**RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**

11 de março de 2024

# - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

**Controlador:** FIAP Pós Tech - Tech Challenge

**Operador(es):** Gabriel Almeida dos Santos, Paulo Lobo Neto

**Encarregado:** FIAP - Centro Universitário

**e-mail do encarregado:** contato@fiap.com.br **telefone:** 11 3585-8010

# - 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.

# - DESCRIÇÃO DO TRATAMENTO

Relativamente à natureza, escopo, contexto e finalidade do tratamento, a CONTROLADORA informa que, diante de sua atividade principal de prestação de serviços de fast food, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

* 1. coleta e trata dados pessoais e sensíveis relativos à CPF, nome e email vinculados ao TITULAR, para melhor experiência e comunicação com as entregas de pedidos;
  2. trata os dados no interesse legítimo da CONTROLADORA, em razão de sua necessidade, conforme solicitado por autoridades judiciais - conforme previsto no Código Tributário Nacional (CTN/66) sobre órgãos de controle do fisco, da fazenda, que remetem à União, aos Estados e aos Municípios - para comprovação dos dados que versam sobre informações tributárias e fiscais, que, em decorrência da atividade econômica da CONTROLADORA, poderá surgir a necessidade de serem encaminhadas para controle tributário e fiscal, conforme previsto na legislação brasileira;
  3. trata dados que podem causar danos materiais e que versam sobre a honra e moral ao TITULAR, referente ao sigilo de informações privadas armazenadas em sistema;

# - PARTES INTERESSADAS CONSULTADAS

Para confecção deste Relatório, Colaboradores de diversos projetos, especialistas em segurança da informação e tecnologia da informação foram analisados.

Realizaram-se avaliações de conformidade à LGPD, sob os aspectos culturais, operacionais e nos sistemas informatizados, segundo padrão metodológico baseado nas melhores práticas de proteção de dados.

# - NECESSIDADE E PROPORCIONALIDADE

Fundamentação legal: artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos 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 solidária ao TITULAR em caso de irregularidade fiscal e tributária:

* o tratamento dos dados sensíveis é indispensável ao cumprimento das exigências da legislação brasileira;
* o processo atual de fato auxilia no propósito almejado.

Todos os dados coletados com essa finalidade são eliminados após o período exigido pela legislação, que é de 5 (cinco) anos. Enquanto perdurar esse prazo, o encarregado manterá todos os arquivos de backup criptografados em mídia física e armazenamento adicional em nuvem com segurança 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

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.

1. **- IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS**

Terminologias para cada item desta tabela:

1. probabilidade (P) - chance de algo acontecer, não importando se definida, medida ou determinada; - numerada em 3 gradações: 5(baixo), 10(médio) e 15(alto)
2. impacto ( I ) - resultado de um evento que afeta o titular; - numerado em 3 gradações: 5(baixo), 10(médio) e 15(alto)
3. nível de risco - magnitude de um risco ou combinação de riscos, combinando probabilidade X impacto (multiplicação)
4. R00 - risco classificado pelo mapeamento de dados como presente na operação

| N. DO RISCO | ESPECIFICAÇÃO DO RISCO | P | I | NÍVEL DE RISCO |
| --- | --- | --- | --- | --- |
| R01 | acesso não autorizado | 10 | 10 | 150 |
| R02 | perda | 5 | 15 | 75 |
| R03 | retenção prolongada dos dados | 5 | 5 | 25 |
| R04 | vinculação indevida, direta ou indireta | 5 | 15 | 75 |
| R05 | falha ou erro de processamento | 5 | 15 | 75 |
| R06 | Invasões, ciberataques e vazamento | 5 | 15 | 75 |

# - MEDIDAS PARA TRATAR OS RISCOS

| RISCO | MEDIDA | EFEITO SOBRE O RISCO | MEDIDA APROVADA |
| --- | --- | --- | --- |
| R01 | 1.controle de acesso lógico | reduzir | sim |
| R02 | 1.controle de acesso lógico | reduzir | sim |
|  | 2.controle criptográfico | reduzir | sim |
|  | 3.proteção física do ambiente | prevenir e reduzir | sim |
|  | 4.backup para restauração de dados | medida profilática pós exposição | sim |
|  | 5.comunicação sobre perda de dados | medida profilática pós exposição | sim |
|  | 6.controle levantamento de danos | medida profilática pós exposição | sim |
| R03 | 1.manutenção programada da aplicação | prevenir e reduzir | sim |
|  | 2.eliminação programada de dados | prevenir e reduzir | sim |
|  | 3.alertas sobre retenções prolongadas | medida profilática pós exposição e prevenção | sim |
| R04 | 1.treinamento para equipe técnica | prevenir e reduzir | sim |
|  | 2.testes de aplicação | prevenir e reduzir | sim |
|  | 3.comunicação sobre vinculação | medida profilática pós exposição | sim |
|  | 4.desvinculação de dados | medida profilática pós exposição | sim |
|  | 5.restrição de coleta de dados para vinculações não desejadas | medida profilática pós exposição, prevenir e reduzir | sim |
| R05 | 1.dimensionamento de hardware | prevenir, reduzir e medida profilática | sim |
|  | 2.monitoramento de indicadores da aplicação | prevenir, reduzir e medida profilática pós exposição | sim |
|  | 3.em falha, retroceder transações de alto impacto | prevenir, reduzir e medida profilática pós exposição | sim |
|  | 4.alertas | prevenir, reduzir e medida profilática pós exposição | sim |
| R06 | 1.gestão de pessoas , controle de credenciais e acesso | prevenir, reduzir e medida profilática pós exposição | sim |
|  | 2.termo de sigilo e confidencialidade para colaboradores | prevenir | sim |
|  | 3.fechadura eletrônica para acesso interno ao toten | prevenir e reduzir | sim |
|  | 4.controle de vulnerabilidades de hardware, totem e corporativo | prevenir e reduzir | sim |
|  | 5.troca periódica de senhas de servidores e cloud | prevenir e reduzir | sim |
|  | 6.firewall, bloqueio de ações, sites, domínios e e-mails suspeitos | prevenir e reduzir | sim |
|  | 7.limitação de requisições por segundos | prevenir e reduzir | sim |
|  | 8.criptografia de dados em repouso | prevenir e reduzir | sim |
|  | 9.criptografia de dados em trânsito | prevenir e reduzir | sim |
|  | 10.restrições de operações via credenciamento | prevenir, reduzir e medida profilática pós exposição | sim |
|  | 11.monitoramento de estresse advindo de comportamento inesperado ou inadequado do software | prevenir, reduzir e medida profilática pós exposição | sim |
|  | 12.consistência e integridade dos dados | prevenir e reduzir | sim |
|  | 13.recomendação de uso de antivírus em maquinário | prevenir e reduzir | sim |
|  | 14.notificação e controle de danos sobre vazamento | medida profilática pós exposição | sim |
|  | 15.alinhamento jurídico e técnico sobre dimensões de danos de vazamentos e ciberataques | medida profilática pós exposição | sim |

# - APROVAÇÃO

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Gabriel Almeida dos Santos

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Paulo Lôbo Neto