RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 08 de agosto de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: iBurguer
Operador(es): Carlos Cardoso, Luan Pereira, Matheus Cardoso, Vinicius Saeta
Encarregado: Escritório FIAP
E-mail do Encarregado: (pessoa.f@fiap.com)
Telefone: (11) 91111-2222

2 - NECESSIDADE DE ELABORAR O RELATÓRIO

Atendimento ao artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos da Lei 13.907/2018 - Lei Geral de Proteção de Dados (LGPD).

3 - DESCRIÇÃO DO TRATAMENTO

Relativamente à natureza, escopo, contexto e finalidade do tratamento, o CONTROLADOR informa que, diante de sua atividade principal de operar um sistema de gestão de lanchonetes e restaurantes, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

1. **Coleta e Trata Dados Pessoais e Sensíveis**:
    - **Nome, CPF, e-mail, telefone e endereço** do TITULAR para inativação de usuário e cadastro de usuário. Estes dados são utilizados para identificar o cliente que realizou a inativação e para que o cliente possa se identificar e realizar pedidos de forma eficiente e personalizada.
    - **CPF** do TITULAR para identificação no totem de autoatendimento, utilizado para que o cliente possa se identificar e realizar pedidos de forma eficiente e personalizada.
    - **Dados Pessoais de Pagamento** do TITULAR para processamento de transações, bem como para fins fiscais e tributários, garantindo que o cliente possa realizar pagamentos de forma segura e eficiente, além de atender às obrigações legais e regulamentares.

4 - PARTES INTERESSADAS CONSULTADAS

Entidades legais consultadas:

2. Secretaria Estadual de Segurança de Dados
3. Encarregado dos dados, como citado na seção 1

4. Especialistas de segurança da CONTROLADORA:
    - Carlos Cardoso
    - Luan Pereira
    - Matheus Cardoso
    - Vinicius Saeta
4. Time de operação de negócio da CONTROLADORA:
    - Alex Dias
    - Leonor Rodrigues
    - Giovana Santos, responsável pelo treinamento e acompanhamento do time em questões de segurança de dados e qualidade da operação

Todas as partes interessadas participaram, em diferentes momentos, do processo de criação do presente documento. O time de operação de negócio participou na identificação dos dados operados, no apoio à definição do contexto de operação dos dados, e foi treinado para operar os dados de acordo com a política de dados definida. Os especialistas de segurança prepararam os relatórios técnicos que serviram de base à criação da política de dados e a este relatório. O Encarregado dos dados, junto aos representantes jurídicos do CONTROLADOR, elaborou este documento, que foi posteriormente validado com as entidades competentes.

5 - NECESSIDADE E PROPORCIONALIDADE

Fundamentação legal: artigo 5º, inciso II, artigo 10, parágrafo 3º, artigo 14 e artigo 42 da Lei 13.907/2018 - Lei Geral de Proteção de Dados.

Tendo em vista que o legítimo interesse do CONTROLADOR é uma das fundamentações em razão de sua responsabilidade em garantir a correta identificação e pagamento por parte do TITULAR:

- O tratamento dos dados pessoais (nome, CPF, e-mail) é indispensável para a opção de identificação do cliente no totem de autoatendimento e para a realização de pagamentos de forma segura e eficiente.
- Não há outra base legal possível de se utilizar para alcançar o mesmo propósito, considerando a necessidade de permitir a opção de identificação correta do cliente para fins de pedidos e pagamentos.
- O processo atual de fato auxilia no propósito almejado, que é fornecer um serviço eficiente e personalizado ao cliente.

Os clientes têm o direito de inativar os seus dados pessoais armazenados pela lanchonete, conforme previsto na legislação aplicável. Para exercer esses direitos, o cliente pode entrar em contato com o encarregado de dados da lanchonete ou realizar a operação diretamente no sistema. Para fins legais, o direito ao esquecimento será garantido para os dados usados em processos transacionais.

Todos os dados coletados com essa finalidade são eliminados após o período exigido pela legislação, que é de cinco (5) anos. Enquanto perdurar esse prazo, o encarregado manterá todos os dados criptografados com chaves assimétricas, armazenados em dois fornecedores de nuvem diferentes, com segurança de nuvem e de implementação, e duplo fator de autenticação, inclusive para fins de recuperação de arquivos de segurança e recibos de transmissão e evidência de cumprimento de obrigação acessória e principal.

As informações de privacidade aos titulares seguem as diretrizes da obrigatoriedade de se manterem arquivadas todas as evidências fiscais, tributárias e trabalhistas de todas as informações enviadas aos sistemas oficiais da autoridade tributária brasileira.

A entidade CONTROLADORA poderá, a pedido do TITULAR, transferir a ele a guarda de tais informações, ressalvadas àquelas que o próprio CONTROLADOR, por dever de ofício, deve possuir pelo período constante da legislação. É importante constar que não há, por legislação, a retroatividade do processamento dos dados, em caso de transferência de guarda de informações.

6 - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Identificamos os seguintes riscos, classificados de acordo com sua probabilidade (P) e seu impacto (I). O nível de risco se dá pela multiplicação dos dois fatores. As gradações são 5 (baixo), 10 (médio) e 15 (alto).

N do Risco	Especificação do Risco	P	I	Nível de Risco
R01	Acesso não autorizado	3	5	15
R02	Operação incorreta dos dados	2	5	10
R03	Desfiguração de dados por falha de software	3	4	12
R04	Indisponibilidade do sistema de operação dos dados	4	3	12
R05	Falhas na criptografia	2	5	10

7 - MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida	Efeito sobre o risco	Medida aprovada
R01	1. controle do acesso lógico2. monitoramento ativo de ações suspeitas no ambiente de	reduzir	sim
R02	1. treinamento2. redução de dados para operação	reduzir	sim
R03	1. efetuar testes completos e documentados antes de iniciar o uso	mitigar	sim
R04	1. controle de failover para falhas que causem indisponibilidade2. monitoramento de todos os componentes da solução	reduzir	sim

Implementamos as seguintes medidas para mitigar os riscos identificados:

1. **Acesso não autorizado aos dados**:
    - Implementação de controle de acesso rigoroso com autenticação multifator.
    - Monitoramento contínuo de atividades suspeitas.
2. **Perda de dados devido a falhas no sistema**:
    - Backup regular dos dados em múltiplas localizações seguras.
    - Planos de recuperação de desastres testados periodicamente.
3. **Roubo de dados durante transmissão**:
    - Uso de protocolos seguros (TLS/SSL) para transmissão de dados.

    - Monitoramento contínuo de redes para detectar atividades suspeitas.
4. **Erros humanos no tratamento dos dados**:
    - Treinamento contínuo dos funcionários em práticas seguras de tratamento de dados.
    - Revisão periódica das políticas e procedimentos de segurança de dados.
5. **Falhas na criptografia**:
    - Atualização contínua das práticas de criptografia com as melhores práticas da indústria.
    - Auditorias regulares de segurança para identificar e corrigir vulnerabilidades.

8 - APROVAÇÃO

Assinaturas:

Representante do IBurguer

Encarregado do Escritório FIAP