

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

<Local>, 07 de agosto de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
XX/XX/20XX	1.0	Conclusão da primeira versão do relatório	XXXXXXXXXXXXXX
XX/XX/20XX	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	XXXXXXXXXXXXXX

ATENÇÃO!

<Os trechos marcados em azul neste template são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário>.

<Template Versão 2.0 - Atualizado em
08/05/2024>

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

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

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

Controlador: **Tribunal de Contas do Estado de Santa Catarina**

Endereço: **Rua Bulcão Viana, 90, Centro - Florianópolis, SC.**

CEP: **88020-160**

e-mail: encarregado@tcesc.tc.br

Telefone: **(48) 3221-3833**

Operador

<Nome da pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, VII)>.

Encarregado

Wallace da Silva Pereira

E-mail Encarregado

wallace.pereira@tcesc.tc.br

Telefone Encarregado

(48) 3221-3959.

2 - NECESSIDADE DE ELABORAR O RELATÓRIO

<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 instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.>

<Além dos casos específicos previstos pela LGPD no início desta seção 2 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, 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.

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

3 - DESCRIÇÃO DO TRATAMENTO

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

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

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

3.1 - NATUREZA DO TRATAMENTO

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

<Importante descrever, por exemplo:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
- com quais órgãos, entidades ou empresas 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.>

<Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.>

3.2 - ESCOPO DO TRATAMENTO

<O **escopo** representa a abrangência do tratamento de dados.>

< Nesse sentido, considerar destacar:

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

< O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.>

3.3 - CONTEXTO DO TRATAMENTO

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

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

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

3.4 - FINALIDADE DO TRATAMENTO

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

<Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo arts. 7º e 11 da LGPD), no que for aplicável:

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

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

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

- 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.>

< Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - Apoio e promoção de atividades do controlador; e

II - Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os

dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento

de dados baseados em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

<Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.>

4 - PARTES INTERESSADAS CONSULTADAS

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

<Nessa seção, é importante identificar:

- quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos etc.; e

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

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

5 - NECESSIDADE E PROPORCIONALIDADE

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

III). >

< Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:
 - Esse tratamento de dados pessoais é indispensável;
 - Não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
 - Esse processamento de fato auxilia no propósito almejado.
- Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
- Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
- Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
- Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
- Quais são as salvaguardas para as transferências internacionais de dados.>

< O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador

ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.>

6 - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

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

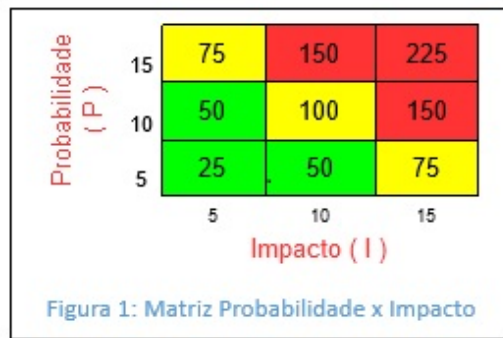
<Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.>

<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

<A figura a seguir 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; 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 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>			

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).

<A título 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 e impacto dos riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto da unidade.** Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.>

Os valores e cálculos

inseridos pela UGI



Id	Risco referente ao tratamento de dados pessoais (Sugestão da Unidade)	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 pseudoanonimizados.	5	15	75

7 - MEDIDAS PARA TRATAR OS RISCOS - PARA PREENCHIMENTO PELA UGI

<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.**>

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.

<A seguir são 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	Reduzir	5	10	50	Sim
	2. DESENVOLVIMENTO SEGURO					
	3. SEGURANÇA EM REDES					
R04 Roubo.	1. CONTROLE DE ACESSO LÓGICO	Reduzir	5	5	25	Sim
	2. CONTROLES CRIPTOGRÁFICOS					
	3. PROTEÇÃO FÍSICA E DO AMBIENTE					
R06 Coleção excessiva.	1. Limitação da coleta.	Reduzir	5	10	50	Sim

8 - APROVAÇÃO - **PREENCHIMENTO PELA AGET-ED**

<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. Detalhes sobre a necessidade de revisão do RIPD podem ser observados no **item 2.5.2.9 do Guia de Boas Práticas LGPD, disponível em:** <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>>

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<p>_____</p> <p><Nome do responsável></p> <p>Matrícula/SIAPE: xxxxx</p> <p><Local>, <dia> de <mês> de <ano></p>	<p>_____</p> <p>Wallace da Silva Pereira</p> <p>Matrícula/SIAPE: 450725-8</p> <p><Local>, <dia> de <mês> de <ano></p>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
<hr/> <p>Herneus João de Nadal Matrícula/SIAPE: 451019-4 <Local>, <dia> de <mês> de <ano></p>	<hr/> <p><Nome do representante> Matrícula/SIAPE: xxxxx <Local>, <dia> de <mês> de <ano></p>

24.0.000003691-5

0334500v1