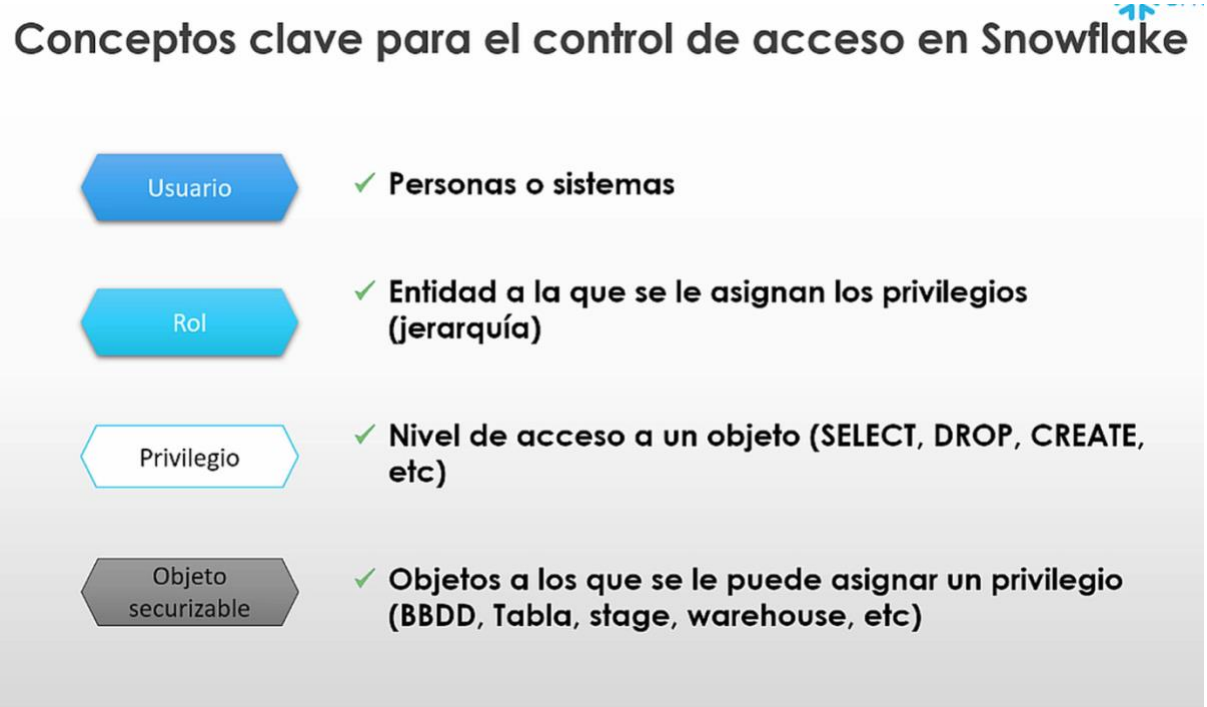
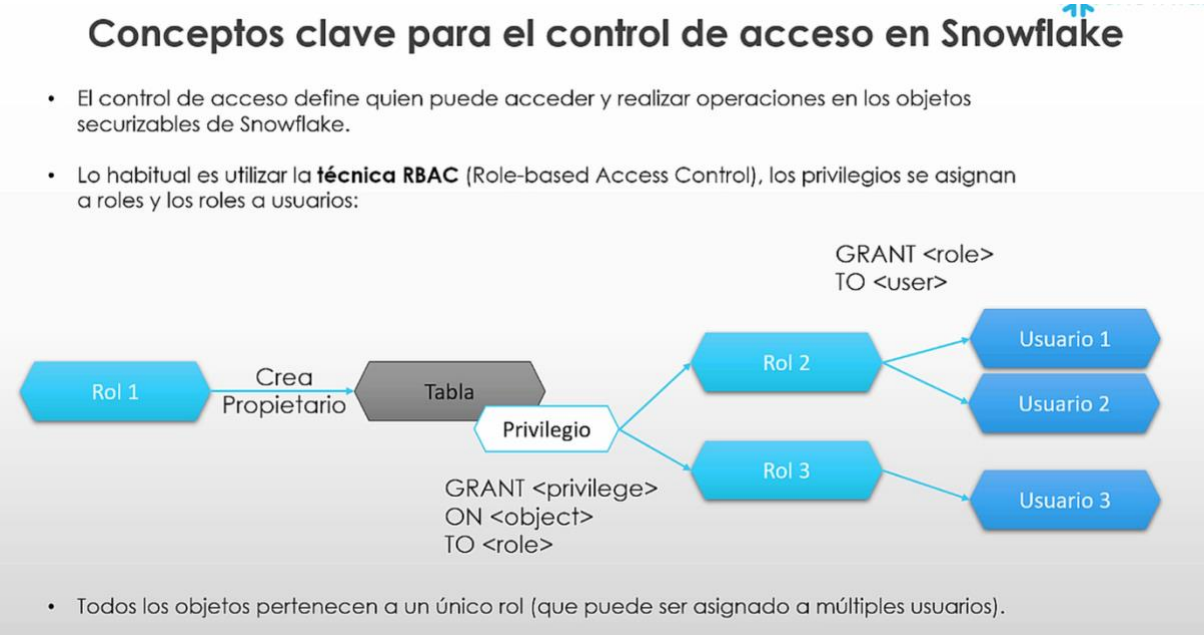
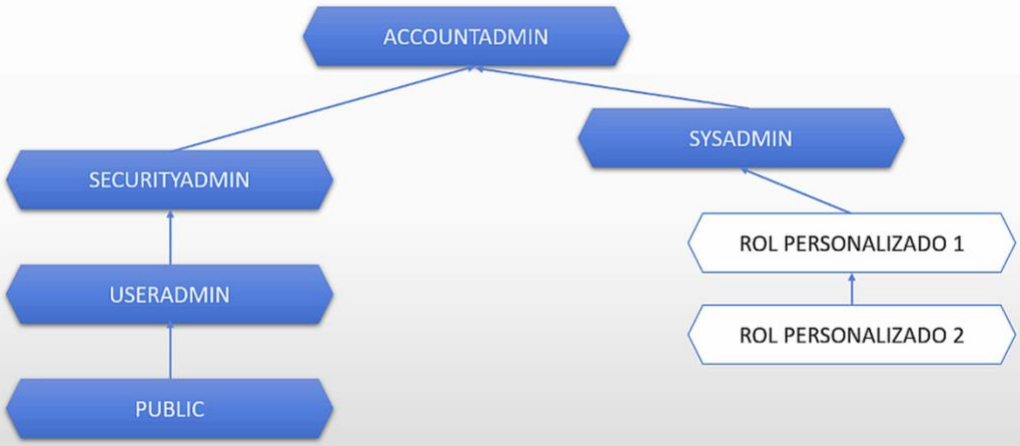
Roles in Snowflake:





Conceptos clave para el control de acceso en Snowflake

- **ROLES SNOWFLAKE**



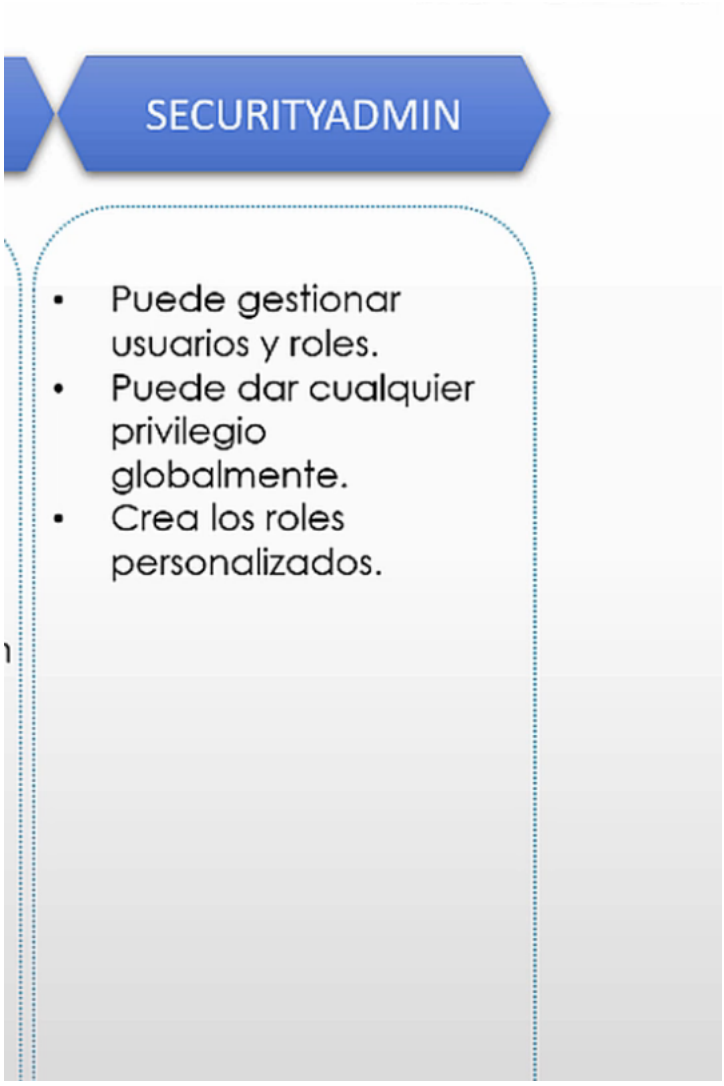
- **Cada nivel contiene además los privilegios de los roles de menor jerarquía.**

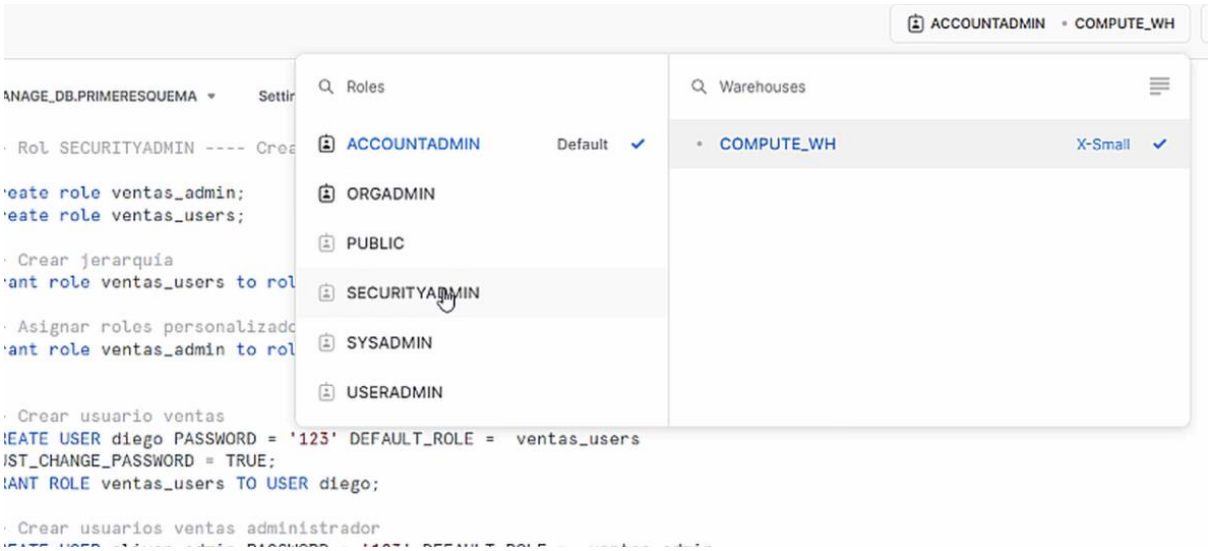
ACCOUNTADMIN

- Rol más alto en el sistema.
- El primer usuario tiene este rol.
- Solo debe darse a un número limitado de usuarios (al menos deben ser 2 usuarios).

MANAGE_DB.PRIMERESQUEMA ▾ Settings ▾

```
--- Creación usuario ACCOUNTADMIN 2 ---
CREATE USER maria PASSWORD = '123'
DEFAULT_ROLE = ACCOUNTADMIN
MUST_CHANGE_PASSWORD = TRUE;

GRANT ROLE ACCOUNTADMIN TO USER maria;


--- Creación usuario SECURITYADMIN ---
CREATE USER fran PASSWORD = '123'
DEFAULT_ROLE = SECURITYADMIN
MUST_CHANGE_PASSWORD = TRUE;

GRANT ROLE SECURITYADMIN TO USER fran;


--- Creación usuario SYSADMIN ---
CREATE USER alberto PASSWORD = '123'
DEFAULT_ROLE = SYSADMIN
MUST_CHANGE_PASSWORD = TRUE;

GRANT ROLE SYSADMIN TO USER alberto;
```

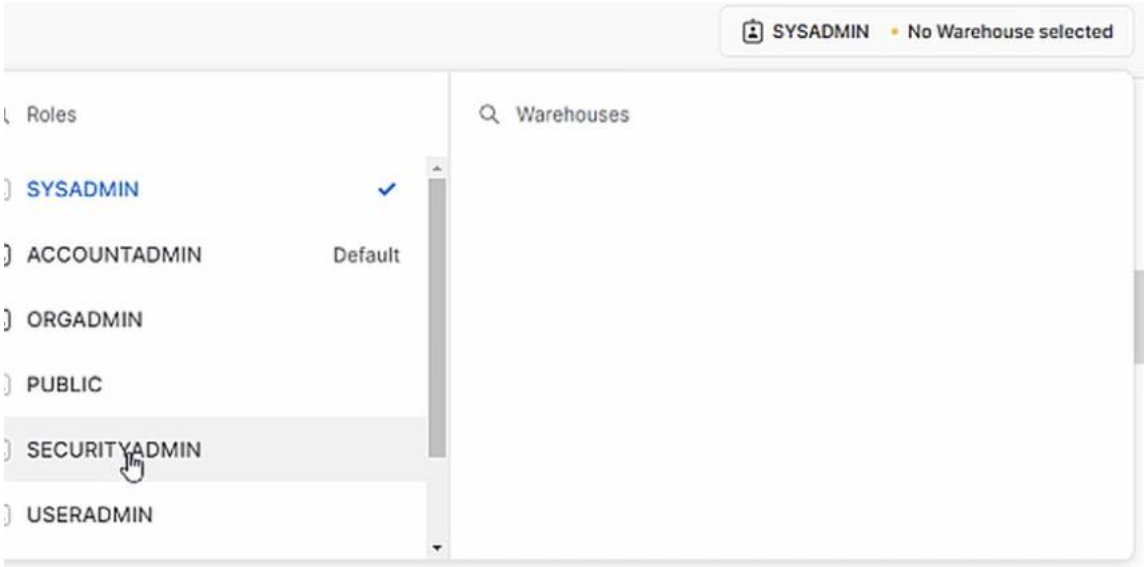

SECURITYADMIN
Puede gestionar usuarios y roles.
Puede dar cualquier privilegio globalmente.
Crea los roles personalizados.


ACCOUNTADMIN • COMPUTE_WH
ANAGE_DB.PRIMERESQUEMA
Rol SECURITYADMIN ---- Crea
eate role ventas_admin;
eate role ventas_users;
Crear jerarquía
ant role ventas_users to rol
Asignar roles personalizado
ant role ventas_admin to rol
Crear usuario ventas
EATE USER diego PASSWORD = '123' DEFAULT_ROLE = ventas_users
ST_CHANGE_PASSWORD = TRUE;
ANT ROLE ventas_users TO USER diego;
Crear usuarios ventas administrador
Roles
ACCOUNTADMIN Default
ORGADMIN
PUBLIC
SECURITYADMIN
SYSADMIN
USERADMIN
Warehouses
COMPUTE_WH X-Small

```sql
-- Rol SECURITYADMIN ---- Creación y gestión de roles y usuarios --

create role ventas_admin;
create role ventas_users;

-- Crear jerarquía
grant role ventas_users to role ventas_admin;

-- Asignar roles personalizados a SYSADMIN como buena práctica
grant role ventas_admin to role SYSADMIN;


-- Crear usuario ventas
CREATE USER diego PASSWORD = '123' DEFAULT_ROLE =  ventas_users
MUST_CHANGE_PASSWORD = TRUE;
GRANT ROLE ventas_users TO USER diego;

-- Crear usuarios ventas administrador
CREATE USER oliver_admin PASSWORD = '123' DEFAULT_ROLE =  ventas_admin
MUST_CHANGE_PASSWORD = TRUE;
GRANT ROLE ventas_admin TO USER  oliver_admin;

```

SYSADMIN

- Creación de bases de datos, tablas, data warehouses y otros objetos.
- Los roles personalizados deben enlazarse por debajo del SYSADMIN, por tanto este rol es el que da privilegios a los roles personalizados.



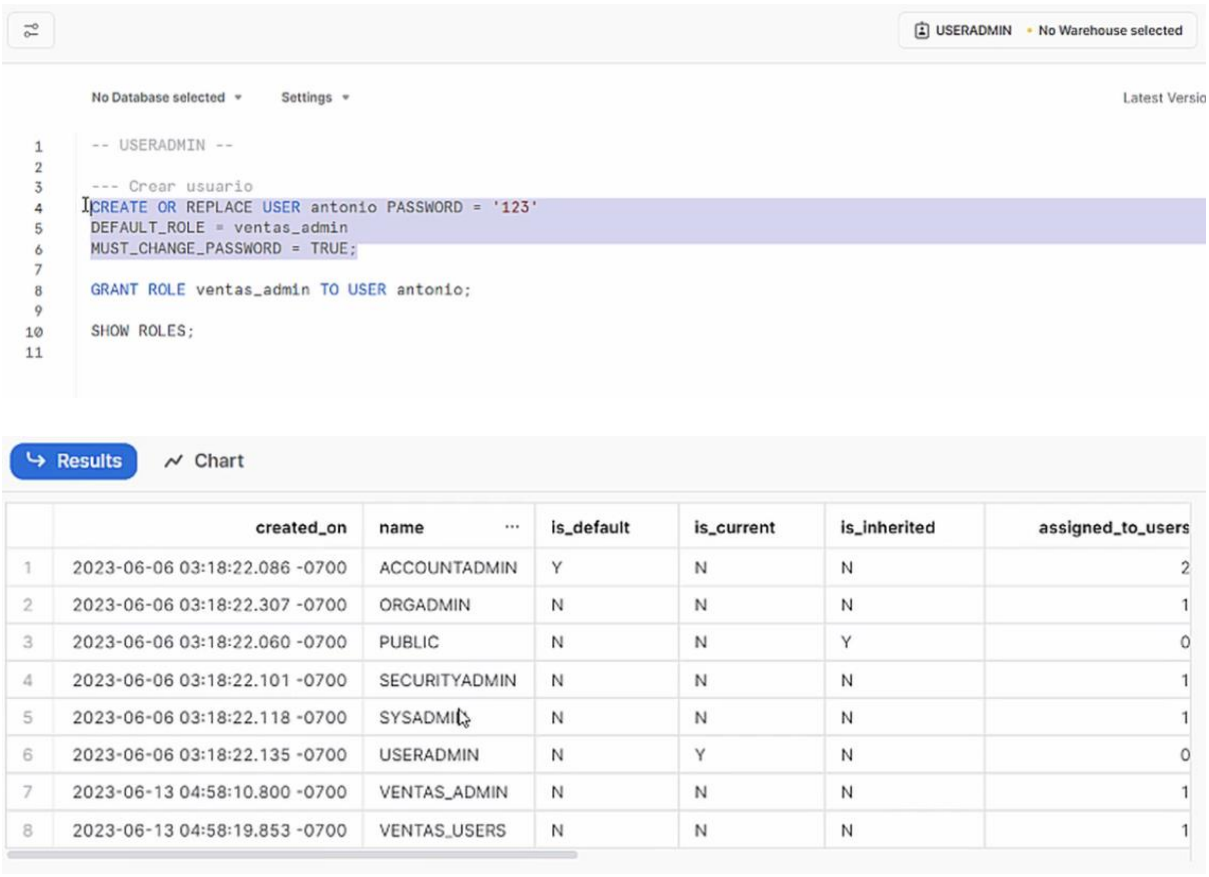

```
to role public
```

```sql
-- SYSADMIN --

-- Crear Data Warehouse X-SMALL
create warehouse public_wh with
warehouse_size='X-SMALL'
auto_suspend=300
auto_resume= true

-- Dar permisos al rol public
grant usage on warehouse public_wh
to role public

-- Crear BBDD accesible para todos
create database common_db;
grant usage on database common_db to role public

-- Crear BBDD Ventas para rol administrador ventas (sales_admin) y darles la propiedad
create database sales_database;
grant ownership on database sales_database to role sales_admin;
grant ownership on schema sales_database.public to role sales_admin

SHOW DATABASES;
```

	created_on	name	is_default	is_current	origin
1	2023-06-14 03:27:49.512 -0700	COMMON_DB	N	N	
2	2023-06-14 03:28:10.804 -0700	SALES_DATABASE	N	Y	
3	2023-06-06 03:18:22.703 -0700	SNOWFLAKE	N	N	SNOWFLAKE.ACCOUNT_USAGE
4	2023-06-06 03:18:27.625 -0700	SNOWFLAKE_SAMPLE_DATA	N	N	SFSALESSHARED.SFC_SAMPLES

USERADMIN

- Dedicado a la gestión de roles y usuarios únicamente.
- Puede crear roles y usuarios.
- No está enfocado a dar privilegios (solo los que posee).



	created_on	name	is_default	is_current	is_inherited	assigned_to_users
1	2023-06-06 03:18:22.086 -0700	ACCOUNTADMIN	Y	N	N	2
2	2023-06-06 03:18:22.307 -0700	ORGADMIN	N	N	N	1
3	2023-06-06 03:18:22.060 -0700	PUBLIC	N	N	Y	0
4	2023-06-06 03:18:22.101 -0700	SECURITYADMIN	N	N	N	1
5	2023-06-06 03:18:22.118 -0700	SYSADMIN	N	N	N	1
6	2023-06-06 03:18:22.135 -0700	USERADMIN	N	Y	N	0
7	2023-06-13 04:58:10.800 -0700	VENTAS_ADMIN	N	N	N	1
8	2023-06-13 04:58:19.853 -0700	VENTAS_USERS	N	N	N	1


PUBLIC
Se asigna automáticamente a todos los usuarios.
CUSTOM
Personalización de roles a las necesidades y con la jerarquía oportuna.


Roles personalizados
ACCOUNTADMIN
Rol más alto en el sistema.
El primer usuario tiene este rol.
Solo debe darse a un número limitado de usuarios (al menos deben ser 2 usuarios).
Evitar crear objetos con este rol a menos que sea necesario.
Puede gestionar y ver todos los objetos.
Verificar facturación y uso de la cuenta.
SECURITYADMIN
Puede gestionar usuarios y roles.
Puede dar cualquier privilegio globalmente.
Crea los roles personalizados.
SYSADMIN
Creación de bases de datos, tablas, data warehouses y otros objetos.
Los roles personalizados deben enlazarse por debajo del SYSADMIN, por tanto este rol es el que da privilegios a los roles personalizados.
CUSTOM
Personalización de roles a las necesidades y con la jerarquía oportuna.
Creados por SECURITYADMIN y privilegios dados por SYSADMIN.
USERADMIN
Dedicado a la gestión de roles y usuarios únicamente.
Puede crear roles y usuarios.
No está enfocado a dar privilegios (solo los que posee).
PUBLIC
Se asigna automáticamente a todos los usuarios.
Puede crear sus propios objetos (y estarán disponibles para todos los demás roles y usuarios).

SALES_DATABASE.PUBLIC Settings

```
USE ROLE ventas_admin;
USE SALES_DATABASE;

-- Crear tabla
create or replace table customers(
  id number,
  full_name varchar,
  email varchar,
  phone varchar,
  spent number,
  create_date DATE DEFAULT CURRENT_DATE);

-- Insertar valores
insert into customers (id, full_name, email,phone,spent)
values
  (1,'Lewiss MacDwyer','lmacdwyer0@un.org','262-665-9168',140),
  (2,'Ty Pettingall','tpettingall1@mayoclinic.com','734-987-7120',254),
  (3,'Marlee Spadazzi','mspadazzi2@txnews.com','867-946-3659',120),
  (4,'Heywood Tearney','htearney3@patch.com','563-853-8192',1230),
  (5,'Odilia Seti','oseti4@globo.com','730-451-8637',143),
  (6,'Meggie Washtell','mwashtell5@rediff.com','568-896-6138',600);
```

	created_on	name	database_name	schema_name	kind	comment	clus
1	2023-06-14 07:09:22.588 -0700	CUSTOMERS	SALES_DATABASE	PUBLIC	TABLE		

```
SHOW TABLES;

-- Consultar la tabla
SELECT* FROM CUSTOMERS;

-- Consultar tabla con rol ventas_users
USE ROLE ventas_users;
SELECT* FROM CUSTOMERS;

USE ROLE PUBLIC;
SELECT* FROM CUSTOMERS;
```

```sql
-- Permitir el uso de la BBDD a ventas_users y privilegio SELECT
USE ROLE ventas_admin;

GRANT USAGE ON DATABASE SALES_DATABASE TO ROLE ventas_users;
GRANT USAGE ON SCHEMA SALES_DATABASE.PUBLIC TO ROLE ventas_users;
GRANT SELECT ON TABLE SALES_DATABASE.PUBLIC.CUSTOMERS TO ROLE ventas_users


-- Validación privilegios
USE ROLE ventas_users;
SELECT* FROM CUSTOMERS;
DROP TABLE CUSTOMERS;
DELETE FROM CUSTOMERS;
SHOW TABLES;

-- Permitir privilegio "DELETE" a ventas_users
USE ROLE ventas_admin;
GRANT DELETE ON TABLE SALES_DATABASE.PUBLIC.CUSTOMERS TO ROLE ventas_users

-- Validación privilegios
USE ROLE ventas_admin;
DELETE FROM CUSTOMERS;
```

	status
1	Table CUSTOMERS successfully created.

	number of rows inserted
1	6

	created_on	name	database_name	schema_name	kind	comment	clus
1	2023-06-14 07:09:22.588 -0700	CUSTOMERS	SALES_DATABASE	PUBLIC	TABLE		

	ID	FULL_NAME	EMAIL	PHONE	SPENT	CREATE_DATE
1	1	Lewiss MacDwyer	lmacdwyer0@un.org	262-665-9168	140	2023-06-14
2	2	Ty Pettingall	tpettingall1@mayoclinic.com	734-987-7120	254	2023-06-14
3	3	Marlee Spadazzi	mspadazzi2@txnews.com	867-946-3659	120	2023-06-14
4	4	Heywood Tearney	htearney3@patch.com	563-853-8192	1,230	2023-06-14
5	5	Odilia Seti	oseti4@globo.com	730-451-8637	143	2023-06-14
6	6	Meggie Washtell	mwashtell5@rediff.com	568-896-6138	600	2023-06-14

	status
1	Statement executed successfully.

	ID	FULL_NAME ···	EMAIL	PHONE	SPENT	CREATE_DATE
1	1	Lewiss MacDwyer	lmacdwyer0@un.org	262-665-9168	140	2023-06-14
2	2	Ty Pettingall	tpettingall1@mayoclinic.com	734-987-7120	254	2023-06-14
3	3	Marlee Spadazzi	mspadazzi2@txnews.com	867-946-3659	120	2023-06-14
4	4	Heywood Tearney	htearney3@patch.com	563-853-8192	1,230	2023-06-14
5	5	Odilia Seti	oseti4@globo.com	730-451-8637	143	2023-06-14
6	6	Meggie Washtell	mwashtell5@rediff.com	568-896-6138	600	2023-06-14

	···	number of rows deleted
1		6