**RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)**

**Sistema de Restaurante - "FIAP - SOAT1 Grupo 17"**

**Data do Relatório:** [Inserir data]

**Elaborado por:** Guilherme de Araujo Nascimento (Controlador), João Eduardo F Lima (Operador), Vinicius Guimarães (Encarregado)

**1. Informações Gerais do Sistema:**

* **Nome da Organização:** FIAP - SOAT1 Grupo 17
* **Infraestrutura:** AWS (EKS, Lambda, RDS)
* **Serviço de Autenticação:** AWS Cognito
* **Gateway de API:** API Gateway
* **Dados Armazenados:** CPF do Cliente (coletado opcionalmente), registros de pedidos relacionados a cada cliente.

**2. Processo de Coleta e Armazenamento de Dados:**

* Os dados dos clientes são coletados durante o processo de compra, com o CPF sendo uma informação opcional.
* Os dados de login do cliente são armazenados exclusivamente no serviço Cognito da AWS.
* Os registros de pedidos relacionados a cada cliente são armazenados no banco de dados RDS.

**3. Responsabilidades dos Envolvidos:**

* **Controlador (Guilherme):** Responsável pelo controle e supervisão dos dados coletados, garantindo conformidade com as políticas de privacidade e regulamentos aplicáveis.
* **Operador (João):** Responsável pela operação do sistema, incluindo a coleta e registro adequado dos dados dos clientes.
* **Encarregado (Vinicius):** Responsável por garantir a segurança e integridade dos dados armazenados, implementando medidas de segurança da informação e monitoramento.

**4. Medidas de Segurança Implementadas:**

* Todas as rotas do sistema passam pelo API Gateway, com rotas protegidas exigindo autenticação através do serviço Cognito.
* A infraestrutura AWS (EKS, Lambda, RDS) é configurada com as melhores práticas de segurança recomendadas pela AWS.
* São implementadas políticas de acesso e controle de permissões para garantir que apenas usuários autorizados tenham acesso aos dados do sistema.
* O sistema passa regularmente por verificações de segurança abrangentes, incluindo avaliações de vulnerabilidades de infraestrutura e conformidade com as diretrizes da OWASP (Open Web Application Security Project).

**5. Conformidade com Regulamentos:**

* O sistema é projetado e operado em conformidade com regulamentos de proteção de dados, incluindo a Lei Geral de Proteção de Dados (LGPD) no Brasil, e quaisquer outras regulamentações aplicáveis.

**6. Detalhes sobre Retenção de Dados:**

* Os registros do cliente são mantidos armazenados no sistema até que o cliente solicite sua exclusão. Nesse momento, todos os dados pessoais associados ao cliente são removidos integralmente do serviço Cognito da AWS.

**7. Procedimentos de Exclusão de Dados:**

* Os clientes têm o direito de solicitar a exclusão de seus dados pessoais do sistema. Quando uma exclusão é solicitada, todos os dados associados ao cliente são removidos do serviço Cognito. O histórico de pedidos relacionados ao cliente será dissociado de suas informações pessoais e atribuído a um cliente anônimo, garantindo a privacidade dos dados.

**8. Monitoramento e Auditoria:**

* O sistema é monitorado regularmente quanto a possíveis violações de segurança ou acesso não autorizado aos dados dos clientes, com procedimentos de auditoria interna ou externa realizados conforme necessário para garantir a conformidade.

**9. Manutenção e Atualização do Sistema:**

* O sistema é mantido atualizado com as últimas tecnologias e patches de segurança disponíveis. Isso inclui atualizações regulares da infraestrutura AWS (EKS, Lambda, RDS) e a aplicação de patches de segurança em bibliotecas e frameworks utilizados pelo sistema.

**10. Considerações Finais:**

Este relatório final resume as políticas e práticas adotadas em relação ao registro de identificação de pessoas no sistema de restaurante da FIAP - SOAT1 Grupo 17. As medidas de segurança, conformidade com regulamentos e procedimentos de exclusão de dados garantem a proteção e privacidade dos dados dos clientes, demonstrando o compromisso da organização com a segurança da informação.