Introdução

Este relatório visa analisar o impacto da proteção de dados pessoas associadas ao sistema de controle de pedidos u5lizado pela lanchonete Express. Além dos aspectos previamente mencionados, serão incluídas considerações Saga Orquestrada, Arquitetura Hexagonal e o uso do MongoDB, Docker, Nodej.js, Azure Cloud e Git como parte do ambiente tecnológico.

Tecnologias U4lizada

O sistema de controle de pedidos da lanchonete também incorpora as seguintes tecnologias:

- **Saga Coreografada**: Este padrão de projeto é utilizado para coordenar transações distribuídas e complexas, garantindo a consistência dos dados e a confiabilidade das operações.
- **Arquitetura Hexagonal**: A arquitetura hexagonal, também conhecida como Ports and Adapters, é adotada para separar as preocupações do núcleo da aplicação das preocupações relacionadas à interação com interfaces externas, como bancos de dados e APIs de terceiros.
- **MongoDB**: Este banco de dados NoSQL é utilizado para armazenar dados não estruturados e semiestruturados, oferecendo flexibilidade e escalabilidade para o sistema.
- **Docker**: Utilizado para facilitar a implantação e o gerenciamento de aplicativos em contêineres, o Docker oferece portabilidade e isolamento de recursos, contribuindo para a eficiência e confiabilidade do sistema.
- **Node.js**: Utilizado para o desenvolvimento do backend do sistema, o Node.js proporciona um ambiente eficiente e flexível para aplicativos web, permitindo uma integração suave com outras tecnologias.
- **Azure Cloud**: A utilização da plataforma Azure Cloud oferece uma infraestrutura de computação em nuvem escalável e segura, garantindo disponibilidade, confiabilidade e segurança dos dados, além de facilitar o gerenciamento e a integração de serviços.
- **Git**: Utilizado como sistema de controle de versão, o Git permite o gerenciamento eficiente do código-fonte do sistema, facilitando o trabalho colaborativo e garantindo a rastreabilidade das alterações.

Necessidade e Proporcionalidade

Conforme estabelecido nos seguintes artigos da Lei 13.907/2018 - Lei Geral de Proteção de Dados.

Artigo 5o, inciso II

Artigo 10, parágrafo 3o.

Artigo 14

Artigo 42

Considerando o legítimo interesse do CONTROLADOR, conforme sua responsabilidade solidária ao TITULAR em caso de irregularidade fiscal e tributária, os seguintes pontos são destacados:

O tratamento dos dados sensíveis é indispensável ao cumprimento das exigências da legislação tributária, fiscal e trabalhista brasileira.

Não há outra base legal possível de se utilizar para alcançar o mesmo propósito.

O processo atual efetivamente contribui para o propósito almejado.

Todos os dados coletados com essa finalidade são eliminados após o período exigido pela legislação, que é de 5 (cinco) anos. Durante esse período, 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 observar que não há, por legislação, a retroatividade do processamento dos dados em caso de transferência de guarda de informações. Para fins legais, o direito ao esquecimento será garantido para os dados usados em processos transacionais.

Esta seção aborda a necessidade e a proporcionalidade do tratamento de dados sensíveis, bem como os procedimentos e salvaguardas implementadas para garantir a conformidade com a legislação vigente.

Análise de Impacto à Proteção de Dados Pessoais

Responsabilidade do Controlador de Dados:

Além das responsabilidades previamente discutidas, o controlador de dados deve garantir que as transações realizadas no contexto da Saga Orquestrada sejam devidamente auditadas e que os dados sensíveis dos clientes não sejam expostos durante essas operações.

Segurança da Nuvem e Segurança na Nuvem:

A segurança da nuvem continua sendo um aspecto crítico para proteger os dados armazenados no MongoDB e garantir a integridade das transações da Saga Orquestrada. A configuração adequada dos recursos de segurança na Azure Cloud é essencial para mitigar riscos de vazamento de dados e acesso não autorizado.

Responsabilidade por Falhas de Fornecedores:

O uso do MongoDB como banco de dados e do Docker para implantação introduz a dependência de novos fornecedores de serviços, exigindo uma avaliação cuidadosa de sua segurança e confiabilidade. O controlador de dados é responsável por monitorar e mitigar os riscos associados a qualquer falha dos fornecedores de serviços do MongoDB e Docker.

Riscos à Proteção de Dados Pessoais

Além dos riscos previamente identificados, a inclusão do Docker, Node.js e Git no ambiente tecnológico acrescenta os seguintes riscos:

- **Vulnerabilidades do Node.js**: Vulnerabilidades específicas do Node.js, como ataques de injeção de código, podem comprometer a segurança do sistema e expor os dados dos clientes a ameaças.

- **Risco de Vazamento de Código-fonte**: A utilização do Git para controle de versão pode expor o código-fonte do sistema a terceiros não autorizados, aumentando o risco de vazamento de informações sensíveis.

Medidas para Mi4gar os Riscos

Além das medidas já propostas, recomenda-se:

- Realizar testes de segurança regulares no código-fonte do sistema, utilizando ferramentas de análise estática e dinâmica para identificar e corrigir vulnerabilidades do Node.js.

- Implementar políticas de controle de acesso e revisão de código no Git para proteger o códigofonte contra acessos não autorizados e garantir a integridade do desenvolvimento do sistema.

Conclusão:

Este relatório destaca a importância contínua da proteção de dados pessoais no contexto do sistema de controle de pedidos da lanchonete Express, considerando as tecnologias adicionais incorporadas, como Saga Orquestrada, Arquitetura Hexagonal, MongoDB, Docker, Node.js, Azure Cloud e Git. A implementação eficaz de medidas de segurança e a adoção de práticas de gestão de riscos são fundamentais para garantir a conformidade com as regulamentações de proteção de dados e proteger a privacidade dos clientes.

Aprovação do Relatório
Este relatório foi revisado e aprovado pelos responsáveis pela proteção de dados da lanchonete Express, em conformidade com as políticas e procedimentos estabelecidos pela empresa.