Pendência, Solução, Texto a ser inserido, Observação), bem como o cenário atual do ponto de vista de governança dos dados em toda a Entidade, desde os aspectos relacionados aos papeis e responsabilidades do Controlador. Elaboração de procedimento e controles estabelecidos nos procedimentos de coletas de dados;
	Execução de plano de ação e implementações de adequações que compreendem a documentação analisada e site do SECOVIMED/RS através dos filtros: Documento, Dados Pessoais e Dados Sensíveis, Aplicação LGPD, Pendência, Solução;

E2 - *ASSESSMENT*	2.1 Apresentação do Plano de Ação (PEA). Análise e adequação de políticas, controles e procedimentos existentes. Elaboração de políticas (proteção e tratamento) de privacidade e governança de dados, controles e procedimentos adicionais necessários. Primeiras divulgações das versões das políticas, controles e procedimentos relevantes. Criação e implementação de controles para garantir a atualização dos dados. Avaliação e adequação da base de dados, elaboração de procedimentos conforme critérios da "Privacy by Design/Privacy by Default". Criação de Modelo de RIPD, permitindo que todos os novos projetos, sistemas, produtos, práticas de negócios e similares, sejam analisados, desde a concepção sob o prisma da privacidade. Definição e adequação de procedimento para tratamento de incidentes. Mapeamento e adequação de contratos relevantes. Criação de procedimentos e políticas para garantir direitos dos titulares dos dados. Estruturação do cargo de encarregado de proteção de dados (DPO). Realização de testes de legítimo interesse e documentação conforme requerimento da legislação. Análise crítica da necessidade de manutenção de dados sensíveis.
E3 - IMPLANTAÇÃO	3.1 Gestão Contínua de Vulnerabilidades de Segurança da Informação. 3.2 Execução das atividades previstas no Plano Estratégico de Adequação. 3.3 Preparação dos profissionais do CONTRATANTE (ou por ele indicado) para manter o compliance da Entidade frente às regulações de proteção de dados. Simulação de ataques ao sistema e testes de vulnerabilidade aos mecanismos de proteção planejados e avaliado, não havendo registro de ataques e violações até o momento de emissão do presente RIPD. Testes de reação do CONTRATANTE frente a situações simuladas. Elaboração dos documentos e outros, necessários para a conformidade com a regulação. Entrega de guias de procedimentos e termos de segurança da informação, sob o ponto de vista jurídico, regulatório e tecnológico. Melhoria nos processos e maior segurança para o CONTRATANTE, bem como ajustes em contratos e outros documentos legais. Intervenções em hardwares e softwares. Elaboração e entrega dos instrumentos, políticas modelos e instrumentos correlatos. Treinamento/sensibilização periódicos aos colaboradores "in loco" e remoto. Monitoramento do trabalho dos parceiros do CONTRATANTE. Avaliação do nível de maturidade na governança de dados dos prestadores de serviços do CONTRATANTE. Recomendação da substituição dos fornecedores que não estiverem de acordo com as políticas de compliance relativas à LGPD. Análise de software para análise de dados;
E4 –DPO / DPO *as a Service*	4.1 Manutenção das atividades do CONTRATANTE em nível adequado de compliance e com a LGPD, bem como normas correlatas. 4.2 Treinamentos periódicos e regulares com colaboradores e fornecedores do CONTRATANTE. 4.3 Gerenciamento de Incidentes de Segurança e Gerenciamento de riscos de terceiros. 4.4 DPO as a Service, orientação sobre alterativa ao Encarregado de Dados interno do Secovimed. Sensibilização dos colaboradores, fornecedores e terceiros quanto à cultura organizacional da Entidade. Conscientização quanto às políticas internas e sua aplicabilidade. Acompanhamento regulatório. Atualização sobre os conceitos e metodologias de Privacy by Design e Privacy by Default. Prevenção e proteção da privacidade e dados nas operações e desenvolvimento de produtos e serviços. Suporte integral à Entidade. Realização das revisões necessárias após a implementação das medidas de atendimento à LGPD. Manutenção, aprimoramento e atualização. Avaliação periódica do programa de proteção de dados e acompanhamento de novas ferramentas tecnológicas. Responsável pelas adequações técnicas e jurídicas. A empresa contratada disponibilizará todo o backoffice de atualizações e suporte de TI. Execução, tanto na parte legal quanto na de TI, das atualizações necessárias. Comitê LGPD composto por Jorge Alberto Dani (Representante do Comitê LGPD), Adriana B. de Souza, Daniel Lopes Cabreira, Fernanda Almeida e Paulo Castro, conforme ata de reunião de 29.05.2025, havida das 13h30min às 15h30min.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

OBJETIVO
O Mapeamento compreende a Etapa 1 para análise dos dados e processos do SECOVIMED/RS e visa descrever o status dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco potenciais. A avaliação dos dados e plano de ação está inserido na Etapa 2 e tem a finalidade de direcionar e organizar quais dados e processos serão objeto de avaliação (*Assessment*) para adequação à LGPD, como preparação à Etapa 3 de Implementação que compreende a emissão de RIP e respectiva reunião de treinamento. O RIPD integra a Etapa 3 e é relativo à operacionalização quanto às Etapas 1 e 2 anteriormente descritas. Parte da documentação e da rotina já estão devidamente adequadas à LGPD e a parcela restante está em processo de adequação. A definição da pessoa responsável por ser DPO ou entidade indicada para ser DPO *as a Service* já está definida na forma deste instrumento, sendo eleito pela entidade a designação de DPO *as a Service* através da ADP Advogados (certificado no curso em LGPD pela Assespro. Além desta designação, a parcela de demandas finais e complementares às anteriores relativas a internalização da cultura, treinamentos e atualizações será desenvolvida após a formalização do presente RIPD. Este documento deve ser arquivado com os demais relacionados a este projeto e comprova para todos os fins de direito o status de adequação da atividade da Entidade à LGPD, incluindo a identificação do Controlador, Operador e Encarregado na forma da legislação vigente. Instruem o presente RIPD os seguintes Apêndices: a) Apêndice II - Termo LGPD SECOVIMED/RS; **Referência Legal:** Art. 5º, XVII da Lei nº 13.709/2018 e correlatos.

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO	
Controlador	
SERVICO SOCIAL DA HABITACAO DO RIO GRANDE DO SUL (“SECOVIMED/RS” ou “Entidade”), CNPJ/MF nº 02.853.061/0001-27, com sede na Rua Sete de Setembro, nº 1.096/4 e 5º andares, Centro Histórico, Porto Alegre/RS, CEP 90.010-191.	
Operador	
Comitê de LGPD, com endereço profissional na Rua Sete de Setembro, nº 1.096 / 4 e 5º andares, Centro Histórico, Porto Alegre/RS, CEP 90.010-191, e-mail comitelgpd@secovimed.com.br .	
Encarregado (*DPO as a Service*)	
Amorim Dorneles e Pedroso Advogados (“ADP Advogados”), com sede na Av. João Pereira de Vargas, nº 620, Centro, Sapucaia do Sul/RS, CEP 93.220-190.	
E-mail Encarregado	**Telefone Encarregado**
lgpd@adpadvogados.com.br	(51) 3234-1231

SUMÁRIO

2. NECESSIDADE DAS ETAPAS 1 (MAPEAMENTO), 2 (AVALIAÇÃO) E 3 (IMPLEMENTAÇÃO) QUE RESULTAM NA EMISSÃO DO RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS ("RIPD")

Os casos específicos previstos pela LGPD em que as Etapas 1, 2 e 3, como preparatórios e integrantes do RIPD, embasam-se e se aplicam:

- para tratamento de dados pessoais realizados para fins de execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (inciso V do art. 7º da Lei 13.709/2018);
- para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII do art. 7º da Lei 13.709/2018);
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (inciso VIII do art. 7º da Lei 13.709/2018);
- quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (inciso IX do art. 7º da Lei 13.709/2018); e
- quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados);
- a qualquer momento sob determinação da ANPD (art. 38).

Nas Etapas 1 e 2 preparatórias e integrantes do RIPD, a Entidade avaliou os programas, sistemas de informação e/ou processos existentes a serem implementados que geram impactos à proteção dos dados pessoais e dados pessoais sensíveis, sendo identificados dados sensíveis na Etapa 1 de Mapeamento que foram objeto de análise e avaliação na Etapa 2.

As Etapas 1 e 2 preparatórias e integrantes do RIPD foram aplicadas a todas as operações de tratamento de dados pessoais para cada projeto, sistema, e serviço que considerou os processos internos de trabalho.

Além dos casos específicos previstos pela LGPD relativos às Etapas 1 e 2 preparatórias e integrantes do RIPD, o presente instrumento considerou o potencial 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 para fins 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, fluxos 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 RIPD

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

O objetivo principal deste RIPD, devidamente preparada pelas Etapas 1 e 2 preparatórias e integrantes do RIPD anteriormente realizadas, é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos. No caso do SECOVIMED/RS o escopo é a adequação à Lei nº 13.709/2018 em relação aos dados internamente armazenados e gerenciamento dos dados das associadas e público alvo de seu escopo de criação no Estado do Rio Grande do Sul.

Quanto à Relação de Funcionários a Entidade irá adotar a base legal da obrigação legal, visto que tem por exigência legal a prestação de informações a órgãos oficiais e aos próprios funcionários relativos ao período em que estiverem vinculados ao SECOVI/RS. Serão avaliados os documentos de contratação atuais e documentação padrão para adequação. Estas informações estarão enquadradas na base legal da obrigação legal.

Quanto à Relação de Contratos com Fornecedores e outros, haverá avaliação caso a caso para adequação específica de cada documento e elaboração de cláusulas aplicáveis a documentos futuros a serem adotados. Estas informações estarão enquadradas na base legal da obrigação contratual.

Quanto aos Titulares Usuários dos serviços da Entidade, haverá avaliação caso a caso para adequação específica de cada documento e elaboração de cláusulas aplicáveis a documentos futuros a serem adotados, com especial atenção e cuidado em relação aos dados pessoais sensíveis. Estas informações estarão enquadradas na base legal da obrigação contratual.

Quanto às Atas de Assembleias, será avaliada a inclusão de texto informativo declarando a necessidade de informação de dados pessoais, estando esta disponibilização de dados pessoais enquadradas na base legal da obrigação legal, em razão da natureza jurídica da Entidade, necessidade de registro e de prestação de contas às Associadas.

Quanto aos serviços de Odontologia, Medicina e Exames, respectivos documentos físicos e/ou eletrônicos conterão disposição de texto informativo declarando o caráter de anuência expressa e voluntária do fornecimento de dados pessoais sob a base legal de obrigação legal e de proteção à saúde, visto ser requisito essencial para registro, arquivamento, prestação de contas e, principalmente, de possibilidade de usufruto dos serviços oferecidos.
Quanto ao mapeado no sítio da Entidade (http://www.secovimed.com.br/site/index.php) houve necessidade de adequação dos seguintes links relacionados: Home, Quem Somos, Responsabilidade Social, Especialidades, Informativos, PCMSO/PPRA, Medicina Ocupacional, Localização, Arquivos e Formulários, Fale Conosco e Mapa do Site, bem como respectivos documentos disponibilizados virtualmente. Em relação a estes links, além da inclusão de textos informativos, adotar-se-á a base legal de obrigação legal e proteção à saúde, visto ser requisito essencial para registro, arquivamento, prestação de contas e, principalmente, de possibilidade de exercício de sua atividade.
Quanto aos documentos físicos foram e serão realizados, além das providências e diligências anteriormente informadas, treinamentos de orientação de sensibilização quanto à cultura de adequação à LGPD. No tocante ao gerenciamento e proteção eletrônica de dados o Encarregado irá orientar sobre a forma de armazenamento, hospedagem e proteção que melhor atenderão às necessidades de proteção de dados pessoais.

3.1 NATUREZA DO TRATAMENTO

A Entidade pretende tratar o dado pessoal com mapeamento, avaliação, implementação e gerenciamento contínuo para manter em conformidade legal:

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

3.2 ESCOPO DO TRATAMENTO

Dizem respeito à abrangência do tratamento de dados da Entidade:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são potencialmente considerados dados pessoais sensíveis;
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;

- o número de titulares de dados afetados pelo tratamento; e
- a abrangência da área geográfica do tratamento.

3.3 CONTEXTO DO TRATAMENTO

Nesta seção, destacam-se os fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados. Neste sentido, o levantamento das informações destacadas a seguir proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos, sendo caracterizado como sendo relativo ao segmento *Business to Business* (*B2B*) e segmento *Business to Customer (B2C)*;
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais será tratado de forma, preferencialmente, automatizada e adotando-se sistemas e softwares de gestão de identidade, criptografia, backup e controle de acessos;
- destaca-se que no tratamento dos dados da Entidade podem envolver crianças, adolescentes ou outro grupo vulnerável na qualidade de dependentes dos Titulares usuários dos serviços da Entidade;
- destaca-se que o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais e dados pessoais e sensíveis. Ou seja, o dado pessoal e dado pessoal sensível não são tratados de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela Entidade ao Titular de dados pessoais e dados pessoais sensíveis;
- foi e será monitorado como está a estrutura de segurança de dados, para orientar implementações pontuais para adequação e atualização à Lei nº 13.709/2018, como, por exemplo, avaliação de reforço à segurança de dados e contratação de software de gestão de identidades e relacionados à LGPD, para maior automatização da forma de coleta, armazenamento e gerenciamento de dados.

3.4 FINALIDADE DO TRATAMENTO

A **finalidade** deste RIPD é identificar o que será avaliado para o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável:

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

Os exemplos de finalidades apresentados neste documento, em que pese terem

exaustivamente mapeados, são aplicáveis ao momento de emissão deste RIPD e possuem caráter mais exemplificativo, visto a organicidade de evolução de eventos e situações a que está exposta a Entidade. Desse modo, na conduta de detalhamento da finalidade do tratamento dos dados pessoais, observamos a necessidade de mapear continuamente e:

- Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Informar os benefícios esperados para o órgão, Entidade ou para a sociedade como um todo.

No presente caso, a finalidade atende às bases legais do cumprimento de obrigação legal ou regulatória pelo Controlador, tutela da proteção da saúde e vida dos Titulares e seus respectivos dependentes, execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados e atender aos interesses legítimos do controlador ou de terceiros.

4 PARTES INTERESSADAS E RESPONSÁVEIS LEGAIS

Foram consultados: SECOVIMED e o Comitê LGPD constituído pelo SECOVIMED conforme atas de reunião como Controlador e Operador respectivamente (LGPD, art. 5º, VII) e ADP Advogados designado para elaboração do presente RIPD como Encarregada de Dados (LGPD, art. 5º, VIII).

5 NECESSIDADE E PROPORCIONALIDADE

As Partes Interessadas e Responsáveis Legais avaliaram a necessidade e proporcionalidade dos dados, mapeando e avaliando as operações realizadas sobre os dados pessoais que limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º e 7º).

Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais;
- Caso o fundamento legal seja embasado no legítimo interesse e obrigação legal do Controlador (LGPD, art. 10), demonstrar que:
  - esse tratamento de dados pessoais e dados pessoais e sensíveis é indispensável;
  - não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
  - esse processamento de fato auxilia no propósito almejado.

6 IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O art. 5º, XVII da LGPD preconiza que o RIPD irá descrever **"medidas, salvaguardas e mecanismos de mitigação de risco"**.

A Entidade adotará parâmetros escalares que 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¤

Adotar-se-á, ainda, a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

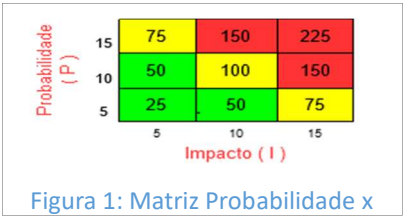

Figura 1: Matriz Probabilidade x

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; e
- vermelho, indica risco alto.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos a ser realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**.

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

Tabela 1 - Legenda: P – Probabilidade; I – Impacto.

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

Como referência, 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 da Entidade**. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017- seção 6.4.4.

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

7 MEDIDAS PARA TRATAR OS RISCOS

Como 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.) a Entidade vai adotar os procedimentos e orientações do Encarregado, com as validações do Operador e Controlador, de forma consensual, salvo situação emergencial.

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 Entidade nem sempre precisa eliminar todos os riscos.

Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto, devido aos benefícios do processamento dos dados pessoais e 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**:

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			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.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

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

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

No quadro abaixo estão apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior.

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 3. PROTEÇÃO FÍSICA E DO	Reduzir	5	5	25	Sim

	AMBIENTE					
R06 Coleção excessiva.	1. LIMITAÇÃO DA COLETA.	Reduzir	5	10	50	Sim

8 APROVAÇÃO

Em vista do mapeamento e avaliação realizados, a Entidade **formaliza a finalização das Etapa 1 à Etapa 3** por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pela Encarregada de Dados e pelas autoridades que representam o Controlador e Operador. O responsável pela elaboração do RIPD pode ser o próprio Encarregado ou qualquer outra pessoa designada pelo Controlador com conhecimento necessário para realizar tal tarefa.

O RIPD ora elaborado constitui o documento final e comprobatório da adequação da Entidade à LGPD, devendo ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela Entidade. Detalhes sobre a necessidade de revisão do RIPD podem ser observados no **item 2.5.2.9 do Guia de Boas Práticas LGDP, disponível em**: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf.

Porto Alegre/RS, 18.12.2024.

PARTES RESPONSÁVEIS PELA ELABORAÇÃO DO RIPD	
_____ ADP Advogados	_____ Comitê LGPD.

CONTROLADOR	**OPERADOR**
_____ Comitê LGPD	_____ Comitê LGPD
ENCARREGADO DE DADOS	
_____ ADP Advogados	

APÊNDICE I - TERMO LGPD SECOVIMED/RS

TERMO DE DISPONIBILIZAÇÃO DE DADOS PESSOAIS ("TDDP")

Atendendo às exigências da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados, declaro para os devidos fins que concordo em receber e disponibilizar dados pessoais com o SERVICO SOCIAL DA HABITACAO DO RIO GRANDE DO SUL ("SECOVIMED/RS"), para poder cumprir minha atividade profissional que se enquadra na base legal da: (i) obrigação legal, (ii) execução contratual e atendimento dos interesses legítimos do controlador ou de terceiros e (iii) tutela e proteção da saúde, sendo estas as principais bases legais da referida disponibilização, nos termos do artigo 7º, Incisos II, V, VIII e IX da Lei 13.709/2018 (LGPD).

Sem mais para o momento, declaro minha anuência.

Porto Alegre/RS, ____ de _____ de 20____.

_____
(NOME OU RAZÃO SOCIAL)
CPF/MF OU CNPJ/MF:

TESTEMUNHAS:

_____ _____
NOME: NOME:
CPF/MF: CPF/MF: