

MODELADO Y GESTIÓN DE BASE DE DATOS

TALLER: IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD CON ROLES Y  
DISPARADORES

PRESENTAN

QUINTERO POVEDA LAURA MARCELA

NEIVA – HUILA

COORPORACIÓN UNIVERSITARIA DEL HUILA – CORHUILA

OCTUBRE DEL 2025

## Tabla de contenido

Introducción .....	4
Justificación .....	4
Alcance .....	5
Glosario .....	5
Mapa de roles y privilegios .....	6
Principios de seguridad en bases de datos .....	7
Capturas de lo realizado .....	8
Reflexión .....	13
Referencias bibliográficas .....	14

### **Tablas de Ilustraciones**

Ilustración 1: Mapa de roles y privilegios.....	6
Ilustración 2: Creación de tablas y base de datos .....	8
Ilustración 3: Creación de roles y asignación de permisos .....	9
Ilustración 4: Creación de triggers de auditoría y validación .....	10
Ilustración 5: Pruebas1 .....	11
Ilustración 6: Pruebas2.....	12

## **Introducción**

En un centro hospitalario la información de pacientes es extremadamente confidencial, ya que se manejan datos personales, historiales médicos, citas y tratamientos. Por eso, es necesario tener un sistema de seguridad en la base de datos, para proteger la información y permitir que solo personas autorizadas accedan a ella, de este modo la confidencialidad de los datos del paciente no se ve afectada y sin alteraciones.

En este taller veremos el caso de Hospital Care, el cual busca implementar un sistema de seguridad basado en roles y disparadores- Los roles asignan permisos según el usuario, evitando que un externo realice acciones cuestionables. Los disparadores ayudan a registrar de manera automática los cambios e impedir operaciones que puedan causar errores. Con estas herramientas se construirá una base de datos segura y confiable.

## **Justificación**

La creación e implementación de los mapas de roles y privilegios es esencial para manejar de manera clara la información y seguridad. Al asignar permisos según el rol, se asegura que las operaciones realizadas por el sistema estén alineadas con sus responsabilidades.

La inclusión de mecanismos como disparadores de auditoría y validación fortalece los principios de seguridad y confidencialidad. Estos recursos permiten registrar cambios en tiempo real, prevenir operaciones inconsistentes y mantener una protección en la base de datos. Por este motivo, se planea lograr un entorno mas seguro y controlado de la gestión de información.

## Alcance



Se centrará en garantizar un control de acceso seguro mediante la asignación de roles con restricciones para cada actor del sistema, de esta manera los administradores, médicos, recepcionistas y auditores cuenten con las alternativas necesarias para cumplir sus funciones. De este modo, se incluyen herramientas automáticas como los dispensadores para las auditorías, ya que registran las operaciones para asegurar la información.

## Glosario

<b>Término</b>	<b>Definición Breve</b>
Auditoría (en Bases de Datos)	Proceso de registro y revisión de la actividad de los usuarios para garantizar la seguridad y la integridad de los datos.
Auditoría y Trazabilidad	Principio que asegura que toda acción en el sistema quede documentada para su revisión (registro de operaciones).
Confidencialidad	Principio que garantiza que la información solo es accesible por usuarios o roles autorizados.
Control de Acceso	Verificación de la identidad del usuario y limitación de sus acciones según su rol y permisos.
Disparador o <i>Trigger</i>	Código asociado a una tabla que se ejecuta automáticamente ante un evento (ej. insertar, modificar o borrar datos).
Integridad	Principio que garantiza que los datos son exactos, coherentes y no han sido manipulados.
Información Confidencial (Hospitalaria)	Datos personales, historiales y tratamientos del paciente que deben protegerse por ley (PHI).
Privilegio (en Bases de Datos)	Autorización específica concedida a un usuario o rol para realizar una acción (ej. leer, insertar, modificar).
Rol (en Bases de Datos)	Conjunto de privilegios que se asignan a un usuario para definir su nivel de acceso y responsabilidades.

**Tabla 1:** Glosario

## Mapa de roles y privilegios

Actor	Descripción	Operaciones Permitidas	Permisoso
Administrador	Es aquel que tiene control total de la Base de Datos, Configura roles y seguridad	<ul style="list-style-type: none"> <li>• CREATE, ALTER, DROP en toda la BD.</li> <li>• IINSERT, UPDATE, DELETE, SELECT en todas las tablas.</li> </ul>	Acceso a todas las tablas. Sin restricciones.
Médico	Es el que gestiona la información clínica y tratamiento de los pacientes	<ul style="list-style-type: none"> <li>• SELECT en pacientes, citas, historiales clínicos y tratamientos.</li> <li>• INSERT y UPDATE en historiales clínicos y tratamientos</li> </ul>	<p>Puede leer datos generales de pacientes y citas.</p> <p>No puede eliminar pacientes, modificar usuarios ni acceder a datos administrativos.</p>
Recepcionista	Es la persona que controla programación de citas y manejo de datos básicos de pacientes	<ul style="list-style-type: none"> <li>• INSERT, UPDATE en citas.</li> <li>• SELECT en pacientes y citas.</li> </ul>	Solo puede registrar, modificar citas y consultar datos generales de pacientes. No puede ver ni editar historiales clínicos ni tratamientos.
Auditor	Supervisa la Base de Datos, con el fin de control y auditoría	<ul style="list-style-type: none"> <li>• SELECT en tablas de auditoría, pacientes, citas, historiales clínicos y tratamientos.</li> </ul>	<p>Acceso único de lectura</p> <p>No puede insertar, actualizar ni eliminar registros en ninguna tabla</p>






Ilustración 1: Mapa de roles y privilegios

## Principios de seguridad en bases de datos

En las bases de datos hay un conjunto de principios esenciales que buscan proteger la información ya sea de manipulación, acceso indebido o pérdida de esta. Estos principios permiten establecer medidas para garantizar la protección de la información. Entre estos principios los más relevantes son:

- **Confidencialidad:** Se asegura que los datos puedan ser consultados o modificador por los usuarios permitidos.
- **Integridad:** Garantiza que la información sea coherente, exacta y clara, sin manipulación de estos.
- **Disponibilidad:** Busca que la información proporcionada sea accesible a quien tiene la autorización, para que sea accesible.
- **Autenticación y control de accesos:** Verifica la identidad de los usuarios y limita sus acciones según el rol correspondiente.
- **Auditoria y trazabilidad:** Garantiza las operaciones, del modo que cualquier acción queda documentada para revisión
- **Prevención de vulnerabilidades:** Aplicación de medidas técnicas para reducir la exposición de manipulación de externos.

## Capturas de lo realizado

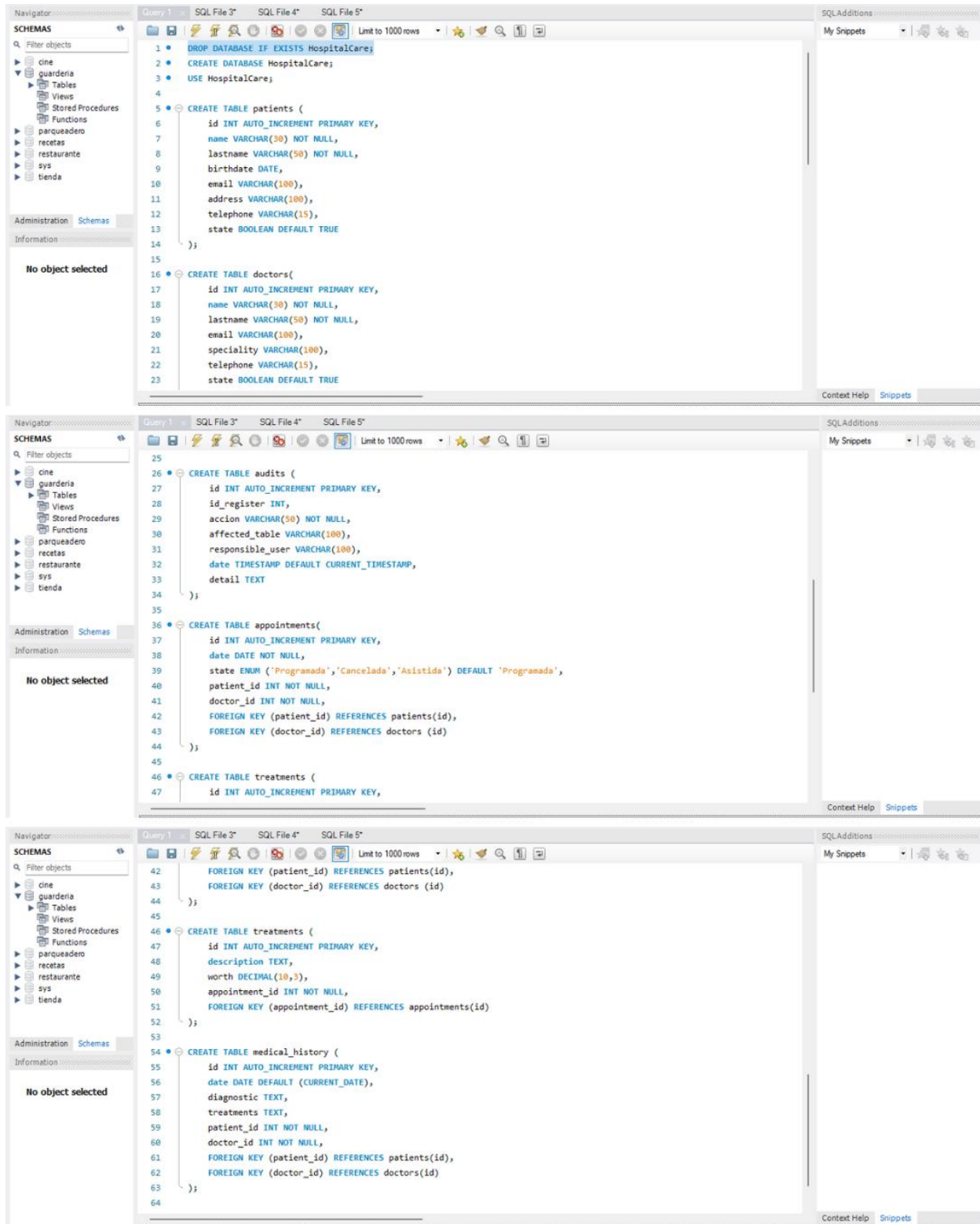


Ilustración 2: Creación de tablas y base de datos



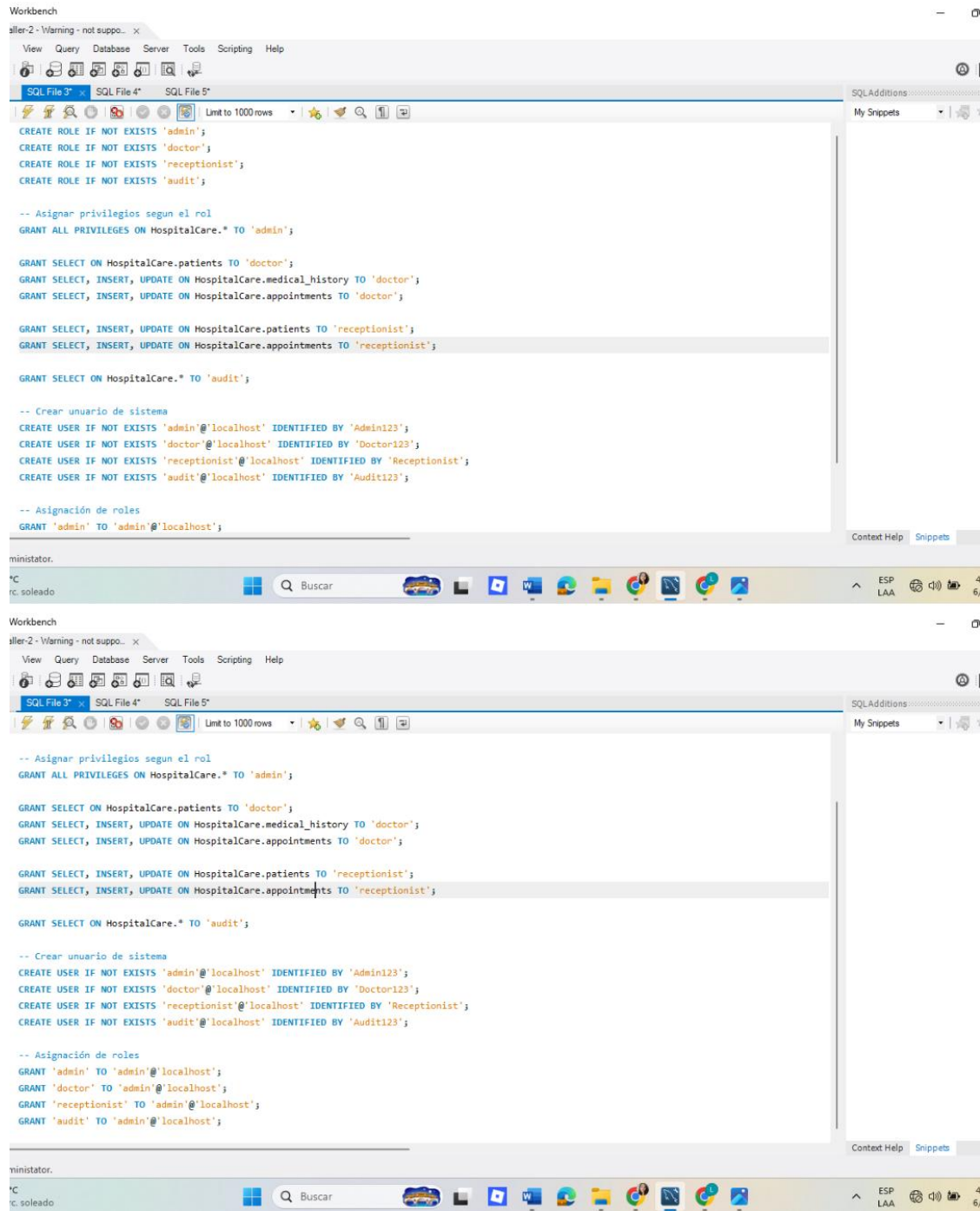


Ilustración 3: Creación de roles y asignación de permisos

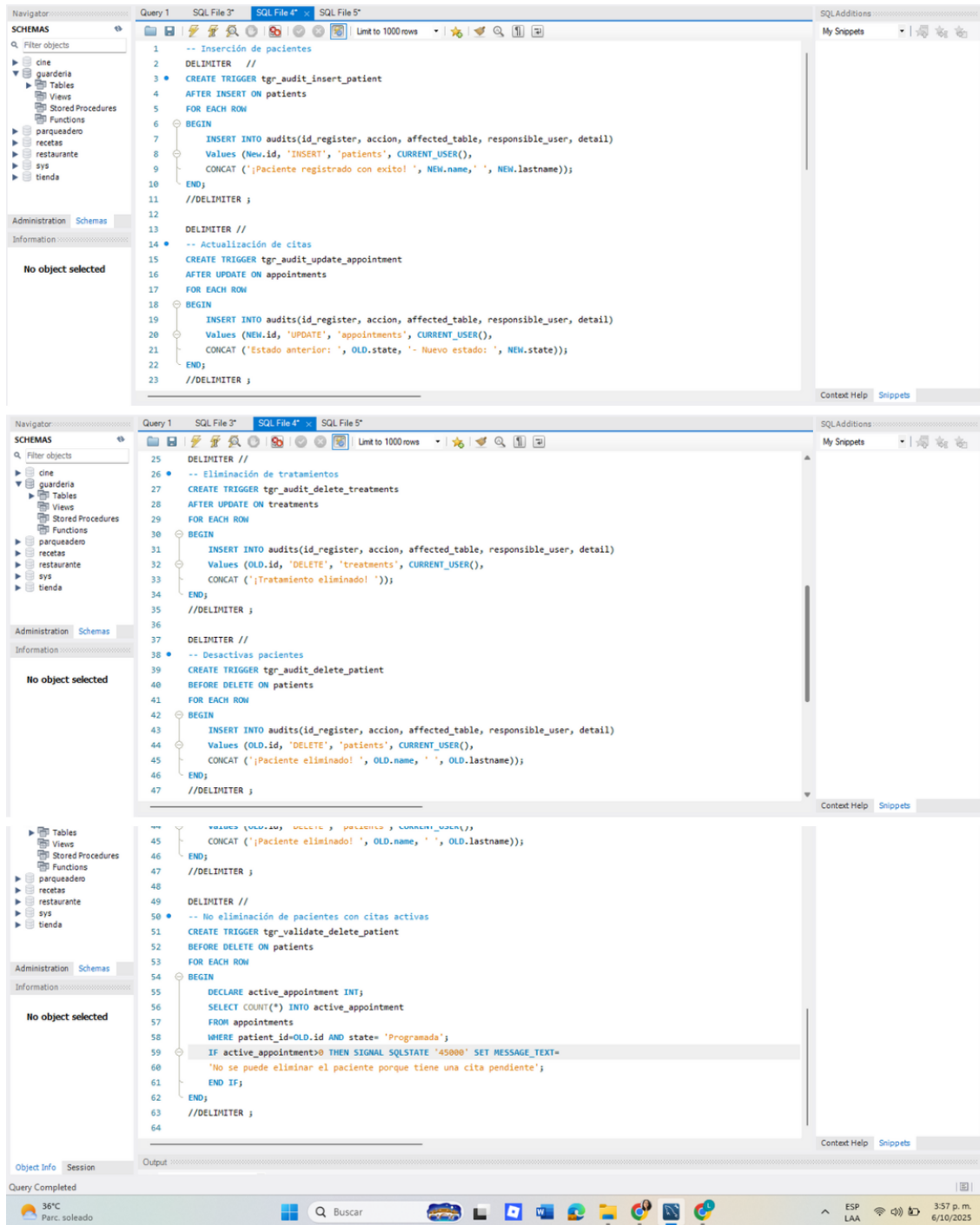


Ilustración 4: Creación de triggers de auditoría y validación

The screenshot displays a SQL IDE interface with a script editor on the left and an output window on the right. The script contains SQL commands for inserting data into tables and deleting records. The output window shows the execution progress, including the number of rows affected and the duration of each operation. The final error message indicates that a patient cannot be deleted because they have a pending appointment.

```

3 -- Insertar pacientes, doctores y citas
4 INSERT INTO patients(name, lastname, birthdate, email, address, telephone) VALUES
5 ('Miriam', 'Cabello Lara', '2000-02-12', 'miricabellolara@gmail.com', 'Calle 12 #20-12', '8282717132'),
6 ('Leonidas', 'Tovar Tamallo', '1962-02-27', 'leostovartamallo@gmail.com', 'Carrera 8 #10-21', '9181818912'),
7 ('Juan Camilo', 'Mora Lima', '1999-05-01', 'juancamimorallma@gmail.com', 'Calle 3 #1-50', '0094411222132');
8
9 INSERT INTO doctors(name, lastname, email, speciality, telephone) VALUES
10 ('Luna', 'Montenegro Diez', 'lunamontenegro@hospital.com', 'Neurocirujano', '3211192822'),
11 ('Jhon Alex', 'Mendez Medina', 'jhonmendezmedina@hospital.com', 'Urologia', '9288273737'),
12 ('Marlon', 'Quintero Lopez', 'marlonquintero@hospital.com', 'Medicina General', '938737721');
13
14 INSERT INTO appointments(date, state, patient_id, doctor_id) VALUES
15 ('2025-10-05', 'Asistida', 1, 2),
16 ('2025-10-05', 'Cancelada', 2, 3),
17 ('2025-12-06', 'Programada', 3, 1);
18
19 -- Tratar de eliminar paciente con cita activa
20 DELETE FROM patients WHERE id=3;
21 SELECT * FROM patients WHERE id=3;
22
23 -- Actualizar estado de la cita de Programada a Asistida
24 UPDATE appointments SET state= 'Asistida' WHERE id=3;
25
26 -- Eliminación del paciente 2(Leonidas)
27 DELETE FROM patients WHERE id=2;
28
29 -- Tabla auditoria
30 SELECT * FROM audits;

```

**Output:**

#	Time	Action	Message	Duration / Fetch
148	15:57:27	-- Desactivar pacientes CREATE TRIGGER tgr_audit_delete_patient BEFORE DELETE ON patient	0 row(s) affected	0.016 sec
149	15:57:27	-- No eliminación de pacientes con citas activas CREATE TRIGGER tgr_validate_delete_patient B...	0 row(s) affected	0.015 sec
150	15:58:08	INSERT INTO patients(name, lastname, birthdate, email, address, telephone) VALUES (Miriam, Ca...	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.031 sec
151	15:58:08	INSERT INTO doctors(name, lastname, email, speciality, telephone) VALUES (Luna, Montenegro D...	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.000 sec
152	15:58:08	INSERT INTO appointments(date, state, patient_id, doctor_id) VALUES (2025-10-05, 'Asistida', 1, 2)...	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.016 sec
153	15:58:27	DELETE FROM patients WHERE id=3	Error Code: 1544. No se puede eliminar el paciente porque tiene una cita pendiente	0.015 sec

**Result Grid:**

id	name	lastname	birthdate	email	address	telephone	state
3	Juan Camilo	Mora Lima	1999-05-01	juancamimorallma@gmail.com	Calle 3 #1-50	0094411222132	1

**Output:**

#	Time	Action	Message	Duration / Fetch
150	15:58:08	INSERT INTO patients(name, lastname, birthdate, email, address, telephone) VALUES (Miriam, Ca...	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.031 sec
151	15:58:08	INSERT INTO doctors(name, lastname, email, speciality, telephone) VALUES (Luna, Montenegro D...	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.000 sec
152	15:58:08	INSERT INTO appointments(date, state, patient_id, doctor_id) VALUES (2025-10-05, 'Asistida', 1, 2)...	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.016 sec
153	15:58:27	DELETE FROM patients WHERE id=3	Error Code: 1544. No se puede eliminar el paciente porque tiene una cita pendiente	0.015 sec
154	15:59:01	SELECT * FROM patients WHERE id=3 LIMIT 0, 1000	1 row(s) returned	0.000 sec / 0.000 sec

Ilustración 5: Pruebas1

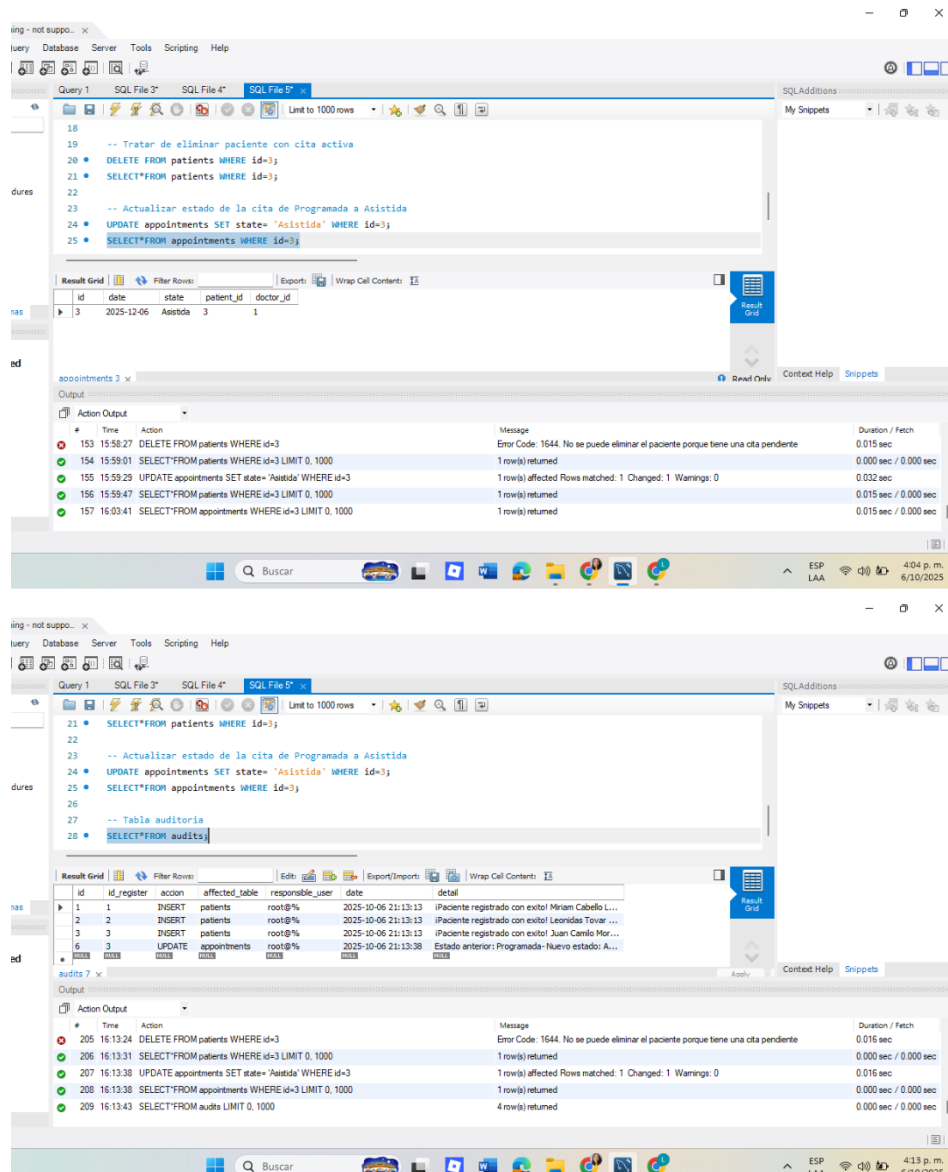


Ilustración 6: Pruebas2

## **Reflexión**

La seguridad en las bases de datos es un aspecto esencial en entorno donde se trabaja con información privada, como sucede en el caso práctico hospitales. En estos centros los datos de los pacientes, médicos citas son altamente confidenciales y requieren protección. Implementar roles y triggers en la base de datos asegurándose que no haya manipulación por personal no autorizado.

El uso de roles establece diferentes accesos y responsabilidades, por ejemplo, en el caso práctico, los administradores controlan toda la base de datos, los médicos pueden consultar y registrar historiales clínicos, los recepcionistas administran las citas y los auditores supervisan la información. Esta organización evita que usuarios sin autorización accedan. De esta manera, los roles se convierten en un soporte fundamental para el ordenamiento, almacenamiento y gestión de la información.

Por otro lado, los triggers o disparadores hacen un complemento de la seguridad mediante la automatización de las tareas. En este proyecto, implementamos triggers para revisar cambios en tablas, registrar automáticamente acciones y operaciones. Esta automatización nos permite un control preciso y asegurando transparencia en las operaciones.

En conclusión, el diseño de seguridad de la base de datos, basado en triggers y roles, es indispensable para cualquier entorno que maneja información personal y delicada. En el caso práctico de Hospital Care, estas medidas no solo protegen la privacidad de los pacientes, si no que al implementarlas asegura una estabilidad, confiabilidad y ética del manejo de datos.

### Referencias bibliográficas

IBM. (s. f.). Seguridad de bases de datos. IBM Think. Recuperado el 4 de octubre de 2025, de <https://www.ibm.com/es-es/think/topics/database-security>

SlideTeam. (2023, 18 de abril). Las 10 plantillas principales de matrices de roles y responsabilidades con ejemplos y muestras. SlideTeam. Recuperado de <https://www.slideteam.net/blog/las-10-plantillas-principales-de-matrices-de-roles-y-responsabilidades-con-ejemplos-y-muestras?lang=Spanish>

DataGuard. (2024, 5 de marzo). Principles of data security: 8 key principles explained. DataGuard Blog. Recuperado de <https://www.dataguard.com/blog/principles-of-data-security/>

Amazon Redshift. (s.f.). Definición de roles de base de datos para concederlos a los usuarios federados en Amazon Redshift sin servidor. Recuperado el 4 de octubre de 2025, de [https://docs.aws.amazon.com/es\\_es/redshift/latest/mgmt/redshift-iam-access-federated-db-roles.html](https://docs.aws.amazon.com/es_es/redshift/latest/mgmt/redshift-iam-access-federated-db-roles.html)

ArcGIS. (s.f.). Tipos de usuarios, roles y privilegios. Recuperado el 4 de octubre de 2025, de <https://enterprise.arcgis.com/es/portal/10.7/use/roles.htm>

Google Cloud. (s.f.). Auditoría de la base de datos de MySQL (Google Cloud for MySQL). Recuperado el 4 de octubre de 2025, de <https://cloud.google.com/sql/docs/mysql/db-audit?hl=es-419>

HubSpot. (s.f.). 5 pasos para hacer una auditoría de base de datos. Recuperado el 4 de octubre de 2025, de <https://blog.hubspot.es/marketing/auditoria-base-de-datos>

IBM. (s.f.). Roles. Recuperado el 4 de octubre de 2025, de <https://www.ibm.com/docs/es/db2/11.1.0?topic=security-roles>

NeoAttack. (s.f.). ¿Qué es un Trigger y para qué sirve? Neo Wiki. Recuperado el 4 de octubre de 2025, de <https://neoattack.com/neowiki/trigger/>

ORSYS. (s.f.). Definición de privilegio. Recuperado el 4 de octubre de 2025, de <https://www.orsys.fr/orsys-lemag/es/glosario/privilegio/>

Radiologyinfo.org. (s.f.). Privacidad de la información médica. Recuperado el 4 de octubre de 2025, de <https://www.radiologyinfo.org/es/info/article-patient-privacy>

Wikipedia. (s.f.). Trigger (base de datos). Recuperado el 4 de octubre de 2025, de [https://es.wikipedia.org/wiki/Trigger\\_\(base\\_de\\_datos\)](https://es.wikipedia.org/wiki/Trigger_(base_de_datos))