Matriz de Permissões e Responsabilidades no Banco de Dados da Concessionária

Este documento detalha o que cada papel (role) de usuário pode e, principalmente, o que **não pode** fazer no sistema do banco de dados. A estrutura foi desenhada seguindo o **Princípio do Menor Privilégio**, garantindo que cada usuário tenha acesso apenas ao necessário para sua função, maximizando a segurança e a integridade dos dados.

1. Papel: `gerente`

O papel de `gerente` é o mais poderoso entre os usuários de negócio, com amplas permissões para gerenciar dados e operações, mas ainda com limitações de segurança importantes.

✅ O que PODE fazer:

- **Conectar ao Banco de Dados:** Acessar o sistema da concessionária.
- **Visualizar Dados de Todas as Tabelas:** Executar `SELECT` em qualquer tabela (`CLIENTE` , `FUNCIONARIO` , `VENDA` , etc.) para gerar relatórios completos, auditar vendas ou analisar o desempenho geral.
- **Inserir Novos Registros:** Usar `INSERT` para cadastrar um novo funcionário, um novo carro no sistema ou adicionar uma loja.
- **Atualizar a Maioria dos Dados:** Usar `UPDATE` para corrigir informações, como o salário de um funcionário, o preço de um carro ou a meta de um vendedor.
- **Executar Quase Todas as Funções:** Utilizar a maioria das funções do sistema, incluindo relatórios gerenciais como `fn_listar_funcionarios_abaixo_meta()` e `fn_loja_campea_de_vendas()` .

❌ O que NÃO PODE fazer (e por quê):

- **NÃO PODE Deletar Registros Diretamente:** A permissão para a função `fn_deletar_da_tabela` foi explicitamente revogada (`REVOKE`).

    - **Motivo:** Deleções são operações perigosas e, muitas vezes, irreversíveis. Impedir que o gerente delete dados diretamente previne a remoção acidental ou maliciosa de registros críticos, como o histórico de uma venda. A remoção de dados deve seguir um protocolo mais rígido, talvez executado apenas por um administrador de banco de dados (DBA).
- **NÃO PODE Alterar a Estrutura do Banco de Dados:** Não pode criar, alterar ou apagar tabelas (`CREATE TABLE` , `DROP TABLE` , `ALTER TABLE`).
    - **Motivo:** A estrutura do banco de dados é a fundação do sistema. Apenas DBAs ou desenvolvedores devem ter permissão para modificá-la, garantindo que o sistema permaneça estável e consistente.
- **NÃO PODE Gerenciar Outros Usuários ou Permissões:** Não pode criar novos usuários (`CREATE USER`) ou conceder permissões (`GRANT`).
    - **Motivo:** A gestão de segurança é uma responsabilidade de alto nível. Centralizar essa tarefa em um administrador de banco de dados evita a proliferação de acessos indevidos.

2. Papel: `funcionario`

O papel de `funcionario` (vendedor) é projetado para as operações do dia a dia. Ele tem acesso para vender e consultar, mas de forma muito controlada.

✅ O que PODE fazer:

- **Conectar ao Banco de Dados:** Acessar o sistema para trabalhar.
- **Consultar Dados Relevantes para Venda:** Usar `SELECT` para ver a lista de carros, seus preços, o estoque disponível e o histórico de um cliente.
- **Executar Funções de Venda:** Utilizar funções específicas para realizar seu trabalho, como `fn_realizar_venda()` e `fn_inserir_na_venda()` . A lógica de negócio (como atualizar o estoque) é encapsulada e automatizada por gatilhos, garantindo que o processo seja seguido corretamente.
- **Consultar Seu Próprio Desempenho:** Executar `fn_listar_vendas_por_funcionario()` para ver seu histórico de vendas.

❌ O que NÃO PODE fazer (e por quê):

- **NÃO PODE Modificar Tabelas Diretamente:** Não tem permissão de `INSERT` , `UPDATE` ou `DELETE` em nenhuma tabela.
    - **Motivo:** Isso impede que um vendedor altere o preço de um carro manualmente, mude o valor de uma venda após o fato ou apague um registro para esconder um erro. Todas as modificações são uma consequência controlada de usar as funções de venda.

- **NÃO PODE Ver Dados Sensíveis de Outros Funcionários:** Não pode consultar a tabela `FUNCIONARIO` para ver o salário ou a meta de seus colegas.
  - **Motivo:** Privacidade e segurança. Informações de RH são confidenciais.
- **NÃO PODE Executar Funções Gerenciais:** Não pode chamar funções como `fn_listar_funcionarios_abaixo_meta()` ou `fn_total_vendido_por_loja()`.
  - **Motivo:** Essas são ferramentas de gestão, e o acesso a elas é restrito ao papel de `gerente` para evitar acesso a informações estratégicas consolidadas.

3. Papel: `cliente`

O papel de `cliente` é o mais restrito de todos, desenhado para um possível portal de autoatendimento onde o cliente consulta apenas suas próprias informações.

✅ O que PODE fazer:

- **Conectar ao Banco de Dados:** Acessar o portal do cliente.
- **Executar Duas Funções Específicas:**
  i. `fn_historico_compras_cliente()` : Para ver a lista de carros que ele já comprou.
  ii. `fn_detalhes_venda()` : Para ver os detalhes de uma compra específica (como um recibo digital).

❌ O que NÃO PODE fazer (e por quê):

- **NÃO PODE Consultar Nenhuma Tabela Diretamente:** Não tem permissão de `SELECT` em *nenhuma* tabela.
  - **Motivo:** Esta é a restrição de segurança mais crítica. Impede que um cliente sequer tente ver a lista de outros clientes, funcionários, ou o estoque da loja. Ele só pode ver os dados que as funções permitidas retornam para ele.
- **NÃO PODE Fazer Absolutamente Nada Além de Consultar o Próprio Histórico:** Qualquer tentativa de `INSERT`, `UPDATE`, `DELETE` ou de chamar outras funções resultará em um erro de "permissão negada".
  - **Motivo:** O cliente é um consumidor de dados, não um participante ativo nas operações do banco de dados. Seu acesso é estritamente "somente leitura" e filtrado para seus próprios dados.