

<Local>, <dia> de <mês> de <ano>



**HISTÓRICO DE REVISÕES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Descrição** | **Autor** |
| XX/XX/20XX | 1.0 | Conclusão da primeira versão do relatório | XXXXXXXXXXXX |

Sumário

[**1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO 3**](#_Toc113007628)

[**2 – NECESSIDADE DE ELABORAR O RELATÓRIO 3**](#_Toc113007629)

[**3 – O SISTEMA 4**](#_Toc113007630)

[**4 – DESCRIÇÃO DO TRATAMENTO 4**](#_Toc113007631)

[**5 – PARTES INTERESSADAS CONSULTADAS 6**](#_Toc113007632)

[**6 – NECESSIDADE E PROPORCIONALIDADE 6**](#_Toc113007633)

[**7 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS 7**](#_Toc113007634)

[**8 – MEDIDAS PARA TRATAR OS RISCOS 8**](#_Toc113007635)

[**9 – PLANOS DE AÇÕES 9**](#_Toc113007636)

[**10 – APROVAÇÃO 10**](#_Toc113007637)

**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** |
| <Nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI)>. |

|  |
| --- |
| **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** | |  |
| <Nome da pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (LGPD, art. 5º, VIII).> | |  |
| **E-mail Encarregado** | **Telefone Encarregado** |  |
| <xxxx@al.senac.br> | <(99)9999-9999> |  |

|  |
| --- |
| 2 – NECESSIDADE DE ELABORAR O RELATÓRIO |

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa um documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados. Versa a LGPD no seu Art. 5º: “Para os fins desta Lei, considera-se: XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que 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 mitigação de risco.

A elaboração deste relatório apresenta-se necessário tendo em vista a importância operacional e a amplitude dos dados pessoais tratados pelo <nome do sistema avaliado e versão> para o SENAC AL. Os principais titulares que possuem dados pessoais tratados e suportados pelo sistema são <listar os principais titulares de dados pessoais >.

|  |
| --- |
| 3 – O SISTEMA |

<descrever o sistema>

|  |
| --- |
| 4 – DESCRIÇÃO DO TRATAMENTO |

**4.1 – 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.>

**4.2 – 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.>

**4.3 – 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.>

**4.4 – 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. 7 º 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 terceiros;

• tutela da saúde;

• atender aos interesses legítimos do controlador ou de terceiros;

• proteção do crédito; e

• garantia da prevenção à fraude e à segurança do titular.>

<Cumpre 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.

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

|  |
| --- |
| 5 – 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.>

|  |
| --- |
| 6 – 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

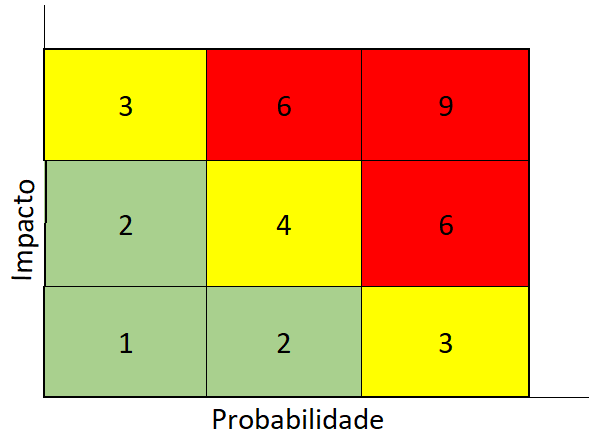
ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.>

|  |
| --- |
| 7 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS |

O processo de avaliação de risco usado nesse documento levará em consideração que os valores de probabilidade e impacto podem variar de 1 a 3, de acordo com a sua intensidade. Os detalhes estão na figura abaixo.



Dessa forma, a criticidade (probabilidade x impacto) de cada risco pode assumir os valores exibidos abaixo.



A tabela abaixomostra o resultado da avaliação dos riscos mais comuns associados a sistemas da informação: <deve ser adaptada para a realidade do sistema avaliado>

| **Id** | **Risco referente ao tratamento de dados pessoais** | **P1** | **I2** | **Nível de**  **Risco**  **(P x I) 3** |
| --- | --- | --- | --- | --- |
| R01 | Acesso não autorizado. |  |  |  |
| R02 | Modificação não autorizada |  |  |  |
| R03 | Perda |  |  |  |
| R04 | Roubo |  |  |  |
| R05 | Remoção não autorizada (usuário não tem a permissão para retirar ou copiar dados pessoais para outro local). |  |  |  |
| R06 | Coleção excessiva (Princípio da finalidade e necessidade |  |  |  |
| R07 | Informação insuficiente sobre a finalidade do tratamento |  |  |  |
| R08 | Tratamento sem o consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente). |  |  |  |
| R09 | Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso). |  |  |  |
| R10 | Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais |  |  |  |
| R11 | Retenção prolongada de dados pessoais sem necessidade |  |  |  |
| R12 | Vinculação/ associação indevida, direta ou indireta, dos dados pessoais ao titular. |  |  |  |
| R13 | Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade |  |  |  |
| R14 | Acesso Indevido às informações do sistema. |  |  |  |
| R15 | Vazamento por intermédio do funcionário |  |  |  |
| R16 | Vazamento de dados no operador |  |  |  |

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).

|  |
| --- |
| 8 – MEDIDAS PARA TRATAR OS RISCOS |

As medidas de tratamento de riscos funcionam como respostas aos riscos identificados. A principal meta é eliminar ou mitigar os efeitos da materialização dos riscos. A tabela abaixomostra a relação entre cada risco e cada medida.

<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**.>

<A seguir é apresentado um exemplo de medida para tratamento de riscos a fim de demonstrar o preenchimento da tabela >.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco** | **Medida(s)** | **Efeito sobre o Risco1** | **Risco Residual2** | | | **Medida(s)3 Aprovada(s)** |
| **P** | **I** | **Nível**  **(P x I)** |
| R01 - Acesso não autorizado. | Adequar o contrato de prestação de serviço ou notificar a empresa de suporte e manutenção do sistema para incluir cláusulas referentes à LGPD. | Compartilhar | 3 | 3 | 9 | sim |
| Funcionalidade para determinação dos usuários com acesso aos dados pessoais contidos no sistema. | Mitigar | 1 | 2 | 2 | não |

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.

Regularmente o DPO deve conduzir auditoria nos processos de negócio à vista da LGPD, esta avaliação inclui sistema avaliado e os dados pessoais por estes mantidos.

O DPO, juntamente com o comitê, é responsável por deliberar quaisquer modificações operacionais e de negócios que impactem a privacidade e a proteção dos dados e os mecanismos de garantia a adequação à LGPD.

|  |
| --- |
| 9 – PLANOS DE AÇÕES |

Para facilitar o trabalho de alocação dos responsáveis, os controles foram agrupados em planos de ações. As informações estão listadas abaixo.

<A seguir é apresentado um exemplo de plano de ação para tratamento de riscos a fim de demonstrar o preenchimento da tabela >.

|  |
| --- |
| 10 – APROVAÇÃO |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nº** | **Medidas** | **Tipo** | **Processos envolvidos** | **Responsável** | **Quando?** |
| 1 | Adequar o contrato de prestação de serviço ou notificar a empresa de suporte e manutenção do sistema para incluir cláusulas referentes à LGPD. | Jurídico | <Listar processos envolvidos> | Setor jurídico |  |
| 2 | Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento | Organizacional | <Listar processos envolvidos> | Setor de TI |  |

A assinatura desse documento atesta que o sistema avaliado terá um nível aceitável de proteção aos dados pessoais, por ele tratados, quando todas as medidas sugeridas nesse relatório forem implementadas dentro das datas definidas.

<**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 LGDP, disponível em**: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>>

|  |  |
| --- | --- |
| **RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO** | **GERENTE DE TI** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <Nome do responsável>  **Matrícula/SIAPE:** xxxxx  <Local>, <dia> de <mês> de <ano> | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <Nome do encarregado>  **Matrícula/SIAPE:** xxxxx  <Local>, <dia> de <mês> de <ano> |

|  |
| --- |
| **ENCARREGADO DE DADOS PESSOAIS (DPO)** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <Nome do representante>  **Matrícula/SIAPE:** xxxxx  <Local>, <dia> de <mês> de <ano> |