Relatório de Impacto à Proteção de Dados Pessoais

(RIPD)

1. Introdução:

Este Relatório de Impacto à Proteção de Dados Pessoais (RIPD) foi elaborado para avaliar o sistema de autoatendimento proposto para a lanchonete em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei n.º 13.709/2018). O objetivo é garantir que as práticas de tratamento de dados pessoais estejam em conformidade com as disposições legais, minimizando riscos e assegurando a proteção dos direitos dos titulares.

2. Identificação dos Agentes de Tratamento e do Encarregado

Controlador:	Pikles FastFood Ltda.
Operador(es):	João Silva Maria Oliveira Pedro Santos Ana Lima
Encarregado:	Patrick Vasconcelos
E-mail do Encarregado:	lgpd@piklesfastfood.com.br
Telefone Encarregado	(51) 91234-5678

3. Necessidade de Elaborar o Relatório

De acordo com a Lei Federal nº 13.709/2018 (LGPD), o Relatório de Impacto à Proteção de Dados (RIPD) poderá ser solicitado a qualquer momento pela Autoridade Nacional de Proteção de Dados (ANPD) (art. 38, Lei nº 13.709/2018).

Durante a realização do data mapping, verificou-se que há tratamento de dados pessoais dos clientes pelo sistema de autoatendimento e pelo sistema de pedidos online da lanchonete Pikles FastFood. Esses dados incluem nome, CPF, endereço, número de telefone e dados de pagamento, quando fornecidos.

Além disso, também foi identificada a existência do tratamento de dados pessoais sensíveis de clientes no contexto de processamento de pedidos e pagamentos. Este tratamento envolve o armazenamento temporário de informações de pagamento para fins de transações.

Em razão da identificação de tais situações quando da realização do mapeamento de dados realizado entre os sistemas e processos da

lanchonete, apresenta-se o presente documento, que foi elaborado com observância das seguintes etapas:

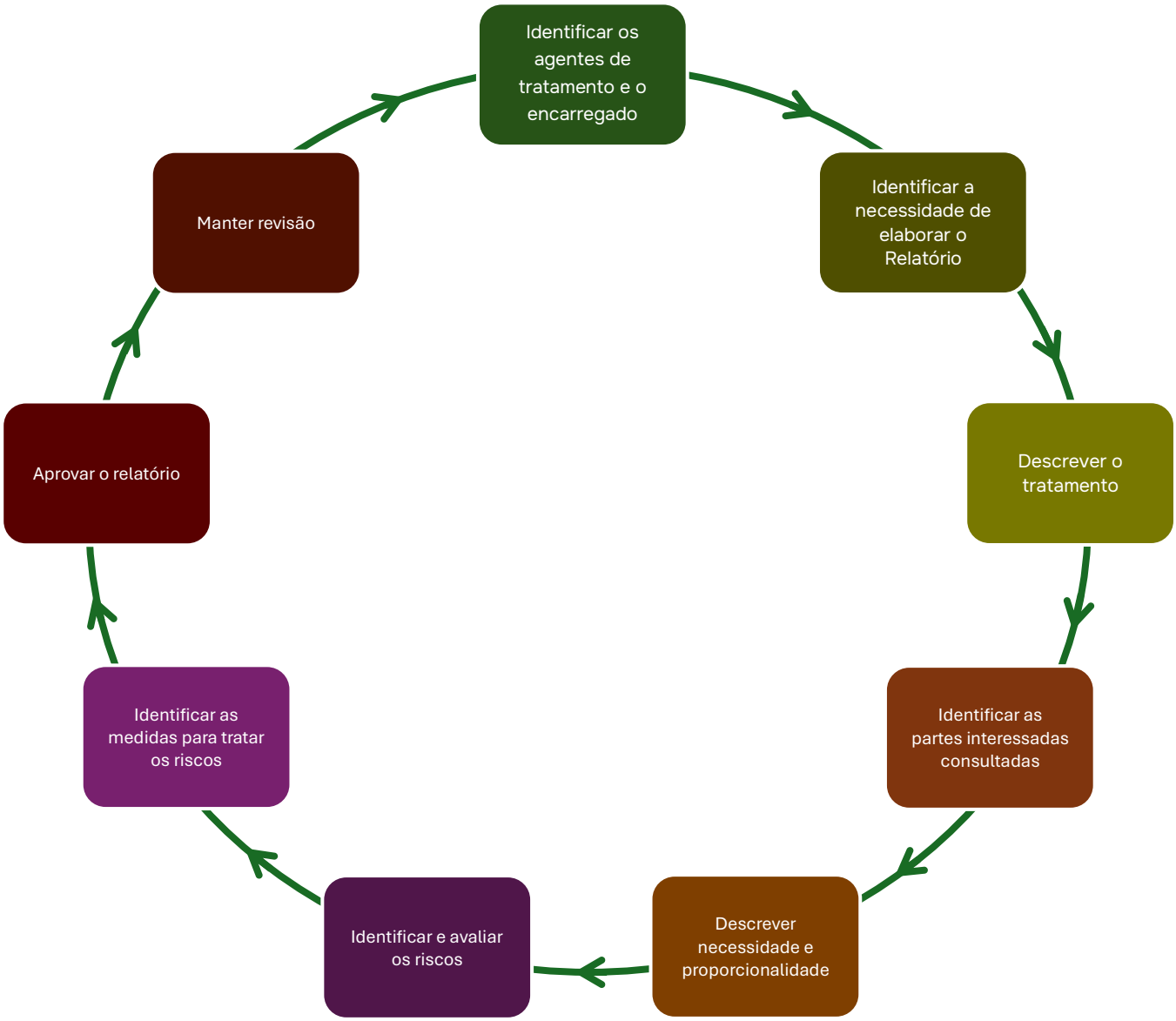

Figura 1 - Etapas construção do RIPD

Optou-se pela elaboração de um documento único, tendo em vista que, a partir do mapeamento dos sistemas e processos, verificou-se que a lanchonete Pikles FastFood não possui um alto grau de complexidade no tratamento dos dados pessoais, não havendo a implementação de vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais.

Entretanto, considerando-se que a implementação da proteção de dados pessoais é um trabalho contínuo, que deve ser objeto de revisões periódicas a fim de manter-se coerente com a realidade das atividades desenvolvidas pela Pikles FastFood, este documento poderá ser oportunamente revisado e, até mesmo, subdividido em tantos quantos se fizerem necessários.

4. Descrição do Sistema:

A lanchonete implementará um sistema de autoatendimento com as seguintes funcionalidades:

- Identificação dos clientes por CPF, cadastro com nome, e-mail e CPF, ou anônimo.
- Interface de seleção de produtos (lanche, acompanhamento, bebida).
- Pagamento via QRCode do Mercado Pago.
- Acompanhamento do pedido (Recebido, Em preparação, Pronto, Finalizado).
- Notificação de pedido pronto para retirada.
- Acesso administrativo para gerenciar clientes, produtos e acompanhar pedidos.

5. Descrição do Tratamento

Conforme previsto na LGPD (art. 5º, X), tratamento consiste em "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".

Com relação ao ciclo de vida do tratamento de dados pessoais, tem-se as seguintes etapas:

Neste contexto, a partir do mapeamento dos processos da lanchonete Pikles FastFood, identificou-se que a empresa realiza o tratamento dos seguintes dados pessoais dos clientes:

- Nome completo;
- Endereço;
- E-mail;

- Número de telefone;
- CPF;

Dados de pagamento (ex. número do cartão de crédito, se armazenado).

Com relação ao clico de vida do tratamento de dados pessoais, tem-se as seguintes etapas:

Figura 2 – Ciclo de vida do tratamento de dados pessoais

Natureza, Escopo, Contexto e Finalidade do Tratamento:

a) Coleta de Dados para Pedidos: Coletamos e tratamos dados pessoais, como nome, CPF, e-mail e número de telefone do cliente, quando este se identifica no sistema de autoatendimento. Esses dados são utilizados para registrar e gerenciar pedidos, bem como para identificar o cliente e fornecer uma experiência personalizada.
b) Dados de Pagamento: Durante o processo de pagamento, coletamos dados de pagamento para processar transações. Para o MVP, a forma de pagamento será via QRCode do Mercado Pago, e os dados de pagamento são tratados de acordo com as políticas de segurança do provedor de pagamento.
c) Acompanhamento de Pedidos: Os dados dos pedidos são utilizados para informar o cliente sobre o status de seu pedido, desde o recebimento até a finalização. Isso inclui a exibição do progresso do pedido em um monitor.
d) Campanhas Promocionais: Com a identificação dos clientes, a lanchonete pode enviar campanhas promocionais, caso o cliente tenha consentido com o uso de seus dados para essa finalidade.

e) Gestão de Produtos e Categorias: Os dados relativos aos produtos, incluindo nome, categoria, preço, descrição e imagens, são gerenciados pela lanchonete para facilitar o processo de pedidos.

Todos os dados são coletados e tratados no contexto da prestação de serviços de alimentação, com a finalidade de melhorar a eficiência do atendimento e a satisfação do cliente. A título exemplificativo, segue link das políticas de privacidade e termos de uso da Pikles FastFood: www.piklesfastfood.com.br/privacidade.

6. Partes Interessadas Consultadas

Foi realizado um mapeamento a partir de questionários preenchidos pelas seguintes áreas da Pikles FastFood:

- Setor de Atendimento ao Cliente: Responsável pelo contato direto com os clientes.
- Departamento de Marketing: Encarregado das campanhas publicitárias e promoções, coleta de dados para ações de marketing direcionadas.
- Setor de Logística e Distribuição: Gerenciamento da entrega de pedidos, incluindo a coordenação com serviços de entrega terceirizados.
- Departamento de Recursos Humanos: Gestão dos dados dos funcionários, incluindo informações pessoais e dados sensíveis relacionados à saúde e dependentes.
- Setor de Tecnologia da Informação: Administração dos sistemas de pedidos online, armazenamento de dados e segurança da informação.
- Departamento Financeiro: Processamento e armazenamento de informações de pagamento de clientes e dados financeiros da empresa.
- Setor de Compras: Aquisição de materiais e insumos, incluindo a coordenação com fornecedores.
- Supervisão de Qualidade e Segurança Alimentar: Garantia da conformidade com normas de segurança alimentar, incluindo auditorias e relatórios de incidentes.

A partir do mapeamento feito, foi possível definir, dentre outros, quais os dados pessoais tratados, sua finalidade, a forma de armazenamento, rotinas de atualização e eliminação e com quem tais dados são compartilhados.

Além dos setores da Pikles FastFood, seus sistemas internos também foram objeto de mapeamento, sendo possível definir, dentre outros, se há acesso de terceiros, se existe rotina de backup, a existência de procedimentos para anonimização dos dados pessoais, bem como a finalidade do tratamento dos dados em tais sistemas.

Foram identificadas as seguintes práticas específicas:

- Setor de Atendimento ao Cliente: Coleta de nome, telefone, e-mail, e endereço para atendimento e entregas.
- Departamento de Marketing: Uso de dados de contato para campanhas de marketing direcionadas.
- Setor de Logística e Distribuição: Armazenamento de informações de entrega e coordenação com serviços de entrega terceirizados.
- Departamento de Recursos Humanos: Armazenamento de dados pessoais e sensíveis de funcionários, incluindo dependentes.
- Setor de Tecnologia da Informação: Implementação de medidas de segurança da informação e backups regulares.
- Departamento Financeiro: Processamento seguro de pagamentos e armazenamento de dados financeiros.
- Setor de Compras: Coordenação com fornecedores para aquisição de insumos, sem compartilhamento de dados pessoais de clientes.

Essas informações foram coletadas com o objetivo de garantir que todas as práticas de tratamento de dados pessoais estejam em conformidade com a LGPD, promovendo a transparência e a segurança no tratamento dos dados dos clientes e funcionários da Pikles FastFood.

7. Necessidade e Porporcionalidade

A Pikles FastFood realiza o tratamento dos dados pessoais mencionados nas seções anteriores para os fins estritamente necessários à consecução de suas finalidades operacionais e comerciais, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Sinteticamente, conforme exposto no item anterior, a Pikles FastFood realiza o tratamento de três categorias de dados (clientes, fornecedores e funcionários) com fundamento no artigo 7º, inciso V, da Lei nº 13.709/2018 ("quando necessário para a execução de contrato"), podendo,

eventualmente, haver o compartilhamento em razão do disposto no artigo 7º, inciso III, da referida Lei.

Para garantir a transparência no tratamento dos dados, bem como assegurar aos titulares o exercício dos seus direitos com a maior efetividade e eficácia possíveis, a Pikles FastFood possui um Portal de Privacidade no qual são elencados, além dos conceitos básicos da legislação, os compromissos da Pikles FastFood com a privacidade e a proteção dos dados pessoais. Este portal detalha como o tratamento dos dados pessoais é realizado, tanto no ambiente físico quanto no digital, incluindo a utilização de nosso site e aplicativo.

Além disso, o Portal de Privacidade fornece os dados de identificação e contato direto com o Encarregado de Dados (DPO) nomeado pela Pikles FastFood, garantindo que os titulares dos dados possam exercer seus direitos de forma rápida e eficiente. Este canal permite que os titulares solicitem informações sobre o tratamento de seus dados, façam pedidos de correção, exclusão ou portabilidade dos dados, e reportem qualquer incidente relacionado à privacidade e proteção de dados.

A Pikles FastFood se compromete a revisar periodicamente suas práticas de tratamento de dados para assegurar que permanecem adequadas, necessárias e proporcionais às finalidades para as quais os dados foram coletados, sempre em conformidade com a LGPD e as melhores práticas de segurança da informação.

8. Identificação e Avaliação dos Riscos

Com base nos termos do art. 5º, inciso XVII da LGPD, o Relatório de Impacto deve conter “medidas, salvaguardas e mecanismos de mitigação de risco”. Diante disso, os parâmetros escalares que serão adotados neste Relatório são os seguintes:

Classificação e Valor

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Tabela 1: Classificação e Valor

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco:

Matriz Probabilidade x Impacto

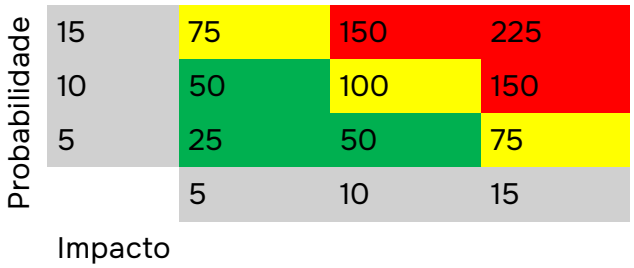

Tabela 2: Matriz Probabilidade x Impacto

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;
- Região amarela representa risco moderado;
- Região vermelha indica risco alto.

Ressalte-se, por oportuno, que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais pela Pikles FastFood é realizado em consonância com a Política de Gestão de Riscos e boas práticas consolidadas e identificadas no mercado.

Tabela de Riscos

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I)[3]
R01	Acesso não autorizado aos dados pessoais armazenados em meio físico e/ou digital	15	10	150
R02	Modificação não autorizada de dados pessoais em meio digital	10	15	150
R03	Informações insuficientes aos titulares sobre a finalidade do tratamento	10	5	50
R04	Armazenamento excessivo de dados pessoais	10	10	100
R05	Armazenamento indevido de dados pessoais em computadores e/ou e-mails	15	10	150
R06	Vazamento e/ou compartilhamento indevido de dados de crianças e/ou adolescentes	15	15	225
R07	Vazamento e/ou compartilhamento de dados sensíveis de empregados	15	15	225
R08	Armazenamento de dados pessoais além dos prazos legais	10	10	100
R09	Falha em considerar os direitos do titular dos dados pessoais	10	5	50
R10	Compartilhamento indevido dos dados pessoais com terceiros	10	15	150
R11	Vazamento e/ou compartilhamento indevido de dados pessoais de clientes	15	10	150

Tabela 3: Tabela de Riscos

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.

9. Medidas para Tratar os Riscos

Conforme fixado pelo artigo 46 da LGPD, 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.

Em razão disso, passa-se a relacionar os riscos e suas medidas:

Tabela de Riscos e Medidas

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
Acesso não autorizado aos dados pessoais	Implantar controles de acesso aos sistemas por meio de usuário e	Reduzir	10	15	150	Sim

armazenados em meio físico e/ou digital	senha, e de acesso físico aos depósitos					
Modificação não autorizada de dados pessoais em meio digital	Implementar rastreabilidade de alteração de dados e fluxo de retificação de dados por solicitação do titular	Reduzir	10	15	150	Sim
Informações insuficientes aos titulares sobre a finalidade do tratamento	Implementar e divulgar o Portal de Privacidade e o fluxo de acesso de dados aos titulares	Evitar	5	5	25	Sim
Armazenamento excessivo de dados pessoais	Solicitar apenas os dados estritamente necessários	Evitar	5	5	25	Sim
Armazenamento indevido de dados pessoais em computadores e/ou e-mails	Realizar capacitação contínua dos colaboradores	Reduzir	10	5	50	Sim
Vazamento e/ou compartilhamento indevido de dados de crianças e/ou adolescentes	Implantar controles de acesso aos sistemas por meio de usuário e senha, e de acesso físico aos depósitos	Reduzir	10	15	150	Sim
Vazamento e/ou compartilhamento de dados sensíveis de empregados	Implantar controles de acesso aos sistemas por meio de usuário e senha, e de acesso físico aos depósitos	Reduzir	10	15	150	Sim
Armazenamento de dados pessoais além dos prazos legais	Implementar como rotina dos setores a eliminação dos dados após os prazos legais	Evitar	5	10	50	Sim
Falha em considerar os direitos do titular dos dados pessoais	Estimular e divulgar o uso do canal de comunicação direto dos titulares com o Comitê Gestor e o DPO	Evitar	5	5	25	Sim
Compartilhamento indevido dos dados pessoais com terceiros	Realizar capacitação dos colaboradores sobre a LGPD, incluindo as hipóteses de compartilhamento	Reduzir	10	10	100	Sim
Vazamento e/ou compartilhamento indevido de dados pessoais de clientes	Implantar controles de acesso aos sistemas por meio de usuário e senha, e de acesso físico aos depósitos	Reduzir	10	15	150	Sim

Legenda:
P – 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).
I – Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
Nível de Risco – magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências.
[1] Efeito sobre o Risco: 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: risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.
[3] Medida(s) Aprovada(s): indicação se as medidas foram aprovadas para implementação.

Assim, com base na tabela acima, a Pikles FastFood irá endereçar as ações mapeadas para as áreas responsáveis viabilizarem a implantação no curto prazo. No decorrer de 2024, caberá ao Comitê Gestor de Privacidade e Proteção de Dados Pessoais monitorar os resultados das medidas, buscando avaliar a assertividade das mesmas e, eventualmente, recomendar ajustes.

10. Conclusão:

A implementação do sistema de autoatendimento será acompanhada de medidas rigorosas para garantir a conformidade com a LGPD e a proteção dos dados pessoais dos clientes. A avaliação contínua e a adoção de práticas de segurança e privacidade são essenciais para mitigar riscos e garantir a confiança dos clientes.

11. Aprovação

RESPONSÁVEIS PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADA DE DADOS (DPO)
_____ Raissa Costa	_____ Giselle Farias

AUTORIDADE REPRESENTANTE DO CONTROLADOR
_____ Ricardo Leite de Castro