Ejercicio 6

Pequeña aclaración, aparte de los 4 sql que subí, hice unos querys que no almacené en un sql, pero en resumen, la base queda como explico en las preguntas y como muestro en las imágenes

**Explicación detallada de la base de datos**

La base de datos implementa un sistema multi-tenant para e-commerce, estructurado con tablas principales como tenants, users, categories, products, orders, order\_items y role\_tenant\_map. El diseño está pensado para que cada empresa cliente (tenant) tenga sus propios usuarios, categorías, productos y órdenes, manteniendo toda la información separada. Cada tabla incluye campos para auditoría y todas mantienen una relación con la tabla tenants mediante el campo tenant\_id, creando una estructura jerárquica donde todo pertenece a un tenant específico.

**Aislamiento de datos entre clientes**

El aislamiento de datos se garantiza mediante Row Level Security, que actúa como un filtro invisible en todas las consultas. Cuando un usuario se conecta, el sistema identifica automáticamente su tenant mediante la función current\_tenant\_id(), que determina a qué tenant pertenece el usuario según el mapeo en role\_tenant\_map. Las políticas de RLS aseguran que cada usuario solo vea los datos de su propio tenant, excepto super\_admin que puede ver todo. Para tablas relacionadas como order\_items, el aislamiento funciona en cascada, verificando la pertenencia al tenant a través de la tabla orders. Esta estrategia asegura que los datos de un cliente nunca sean visibles para otro.

**Roles creados y sus permisos**

Para este ejercicio decidí crear 4 roles que tienen las siguientes características

El rol super\_admin tiene acceso completo a todas las tablas sin restricciones de tenant, pudiendo administrar todo el sistema. Se creó para los administradores de la plataforma.

El rol tenant\_admin tiene permisos totales en todas las tablas pero limitado a su propio tenant, permitiéndole administrar completamente un negocio específico.

El rol sales\_agent tiene permisos limitados, pudiendo ver y eliminar registros relacionados con productos, órdenes y sus ítems, pero no puede insertar ni actualizar. Solo puede ver el resto de tablas. Se creó para el personal de ventas con capacidad para gestionar el inventario existente.

El rol customer principalmente tiene permisos de lectura (select), pudiendo solo crear órdenes y sus ítems. Se diseñó para usuarios finales que realizan compras en la plataforma.

**Configuración de políticas RLS**

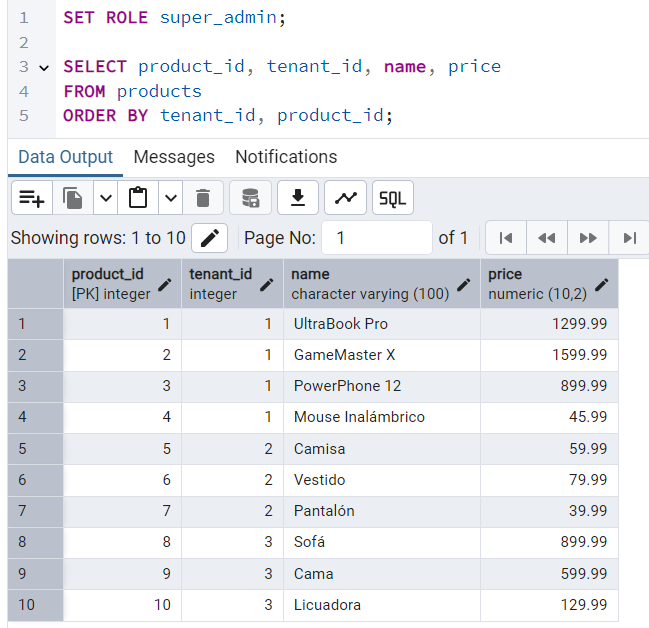
Las políticas RLS se configuraron activando primero esta característica en cada tabla con ALTER TABLE. Luego se crearon políticas de aislamiento que verifican si el tenant\_id del registro coincide con el tenant del usuario actual, obtenido mediante current\_tenant\_id(), o si el usuario es super\_admin. Para order\_items, la política es más compleja y verifica la relación con orders para asegurar el aislamiento. El rol super\_admin fue configurado con BYPASSRLS para permitirle acceder a todos los datos sin restricciones. Este enfoque garantiza que las políticas se apliquen automáticamente a todas las consultas sin necesidad de modificarlas.

**Análisis de resultados de pruebas**

Las pruebas confirmaron que el sistema funciona según lo diseñado, siendo que super\_admin puede acceder a todos los datos sin restricciones; tenant\_admin puede realizar todas las operaciones pero solo en los datos de su propio tenant; sales\_agent puede ver y eliminar registros pero no insertar ni actualizar; y customer principalmente tiene permisos de lectura, pudiendo solo crear órdenes. Cada rol ve únicamente los datos del tenant al que pertenece. El sistema RLS funciona correctamente aislando datos entre tenants mientras permite diferentes niveles de acceso según el rol, garantizando seguridad y privacidad en un entorno multi-cliente.

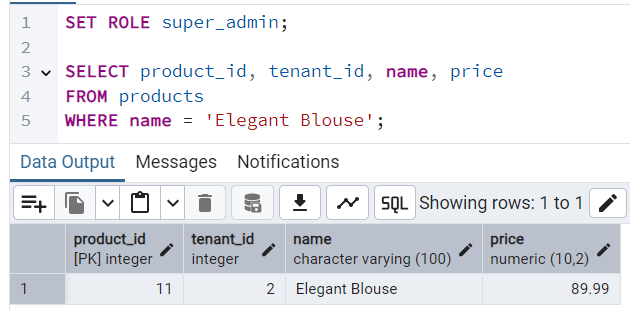
**Evidencias en imágenes**

Super\_admin



Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

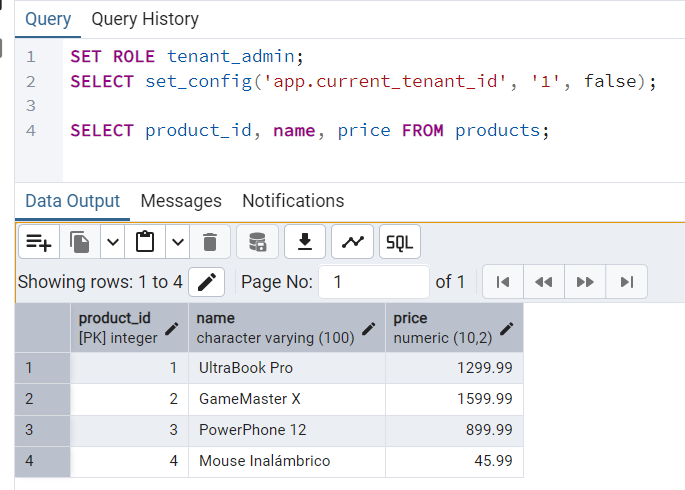
Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

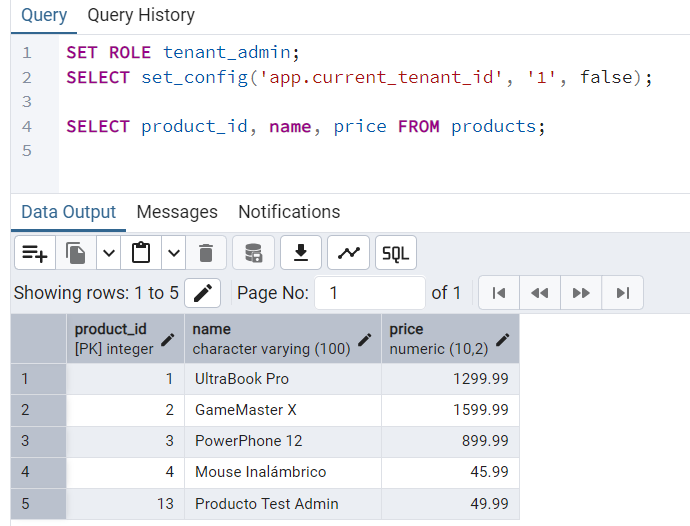
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

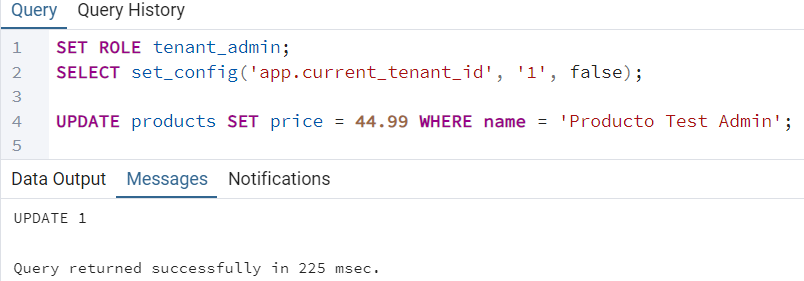
El contenido generado por IA puede ser incorrecto.

tenant\_admin









Tabla

El contenido generado por IA puede ser incorrecto.

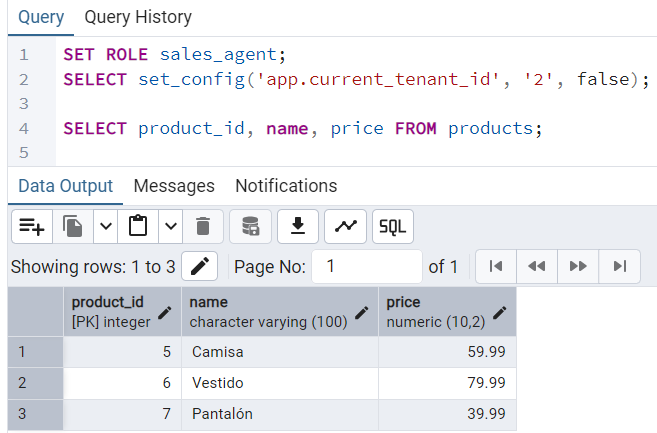
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

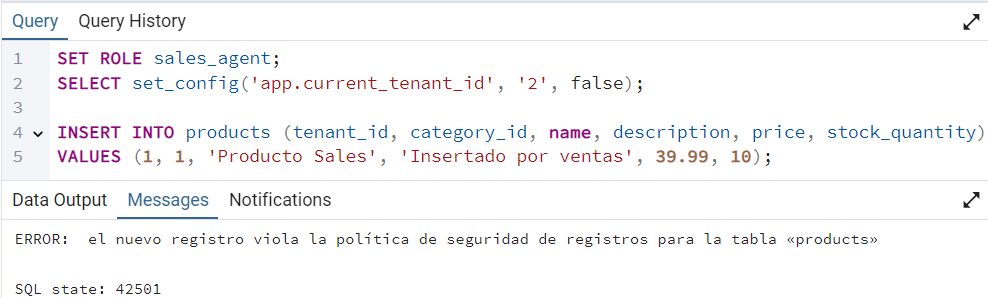
El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

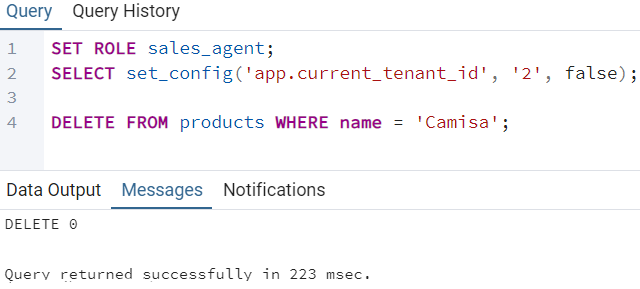
Sales\_agent





Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.



Customer

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.