

# RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

## Histórico de Revisões

Data	Versão	Descrição	Autor
25/02/2024	1.0	Conclusão da primeira versão do relatório	Wellerson W. Reis

# 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

<b>Controlador</b> Departamento de Segurança	
<b>Operador</b> SOAP2 GRUPO 7	
<b>Encarregado</b> Fulano de Tal Silva	
<b>E-mail Encarregado</b> <a href="mailto:privacidade@grupo7.com.br">privacidade@grupo7.com.br</a>	<b>Telefone Encarregado</b> +9999 (0) 999 799 9 799

## 2 – NECESSIDADE DE ELABORAR O RELATÓRIO

O RIPD do FAST FOOD FIAP foi elaborado para os seguintes objetivos:

2.1 Para atendimento à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e regulamentação emanadas pela Autoridade Nacional de Proteção de Dados -ANPD.

2.2 Para orientação e direcionamento dos funcionários do FAST FOOD FIAP com relação ao tratamento das informações pessoais de clientes, colaboradores e demais interlocutores, que por necessidade de negócios são coletadas em seus processos formais.

2.3 Para definição de políticas internas de garantia da segurança e governança dos dados pessoais coletados;

2.4 Para garantia de proteção e mitigação de riscos eventualmente envolvidos evitando:

- i) ameaças ou riscos à privacidade; à segurança; à integridade e/ou à confidencialidade;
- ii) destruição acidental ou ilícita; perda; alteração; divulgação ou acesso não autorizado;
- iii) quaisquer outras formas ilegais de tratamento; e
- iv) incidentes de segurança ou privacidade.

## 3 – DESCRIÇÃO DO TRATAMENTO

Os sistemas e processos do FAST FOOD FIAP foram desenhados para a captação somente dos dados que se fazem pertinentes para a elaboração de contratos comerciais; cadastro de clientes e fornecedores; informações para atendimentos a demandas fiscais e legais; registros de funcionários e para ações de marketing

### 3.1 – NATUREZA DO TRATAMENTO

3.1.1 Os dados pessoais são coletados mediante preenchimento de formulário eletrônico do FAST FOOD FIAP pelo titular dos dados pessoais. Os dados são transferidos e armazenados nos servidores cloud na Amazon Web Services (AWS), administrados pelo FAST FOOD FIAP e localizados no Norte da Virginia, nos EUA.

3.1.2 A fonte de dados é o titular dos dados pessoais mediante o preenchimento de formulário eletrônico do FAST FOOD FIAP.

3.1.3 São compartilhados com o Mercado Pago o Nome e o CPF para emissão do código PIX para pagamento.

3.1.4 O operador de dados pessoais é a administração da empresa FAST FOOD FIAP, o SOAP2 GRUPO 7, o qual é responsável pela implementação do sistema que automatiza todas as

operações de tratamento de dados pessoais (Coleta, Retenção, Processamento, Compartilhamento e Eliminação).

3.1.5 As medidas de segurança atualmente adotadas são: Controle de Acesso Lógico, Controles Criptográficos, Controles de Segurança em Redes, Proteção Física e do Ambiente.

## 3.2 – ESCOPO DO TRATAMENTO

3.2.1 Os dados pessoais tratados pelo FAST FOOD FIAP abrangem: - Informações de identificação pessoal: Nome, e-mail e CPF;

3.2.2 Os dados coletados de acordo com o item 3.2.1 são para estrito cumprimento de relações comerciais, contratuais e legais, protegidos por cláusulas de sigilo. Todo funcionário do FAST FOOD FIAP é treinado e assina termo de ciência com relação as informações;

3.2.3 A quantidade de dados pessoais tratados é de 3 dados pessoais. A frequência de tratamento dos dados pessoais é 24x7 (24 horas por dia nos 7 dias da semana).

3.2.4 Os dados pessoais obtidos serão mantidos armazenados durante a existência da empresa. Esse período de armazenamento poderá ser revisto em alinhamento a qualquer nova disposição legal sobre prazo de retenção.

3.2.5 A abrangência do tratamento de dados pessoais é nacional para manutenção do cadastro único dos clientes.

## 3.3 – CONTEXTO DO TRATAMENTO

3.3.1 Qualquer coleta de dados pessoais é avisada ao titular através de documentos informativos no site do FAST FOOD FIAP no contato via e-mail organizacional e por aditivos de contrato, no caso de funcionários;

3.3.2 A política de sigilo da organização garante ciência por parte de todos os colaboradores do cuidado no trato com as informações pessoais e na proibição de qualquer compartilhamento sem o consentimento pessoal do titular e da organização.

3.3.3 O FAST FOOD FIAP utiliza recursos de segurança robustos para evitar qualquer acesso indevido em sua base de dados.

3.3.4 Qualquer atualização, compartilhamento dos dados pessoais ou acessos suspeitos são avisados ao titular. Embora os campos Nome, CPF e e-mail sejam restritos para alteração. O titular pode requisitar informações sobre seus dados pessoais a qualquer momento.

## 3.4 – FINALIDADE DO TRATAMENTO

A finalidade para a coleta de dados pessoais pelo FAST FOOD FIAP atende exclusivamente:

3.4.1 O cumprimento de obrigação legal fiscal, comercial ou regulatória;

3.4.2 Execução de contrato de compra e venda de mercadorias e outros contratos, assim como de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

3.4.3 Atender aos interesses legítimos para o pleno funcionamento da organização.

**Para a elaboração do presente documento foram consultados representantes internos da organização; consultores jurídicos e analistas das empresas que prestam serviços de armazenamento de informações através das ferramentas contratadas, bem como necessidade de consumidores, clientes e prestadores.**

## 4 – PARTES INTERESSADAS CONSULTADAS

4.1 Analistas de segurança da informação do FAST FOOD FIAP, os quais indicaram as oportunidades de melhoria para aperfeiçoamento da proteção dos dados pessoais tratados.

4.2 Consultor jurídico, responsável por emitir parecer sobre a conformidade do tratamento de dados em relação aos aspectos legais da LGPD.

4.3 Coordenadores, servidores e Diretores do FAST FOOD FIAP a fim de obter informações técnicas e administrativas sobre o processo de trabalho executado.

4.4 Encarregado do tratamento de dados pessoais, que desempenhou o papel de conduzir o levantamento e apreciar as informações técnicas, administrativas, legais e de riscos fornecidas pelas demais partes consultadas.

4.6 Com exceção dos clientes, todas as demais partes consultadas participaram do processo de análise de riscos relativos ao tratamento dos dados pessoais.

## 5 – NECESSIDADE E PROPORCIONALIDADE

### 5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1 A hipótese legal para tratamento de dados pessoais é o art. 7º, I da LGPD: “mediante o fornecimento de consentimento pelo titular”; e II da LGPD: “para o cumprimento de obrigação legal ou regulatória pelo controlador”.

### 5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

5.2.1 A escolha dos dados a serem coletados para implementação dos processos do FAST FOOD FIAP foi baseada na preocupação de coletar o mínimo de dados pessoais necessários para execução das suas atividades para elaboração de contratos comerciais e de contratos trabalhistas.

### 5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

5.3.1 Em períodos planejados, o FAST FOOD FIAP conduz inspeção sobre as medidas de segurança nas suas plataformas de acesso por profissional credenciado internamente, a fim de avaliar se esses processos estão em conformidade com as diretrizes definidas pelo controlador.

5.3.2 Internamente, o acesso aos sistemas que gerenciam e armazenam os dados pessoais possui uma política de senha de acesso individualizada.

5.3.3 Tanto o sistema de segurança quanto a política de sigilo garantem o correto trato das informações coletadas, sendo possível a aplicação de medidas cabíveis em caso de violações.

## 5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.4.1 O Sistema do FAST FOOD FIAP são disponibilizados para que os titulares dos dados pessoais possam demandar as solicitações previstas pelo art. 18º da LGPD. A Política de Privacidade informa sobre o direito que o titular dos dados pessoais tem de realizar qualquer uma das referidas solicitações. A Política de Privacidade pode ser encontrada no link [fastfoodfiap.com.br/politica-privacidade](http://fastfoodfiap.com.br/politica-privacidade).

5.4.2 Caso o usuário identifique alguma falha ou vulnerabilidade de segurança no sistema, é possível reportá-la também pelo e-mail [privacidade@grupo7.com.br](mailto:privacidade@grupo7.com.br).

5.4.3 Quando solicitado pelo titular do dado pessoal, o FAST FOOD FIAP fornecerá informações de privacidade (confirmação de existência ou o acesso a dados pessoais) por meio de e-mail ou sob forma impressa, de acordo com a solicitação do referido titular.

## 5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.5.1 O armazenado de dados em servidores internacionais e consequente transferência internacional de dados, está de acordo com o art. 33º, que define todas as permissões para a transferência internacional de dados pessoais.

## 6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

6.1 Para identificação e avaliação de Riscos do Relatório de Impacto à Proteção de Dados Pessoais tratados pela FAST FOOD FIAP utilizou-se a Matriz Impacto x Probabilidade, como forma de se avaliar o nível dos riscos e descrever medidas, salvaguardas para a mitigação dos mesmos.

6.1.1 Para cada risco identificado, define-se: a probabilidade (P) de ocorrência do evento de risco, o possível impacto (I) caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

6.2.1 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 utilizou-se os seguintes parâmetros escalares apresentados na tabela a seguir:



Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	5	15	75
R02	Coleção excessiva.	5	10	50
R03	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R04	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R05	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.).	10	15	150
R06	Informação insuficiente sobre a finalidade do tratamento.	5	10	50
R07	Modificação não autorizada.	10	15	150
R08	Perda.	15	15	225
R09	Reidentificação de dados pseudonimizados.	5	15	75
R10	Remoção não autorizada.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	5	10	50
R12	Roubo.	10	15	150
R13	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R14	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75

\* verde, é entendido como baixo;

\* amarelo, representa risco moderado; e

\* vermelho, indica risco alto.

## 7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco <sup>1</sup>	Risco Residual <sup>2</sup>			Medida(s) <sup>3</sup> Aprovada(s)
			P	I	Nível (P x I)	
R01 - Acesso não autorizado	Implantação de uma política de acesso às informações.	Evitar	5	15	75	Sim
R03 - Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento	Incluir cláusulas específicas sobre o tratamento e	Evitar	5	5	25	Sim

do titular dos dados pessoais.	compartilhamento de dados pessoais.					
R04 - Falha em considerar os direitos do titular dos dados pessoais	Realizar auditoria para verificar o cumprimento dos direitos dos titulares.	Evitar	5	5	25	Sim
R05 - Falha/erro de processamento	Implementar testes automatizados para verificar a integridade do processamento.	Reduzir	5	15	75	Sim
R07 - Modificação não autorizada.	Implementar controles rigorosos de acesso aos dados pessoais	Evitar	5	15	75	Sim
R08 - Perda	Manter cópias de backup dos dados e criar um plano de recuperação de dados em caso de perdas acidentais.	Reduzir	5	15	75	Sim
R09 - Reidentificação de dados pseudonimizados	Manter os dados pseudonimizados separados dos dados identificáveis e implementar controles rigorosos de acesso aos dados pseudonimizados.	Evitar	5	5	25	Sim
R10 - Remoção não autorizada	Manter cópias de backup dos dados, manter registros detalhados das operações de exclusão e estabelecer mecanismos de monitoramento para detectar atividades suspeitas.	Evitar	5	10	50	Sim
R12 - Roubo	Restringir o acesso apenas a usuários autorizados.	Evitar	5	15	75	Sim
R13 - Tratamento sem consentimento do titular dos dados pessoais	Obter consentimento explícito dos titulares e manter uma política de	Evitar	5	5	25	Sim

	privacidade acessível e compreensível					
R14 - Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	Adotar medidas que preservem a privacidade e a confidencialidade desses dados com a pseudonimização correta dos dados pessoais.	Evitar	5	5	25	Sim

Legenda:

<sup>1</sup> 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**.

<sup>2</sup> Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

<sup>3</sup> Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

## 8 – APROVAÇÃO

*Rúbrica*

Responsável pela elaboração do RIPD

*Rúbrica*

Encarregado

*Rúbrica*

Autoridade  
Representante do Controlador

*Rúbrica*

Autoridade  
Representante do Operador