

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 07 de agosto de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
07/08/2024	1.0	Conclusão da primeira versão do relatório	Fernanda Moraes Pedreira Fossa

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

Lanchonete grupo 33, representado pelo grupo 33 da Pós Tech de arquitetura de software na FIAP.

Operador

Thiago Bernardo Santiago do Nascimento

Encarregado

Fernanda Moraes Pedreira Fossa

E-mail Encarregado

fernanda.pedreira@dpo.gov.br

Telefone Encarregado

(11) 98754-1234

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Atendendo as exigências da Lei Geral de Proteção de Dados (LGPD), é necessário a elaboração do relatório de risco à proteção de dados (RIPD) pois a Lanchonete Grupo 33 opera dados pessoais sensíveis. Desta forma, a Lanchonete Grupo 33 avaliou e mapeou riscos existentes nas operações de tratamentos de dados pessoais e adotou medidas para diminuí-los ou eliminá-los.

LANCHONETE GRUPO 33

Com isso, a Lanchonete Grupo 33 implementa um programa de governança e privacidade dos dados, garantindo que seus clientes estejam cientes do uso de seus dados e garantindo que os dados desses clientes serão utilizados exclusivamente para os fins estabelecidos e previamente consentidos pelo usuário.

3 – DESCRIÇÃO DO TRATAMENTO

Os dados pessoais dos clientes da Lanchonete Grupo 33 serão utilizados para analisar o perfil de seus clientes e proporcionar notificações sobre promoções e inauguração de novas filiais.

Esses dados serão utilizados pelo operador, não de forma que identifique o cliente especificamente, mas sim identifique características comuns em seus clientes por região. Com isso, a Lanchonete Grupo 33 também visa notificar seus clientes sobre promoções, a fim de promover um relacionamento próximo e benéfico para ambas as partes.

3.1 – NATUREZA DO TRATAMENTO

Os dados pessoais dos clientes serão informados pelo próprio titular, através de um cadastro no totem de atendimento da Lanchonete Grupo 33. Os dados são armazenados em uma base de dados MariaDb, que está hospedado na nuvem Amazon. E serão armazenados por 5 anos e após este período, os dados serão apagados, sem opção de recuperação.

Os dados não serão compartilhados com nenhuma empresa ou entidade, sendo utilizados apenas pela Lanchonete Grupo 33 para entender o perfil de seus clientes por região, notificar sobre promoções e inauguração de novas filiais.

3.2 – ESCOPO DO TRATAMENTO

A Lanchonete Grupo 33 oferece serviço de fast food e para usufruir de possíveis promoções, permite que o cliente realize um cadastro e insira seus dados pessoais.

São eles:

- Nome
- CPF
- Endereço
- Telefone

- Email

Para que o cliente tenha acesso a campanhas promocionais, deverá realizar um cadastro simples no próprio totem de atendimento, inserindo as informações listadas acima (Nome, CPF, endereço, telefone e email).

É importante ressaltar que o cadastro de seus dados no sistema da Lanchonete Grupo 33 é opcional. E quando o cadastro for efetuado pelo cliente, é obrigatório o aceite do consentimento, atendendo a LGPD.

3.3 – CONTEXTO DO TRATAMENTO

A Lanchonete Grupo 33 trata os dados pessoais dos clientes de acordo com o que exige as leis e regulamentos vigentes, de acordo com a finalidade deles e conforme acordado e consentido pelo próprio cliente previamente.

O cliente possui autonomia quanto aos seus dados pessoais, de forma que podem solicitar a inativação dos dados a qualquer momento. A inativação consiste em uma exclusão lógica dos dados e descaracterização deles. Com isso, os dados continuarão existindo na base de dados do sistema da Lanchonete Grupo 33, porém sem identificação do cliente e sem a possibilidade de desfazer tal descaracterização.

Apenas o usuário administrador do sistema terá acesso aos dados dos clientes e este acesso será sempre em uma visão geral e resumida dos dados, visando mostrar a preferência dos clientes em determinada região. Este acesso será sempre em uma visão geral dos dados, visando mostrar a preferência dos clientes em determinada região.

Os dados serão trafegados na rede de forma criptografada, para dificultar qualquer interceptação deles.

Adotada autenticação multifatorial (MFA) para acesso aos sistemas, reforçando a segurança e reduzindo significativamente os riscos de invasões.

Realização de testes de vulnerabilidade e penetração para identificar e corrigir potenciais pontos fracos na infraestrutura e segurança.

3.4 – FINALIDADE DO TRATAMENTO

A finalidade do tratamento dos dados pessoais é única e exclusivamente para oferecimento de

LANCHONETE GRUPO 33

promoções, notificações de novidades, ofertas e inauguração de novas unidades da Lanchonete Grupo 33.

4 – PARTES INTERESSADAS CONSULTADAS

Para elaboração deste relatório, todos os colaboradores da Lanchonete Grupo 33 foram consultados. Cada parte consultada indicou aspectos importantes a serem observados no tratamento dos dados pessoais, com foco nos possíveis riscos associados às atividades de tratamento em análise. Além disso, é essencial considerar os riscos de não conformidade com a LGPD e os instrumentos internos de controle, como políticas, processos e procedimentos voltados à proteção de dados e privacidade.

Registrar essas opiniões (sejam elas convergentes ou divergentes), juntamente com as justificativas para as opções adotadas, pode ser considerado uma boa prática em termos de transparência, responsabilização e prestação de contas.

5 – NECESSIDADE E PROPORCIONALIDADE

A Lanchonete Grupo 33 utilizará os dados de seus clientes exclusivamente para finalidade já mencionada neste relatório: análise do perfil e preferências de seus clientes por região e notificação de promoções e inauguração de novas lojas.

Desta forma, para minimizar riscos, a Lanchonete Grupo 33 reduziu a quantidade de dados coletados no cadastrado, garantindo assim que sejam coletados apenas os dados necessários para as finalidades aqui descritas neste documento.

No sistema que atende a Lanchonete Grupo 33 foi implementado as seguintes medidas que asseguram o direito de o titular dos dados obter do controlador, conforme previsto no artigo 18 da LGPD:

- Serviço para inativação de dados do cliente: Este serviço inativará os dados de forma lógica e fará a descaracterização deles; uma vez solicitada e executada tal ação, não será possível desfazer.
- Serviço para que o cliente atualize ou complete seus dados: A qualquer momento, através do totem de atendimento, o cliente poderá efetuar atualizações cadastrais.

A privacidade e uso dos dados serão conhecidas pelos clientes antes de efetuarem o cadastro no sistema da Lanchonete Grupo 33. E, caso haja atualização, os clientes serão notificados e receberão

na integra todas as alterações de forma clara.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

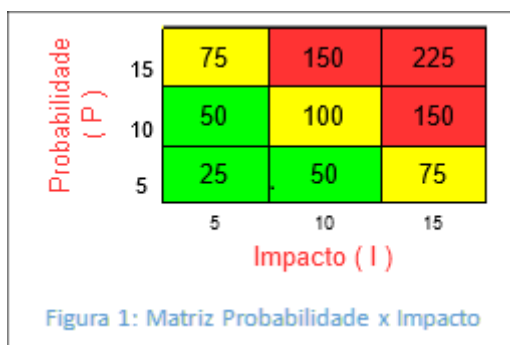
Dentre os riscos identificados no diagnostico, podemos destacar os riscos em relação ao acesso indevido as informações pessoais dos clientes. Evento este que geraria alto impacto aos clientes e a Lanchonete Grupo 33.

A seguir, apresentam-se riscos iniciais, não exaustivos, de riscos identificados e mensurados, de acordo com a metodologia de gerenciamento de riscos operacionais à proteção de dados pessoais:

Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

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



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.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em

LANCHONETE GRUPO 33

harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**.

Id	Risco referente ao tratamento de dados pessoais	P¹	I²	Nível de Risco (P x I) ³
R01	Acesso não autorizado.	10	15	150
R02	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R03	Reidentificação de dados pseudoanonimizados.	5	15	75
R04	Repasse de senhas para acesso a softwares e sistemas.	5	15	75
R05	Utilização de e-mail pessoal ou particular dentro da empresa.	10	10	100
R06	Repasse de senhas do PC/Notebook.	10	10	100
R07	Utilização de ferramentas de comunicação online.	10	10	100
R08	Retenção prolongada de dados pessoais sem necessidade.	5	5	25

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

Como medidas de tratamento de risco é necessário que a Lanchonete Grupo 33 execute medidas administrativas e de avaliação de forma contínuas. Isso inclui (mas não se limita) treinamentos de seus colaboradores, controle de programas instalados nas máquinas corporativas, controle de vencimento e renovação de senhas contínuos.

LANCHONETE GRUPO 33

Além dessas medidas administrativas, implementamos as medidas abaixo para redução de alguns riscos mapeados:

Risco	Controle/Medida	Efeito sobre o Risco ¹	Risco Residual ²			Controle/Medida ³ Aprovado (a)
			P	I	Nível (P x I)	
R01 – Acesso não autorizado	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso; Uso de MFA.	Reduzir	5	10	50	Sim
R08 - Retenção prolongada de dados pessoais sem necessidade	MINIMIZAÇÃO DE DADOS: Coleta somente dos dados necessários para a finalidade; Revisão periódica dos dados pessoais coletados para alinhamento com a finalidade.	Reduzir	5	10	50	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.

LANCHONETE GRUPO 33

8 – APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<hr/> <p>Fernanda Moraes Pedreira Fossa</p> <p>Matrícula: 123456</p> <p>São Paulo, 07 de agosto de 2024</p>	<hr/> <p>Fernanda Moraes Pedreira Fossa</p> <p>Matrícula: 616541</p> <p>São Paulo, 07 de agosto de 2024</p>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
<hr/> <p>Filipe Xavier Silva</p> <p>Matrícula: 965168</p> <p>São Paulo, 07 de agosto de 2024</p>	<hr/> <p>Thiago Bernardo Santiago do Nascimento</p> <p>Matrícula: 658152</p> <p>São Paulo, 07 de agosto de 2024</p>