**APUNTE PROYECTO INTEGRADOR BD I**

**TEMA: MANEJO DE PERMISOS A NIVEL DE USUARIOS DE BASE DE DATOS.**

Índice

[Usuarios. 2](#_Toc180778366)

[¿Qué son los usuarios? 2](#_Toc180778367)

[¿Qué son los inicios de sesión? 2](#_Toc180778368)

[¿Cómo se crea un usuario? 3](#_Toc180778369)

[Permisos. 4](#_Toc180778370)

[¿Qué son los permisos? 4](#_Toc180778371)

[¿Por qué son importantes estos permisos? 4](#_Toc180778372)

[¿Cómo se otorgan/eliminan estos permisos? 5](#_Toc180778373)

[¿Qué ventajas nos dan los permisos? 5](#_Toc180778374)

# Usuarios.

# ¿Qué son los usuarios?

Al igual que en otros servicios, SQL Server ofrece la opción de crear diferentes tipos de usuarios. Un usuario es una entidad de seguridad de la base de datos. Dependiendo del usuario, puede haber o no un inicio de sesión ligado a él.

Un usuario y un inicio de sesión **NO SON LO MISMO.**

Un usuario puede tener permisos dentro de la base de datos, pero sin un inicio de sesión no podrá conectarse al servidor.

A continuación, se detallan los tipos de usuarios más comunes:

* **SQL User sin Login**: Usuario que existe solo en la base de datos y no tiene un inicio de sesión asociado a nivel de servidor.
* **SQL User con Login**: Usuario de la base de datos que está asociado a un inicio de sesión de SQL Server (Login). Este login puede ser de autenticación SQL o autenticación de Windows.
* **Windows User**: Usuario de Windows que tiene permisos de acceso a la base de datos a través de su cuenta de Active Directory.
* **Application Role (Rol de Aplicación)**: Rol que se utiliza dentro de una aplicación para ejecutar con permisos específicos, sin estar ligado a un usuario individual.

# ¿Qué son los inicios de sesión?

Un inicio de sesión es una entidad de seguridad o una entidad que puede ser autenticada por un sistema seguro. Los usuarios necesitan un nombre de usuario para conectarse a SQL Server. Puede crear un inicio de sesión basado en una entidad de seguridad de Windows (como un usuario de dominio o un grupo de dominio de Windows) o puede crear un inicio de sesión que no esté basado en una entidad de seguridad de Windows (como un inicio de sesión de SQL Server).

Los inicios de sesión deben estar asignados a un usuario para poder conectarse a una base de datos. Un inicio de sesión se puede asignar a bases de datos diferentes como usuarios diferentes, pero solo se puede asignar como un usuario en cada base de datos.

Alguno de los inicios de sesión de SQL Server son los siguientes:

* **SQL Login**: Usuario autenticado mediante SQL Server Authentication, donde se crea un nombre de usuario y una contraseña dentro de SQL Server.
* **Windows Login**: Usuario autenticado mediante Windows Authentication, utilizando las credenciales de Active Directory.
* **Login de Certificado**: Basado en certificados para la autenticación.
* **Login de Asimetría (Asymmetric Key Login)**: Basado en claves asimétricas para la autenticación.

# ¿Cómo se crea un usuario?

1. **Usuario que se autentica en la base de datos contenida (contained database users):** Estos usuarios se crean y se autentican **dentro de la base de datos especificada**, por lo que solamente tendrán acceso a esa base de datos. No dependen de un inicio de sesión. Se crean utilizando las siguientes cláusulas:

CREATE USER NombreUsuario WITH PASSWORD = 'Contraseña';

1. **Usuarios basados en inicios de sesión en la base de datos principal:** Estos usuarios dependen de un inicio de sesión. El inicio de sesión se crea a nivel del servidor y, luego, los usuarios a nivel de base de datos se asocian a ese inicio de sesión.

Primero creamos el inicio de sesión:

CREATE LOGIN NombreLogin CON PASSWORD = 'Contraseña';

Luego creamos el usuario dentro de la base de datos que se asocia con ese inicio de sesión

USE consorcio;

CREATE USER NombreUsuario FROM LOGIN NombreLogin;

1. **Usuarios sin inicio de sesión**: Estos son usuarios creados en la base de datos que no están asociados a ningún inicio de sesión en el servidor. Al no tener ningún login asociado en el servidor, son útiles para escenarios de acceso limitado o automatización.

CREATE USER NombreUsuario WITHOUT LOGIN;

# Permisos.

# ¿Qué son los permisos?

En una base de datos existen “permisos”, los cuales son derechos que determinan lo que un usuario puede o no puede hacer con el manejo de los datos, específicamente con las tablas, datos, procedimientos, etc.…

Los permisos a nivel de usuario pueden incluir algunos de los siguientes derechos:

1. **SELECT:** Permite ver o consultar datos (leer información de una tabla).
2. **INSERT:** Permite agregar nuevos registros a una tabla.
3. **UPDATE:** Permite modificar registros existentes.
4. **DELETE:** Permite eliminar registros de una tabla.
5. **EXECUTE:** Permite ejecutar procedimientos almacenados

Un ejemplo sería el que tiene la capacidad de hacer cualquier acción sobre los datos, el llamado “super admin”.

# ¿Por qué son importantes estos permisos?

Nos permiten un control personalizado, se puede definir exactamente qué partes de la base de datos puede ver o modificar cada persona.

Este control de acceso es crucial para asegurar que solo las personas autorizadas puedan ver o modificar los datos, garantizando la integridad y la seguridad de la información almacenada.

Por ejemplo, un usuario podría tener permiso de lectura en una tabla (para ver los datos) pero no de escritura (para insertar o modificar información).

# ¿Cómo se otorgan/eliminan estos permisos?

Los administradores de la base de datos pueden otorgar estos permisos individualmente a cada usuario, mediante la cláusula *GRANT* y para eliminar se utiliza la cláusula *REVOKE.*

**GRANT** SELECT, INSERT, UPDATE, DELETE ON consorcio TO Admin;

Ejemplo para otorgar todos los permisos a un administrador en la tabla consorcio

**REVOKE** INSERT ON consorcio FROM Admin;

Ejemplo para eliminar el permiso de insertar a un administrador en la tabla consorcio

# ¿Qué ventajas nos dan los permisos?

* Seguridad: Solo los usuarios autorizados tienen acceso a funciones específicas, minimizando el riesgo de pérdida o modificación indebida de datos.
* Flexibilidad: Los permisos se pueden ajustar según las responsabilidades de cada usuario en la organización.
* Auditoría: Es más fácil rastrear quién tiene acceso a qué y controlar cómo se utiliza esa información.