

# Seguridad en SQL Server 2008

SQL Server 2008 incluye un conjunto de características diseñadas para garantizar la seguridad de los datos y las operaciones. Este módulo explora las opciones de autenticación, seguridad en la base de datos, credenciales y el uso de EXECUTE AS.

## Modos de Seguridad

SQL Server ofrece dos modos principales de autenticación para controlar el acceso al servidor:

### Autenticación de Windows

- Este modo utiliza las credenciales del sistema operativo Windows para autenticar a los usuarios.
- Es más seguro, ya que aprovecha las políticas de seguridad de Windows, como contraseñas fuertes y autenticación basada en dominio.
- **Ejemplo:** El acceso se gestiona directamente mediante cuentas de usuario o grupos de Windows, configurados en SQL Server.

### Autenticación de SQL Server

- Este modo permite gestionar credenciales directamente en SQL Server, creando usuarios con nombres y contraseñas específicos para la base de datos.
- Es útil en entornos donde los usuarios no están integrados en Active Directory.
- **Ejemplo:**

```
CREATE LOGIN MiUsuario WITH PASSWORD = 'ContraseñaSegura';
```

## Seguridad a Nivel de Base de Datos

La seguridad a nivel de base de datos incluye permisos y roles para controlar el acceso a objetos específicos dentro de una base de datos.

- **Roles predefinidos:** Roles como db\_owner, db\_datareader, y db\_datawriter se asignan a usuarios para gestionar permisos fácilmente.
- **Permisos granulares:** Los permisos pueden asignarse a tablas, vistas, procedimientos, etc., utilizando comandos como GRANT, DENY, y REVOKE.
  - **Ejemplo:**

```
GRANT SELECT ON MiTabla TO MiUsuario;  
DENY INSERT ON MiTabla TO MiUsuario;
```

## Credenciales

Las credenciales permiten a SQL Server almacenar información de autenticación externa, como cuentas de Windows, para realizar tareas específicas fuera del entorno de la base de datos.

- **Creación de una credencial:**

```
CREATE CREDENTIAL MiCredencial
WITH IDENTITY = 'Dominio\Usuario',
SECRET = 'ContraseñaSegura';
```

- **Uso de credenciales:** Las credenciales se pueden asociar con inicios de sesión o tareas específicas, como acceder a recursos externos.

## Execute As

El comando EXECUTE AS permite a los usuarios ejecutar consultas o procedimientos almacenados con los permisos de otro usuario, facilitando la delegación y control de acceso.

- **Modos de uso:**
  - **EXECUTE AS USER:** Permite ejecutar con el contexto de un usuario específico dentro de la base de datos.
  - **EXECUTE AS LOGIN:** Cambia el contexto al de un inicio de sesión en el servidor.
- **Ejemplo:**

```
EXECUTE AS USER = 'MiUsuario';
SELECT * FROM MiTabla;
REVERT; -- Vuelve al contexto original
```