**Questões de LGPD para Melhores Compras**

**Grupo 72**

Daniel Severo - RM553966

Jamyly Melo – RM552795

Marianna Amaral - RM553964

Patricia Demitroff - RM553639

**a) Qual é o papel da TI em relação à LGPD dentro da plataforma de e-commerce e no dia a dia de uso operacional dentro da organização?**

Em uma plataforma de e-commerce e em sua operação, TI tem um papel fundamental em relação à LGPD por ser um habilitador e em várias necessidades e processos:

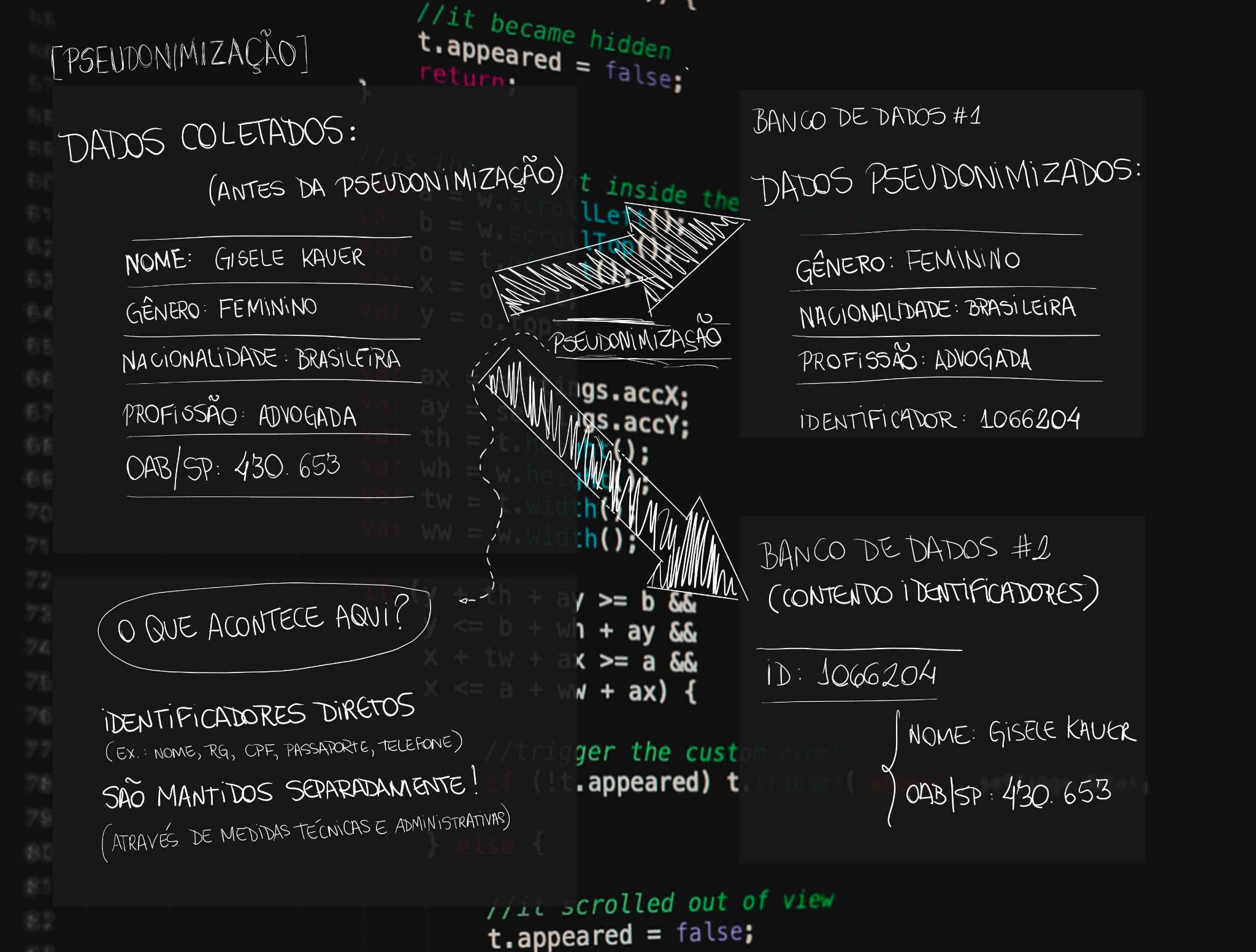
1. **Mapeamento dos dados:** é o time de TI o responsável pelo mapeio e categorização dos dados, pontos de coleta, métodos de armazenamento e processamento de dados pessoais dentro da plataforma. Isso inclui identificar e tratar adequadamente dados pessoais e dados sensíveis eventualmente coletados.
2. **Segurança de Dados:** A TI deve implementar medidas de segurança no nível do sistema e do banco de dados para proteger os dados pessoais e sensíveis contra acessos não autorizados e vazamentos. Isso envolve a criptografia de dados, a gestão de acesso e a monitorização contínua.
3. **Políticas de Retenção de Dados:** A TI, em conjunto com o departamento jurídico, devem definir políticas claras de retenção de dados, garantindo que os dados pessoais não sejam armazenados por mais tempo do que o necessário.
4. **Acesso a Dados Pessoais:** A TI deve implementar mecanismos de controle de acesso para garantir que apenas funcionários autorizados tenham acesso aos dados pessoais de clientes e funcionários da empresa.
5. **Notificação de Incidentes:** Em caso de violação de dados, a TI deve ser capaz de identificar rapidamente o incidente e tomar medidas corretivas imediatas. A LGPD exige que incidentes sejam notificados às autoridades e às partes afetadas em um prazo específico. O responsável por essa notificação é o DPO (Data Privacy Officer), que deve trabalhar em conjunto com a TI, estabelecendo processos e métodos de correção imediata em casos de incidentes.
6. **Auditoria e Monitoramento:** A TI deve estabelecer procedimentos técnicos para atender necessidades de auditoria e monitoramento.
7. **Proteção de Dados por Design (Privacy by Design):** A TI deve incorporar a proteção de dados desde o início do desenvolvimento de sistemas e aplicativos, garantindo que os princípios de privacidade sejam considerados em todas as etapas do ciclo de vida do software.
8. **Gestão de Fornecedores:** Ao contratar terceiros, a área de TI deve monitorar os fornecedores de tecnologia e serviços para garantir que eles também estejam em conformidade com a LGPD, pois a responsabilidade se estende aos parceiros de negócios.

**b) Crie no mínimo 2 recomendações de proteção aos dados possíveis de serem implementadas explicando como deve ser implantada dentro da Melhores Compras. Como é possível atender a LGPD com tantas pessoas acessando dados sensíveis dos clientes?**

1. **Anonimização de dados pessoais de clientes e funcionários por meio de:**
2. **Pseudonimização**, segregando dados que permitam identificar clientes e suas informações pessoais ou sensíveis.

No exemplo abaixo (KAUER, 2019), podemos compreender por meio de um exemplo como a pseudonimização ocorreria. Dados que permitam identificar seu titular (Nome, código OAB) devem ser segregados e armazenados em um ambiente distinto.   
  
Segundo KAUER, "*a ideia é que estes sejam mantidos de forma separada. É comum que os dados pessoais, como nome e números de documentos, sejam substituídos por identificadores indiretos (um número ou código alfanumérico que possa ser utilizado para reunir os dados pessoais identificáveis com aqueles que, por ora, encontram-se pseudonimizados)*".

No entanto, nem todos os dados podem ser substituídos por códigos - isso acarretaria perdas de para o cliente e o negócio (impossibilidade de entrega de compras, duplicidade de registros - clientes - no banco, etc.). Dessa forma, a Pseudonimização torna-se uma alternativa pertinente e mais segura de armazenamento de dados.



1. **Criptografia** dos dados no Banco de Dados

Outra forma de anonimização dos dados é por meio da Criptografia, onde codifica-se e decodifica-se dados para seu uso no momento em que são necessários.

1. **Mascaramento** de dados pessoais que, em conjunto, possam identificar clientes

2**. Controle de Acesso:**

Políticas de senhas fortes, bem como restrições de acesso por função, rastreamento de acessos (logs) e acesso físico ao Banco de Dados são pontos importantes para manter a segurança e integridade dos dados.

**3. Políticas de Privacidade e Segurança da Informação em toda a operação da empresa**

A segurança dos dados é responsabilidade de toda a empresa. Dessa forma, a conscientização sobre os níveis de confidencialidade dos dados (Pessoais, Sensíveis, etc) é de extrema importância, bem como:

1. Treinamentos preventivos contra vazamento de dados, incluindo ataques de Hackers via engenharia social
2. Processos estabelecidos para incidentes, incluindo um canal de denúncias para casos de vazamento de dados
3. Uso de sistemas de proteção, como VPNs e controles de acessos e monitoramento da operação

**c) Na situação dos dados dos clientes estarem bem completos e a aplicação da LGPD, defina 5 dados anonimizados para os clientes. Defina como seria o uso desses dados dentro e fora da empresa Melhores Compras?**

Para clientes, considerando-se o modelo de dados do Melhores Compras, é recomendável anonimizar:

| **Tabela** | **Dado** | **Finalidade do dado** | **Recomendação de uso dos dados dentro da empresa** |
| --- | --- | --- | --- |
| MC\_CLIENTE | nm\_cliente | Usado para personalização de comunicação entre a Melhores Compras e o cliente, assim como parte da identificação do cliente em chamados telefônicos. | Armazenamento deve ser criptografado no Banco de Dados e desvinculado de informações sensíveis e outros dados pessoais. |
| ds\_email | Usado para envio de comunicações promocionais (desde que haja consentimento do cliente) ou comunicações transacionais (confirmação de compra, envio, etc) | Armazenamento deve ser criptografado no Banco de Dados e desvinculado de informações sensíveis e outros dados pessoais |
| nr\_telefone | Usado para envio de mensagens SMS ou Whatsapp, desde que haja consentimento do cliente | Armazenamento deve ser criptografado no Banco de Dados e desvinculado de informações sensíveis e outros dados pessoais |
| MC\_CLI\_FISICA | nr\_cpf | Utilizado para identificação do cliente e unificação do registro. | Dado deve ser pseudonimizado em um ambiente distinto e seu acesso, restringido |
| MC\_END\_CLI | nr\_end | Utilizado para realização de entregas de produtos | Dado deve ser mascarado na tabela e utilizado apenas para sua única finalidade |
| ds\_complemento\_end | Utilizado para realização de entregas de produtos | Dado deve ser mascarado na tabela e utilizado apenas para sua única finalidade |

**Referências:**

<https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd#:~:text=A%20base%20da%20LGPD%20%C3%A9,de%20forma%20expl%C3%ADcita%20e%20inequ%C3%ADvoca> - acessado em 29/10/2023

KAUER, Gisele, 2019. Anonimização, pseudonimização e criptografia: Perguntas frequentes, definições e o que diz a LGPD - <https://www.infranewstelecom.com.br/anonimizacao-pseudonimizacao-e-criptografia-perguntas-frequentes-definicoes-e-o-que-diz-a-lgpd/> - acessado em 29/10/2023

<https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd> - acessado em 29/10/2023