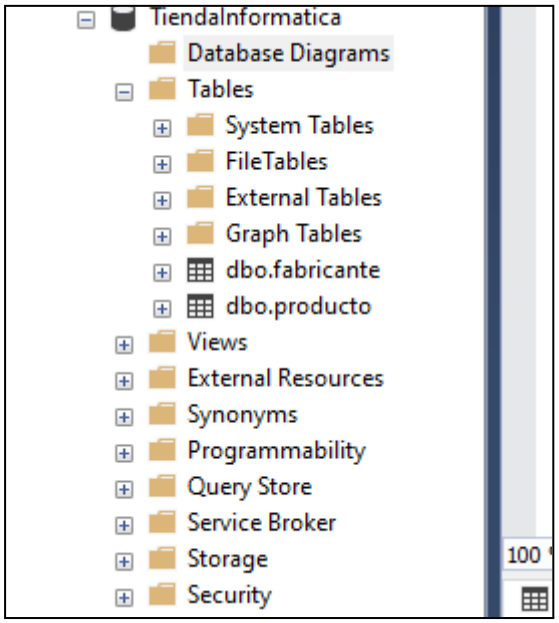
BASE DE DATOS USADA:



1.-Introducción a la seguridad en SQL Server

La seguridad en SQL Server es el conjunto de mecanismos y prácticas que protegen los datos y recursos del servidor de accesos no autorizados, garantizando la confidencialidad, integridad y disponibilidad de la información.

Partes fundamentales de la seguridad en SQL Server

1. **Autenticación**
   Controla quién puede conectarse al servidor. Puede ser:
   - **Autenticación de Windows** (más segura)
   - **Autenticación mixta** (Windows + SQL Server)
2. **Autorización**
   Determina qué acciones puede realizar un usuario o rol sobre los objetos (bases de datos, tablas, vistas, etc.) mediante permisos.
3. **Roles y permisos**
   - **Roles fijos de servidor y base de datos**: agrupan usuarios con permisos comunes.
   - **Permisos**: se asignan para permitir (o denegar) operaciones específicas (SELECT, INSERT, EXECUTE, etc.).
4. **Cifrado**
   Protege la información sensible mediante técnicas como:
   - Cifrado de datos a nivel de columna
   - Transparent Data Encryption (TDE)
   - Cifrado de conexión
5. **Auditoría y monitoreo**
   Registro de eventos relacionados con el acceso y uso de datos, para detectar actividades sospechosas o no autorizadas.

EJERCICIOS:

CREACIÓN DE UN LOGIN

```
CREATE LOGIN EmpleadoVentas WITH PASSWORD ='gatito',
```

CREAR UN USUARIO

```
CREATE USER EmpleadoVentas FOR LOGIN EmpleadoVentas
```

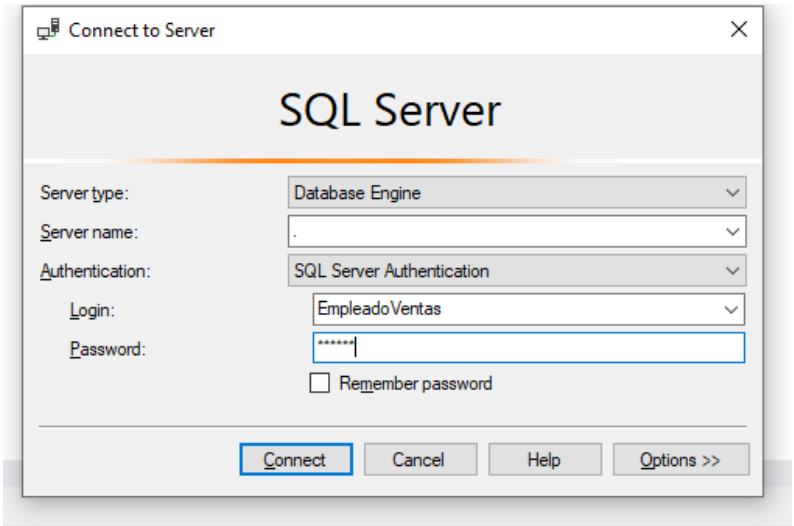
CREAR UN ROL PERSONALIZADO

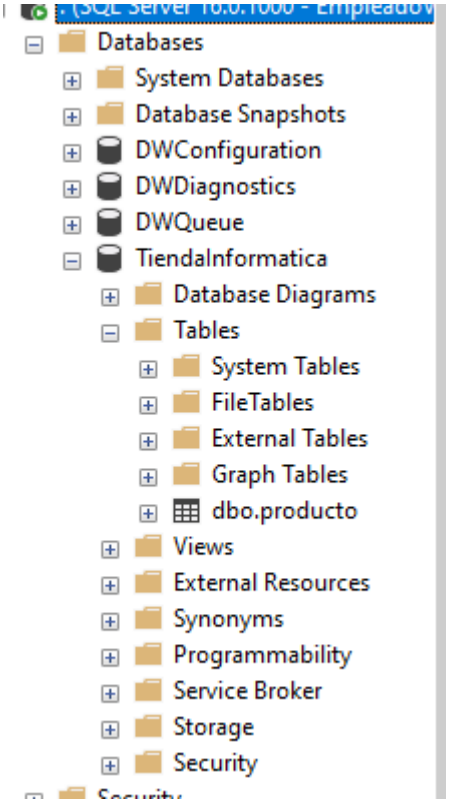
```
CREATE ROLE Ventas

GRANT SELECT ON producto TO  Ventas;
GRANT UPDATE ON producto TO Ventas;
```

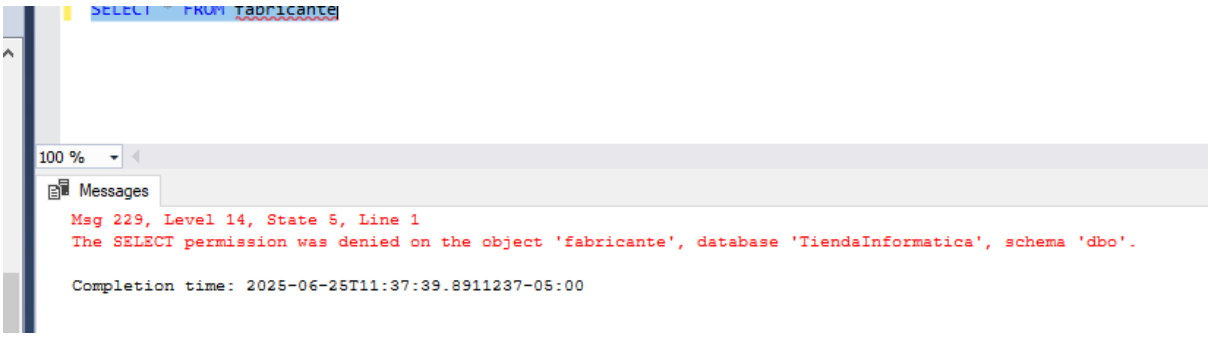
AGREGAR AL USUARIO

```
ALTER ROLE Ventas ADD MEMBER EmpleadoVentas;
```

PROBAR LA CONFIGURACION







cuando se trata de ingresar sin los permisos

2.Protección de datos en SQL Server

La protección de datos en SQL Server se basa en aplicar mecanismos que aseguren que la información almacenada esté resguardada contra accesos no autorizados, pérdidas, alteraciones o robos, garantizando su confidencialidad, integridad y disponibilidad.

Componentes clave de la protección de datos

1. **Cifrado de datos**
   Consiste en convertir los datos en un formato ilegible para quienes no tengan la clave adecuada. SQL Server ofrece:
   - **Cifrado de columnas** (por ejemplo, Always Encrypted)
   - **Transparent Data Encryption (TDE)** para cifrar la base de datos completa
   - **Cifrado de conexión SSL/TLS** para proteger los datos en tránsito
2. **Controles de acceso**
   Son reglas y configuraciones que determinan quién puede acceder a qué datos y qué operaciones puede realizar. Esto se logra mediante:
   - Autenticación (verificación de identidad)
   - Autorización (asignación de permisos)
   - Uso de **roles**, **usuarios** y **permisos granulares**
3. **Auditoría de seguridad**
   Registra y supervisa las acciones realizadas sobre los datos para detectar accesos indebidos o actividades sospechosas. Incluye:
   - SQL Server Audit (auditoría integrada)
   - Extended Events
   - Triggers para auditoría personalizada

3. Prevención de ataques en SQL Server

La prevención de ataques en SQL Server implica identificar y reducir vulnerabilidades del sistema, aplicar medidas de defensa activas y preparar un plan de respuesta eficaz ante posibles incidentes de seguridad.

---

1. Vulnerabilidades comunes en SQL Server

- **Inyección SQL**: cuando un atacante inserta código malicioso en consultas SQL.
- **Credenciales débiles**: contraseñas fáciles de adivinar o por defecto.
- **Exceso de permisos**: usuarios con más privilegios de los necesarios.
- **Falta de parches**: versiones del servidor sin actualizaciones de seguridad.
- **Exposición del puerto de SQL Server (1433)** a internet sin protección adecuada.

---

2. Medidas de protección contra ataques

- **Uso de parámetros en las consultas** para evitar inyección SQL.
- **Principio de mínimo privilegio**: asignar solo los permisos estrictamente necesarios.
- **Autenticación segura**: exigir contraseñas fuertes y usar autenticación de Windows si es posible.
- **Firewall y cifrado de conexiones** para proteger el acceso remoto.
- **Actualizaciones periódicas** del servidor y los sistemas asociados.

---

3. Plan de respuesta a incidentes

- **Detección temprana**: activar alertas y monitoreo (auditorías, logs).
- **Aislamiento del ataque**: desconectar el servidor comprometido si es necesario.
- **Análisis forense**: revisar los registros de eventos y actividades sospechosas.
- **Notificación interna** al equipo de TI y, si corresponde, a los usuarios afectados.
- **Corrección y documentación**: cerrar la vulnerabilidad y registrar el incidente para prevenir futuros casos.

LQuery8.sql - (l...PC24\USER 17 (113))* | SQLQuery7.sql - (l...PC24\USER 17 (108))*

```sql
INSERT INTO producto (nombre, precio, id_fabricante) VALUES
('Portátil Lenovo ThinkPad E15', 850.00, 1),
('Impresora HP LaserJet Pro', 150.00, 2),
('Monitor Asus 24 pulgadas', 200.00, 3);


CREATE LOGIN AppLogin WITH PASSWORD ='gatitos',
CHECK_POLICY= ON;

CREATE USER AppUser FOR LOGIN AppLogin

GRANT SELECT ON producto TO AppUser
```

```sql
DECLARE @SearchTerm_Safe NVARCHAR(200);

SET @SearchTerm_Safe = 'Teclado" OR 1=1; --';
DECLARE @SQL_Safe NVARCHAR(MAX);
SET @SQL_Safe = 'SELECT * FROM Productos WHERE NombreProducto = @P1';
PRINT @SQL_Safe;
EXEC sp_executesql
@SQL_Safe,
N'@P1 NVARCHAR(200)',
@P1 = @SearchTerm_Safe;
--
SELECT * FROM Productos WHERE Nombre Producto = @SearchTerm_Safe;
```