<ESPAÇO DESTINADO À IDENTIFICAÇÃO/LOGO DA EMPRESA/ÓRGÃO>

# RELATÓRIO DE IMPACTO

# À PROTEÇÃO DE DADOS PESSOAIS

<Logo Cliente>

<Local>, <dia> de <mês> de <ano>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO/LOGO DA EMPRESA/ÓRGÃO>

**Histórico de Revisões**

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| XX/XX/20XX | 1.0 | XXXXXXXXXXXXXXXXXXXXX | XXXXXXXXXXXX |
| XX/XX/20XX | 2.0 | XXXXXXXXXXXXXXXXXXXXX | XXXXXXXXXXXX |
| | | | |
| | | | |

**ATENÇÃO!**

<Os trechos marcados em azul neste MODELO são campos do **PRIVA**, editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário>.
**<Template Versão 1.0 – Atualizado em 10/03/2025>**

<ESPAÇO DESTINADO À IDENTIFICAÇÃO/LOGO DA EMPRESA/ÓRGÃO>

# RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

| OBJETIVO |
|---|
| Este RIPD, Relatório de Impacto à Proteção de Dados Pessoais, visa descrever os processos de tratamento de dados pessoais na **<Nome Controladora>** que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.<br><br>**Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD). |

## 1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

| **Controlador** | |
|---|---|
| **<Nome Controladora>, <CNPJ Controladora>, <Endereço Controladora>, <Email Controladora>, <Telefone Controlador>, <Site Controlador>** | |
| **Operador** | |
| **Controlador <Nome Controlador>, <Email Controlador>** | |
| **Encarregado** | |
| **Encarregado <Nome Encarregado>** | |
| **E-mail Encarregado** | **Telefone Encarregado** |
| **<Email Encarregado>** | **<Telefone Encarregado>** |

## 2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Para os fins da **LGPD**, de acordo com o **Art. 38**, caput, a qualquer momento, a **Autoridade de Proteção de Dados Pessoais (ANPD)** pode determinar à **<Nome Controladora>,** que entregue relatório de impacto à proteção de dados pessoais demonstrando como se dá o tratamento de dados pessoais e sensíveis na organização, ensejando assim a necessidade de confecção deste documento.

O RIPD reporta a análise sistemática e compreensiva das atividades operacionais, reportando a identificação e ações para mitigação de riscos relacionados à proteção dos dados pessoais. Para isso, identifica os riscos de *compliance* aos requisitos de proteção aos dados pessoais que prevê a Lei 13.709 e como possam impactar a **<Nome Controladora>** e as liberdades individuais dos titulares dos dados, e o potencial de causar impactos econômicos e sociais significantes. O foco, portanto, é no potencial de impacto do risco à **<Nome Controladora>** e aos indivíduos ou à sociedade de forma geral, seja o risco material ou não.

Este documento foi elaborado com base no Guia de Boas Práticas – Lei Geral de Proteção de Dados Pessoais (LGPD), versão 2.0 e Guia de elaboração de RIPD, ambos disponibilizados pelo Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital no link https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

## 3 – DESCRIÇÃO DO TRATAMENTO

Os processos da empresa **<Nome Controladora>** tratam dados pessoais de partes interessadas internas e externas, por meios digitais ou físicos, podendo reter documentos em arquivos físicos ou digitais.

Os dados pessoais são analisados em entrevistas com as áreas de forma a identificar a coleta, o armazenamento, tratamento, compartilhamento, eliminação e a finalidade e a base legal para o processamento, dentre outros aspectos legais de forma a assegurar que os propósitos do tratamento são legítimos, específicos e compatíveis com a finalidade para a qual foram coletados (Art. 5º , X, LGPD). Também são verificadas as ações necessárias para a manutenção da segurança e privacidade e *compliance* com a LGPD.

Os processos têm a gestão concentrada no <**TOTVS Datasul>**, que armazena e processa a maioria dos dados pessoais tratados na empresa **<Nome Controladora>.** Outras ferramentas de apoio ao Datasul e aplicações especificas são utilizadas como **planilhas Excel, TOTVS Fluig, Office 365**. O acesso a Arquivos e pastas físicas é monitorado com controle de acesso e câmeras.

O compartilhamento de dados com terceiros quando acontece é por finalidade específica amparada por contratos.

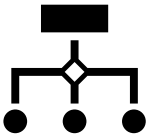
Os dados pessoais tratados na empresa **<Nome Controladora>** são categorizados como abaixo:

**<PRIVA – Categoria de Dados Pessoais>**

| Categoria dos Dados Pessoais | Tipo | Aplicável à <Nome Controladora> |
|---|---|---|
| **Dados de Identificação Pessoal** | Pessoal | Sim |
| **Dados financeiros** | Pessoal | Sim |
| **Características Pessoais** | Pessoal | Sim |
| **Hábitos pessoais** | Pessoal | Pouco provável |
| **Características psicológicas** | Pessoal | Sim |
| **Composição familiar** | Pessoal | Sim |
| **Interesses de lazer** | Pessoal | Pouco provável |
| **Associações** | Pessoal | Sim |
| **Processos judiciais, cíveis e criminais** | Pessoal | Sim |
| **Hábitos de consumo** | Pessoal | Pouco provável |
| **Dados residenciais** | Pessoal | Sim |
| **Educação e treinamento** | Pessoal | Sim |
| **Registros de vídeo, imagem e voz** | Sensível | Sim |
| **Dados biométricos** | Sensível | Não |
| **Dados genéticos** | Sensível | Sim |
| **Dados que identifiquem convicção religiosa** | Sensível | Pouco provável |
| **Dados que identifiquem filiação a organização de caráter religioso** | Sensível | Pouco provável |
| **Dados que identifiquem filiação a sindicato** | Sensível | Sim |
| **Dados que identifiquem crença filosófica** | Sensível | Pouco provável |
| **Dados que identifiquem preferências políticas** | Sensível | Pouco provável |
| **Dados que revelem opinião política** | Sensível | Pouco provável |
| **Dados que identifiquem origem racial ou ética** | Sensível | Sim |
| **Dados relacionados à saúde ou à vida sexual** | Sensível | Sim |

São diferentes os controles internos para mitigar eventuais riscos de falha na proteção de dados pessoais, considerando os fundamentos da proteção de dados pessoais (Art. 2º e incisos, LGPD), a boa-fé e os demais princípios a serem observados nas atividades de tratamento de dados pessoais (Art. 6º e incisos, LGPD).

O monitoramento da adequação à LGPD na empresa **<Nome Controladora>** é feito de forma contínua, seja pela revisão periódica dos processos que tratam dados pessoais seja pela atualização e revisão dos processos quando da adoção de novas ferramentas ou tecnologias.



**<Inserir Fluxo de Processos>**

## 4 – PARTES INTERESSADAS CONSULTADAS

Este foi elaborado com o suporte de consultoria externa e tecnologia aplicada à Proteção de dados Pessoais, **aplicativo PRIVA**, que consolida e processa as informações levantadas junto às áreas da **<Nome Controladora>** para validação da pertinência de tratamento e base regulatória e os controles necessários para a mitigação de riscos.

## 5 – NECESSIDADE E PROPORCIONALIDADE

### 5.1 – Fundamentação Legal

A finalidade e necessidade do tratamento de dados pessoais estão amparadas no Art. 7º,incisos II,III e VI da LGPD.

O compartilhamento de dados só será realizado com o Consentimento do Titular ou na condição que dispense o consentimento, casos da Receita Federal do Brasil, INSS, Ministério do Trabalho e outros órgão competentes governamentais.

### 5.2 – Qualidade e Minimização dos Dados

A coleta de dados pessoais realizada na **<Nome Controladora>** está limitada ao mínimo necessário para o cumprimento da finalidade de tratamento.

### 5.3 – Transferência Internacional de Dados

**<Nome Controladora>** não realiza qualquer tipo transferência internacional de dados. Informações armazenadas em copias backup possuem rastreabilidade.

## 6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

### 6.1 – Metodologia de classificação de Riscos

Esta seção identifica "medidas, salvaguarda e mecanismos de mitigação de riscos" conforme preconiza o Art. 5º, inciso XVII da LGPD.

Para poder identificar os riscos como preconiza o inciso citado, todos os processos na empresa **<Nome Controladora>** foram analisados sob a perspectiva do tratamento de dados pessoais e dos Riscos relacionados à LGPD, conforme mostra tabela **<PRIVA – Tabela Riscos LGPD>** abaixo.

Os **Riscos** foram então identificados e analisados de acordo com a **Probabilidade** de ocorrência e **Impacto** para **<Nome Controladora>** e titulares dos dados.

O método utilizado segue as diretrizes e técnicas de segurança para avaliar o impacto na privacidade de acordo com a seção 6.4.4 da norma ISSO/IEC 29134:2017, que deve ser utilizada na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).

#### 6.1.1 - Riscos relacionados ao tratamento de Dados Pessoais

**<PRIVA – Tabela Riscos LGPD>**

| Id | Risco | Descrição |
|---|---|---|
| R01 | Acesso não autorizado. | Acesso indevido (permissões indevidas) a um ambiente físico, lógico ou virtual |
| R02 | Modificação não autorizada. | Modificação de dados pessoais efetuada por usuário sem permissão. Um processamento indevido pode provocar uma modificação não autorizada. |
| R03 | Perda. | Perdas provocadas por ações intencionais de usuários, uma exclusão indevida, ou devida e não comunicada e provenientes de ações não intencionais como falhas de sistemas, sobrescrita de dados, falhas em hardware, dentre outras. |
| R04 | Roubo. | Dados roubados do Controlador/Operador, falhas nos controles de segurança dos sistemas (ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), dentre outras |
| R05 | Remoção não autorizada. | Retirada ou cópia de dados pessoais para outro local por usuário sem permissão |
| R06 | Coleção excessiva. | Coleta de dados pessoais em quantidade superior à necessária para cumprimento da finalidade do tratamento do dado pessoal. Ausência de políticas internas de descarte e eliminação de dados. |
| R07 | Informação insuficiente sobre a finalidade do tratamento. | O tratamento de dados pessoais é feito de forma não embasada e justificada legalmente, sem transparência para o titular dos dados |
| R08 | Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente). | Tratamento de dados efetuado sem o Consentimento do titular. |
| R09 | Falha em garantir os direitos do titular (Ex.: perda do direito de acesso). | Falha nas garantias de atendimento ao titular dos dados pessoais como previsto nos artigos 17º a 23º da LGPD. |

| | | |
|---|---|---|
| R10 | Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais. | Compartilhamento de dados pessoais com terceiros , sem obtenção do Consentimento do titular (Art. 27º, LGPD) |
| R11 | Retenção prolongada de dados pessoais sem necessidade. | Término da finalidade legal para o tratamento dos dados sem que haja a exclusão ou descarte dos dados tratados. |
| R12 | Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular. | Qualquer acesso ou processamento de dados pessoais efetuado por vinculações ou associações indevidas. |
| R13 | Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal de forma equivocada, falha na validação dos dados de entrada etc.). | Processamento / tratamento de dados pessoais de forma a alterar de maneira indevida a informação. |
| R14 | Falha na reidentificação de dados pseudoanonimizados. | Falhas na execução de scripts para reversão de algoritmos de pseudoanonimização. (Art. 12º e 13º, LGPD). |

Os **Riscos** são classificados de acordo com os aspectos **Probabilidade (**Frequência) e **Impacto (**Consequência**)**, como mostrados abaixo.

| Probabilidade | | | | | |
|---|---|---|---|---|---|
| Aspectos avaliados | Circunstancias excepcionais | Eventualmente | Eventualmente | Quase sempre | Sempre |
| Frequencia | Muito baixa <10% | Baixa >=10% <=30% | Média >30% <=50% | Alta >50% <=90% | Muito alta >90% |
| Peso | 1 | 2 | 3 | 4 | 5 |

<PRIVA – Tabela Probabilidade>

| Impacto | | | | | |
|---|---|---|---|---|---|
| Aspectos | Insignificante | Pequeno | Moderado | Elevado | Grande |
| Consequencia | Muito baixa <10% | Baixa >=10% <=30% | Média >30% <=50% | Alta >50% <=90% | Muito alta >90% |
| Peso | 1 | 2 | 3 | 4 | 5 |

<PRIVA –Tabela Impacto>

O **Peso** apurado pela multiplicação dos pesos estabelecidos para os critérios **Probabilidade** e **Impacto** é então utilizado para estabelecer o **Grau de Risco**, de acordo com a **Matriz de Probabilidade x Impacto** abaixo.

| | Probabilidade | Impacto | | | | |
|---|---|---|---|---|---|---|
| | | Sem impacto | Leve | Médio | Grave | Gravíssimo |
| 5 | Quase certo | 5 | 10 | 15 | 20 | 25 |
| 4 | Alta | 4 | 8 | 12 | 16 | 20 |
| 3 | Média | 3 | 6 | 9 | 12 | 15 |
| 2 | Baixa | 2 | 4 | 6 | 8 | 10 |
| 1 | Rara | 1 | 2 | 3 | 4 | 5 |
| | | 1 | 2 | 3 | 4 | 5 |

<PRIVA – Tabela Probabilidade x Impacto>

O **Peso** obtido pela multiplicação dos fatores **Probabilidade** e **Impacto** classificam o Risco de acordo com a tabela abaixo.

| Peso | Tipo Risco | Ação Esperada |
|---|---|---|
| 1 | Risco Baixíssimo | Aceitar o risco, tratar evento mantendo práticas e procedimentos existentes |
| =>2 <= 4 | Risco Baixo | Aceitar o risco, tratar evento mantendo práticas e procedimentos existentes |
| =>5 <=8 | Risco Moderado | Mitigar, transferir, compartilhar o risco. Ações para reduzir a probabilidade e impacto (revisar contratos) |
| =9 <=14 | Risco Elevado | Reduzir, intervir. Ações para reduzir Probabilidade e Impacto |
| =>15 | Risco Extremo | Evitar, eliminar. Rever / descontinuar ações que geram Risco extremo |

<PRIVA – Grau de Riscos>

### 6.2 –Riscos identificados por Área

Em entrevistas com as Áreas da empresa <Nome Controladora>, todos os Processos de negócio são avaliados em relação aos Riscos relacionados à LGPD. A classificação gera um *score* de **Risco** por **Áreas** com semáforos que mostram o **Grau de Risco** de acordo com a tabela abaixo, **detalhados nos Relatórios de Riscos do PRIVA**, de forma a fornecer ao Controlador informações detalhadas que apontam para planos de ações diligentes e em compliance com a LGPD.

<Nome Controladora> - <PRIVA – Tabela Grau de Riscos por Área>

| Risco | Risco relacionado ao tratamento de Dados Pessoais | Comercial | Compras | Contabilidade | Financeiro | Logística | Qualidade | RH | SESMT | TI |
|---|---|---|---|---|---|---|---|---|---|---|
| R01 | Acesso não autorizado. | | | | | | | | | |
| R02 | Modificação não autorizada. | | | | | | | | | |
| R03 | Perda. | | | | | | | | | |
| R04 | Roubo. | | | | | | | | | |
| R05 | Remoção não autorizada. | | | | | | | | | |
| R06 | Coleção excessiva. | | | | | | | | | |
| R07 | Informação insuficiente sobre a finalidade do tratamento. | N/A | | | | | | | | |
| R08 | Tratamento sem consentimento do titular dos dados pessoais | | | | | | | | | |
| R09 | Falha em garantir 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** | Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal de forma equivocada, falha na validação dos dados de entrada etc.). | N/A | | | | | | | | |
| **R14** | Falha reversão pseudoanonimização | | | | | | | | | |

### 6.3 –Classificação dos Riscos

Após apurados os Riscos para cada **Processo** de cada **Área** da **<Nome Controladora>,** os Riscos à LGPD são classificados conforme tabela abaixo.

| | | | | | Grau de Risco | |
|---|---|---|---|---|---|---|
| **Risco** | **Risco relacionado ao tratamento de Dados Pessoais** | **Nº Processos** | **Probabilidade** | **Impacto** | **P x I** | **Nivel Risco** |
| **R01** | Acesso não autorizado. | 54 | 2 | 3 | **6** | **Risco Moderado** |
| **R02** | Modificação não autorizada. | 50 | 2 | 1 | **2** | **Risco Baixo** |
| **R03** | Perda. | 2 | 3 | 5 | **15** | **Risco Extremo** |
| **R04** | Roubo. | 2 | 2 | 5 | **10** | **Risco Elevado** |
| **R05** | Remoção não autorizada. | 2 | 2 | 3 | **6** | **Risco Moderado** |
| **R06** | Coleção excessiva. | 2 | 1 | 2 | **2** | **Risco Baixo** |
| **R07** | Informação insuficiente sobre a finalidade do tratamento. | N/A | | | | |
| **R08** | Tratamento sem consentimento do titular dos dados pessoais | 6 | 2 | 3 | **6** | **Risco Moderado** |
| **R09** | Falha em garantir os direitos do titular (Ex.: perda do direito de acesso). | 4 | 2 | 3 | **6** | **Risco Moderado** |
| **R10** | Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais. | 4 | 1 | 3 | **3** | **Risco Baixo** |
| **R11** | Retenção prolongada de dados pessoais sem necessidade. | 10 | 2 | 3 | **6** | **Risco Moderado** |
| **R12** | Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular. | 2 | 2 | 2 | **4** | **Risco Baixo** |
| **R13** | Falha/erro de processamento (Ex.: execução de script que atualiza dado forma equivocada, falha na validação dos dados de entrada etc.). | N/A | | | | |
| **R14** | Falha Reidentificação de dados pseudoanonimizados. | N/A | | | | |

## 7 – MEDIDAS DE TRATAMENTO DE RISCOS

### 7.1 –Ações Preventivas

Como Plano de Ações preventivas de respostas a Riscos a empresa **<Nome Controladora>** segue o as diretrizes estabelecidas na tabela **<PRIVA – Tabela Ações Preventivas>** a seguir.

| Ameaça | Solução para Mitigação |
|---|---|
| Perda econômica e dano reputacional pelo não cumprimento da legislação | · Capacitação dos colaboradores sobre proteção de dados.<br>· Monitoramento de processos e colaboradores em relação ao cumprimento da política de privacidade da organização, bem como às sanções pelo não cumprimento. |
| Perdas econômicas de clientes e danos reputacionais por falta de medidas de segurança adequadas ou ineficazes, causando perda de dados pessoais | · Capacitação dos colaboradores sobre proteção de dados.<br>· Monitoramento de processos e colaboradores em relação ao cumprimento à política de privacidade da organização, bem como às sanções pelo não cumprimento. |
| Dificultar a revogação do consentimento ou manifestação de oposição | · Estabelecer procedimentos claros para manifestação da revogação do consentimento e solicitação de oposição à determinado tratamento. |
| Solicitar e tratar dados sensíveis sem necessidade ou adotar medidas preventivas necessárias | · Verificar se o tratamento do dado é necessário para a finalidade pretendida · Verificar se o tratamento tem previsão legal, caso contrário, que tenha a autorização expressa do consentimento. |
| Dificultar a divulgação de informação de proteção de dados utilizando linguagem confusa e imprecisa que impeça a compreensão da transparência do tratamento de dados pessoais | · Elaborar políticas claras, concisas e facilmente acessíveis pelos envolvidos, em formatos padrões em uniformidade com todos os ambientes da organização. |
| Utilizar dados pessoais para finalidades não especificadas ou incompatíveis com as declaradas. | · Elaborar comunicação transparente e clara para que se tratem os dados pessoais por meio de política de privacidade visível e acessível. · Fornecer informações sobre os critérios utilizados na tomada de decisão de tratamento de dados, revisada pooutr pessoa que não o autor. · Fornecer informações claras sobre o equilíbrio entre legítimo interesse do controlador no tratamento de determinado dados pessoal e os direitos fundamentais dos afetados. |
| Acesso não autorizados aos dados pessoais | · Capacitação dos colaboradores sobre proteção de dados. .<br>Estabelecer mecanismos e procedimentos de conscientização dos colaboradores sobre a obrigação de guardar segredo sobre os dados pessoais que conheçam em virtude do exercício de sua atividade contratual. .<br>Estabelecer procedimentos para garantir a destruição do armazenamento dos dados pessoais que já possam ser eliminados. -<br>Monitoramento de processos e colaboradores em relação ao cumprimento à política de privacidade da organização, bem como às sanções pelo não cumprimento.<br>. Notificar aos colaboradores que informará às autoridades competentes, toda a violação de confidencialidade que possam trazer responsabilidades penais.<br>. Estabelecer procedimentos que notifiquem formalmente aos colaboradores que acessem dados pessoais do dever de sigilo e as consequências da sua violação, aplicável a colaboradores, diretoria e prestadores de serviço |
| Tratamento incorreto por parte do operador | · Notificação ao prestador de serviço da falha ocorrida. ·<br>Comunicação da falha ocorrida à ANPD e autoridades cabíveis. ·<br>Elaboração de contrato/aditivo estabelecendo pactuações e diretrizes para o tratamento de dados pessoais. |
| Gestão ineficiente da supervisão do acesso de terceirizados (operadores e subcontratados) para garantir o cumprimento de medidas de segurança e diretrizes estabelecidas pela empresa. | · Estabelecer mecanismos e procedimentos que garantam o controle e que tenham, se necessário, um encarregado de dados. ·<br>Auditorias periódicas para o cumprimento das obrigações contratuais e da proteção de dados pessoais. |
| Dificultar ou impossibilitar o exercício do direito dos interessados (comunicação, retificação, cancelamento e oposição). | · Sistemas que permitam o acesso de forma fácil, direta e com segurança para o exercício de seus direitos. ·<br>Definição de procedimentos de gestão e ferramentas para quem cedeu seus dados pessoais. |
| Falta de medidas de segurança e aplicação ineficiente, indefinição de funções de segurança e estabelecimento de competências. | · Nomeação de um responsável de segurança com competências, atribuições em gestão e desenvolvimento de projetos. ·<br>Estabelecer Políticas de acesso e segurança da informação.<br>· Escritórios com poucos documentos físicos para evitar o acesso não autorizado. |
| Deficiência na organização na gestão de controle de acessos. | · Procedimentos que garantam a revogação de permissões e acessos quando do desligamento da organização. |
| Deficiências técnicas que permitam que pessoas não autorizadas acessem e subtraiam dados pessoais. | · Inventariar os recursos que contenham dados pessoais acessíveis através de rede de telecomunicações. ·<br>Ferramentas de software e hardware que permitam uma gestão eficaz da segurança e dos compromissos na área de proteção de dados pessoais. |

### 7.2 –Plano de Ação e Resposta a Riscos

Após os **Riscos** serem **Classificados** Por **Área** e **Processo** é estabelecido uma **Plano de Ação** com medidas de segurança, técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e demais riscos advindos de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento de dados pessoais inadequado ou ilícito, como ditado pelo Art. 46º da LGPD. Planos de Ação por Área podem ser detalhados no relatório **<PRIVA – Planos de Ação e Resposta por Área>**

Ainda que não seja possível eliminar todos os riscos, é necessário estabelecer parâmetros de riscos aceitáveis, controláveis por ações de prevenção e mitigação, sempre em revisão e atualização. Implementadas todas as ações, espera-se como resultado desta estratégia que os riscos sejam reduzidos ao mínimo grau esperado e tenham a gestão facilitada. Os **Planos de Ação e Resposta a Riscos** detalhados como abaixo devem ser revisados e aprovados pelo Comitê interno de **<Nome Controladora>** que estabelece as diretrizes para a Politica de Privacidade de dados da organização.

As medidas para tratamento de riscos na empresa de **<Nome Controladora>** estão compiladas no Relatório do PRIVA , **<PRIVA – Planos de Ação e Resposta a Riscos>**, como mostrado abaixo.

**(exemplo de saída de relatório)**

**<PRIVA – Planos de Ação e Resposta a Riscos>**

| Risco | Medida(s) | Efeito sobre o Risco | Risco Tolerado | | | Medida(s) Aprovada(s) |
|---|---|---|---|---|---|---|
| | | | P | I | Nível (P x I) | |
| R01 Acesso não autorizado. | 1. Controle de acesso lógico<br>2. Desenvolvimento seguro<br>3. Segurança em redes<br>4. Responsabilização | Reduzir | 2 | 2 | Risco Baixo | Sim |
| R02 Modificação não autorizada | 1. Controle de acesso lógico<br>2. Segurança em redes<br>3. Capacitação de colaboradores<br>4. Responsabilização | Reduzir | 2 | 2 | Risco Baixo | Sim |
| R04 Roubo. | 1. Controle de acesso lógico<br>2. Controles criptográficos<br>3. Proteção e monitoramento cftv ambientes físicos | Reduzir | 1 | 5 | Risco Moderado | Sim |
| R06 Coleção excessiva. | 1. Estabelecer ciclo de vida dado pessoal<br>2. Desenvolvimento de procedimentos e scripts de exclusão dados com finalidade de tratamento vencida. | Reduzir | 1 | 1 | Risco Baixíssimo | Sim |

### 7.3 –Planos de Contingência

Planos de Contingência devem ser aplicados para riscos acontecidos. Antecipados aos riscos, pode auxiliar a reduzir enormemente o custo de uma ação quando do seu acontecimento. Um plano de retrocedimento é desenvolvido se o risco tem um alto impacto, ou se a estratégia selecionada não for totalmente eficaz. A resposta mais comum é o aceite do risco com o estabelecimento de uma reserva de contingencia em tempo, dinheiro e recursos, determinada pelo impacto computado em um nível de exposição de risco aceitável, para o risco que tem de ser aceito.

O Plano de Contingencia abaixo exibe as Ações sugeridas para cada Risco, incluindo o Tempo de Resposta e comunicação de Incidentes à ANPD, de acordo com o Art. 48º da LGPD.

## <PRIVA – Planos de Contingência>

| Riscos Ocorridos | Descrição | Causas | Consequências | Interessados | Ações Sugeridas | Tempo de resposta |
|---|---|---|---|---|---|---|
| **Acesso não autorizado** | Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado ao titular, salvo exceções legais | Ataques cibernéticos<br>Falha de processamento | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar aos interessados<br>Reforçar a segurança do sistema | Até 72 horas |
| **Modificação não autorizada** | Modificação de dados pessoais sem a anuência do titular | Falha humana<br>Ataques cibernéticos<br>Falha de processamento | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar aos interessados<br>Reforçar a segurança do sistema | Até 24 horas |
| **Perda de dados** | Eliminação, destruição ou extravio de dados pessoais | Desastres naturais<br>Blackouts<br>Ataques cibernéticos<br>Falha de processamento | Impactos ao cidadão<br>Impactos à organização<br>Não compliance | Titular dos dados e<br>Controladora | Comunicar aos interessados e à ANPD<br>Reforçar segurança sistema | Até 24 horas |
| **Vazamento de dados** | Por apropriação ou uso indébito de dados pessoais | Ataques cibernéticos<br>Falha de processamento | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar aos interessados e à ANPD<br>Reforçar a segurança do sistema | Até 48 horas |
| **Eliminação não autorizada** | Eliminação de dados pessoais sem autorização do titular | Ataques cibernéticos<br>Falha de processamento | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar interessados.<br>Recuperar os dados eliminados. | Até 24 horas |
| **Coleção excessiva** | Coleta de mais dados que o necessário | Falha governança proteção dados | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar interessados.<br>Eliminar ou anonimizar os dados em excesso. | Até 48 horas |
| **Finalidade de tratamento não comprovada** | A finalidade de tratamento declarada é insatisfatória, não se comprova | Falha governança proteção dados | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar aos interessados a real necessidade de tratamento. | Até 24 horas |
| **Tratamento sem consentimento** | Tratamento de dados sem a previa permissão expressa, inequívoca e informada do titular, salvo exceções legais | Falha governança proteção dados | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar interessados.<br>Obter o consentimento ou eliminar tratamento<br>Caso não obtenha, eliminar ou anonimizar os dados. | Até 48 horas |
| **Compartilhamento de dados pessoais com terceiros sem consentimento do titular** | Compartilhamento de dados sem o consentimento do titular | Falha governança proteção dados | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados<br>Controladora e Operadores | Comunicar aos interessados.<br>Obter ou não o consentimento.<br>Caso não obtenha, eliminar ou anonimizar os dados. | Até 48 horas |
| **Falha ou erro de processamento** | Falhas em processamento de dados que causem atualizações equivocadas ou imperfeitas ou **vazamento de informações** | Desastres naturais<br>Blackouts<br>Ataques cibernéticos<br>Falha governança proteção dados | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar aos interessados e à ANPD<br>Reforçar a segurança do sistema. | Até 48 horas |
| **Re-identificação de dados anonimizados** | Falhas na anonimização ou anonimizados / pseudoanonimizados que impossibilitem a identificação do titular e perda de informações | Falha governança proteção dados | Impactos ao cidadão<br>Impactos à organização<br>Não *compliance* | Titular dos dados e<br>Controladora | Comunicar aos interessados e à ANPD<br>Reforçar a segurança do sistema, ajustando o tratamento dos dados anonimizados. | Até 48 horas |

<ESPAÇO DESTINADO À IDENTIFICAÇÃO/LOGO DA EMPRESA/ÓRGÃO>

## 8 – APROVAÇÃO

Este RIPD, Relatorio de Impacto à Proteção de Dados, foi revisado e aprovado em Comitê e segue assinado pelos representantes de **<Nome Controladora>**.

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento de dados pessoais, como sugerido pelas diretrizes do guia utilizado para elaboração deste relatório, citado à página 2 deste relatório.

| REPRESENTANTE DO CONTROLADOR | ENCARREGADO |
|---|---|
| _____ | _____ |
| <Nome do representante> | <Nome do representante> |
| **Matrícula:** xxxxx | **Matrícula:** xxxxx |
| <Local>, <dia> de <mês> de <ano> | <Local>, <dia> de <mês> de <ano> |