INSTITUTO TECNOLÓGICO DE COSTA RICA
ESCUELA DE COMPUTACIÓN
BASES DE DATOS II
IC-4302

Proyecto Programado #2

Grupo 20

Integrantes:

Araya Nash Hengerlyn D Angiely

Gonzalez Barrantes Jose Miguel

Salas Cordero Jefferson Jose

Profesor:

Alberto Shum Chan

23 de octubre de 2024.

II Semestre 2024. Instituto Tecnológico de Costa Rica, Sede Alajuela.

1. Base de datos para alquiler de películas

1.1 Funciones y procedimientos del sistema transaccional:

- **Insertar un nuevo cliente:**

Para la funcionalidad se trata de insertar un nuevo cliente en la base de datos, para ello se desarrolló un procedimiento almacenado en donde se realiza la acción mencionada anteriormente.

Atributos: Son todos aquellos datos de entrada o salida del procedimiento almacenado. En este caso solo son datos de entrada.

Atributo	Explicación
in_first_name	Entrada de primer nombre
in_last_name	Entrada de último nombre
in_email	Entrada de correo electrónico
in_address_id	Identificador de dirección
in_store_id	Identificador de tienda
in_active_bool	Booleano de activo
in_create_date	Fecha de creación
in_last_update	Fecha de última modificación

in_active	Entero de activo

El procedimiento almacenado consiste en ingresar los respectivos atributos que fueron mencionados anteriormente. Se debe tomar en cuenta lo siguiente: Durante la inserción se asume que el identificador de la tienda y la dirección es de datos que ya existen en la base de datos, de lo contrario no se realizará la inserción. Como cualquier inserción se utiliza la el elemento de la línea 17 a la línea 24, si se realiza de manera correcta, levanta una noticia avisando con el nombre del nuevo cliente insertado. A continuación adjunta el código correspondiente:

```
1  CREATE OR REPLACE PROCEDURE insertar nuevo cliente(
2      in_first_name VARCHAR,
3      in_last_name VARCHAR,
4      in_email VARCHAR,
5      in_address_id INT,
6      in_store_id INT,
7      in_active_bool BOOLEAN,
8      in_create_date DATE,
9      in_last_update TIMESTAMP WITHOUT TIME ZONE,
10     in_active INT
11 )
12 LANGUAGE plpgsql
13 SECURITY DEFINER
14 AS $$
15 BEGIN
16     -- Insertar cliente
17     INSERT INTO public.customer(
18         store_id, first_name, last_name, email, address_id, activebool, create_date,
19 last_update, active
20     )
21     VALUES (
22         in_store_id, in_first_name, in_last_name, in_email,
23         in_address_id, in_active_bool, in_create_date, in_last_update, in_active
24     );
25     RAISE NOTICE 'Nuevo cliente registrado correctamente, nombre: % %', in first_name,
26     in_last_name;
27
28 EXCEPTION
29     WHEN unique_violation THEN
30         RAISE NOTICE 'El cliente ya existe con el email %.', un email;
31     WHEN foreign_key_violation THEN
32         RAISE NOTICE 'El store_id o address_id no son válidos.';
33     WHEN others THEN
34         RAISE NOTICE 'Ocurrió un error: %', SQLERRM;
35 END;
```

- **Registrar un alquiler:**

Para el caso del registro de un alquiler, se desarrolló un procedimiento almacenado en la base de datos en donde se realiza la acción mencionada anteriormente. Note que se asume que el registro de inventario y de staff ya existen en sus respectivas tablas de la base de datos.

Atributos: Son todos aquellos datos de entrada o salida del procedimiento almacenado. En este caso solo son datos de entrada.

Atributo	Explicación
in_rental_date	Fecha de renta de película
in_inventory_id	Identificador de inventario
in_customer_id	Identificador de cliente
in_return_date	Fecha de regreso de película
in_staff_id	Identificador de empleado
in_last_update	Fecha de última modificación

Parecido al caso del procedimiento almacenado anteriormente, primero mediante un comando SQL representado en la línea 14 a la línea 20 se insertan los datos correspondientes, en caso que ocurra un error al momento de hacer la acción, salta una noticia del error presentado y su respectiva causa.

```
 1 CREATE OR REPLACE PROCEDURE registrar_alquiler(
 2     in_rental_date TIMESTAMP WITHOUT TIME ZONE,
 3     in_inventory_id INT,
 4     in_customer_id SMALLINT,
 5     in_return_date TIMESTAMP WITHOUT TIME ZONE,
 6     in_staff_id SMALLINT,
 7     in_last_update TIMESTAMP WITHOUT TIME ZONE
 8 )
 9 LANGUAGE plpgsql
10 SECURITY DEFINER
11 AS $$
12 BEGIN
13     -- Registra un alquiler en la tabla de alquileres
14     INSERT INTO rental (
```

```
        rental_date, inventory_id, customer_id, return_date, staff_id,
last_update
    )
    VALUES (
        in_rental_date, in_inventory_id, in_customer_id,
        in_return_date, in_staff_id, in_last_update
    );

    RAISE NOTICE 'Alquiler registrado correctamente';


EXCEPTION
    WHEN unique_violation THEN
        RAISE NOTICE 'El ID de alquiler ya existe.';

    WHEN foreign_key_violation THEN
        RAISE NOTICE 'El inventory_id, customer_id o staff_id no son válidos.';

    WHEN others THEN
        RAISE NOTICE 'Ocurrió un error: %', SQLERRM;

END;
$$;
```

- **Registrar una devolución**

Para el caso de la funcionalidad de registrar una devolución, se debe primero entender qué es la devolución en el contexto de la base de datos. En este caso hace referencia a la acción de registrar la devolución de una película por parte del cliente.

Atributos: Son todos aquellos datos de entrada o salida del procedimiento almacenado. En este caso solo son datos de entrada. A continuación se presentan todos los datos de entrada que utiliza este procedimiento almacenado:

Atributo	Explicación
InRental_id	Identificador de renta realizada
InReturn_date	Fecha de devolución.

```
CREATE OR REPLACE PROCEDURE registrar_devolucion(InRental_id INT, InReturn_date
DATE)
LANGUAGE plpgsql
SECURITY DEFINER
AS $$
DECLARE
```

```
    IdInventory INT;
BEGIN
    -- Actualizar la fecha de devolución en la tabla rental
    UPDATE rental
    SET return_date = InReturn_date
    WHERE rental_id = InRental_id;

    -- Obtener el inventory id asociado con el rental id
    SELECT inventory_id INTO IdInventory
    FROM rental
    WHERE rental_id = InRental_id;

    -- Actualizar la disponibilidad en la tabla inventory
    UPDATE inventory
    SET last_update= NOW()
    WHERE inventory_id = IdInventory;

    -- Confirmar la transacción
    RAISE NOTICE 'Devolución registrada exitosamente para rental id: %',InTernal
id;

EXCEPTION
    WHEN OTHERS THEN
     -- Revertir la transacción en caso de error

         RAISE NOTICE 'Error al registrar la devolución: %', SQLERRM;

END;
$$;
```

Primero se declara una variable de tipo entera para poder guardar el identificador del inventario, a partir de esto después se actualiza la fecha de devolución con la fecha de devolución de entrada, aquellos registros donde el identificador de la renta concuerde con el identificador de entrada. Después se busca el identificador de inventario que esté asociado al identificador de la renta, adicionalmente de actualiza la disponibilidad de la tabla de inventario a partir del identificador de este mismo.

Finalmente se confirma la transacción con una noticia.

1.2 Seguridad y manejo de roles:

- **Creación de los roles**

EMP: solo tiene el derecho de ejecutar los siguientes procedimientos almacenados; no puede leer ni actualizar ningún objeto de la base de datos .

▪ Registrar un alquiler

▪ Registrar una devolución

▪ Buscar una película

Para la creación del rol "**emp**" el cual solo puede ejecutar procedimientos especificados, y estos estén ligados al rol. Para lo anterior se utiliza el siguiente código, el cual lo que realiza es la creación de un rol de nombre "**emp**".

Código de creación del rol de "EMP":

```
-> CREATE ROLE emp;
```

A continuación, se muestran las funciones las cuales fueron mencionadas y explicadas ampliamente en el apartado pasado.

- *Registrar un alquiler*
- *Registrar devolucion:*
- *Buscar una película*

Estos procedimientos creados dentro de la base de datos hay que otorgarles a los procedimientos la opción para que el rol "**emp"** pueda usarlos correctamente.

Para realizar esto escribimos las siguientes líneas de código, estas lo que hacen es que al usuario "**emp**" se le otorga permisos para poder utilizar los procedimientos.

Código para otorgar los permisos:

```
- > GRANT EXECUTE ON PROCEDURE registrar_alquiler(TIMESTAMP WITHOUT TIME ZONE,
INT, SMALLINT, TIMESTAMP
-> WITHOUT TIME ZONE, SMALLINT, TIMESTAMP WITHOUT TIME ZONE) TO emp;
-> GRANT EXECUTE ON PROCEDURE registrar_devolucion(INT, DATE) TO emp;
-> GRANT EXECUTE ON PROCEDURE buscar_pelicula(VARCHAR) TO emp;
```

Como explicación de las líneas del código mostrado anteriormente, se tiene las siguientes explicaciones:

GRANT EXECUTE: Otorga permisos de ejecución.

ON FUNCTION NombreFuncion(): Indica que se otorga permisos de ejecución para la función llamada NombreFuncion().

TO emp: Especifica el rol al cual se le otorgan los permisos.

ADMIN: Tiene el derecho de un empleado más el derecho de ejecutar los siguientes procedimientos almacenados; no puede leer ni actualizar ningún objeto de la base de datos

▪ Insertar un nuevo cliente

Al igual que el rol **"emp"**, el rol "**admin**" solo puede ejecutar procedimientos especificados, y estos estén ligados al rol. Aparte de los procedimientos ligados al rol "**admin**" este podrá ejecutar los procedimientos que estén ligados al rol **"emp"**-

Para la creación del rol “**admin**” el cual solo puede ejecutar procedimientos especificados y estén ligados al rol se utiliza el siguiente código.

```
-> CREATE ROLE admin;

-> GRANT emp TO admin;
```

Lo que realiza el “GRANT emp TO admin;” es asignar que el rol **admin** se cómo una extensión o hereda del rol **emp**. Esto lo que hace es que el rol **admin** tiene ahora todos los privilegios que se le han otorgado al rol **emp**.

Como se menciona el rol “**admin**” tiene una serie de procedimientos que solo él puede utilizar. A continuación, se muestra las funciones las cuales el rol puede utilizar.

Los procedimientos que corresponden al rol “**admin**” es el siguiente:

- Insertar un nuevo cliente

Recordemos que el rol **admin** es una extensión del rol **emp**, es por ello que el rol admin puede hacer uno de los procedimientos ligados al rol **emp**. Que son lo procedimientos de:

▪ Registrar un alquiler
▪ Registrar una devolución
▪ Buscar una película

Ya con el procedimiento creado lo que tenemos que realizar es la otorgación de permisos al rol **admin** para que pueda realizar uso del procedimiento. Para poder realizar esto lo que tenemos que hacer es utilizar la siguiente línea de código.

```
->GRANT EXECUTE ON PROCEDURE insertar_nuevo_cliente(VARCHAR, VARCHAR, VARCHAR, INT, INT, BOOLEAN, DATE, TIMESTAMP WITHOUT TIME ZONE, INT) TO admin;
```

Las líneas anteriores lo que realizan lo siguiente:

GRANT EXECUTE: Otorga permisos de ejecución.

ON FUNCTION NombreFuncion(): Indica que se otorga permisos de ejecución para la función llamada NombreFuncion().

TO emp: Especifica el rol al cual se le otorgan los permisos.

Video: no login, dueño de todas las tablas y de todos los procedimientos creados.

Para realizar esto simplemente se creará un rol de nombre **video** el cual tiene permisos a todas las tablas y procedimientos sin necesidad de permisos de login, ósea el rol **NO** podrá iniciar sesión a la base.

Para ello se escribe la siguiente línea de comando.

```
-> CREATE ROLE video NOLOGIN;
```

Acá se crea un rol llamado **video** y el **NOLOGIN** indica que este rol no tiene permiso para iniciar sesión en la base de datos.

Como se mencionó este tiene acceso sobre las tablas; para poder darle acceso a todas las tablas en la base de datos al rol "**video**" se utiliza el siguiente comando:

-> GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO video;

-> ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO video;

Para poder utilizar los procedimientos desde del rol de **video** se utiliza los siguientes comandos, estos lo que realizan es que convierten al rol **video** como el dueño de los procesos.

-> ALTER PROCEDURE registrar_alquiler(TIMESTAMP WITHOUT TIME ZONE, INT, SMALLINT, TIMESTAMP WITHOUT TIME ZONE, SMALLINT, TIMESTAMP WITHOUT TIME ZONE) OWNER TO video;

-> ALTER PROCEDURE registrar_devolucion(INT, DATE) OWNER TO video;

-> ALTER PROCEDURE buscar_pelicula(VARCHAR) OWNER TO video;

-> ALTER PROCEDURE insertar_nuevo_cliente(VARCHAR, VARCHAR, VARCHAR, INT, INT, BOOLEAN, DATE, TIMESTAMP WITHOUT TIME ZONE, INT) OWNER TO video;

Para poder limitar el uso del procedimiento y que solo los roles que tengan acceso a los procedimientos se revocaron los permisos del rol **PUBLIC**, el rol **PUBLIC** es un rol el cual automáticamente se asocia a los procesos. Para revocar el permiso se utiliza los siguientes códigos:

```
-> REVOKE ALL ON PROCEDURE registrar_alquiler FROM PUBLIC;
-> REVOKE ALL ON PROCEDURE registrar_devolucion FROM PUBLIC;
-> REVOKE ALL ON PROCEDURE buscar_pelicula FROM PUBLIC;
-> REVOKE ALL ON PROCEDURE insertar_nuevo_cliente FROM PUBLIC;
```

El rol de **video** no cuenta con permisos para realizar secuencias en algunas tablas utilizadas en los procesos es por ello por lo que se tienen que dar permisos al rol de **video** para que al hacer uso del proceso todo funcione de forma correcta. Para ello se utiliza los siguientes códigos:

```
-> GRANT USAGE, SELECT ON SEQUENCE public.customer_customer_id_seq TO video;
-> GRANT USAGE, SELECT ON SEQUENCE public.rental_rental_id_seq TO video;
```

El propósito de estas líneas es asegurarse que las funciones se ejecuten bajo las credenciales del rol **video**, lo que es útil si se utilizan los mecanismos de seguridad definidos para limitar el acceso a los datos.

- **Creación de usuarios**

Empleado1: Un usuario con rol **EMP**. Para crear un nuevo empleado de ron "**emp**" se utiliza las siguientes líneas:

```
-> CREATE USER empleado1 WITH PASSWORD ' Jeffer123 ';
-> GRANT emp TO empleado1;
```

Estas líneas crean un nuevo usuario **empleado1** con una contraseña y le asignan el rol **emp**, lo que le otorga ciertos permisos específicos sobre la base de datos.

Este usuario tendrá acceso a los procedimientos asociados con el rol **emp**. Aparte también se podrá realizar login utilizando el usuario y la contraseña asignada.

Administrador1: Un usuario con rol **ADMIN.** Para poder crear un empleado el cual tenga privilegio de administrador se utiliza el siguiente código.

```
-> CREATE USER administrador1 WITH PASSWORD 'Pass123';

-> GRANT admin TO administrador1;
```

Estas líneas crean un nuevo usuario **administrador1** con una contraseña y le asignan el rol **admin**. Esto le da a **administrador1** todos los privilegios que tiene el rol **admin.** Al igual que empleado1 el **administrador1** tiene la posibilidad de realizar un login utilizando el usuario y la contraseña asignada.

- **Seguridad en procedimientos almacenados:**

Los procedimientos almacenados deben correr usando las credenciales de su dueño, **video**.

Para hacer que los procedimientos almacenados se ejecuten utilizando las credenciales de su propietario, en este caso, **video.**

Lo que se hace es tener un rol llamado **video** y hay que agregarle a los procedimientos almacenados la cláusula **SECURITY DEFINER**. Esto asegura que los procedimientos se ejecuten con los privilegios del rol del creado, en este caso es **video**.

También hay que asegurar que el propietario del proceso sea asignado.

Crear el Rol video

- > CREATE ROLE video NOLOGIN;

Definir los Procedimientos con SECURITY DEFINER

```
CREATE OR REPLACE PROCEDURE inserter_nuevo_cliente(
    in_first_name VARCHAR,
    in_last_name VARCHAR,
    in_email VARCHAR,
    in_address_id INT,
    in_store_id INT,
    in_active_bool BOOLEAN,
    in_create_date DATE,
    in_last_update TIMESTAMP WITHOUT TIME ZONE,
    in_active INT
)
LANGUAGE plpgsql
SECURITY DEFINER <----------------------
AS $$
BEGIN
    -- Insertar cliente
    INSERT INTO public.customer(
        store_id, first_name, last_name, email, address_id, activebool, create_date, last_update, active
    )
    VALUES (
        in_store_id, in_first_name, in_last_name, in_email,
        in_address_id, in_active_bool, in_create_date, in_last_update, in_active
    );


    RAISE NOTICE 'El cliente se creo correctamente';
EXCEPTION
    WHEN unique_violation THEN
        RAISE NOTICE 'El cliente ya existe con el email %.', in_email;
    WHEN foreign_key_violation THEN
        RAISE NOTICE 'El store_id o address_id no son válidos.';
    WHEN others THEN
        RAISE NOTICE 'Ocurrió un error: %', SQLERRM;
END;
```

;

SECURITY DEFINER:

El **SECURITY DEFINER** permite que los procedimientos que han sido creados como procedimiento con la cláusula SECURITY DEFINER permite que se ejecuten con los privilegios del creador, en este caso el usuario **video.**

Asignar el Propietario del Procedimiento:

-> ALTER PROCEDURE insertar_nuevo_cliente(VARCHAR, VARCHAR, VARCHAR, INT, INT, BOOLEAN, DATE, TIMESTAMP WITHOUT TIME ZONE, INT) OWNER TO video;

Permisos a tablas:

Para poder darle acceso a todas las tablas en la base de datos al rol "**video**" se utiliza el siguiente comando:

-> GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO video;

-> ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO video;

Nota: Este es el único rol el cual tiene permisos a todas las tablas.