RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 24 de fevereiro de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
24/02/2024	1.0	Conclusão da primeira versão do relatório	Felipe Bento Gabriel Santos

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 alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e 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	
Felipe Bento Gabriel Santos	
Operador	
Benjamin Luiz Nelson Almada	
Encarregado	
Luiz Antonio Bryan Caldeira	
E-mail Encarregado	**Telefone Encarregado**
luiz-caldeira77@img.com.br	(69) 98845-1029

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

A Tech Challenge Fast-Food, como controladora de dados pessoais, reconhece a importância e a necessidade de desenvolver este RIPD em conformidade com a artigo 5, inciso II, artigo 10, parágrafo 3, artigo 14, artigo 42 todos da Lei 13.907/2018 - Lei Geral de Proteção de Dados do Brasil (LGPD). Este relatório visa documentar o tratamento de dados dentro da empresa, avaliar os riscos associados e estabelecer medidas para tratá-los, garantindo a proteção dos dados pessoais de clientes conforme ditam as obrigações legais.

3 – DESCRIÇÃO DO TRATAMENTO

A descrição do tratamento inclui o processamento de informações como CPF, Nome Completo e E-mail de clientes para a realização de pedidos online, gestão de contas, comunicações de marketing e processamento de pagamentos. Estes processos são necessários para a prestação adequada dos serviços oferecidos pela Tech Challenge Fast Food e incluem o armazenamento em banco de dados seguro até a sua exclusão conforme a política de retenção de dados da empresa.

4 – PARTES INTERESSADAS CONSULTADAS

Para a elaboração deste RIPD, foram consultados representantes dos departamentos Jurídico, de Tecnologia da Informação, Atendimento ao Cliente e Marketing. Além disso, a empresa buscou o aconselhamento de especialistas externos em proteção de dados para garantir que todas as perspectivas fossem consideradas na avaliação do tratamento de dados pessoais.

5 – NECESSIDADE E PROPORCIONALIDADE

As atividades de processamento são justificadas pela necessidade de fornecer os serviços contratados pelos clientes e para a melhoria contínua desses serviços. A Tech Challenge Fast Food assegura que o processamento seja limitado ao necessário em relação aos fins para os quais os dados pessoais são processados e é proporcional aos benefícios esperados tanto para a empresa quanto para os clientes.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Foi identificado que o tratamento de dados pode implicar riscos como acesso não autorizado, perda de dados, vazamento de informações sensíveis e uso indevido dos dados para fins fraudulentos. A avaliação considera a probabilidade e a severidade desses riscos para os direitos e liberdades dos titulares dos dados.

A análise a seguir considera a seguinte classificação:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

A seguir é apresentada a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

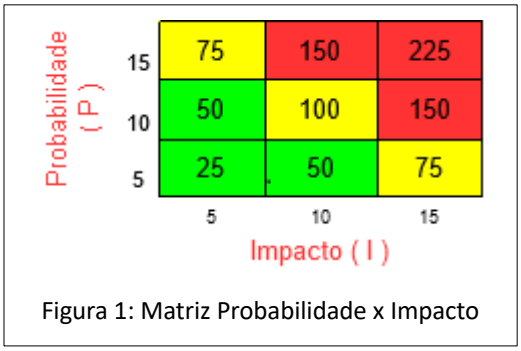

Figura 1: Matriz Probabilidade x Impacto

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;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	Acesso não autorizado.	15	15	225
R02	Uso indevido de informações pessoais.	15	15	225
R03	Vazamento de dados.	15	15	225
R04	Remoção não autorizada.	15	10	150
R05	Informação insuficiente sobre a finalidade do tratamento.	10	5	50
R06	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R07	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R08	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	15	5	75
R09	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.).	15	10	150
R10	Reidentificação de dados pseudoanonimizados.	10	15	150

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).

7 – MEDIDAS PARA TRATAR OS RISCOS

Para mitigar os riscos identificados, a Tech Challenge Fast Food implementará medidas como sistemas de segurança robustos, criptografia de dados, acesso restrito baseado no menor privilégio e treinamentos regulares para funcionários. Processos de resposta a incidentes de segurança também foram estabelecidos para agir de maneira rápida e eficaz na eventualidade de um problema de segurança de dados.

Risco	Controle/Medida	Efeito sobre o Risco[1]	Risco Residual[2]			Controle/ Medida[3] Aprovado (a)
			P	I	Nível (P x I)	
R1 Acesso não autorizado.	Controle de Acessos; Criptografia dos Dados; Monitoramento e análise de logs; Segurança de Rede.	Reduzir	5	15	75	Sim

R2 Uso indevido de informações pessoais.	Definição de Política de Uso de Dados; Estabelecimento de Acessos Baseados em Função; Auditoria e Rastreabilidade; Treinamento e Conscientização; Acordos de Confidencialidade e Cláusulas Contratuais.	Reduzir	5	15	75	Sim
R3 Vazamento de dados.	Análise de Risco e Proteção de Dados por Design e por Padrão; Controles Físicos e Lógicos de Acesso; Medidas de Segurança Técnica; Políticas Organizacionais e Treinamento de Conscientização.	Reduzir	5	15	75	Sim
R4 Remoção não autorizada.	Políticas e Procedimentos de Gerenciamento de Dados; Controles de Acesso e Privilegiamento; Auditorias e Monitoramento; Controles Técnicos como Criptografia e DLP (Data Loss Prevention).	Reduzir	5	10	50	Sim
R5 Informação insuficiente sobre a finalidade do tratamento.	Elaboração de Notificações de Privacidade Detalhadas; Processos de Consentimento Claros e Revisáveis; Treinamento e Conscientização Interna; Revisão e Auditoria dos Procedimentos de Informação.	Reduzir	5	5	25	Sim
R6 Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	Política de Consentimento Rigorosa; Acordos de Processamento de Dados; Práticas Rigorosas de Avaliação de Terceiros; Monitoramento e Controle Contínuo.	Reduzir	5	15	75	Sim
R7 Retenção prolongada de	Política de Retenção de	Reduzir	5	5	25	Sim

dados pessoais sem necessidade.	Dados; Inventário e Classificação de Dados; Processos de Exclusão e Anonimização; Revisões Periódicas e Auditorias.					
R8 Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	Anonimização e Pseudonimização de Dados; Controle de Acesso Baseado em Privilégios Mínimos; Criptografia de Dados; Políticas de Retenção e Eliminação de Dados.	Reduzir	5	5	25	Sim
R9 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.).	Validação de Dados de Entrada; Testes e Revisões de Qualidade de Software; Gerenciamento de Mudanças e Controle de Versão; Logs e Monitoramento de Atividades de Processamento.	Reduzir	5	10	50	Sim
R10 Reidentificação de dados pseudoanonimizados.	Fortalecimento da Técnica de Pseudonimização; Análise de Risco de Reidentificação Regular; Controle de Acesso e Segregação de Dados; Revisão e Atualização de Políticas e Protetores.	Reduzir	5	15	75	Sim

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 do(s) controle(s) descrito(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 controles para tratar o risco.

[3] Controle/medida aprovado(a) pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 – APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
Felipe Bento Gabriel dos Santos Felipe Bento Gabriel Santos São Paulo, 24 de fevereiro de 2024	Luiz Antonio Bryan Caldeira Luiz Antonio Bryan Caldeira São Paulo, 24 de fevereiro de 2024

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
Felipe Bento Gabriel dos Santos Felipe Bento Gabriel Santos São Paulo, 24 de fevereiro de 2024	Benjamin Luiz Nelson Almada Benjamin Luiz Nelson Almada São Paulo, 24 de fevereiro de 2024