Manejo de Permisos a Nivel de Usuario en Base de Datos SQL Server

Para administrar con facilidad los permisos en las bases de datos, SQL Server proporciona varios roles, que son las entidades de seguridad que agrupan otras entidades de seguridad.

Se refiere al proceso de controlar y asignar qué acciones puede realizar un usuario específico dentro de una base de datos SQL Server. Esto implica determinar qué datos puede ver, modificar, eliminar o crear, así como qué comandos SQL puede ejecutar.

Para agregar y quitar usuarios en un rol de base de datos, se utiliza las opciones ADD MEMBER y DROP MEMBER de la instrucción [ALTER ROLE](https://learn.microsoft.com/es-es/sql/t-sql/statements/alter-role-transact-sql?view=sql-server-ver16) .

Existen dos tipos de roles en el nivel de base de datos: los *roles fijos de base de datos* que están predefinidos en la base de datos y los *roles de base de datos definidos por el usuario* que el usuario puede crear.

Los roles fijos de base de datos se definen en el nivel de base de datos y existen en cada una de ellas. Los miembros de los roles de base de datos db\_owner pueden administrar la pertenencia a roles fijos de base de datos.

Los permisos de los roles de base de datos definidos por el usuario se pueden personalizar con las instrucciones [GRANT](https://learn.microsoft.com/es-es/sql/t-sql/statements/grant-transact-sql?view=sql-server-ver16), [DENY](https://learn.microsoft.com/es-es/sql/t-sql/statements/deny-transact-sql?view=sql-server-ver16) y [REVOKE](https://learn.microsoft.com/es-es/sql/t-sql/statements/revoke-transact-sql?view=sql-server-ver16).

El manejo de permisos en SQL Server es fundamental para garantizar la seguridad y la integridad de los datos. Al comprender los conceptos básicos y las herramientas disponibles, se puede implementar una estrategia de seguridad efectiva y adecuada a las necesidades del proyecto.