Tarea 3

Mariana Daniela Hernandez Perez

24 de agosto 2025

1. Introducción

En la administración de bases de datos, la gestión de usuarios y roles es un aspecto esencial para garantizar la seguridad, confidencialidad e integridad de la información. Un usuario representa a una entidad que accede a la base de datos, mientras que los roles permiten agrupar permisos y asignarlos de manera más eficiente.

En este documento se ejemplifica el proceso de creación de un usuario con limitaciones específicas y la asignación de permisos a través de un rol. El enfoque práctico está orientado al uso de un sistema de gestión de bases de datos como *PostgreSQL*, donde estas funcionalidades se implementan mediante sentencias SQL.

2. Creación de Usuario

Se procede a la creación de un usuario denominado `estudiante_usuario`. Dicho usuario se configura con las siguientes restricciones:

- Una contraseña segura.
- Un límite de tres conexiones simultáneas.
- Una vigencia de un mes a partir de la fecha actual.

El siguiente código SQL refleja esta configuración:

```
-- Crear usuario con l mite de conexiones y vigencia de un mes
CREATE USER estudiante_usuario
WITH PASSWORD 'Contrase aSegura123'
CONNECTION LIMIT 3
VALID UNTIL CURRENT_DATE + INTERVAL '1 month';
```

3. Creación de Rol y Asignación de Permisos

Posteriormente, se crea un rol denominado `rol_estudiante`, al cual se le asignan permisos sobre la tabla `estudiante`. Los permisos incluyen lectura (`SELECT`), actualización (`UPDATE`) y eliminación de registros (`DELETE`).

```
-- Crear rol
CREATE ROLE rol_estudiante;

-- Asignar permisos sobre la tabla estudiante
GRANT SELECT, UPDATE, DELETE ON TABLE estudiante TO rol_estudiante;

-- Asignar el rol al usuario creado previamente
GRANT rol_estudiante TO estudiante_usuario;
```

4. Verificación de Permisos

Para comprobar la correcta asignación de roles y privilegios, es posible consultar los roles otorgados al usuario mediante el comando:

```
-- Mostrar roles asociados al usuario
\du estudiante_usuario
```

De igual forma, se pueden ejecutar operaciones de lectura, actualización o borrado sobre la tabla `estudiante` para validar la funcionalidad del rol asignado.

5. Conclusiones

La correcta gestión de usuarios y roles en bases de datos relacionales es un pilar fundamental para la seguridad y eficiencia en la administración de sistemas de información. A través del ejercicio realizado, se comprobó lo siguiente:

- Es posible establecer restricciones de seguridad a nivel de usuario, tales como límites de conexión y vigencia temporal.
- La creación de roles permite centralizar y simplificar la asignación de permisos.
- La asignación de roles a usuarios garantiza un control granular sobre los accesos, reforzando la protección de los datos.

Este procedimiento constituye una práctica recomendable en ambientes empresariales y académicos, donde la integridad de la información debe estar garantizada.

Referencias

[1] PostgreSQL Global Development Group, "Role Attributes and Management," *PostgreSQL Documentation*, [En línea]. Disponible en: `https://www.postgresql.org/docs/current/user-manag.html`. [Accedido: 24-ago-2025].

[2] A. Silberschatz, H. F. Korth y S. Sudarshan, *Database System Concepts*, 7a ed., New York, NY, USA: McGraw-Hill, 2020.