UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Tarea 2

Bases de Datos

ALUMNO:
Pali Figueroa Santiago

PROFESOR:
Ing. Fernando Arreola

Ciudad Universitaria, Ciudad de México,
17 de agosto de 2025

1. ¿Qué se requiere para conectarse a una base de datos?

Para conectarse a una base de datos se necesita una autenticación mediante un login o usuario que valide las credenciales en el gestor de base de datos. El login se asocia con un usuario dentro de la base de datos, y este debe contar con el permiso de conexión (`CONNECT`) para acceder. Además, es necesario contar con permisos adicionales sobre esquemas u objetos dependiendo de la operación que se quiera realizar [8, 4].

2. Permisos a nivel sistema y a nivel objeto

Los permisos de sistema permiten ejecutar tareas administrativas a nivel global, como la creación de bases de datos, usuarios o configuraciones. En cambio, los permisos de objeto se limitan a operaciones específicas sobre elementos de la base de datos, tales como `SELECT`, `INSERT`, `UPDATE`, o `DELETE` [6, 3, 1].

3. ¿Cómo dar o quitar permisos?

La gestión de permisos se realiza mediante sentencias del lenguaje de control de datos (DCL). Los comandos principales son:

- `GRANT`: otorga permisos.
- `REVOKE`: elimina permisos otorgados previamente.
- `DENY`: en algunos sistemas, niega explícitamente permisos incluso si son heredados.

Estos comandos permiten controlar el acceso tanto a nivel de sistema como de objetos [7, 1, 4].

4. Diferencia entre rol y usuario

El **usuario** representa la identidad con la cual se autentica una persona o aplicación en la base de datos.

El **rol** es una agrupación de permisos que puede asignarse a uno o varios usuarios, facilitando la administración de privilegios. Los usuarios pueden heredar múltiples roles, y los roles pueden existir con o sin la capacidad de iniciar sesión [5, 8, 2].

Conclusión

Para conectarse a una base de datos se requiere un usuario autenticado y permisos adecuados. Estos permisos se dividen en dos niveles: sistema y objeto. Su gestión se hace mediante `GRANT`, `REVOKE` y, en algunos casos, `DENY`. Finalmente, los roles simplifican la administración al permitir asignar privilegios agrupados a usuarios.

Referencias

[1] Microsoft, "Permissions in the Database Engine," Microsoft Learn, 2025. [En línea]. Disponible en: `https://learn.microsoft.com/en-us/sql/relational-databases/security/permissions-database-engine?view=sql-server-ver17`. [Accedido: 22-ago-2025].

[2] Microsoft, "Roles de nivel de base de datos - SQL Server," Microsoft Learn, 2025. [En línea]. Disponible en: https://learn.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver17. [Accedido: 22-ago-2025].

[3] IBM, "System and Object Permissions," IBM Docs, 2025. [En línea]. Disponible en: https://www.ibm.com/docs/es/netcoolomnibus/8.1.0?topic=roles-system-object-permissions. [Accedido: 22-ago-2025].

[4] Qualoom, "Administración de usuarios y roles de PostgreSQL," Qualoom.es, 2025. [En línea]. Disponible en: https://www.qualoom.es/administracion-usuarios-roles-postgresql/. [Accedido: 22-ago-2025].

[5] V. Jadhav, "Understanding User, Roles and Privileges in PostgreSQL," Medium, 2023. [En línea]. Disponible en: https://medium.com/@vedantjdv/understanding-user-roles-and-privileges-in-postgresql-101fdba2ee18. [Accedido: 22-ago-2025].

[6] Wikipedia, "Database Security," Wikipedia, 2025. [En línea]. Disponible en: https://en.wikipedia.org/wiki/Database_security. [Accedido: 22-ago-2025].

[7] Wikipedia, "Data Control Language," Wikipedia, 2025. [En línea]. Disponible en: https://en.wikipedia.org/wiki/Data_control_language. [Accedido: 22-ago-2025].

[8] Universidad Don Bosco, "Guía Autenticación y Autorización Usuarios y Esquemas Seguridad," UDB, 2019. [En línea]. Disponible en: https://www.udb.edu.sv/udb_files/recursos_guias/informatica-ingenieria/base-de-datos-i/2019/i/guia-12.pdf. [Accedido: 22-ago-2025].