Guia Relatório de Impacto à Proteção de Dados Pessoais

## 1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Grupo 48

Operadores: André Biaggio, André Laus e Mateus Lima

Encarregado: AWS

## 2 - NECESSIDADE DE ELABORAR O RELATÓRIO

o RIPD deve ser elaborado e/ou atualizado, por existir a possibilidade de ocorrer (mesmo esporadicamente) impacto na privacidade dos dados pessoais, resultante de:

* uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
* tratamento de dados pessoais como nome, email e CPF;
* processamento de dados pessoais usados para criar e finalizar pedidos no aplicativo;
* processamento de dados pessoais para pagamento do pedido.

## 3 - DESCRIÇÃO DO TRATAMENTO

Reitera-se que a LGPD (art. 5º, X) considera tratamento “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”.

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

## 3.1 NATUREZA

São adotadas medidas 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 difusão.

### 3.1.2 Tratamento dos dados

Os dados são coletados e armazenados em uma base na AWS criptografada.

## 3.2 – ESCOPO DO TRATAMENTO

Para acessar os serviços não é necessário efetuar o cadastro, mas caso o usuário deseje, serão solicitados dados como nome, e-mail e CPF, para que o usuário seja corretamente identificado e receba login e senha de autenticação.

Contudo, o usuário poderá se desejar, ter acesso aos dados, editá-los e retificá-los sempre.

## 4 - PARTES INTERESSADAS CONSULTADAS

## 5 - NECESSIDADE E PROPORCIONALIDADE

O tratamento de dados é limitado ao mínimo necessário para a realização das finalidades informadas ao titular. Quando necessário, tem abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

O tratamento é feito apenas quando é indispensável e com o propósito de cumprimento de obrigação legal e regulatória, monitoramento do sistema financeiro, pesquisa e divulgação de estatísticas para cálculo e divulgação de indicadores agregados (sem consultas individualizadas).

Com o objetivo de assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição, todo servidor ou terceirizado deve seguir o Código de Conduta dos servidores do BC. Além disso, os sistemas de informação possuem logs e controles de acesso.

## 6 - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

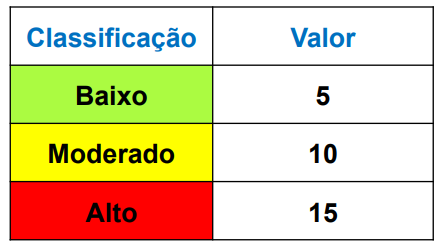
Dentre os tipos de risco operacional verificados no diagnóstico, destacam-se os riscos à proteção de dados e informações armazenadas pela entidade, em especial aos dados pessoais sensíveis.

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

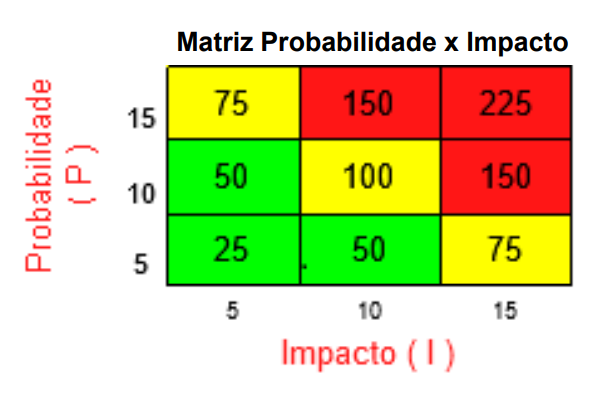
* vazamento de dados pessoais;
* alteração de dados pessoais;
* acesso indevido a dados pessoais;
* perda de dados pessoais.

Seguindo as evidências de fragilidades listadas acima, a Matriz de Probabilidade de Impacto, ajuda na tomada de decisão com relação às sugestões de melhoria que serão disponibilizadas para adequação a LGPD.

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



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;
* 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 harmonia com a Política de Gestão de Riscos.

| **Id** | **Risco referente ao tratamento de dados pessoais** | **P1** | **I2** | **Nível de Risco (P x I)3** |
| --- | --- | --- | --- | --- |
| R1 | Armazenamento e exclusão de dados | 15 | 15 | 225 |
| R2 | Armazenamento de senhas | 10 | 15 | 150 |

## 7 - MEDIDAS PARA TRATAR OS RISCOS

Neste ponto, parece pertinente descrever, em princípio, algumas medidas que compõem o referencial para lidar com os riscos. Sendo assim, inicialmente, se propõe:

| **Medida** | **Descrição** |
| --- | --- |
| MD01 | Criptografia do banco de dados |
| MD02 | Controle de acesso a unidade |
| MD03 | Proteção lógica (antivírus, senhas, atualizações regulares e testes) |

Concluindo, bastaria associar estas medidas aos riscos, conforme sugere o Guia de Boas Práticas da LGPD

| **Risco** | **Medida(s)** | **Efeito sobre o risco** | **P** | **I** | **(PxI)** | **Medidas Aprovadas** |
| --- | --- | --- | --- | --- | --- | --- |
| R01 | MD01, MD02, MD03 | Reduzir | 5 | 10 | 50 | Sim ou Não |
| R02 | MD01, MD02, MD03 | Reduzir | 5 | 10 | 50 | Sim ou Não |

## 

## 8 - APROVAÇÃO

**Responsável pela elaboração do relatório**

| **Grupo 48** |
| --- |

**Encarregado**

|  |
| --- |

**Autoridade representante do controlador**

|  |
| --- |

**Autoridade representante do operador**

|  |
| --- |