## Relatório de Impacto à Proteção de Dados (RIDP)

### 1. ****Introdução****

Este Relatório de Impacto à Proteção de Dados (RIDP) foi elaborado para avaliar o tratamento de dados pessoais e sensíveis no âmbito do projeto em que um dispositivo será utilizado para capturar dados de saúde de usuários. Esses dados serão processados por uma aplicação que armazenará as informações em um banco de dados, gerando métricas e relatórios para o proprietário da aplicação.

### 2. ****Descrição do Projeto****

O projeto envolve um **dispositivo de captura de dados de saúde** que utiliza sensores para coletar informações dos usuários, como sinais vitais, condições de saúde e outros parâmetros relacionados à saúde. Os dados coletados são processados em uma **aplicação centralizada**, armazenados em um **banco de dados** e utilizados para gerar relatórios e métricas que são entregues ao proprietário da aplicação. O objetivo final é oferecer uma visão detalhada e informativa sobre o estado de saúde dos usuários com base nos dados capturados.

### 3. ****Dados Pessoais e Sensíveis Coletados****

Os dados coletados e tratados no projeto incluem:

* **Dados Pessoais**:
  + Nome completo do usuário
  + CPF e RG
  + Endereço
  + Idade
  + Login e senha (gerados e armazenados no sistema)
* **Dados Sensíveis**:
  + Informações de saúde capturadas pelos sensores (sinais vitais, dados biométricos e outros parâmetros de saúde)
  + Histórico de dados de saúde armazenado no banco de dados

### 4. ****Base Legal para o Tratamento de Dados****

De acordo com a Lei Geral de Proteção de Dados (LGPD), o tratamento de dados pessoais e sensíveis deve ter uma base legal adequada. As bases legais relevantes para este projeto são:

* **Execução de contrato**: o tratamento de dados é necessário para fornecer o serviço de monitoramento e geração de relatórios para o proprietário da aplicação.
* **Consentimento do titular**: o titular dos dados dará seu consentimento explícito para a captura e processamento de seus dados de saúde.
* **Legítimo interesse**: o processamento de dados é feito para garantir a qualidade e continuidade do serviço, além de gerar relatórios ao proprietário da aplicação.

### 5. ****Ciclo de Vida dos Dados****

1. **Coleta**: Os dados são coletados automaticamente pelo dispositivo por meio de sensores instalados. Dados como nome, CPF e login são cadastrados manualmente.
2. **Processamento**: O processamento dos dados ocorre dentro da aplicação para gerar métricas e relatórios sobre a saúde dos usuários.
3. **Armazenamento**: Os dados são armazenados em um banco de dados seguro, com medidas de criptografia para proteger dados pessoais e sensíveis.
4. **Anonimização**: Dados pessoais, como CPF, RG e nome, podem ser anonimizados, quando necessário, para reduzir os riscos em caso de vazamento de informações.
5. **Eliminação**: Os dados serão eliminados após o término da relação com o titular ou em caso de solicitação de exclusão, respeitando os prazos legais para retenção de informações.

### 6. ****Medidas de Segurança Implementadas****

Para garantir a proteção dos dados tratados, as seguintes medidas de segurança foram adotadas:

* **Criptografia**: Dados sensíveis como senhas são criptografados antes de serem armazenados. O uso da biblioteca cryptography no código garante que senhas e informações confidenciais estejam protegidas.
* **Anonimização**: CPF e RG são parcialmente anonimizados no processo, reduzindo o risco de identificação indevida em caso de vazamento.
* **Controle de acesso**: Acesso aos dados é restrito e monitorado, sendo permitido apenas para usuários autorizados.
* **Autenticação segura**: Geração de logins e senhas complexas para proteger o acesso ao sistema.
* **Auditoria e monitoramento**: Monitoramento contínuo do acesso aos dados e da utilização da aplicação para identificar qualquer comportamento suspeito.

### 7. ****Riscos e Impactos****

Os principais riscos identificados no tratamento dos dados incluem:

* **Vazamento de dados pessoais e sensíveis**: Risco de divulgação não autorizada de informações de saúde dos usuários.
* **Acesso indevido**: Risco de que terceiros não autorizados acessem os dados por falhas de segurança ou credenciais fracas.
* **Perda de dados**: Em caso de falhas no sistema ou ataques cibernéticos, há risco de perda de dados armazenados.

**Impacto potencial**: A exposição de dados sensíveis de saúde pode gerar sérios danos à privacidade dos titulares, além de violações à LGPD, sujeitando a empresa a sanções e perda de confiança por parte dos usuários.

### 8. ****Mitigação de Riscos****

* **Criptografia avançada**: Fortalecer a criptografia de dados sensíveis durante o armazenamento e transmissão.
* **Backup regular**: Implementar uma política de backups regulares para garantir a recuperação de dados em caso de falha ou perda.
* **Treinamento**: Treinamento contínuo para a equipe responsável pelo tratamento de dados sobre as melhores práticas de segurança da informação e conformidade com a LGPD.

### 9. ****Conclusão****

Este relatório avalia os impactos à proteção de dados pessoais e sensíveis no projeto. Com as medidas de segurança e mitigação propostas, o projeto está em conformidade com a LGPD e oferece proteção adequada aos dados dos usuários, assegurando transparência, segurança e respeito à privacidade.