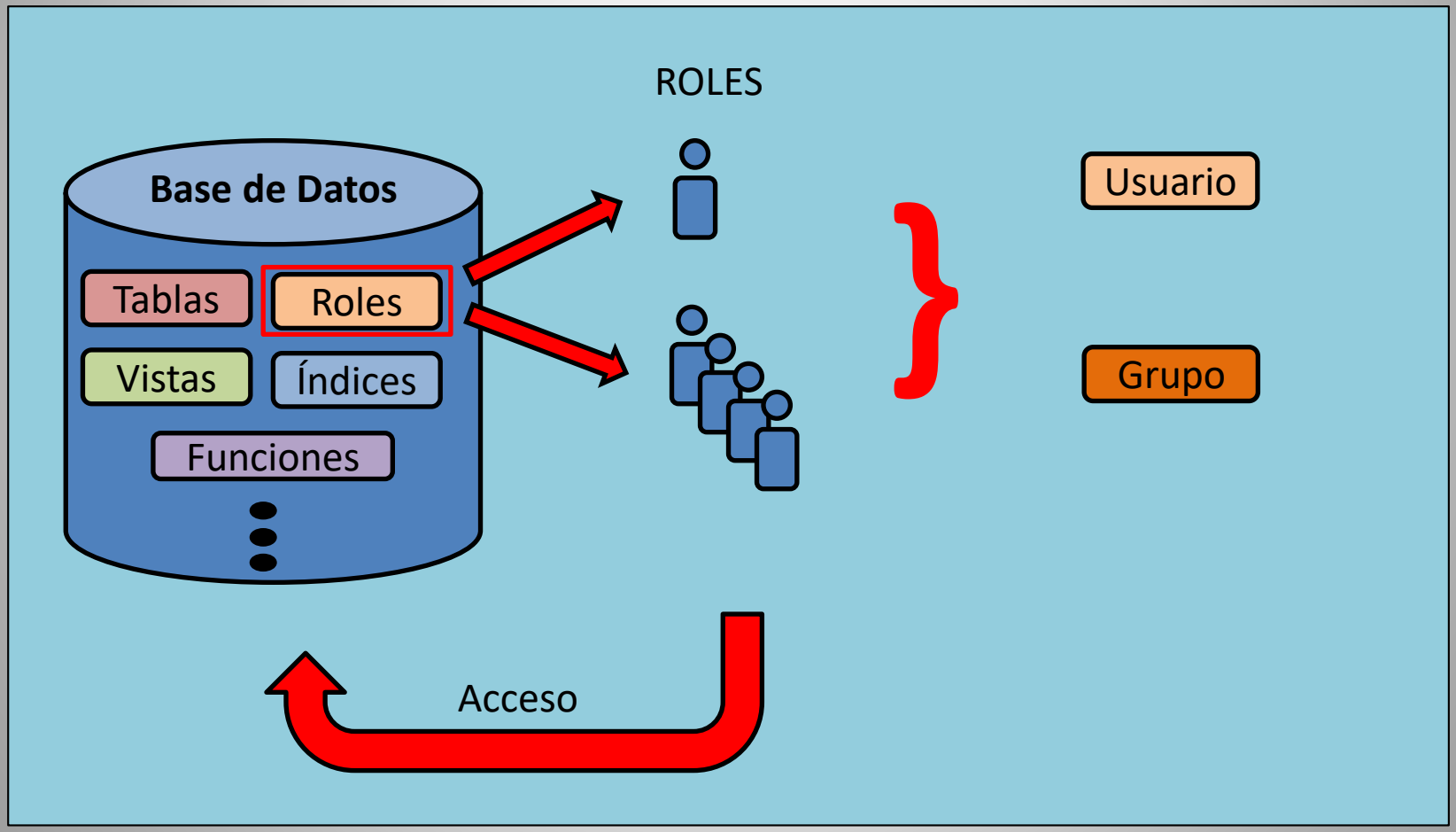
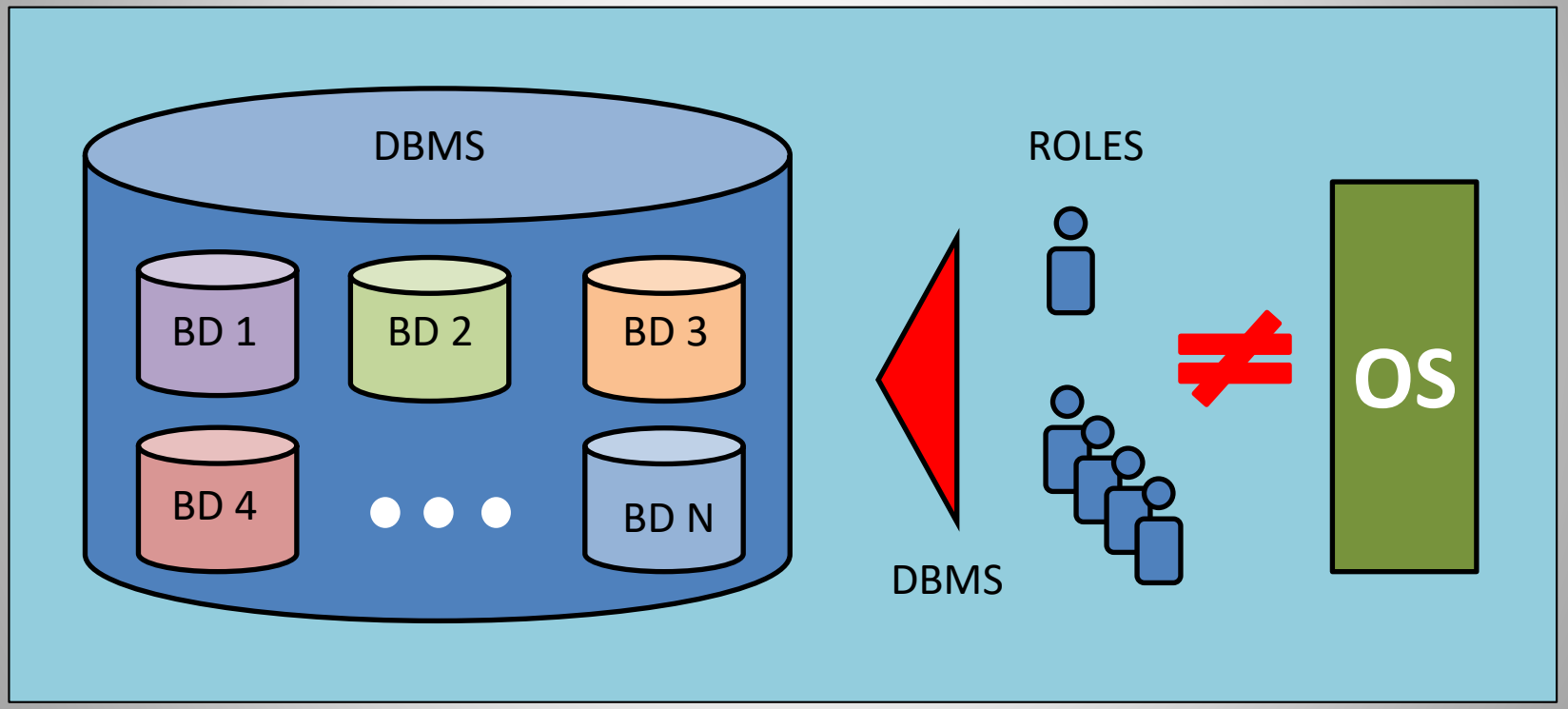
# BASES DE DATOS
# SQL

## Usuarios y Roles
## Privilegios

# Usuarios y Roles



# Usuarios y Roles



# Usuarios y Roles

```
CREATE ROLE nombre;
DROP ROLE nombre;
```

```
CREATE USER nombre;
DROP USER nombre;
```

En el catálogo de la base de datos se puede consultar los roles existentes

```
SELECT rolname FROM pg_roles;
```

# Usuarios y Roles

```
CREATE ROLE name [ [ WITH ] option [ ... ] ]
    where option can be:
      SUPERUSER | NOSUPERUSER
    | CREATEDB | NOCREATEDB
    | CREATEROLE | NOCREATEROLE
    | INHERIT | NOINHERIT
    | LOGIN | NOLOGIN
    | REPLICATION | NOREPLICATION
    | BYPASSRLS | NOBYPASSRLS
    | CONNECTION LIMIT connlimit
    | [ ENCRYPTED ] PASSWORD 'password' | PASSWORD NULL
    | VALID UNTIL 'timestamp'
    | IN ROLE role_name [, ...]
    | IN GROUP role_name [, ...]
    | ROLE role_name [, ...]
    | ADMIN role_name [, ...]
    | USER role_name [, ...]
    | SYSID uid
```

# Usuarios y Roles

## Atributos de Role

Privilegio ***login***

Permite que el role se conecte a la base de datos

CREATE ROLE ***nombre*** LOGIN;
CREATE USER ***nombre***;

*Create user* por defecto incluye *login*, mientras que *create role* no

# Usuarios y Roles

## Atributos de Role

Privilegio ***superuser***

Permite que el role se pasen todas las verificaciones de permisos, con excepción de login.

CREATE ROLE ***nombre*** SUPERUSER;

Para que un role pueda crear otro role que sea superuser, debe ser un role con el privilegio de superuser.

# Usuarios y Roles

## Atributos de Role

Privilegio ***createdb***

Permite que el role pueda crear una base de datos.
Los roles que son superuser pueden pasarse todas las verificaciones.

```
CREATE ROLE nombre CREATEDB;
```

Privilegio ***createrole***

Permite que el role pueda crear otro roles.
Los roles que son superuser pueden pasarse todas las verificaciones.
Pueden alterar o borrar otros roles, menos de superusuarios, a menos que también sea un superusuario

```
CREATE ROLE nombre CREATEROLE;
```

# Usuarios y Roles

## Atributos de Role

Privilegio ***replication***

Permite que el role pueda inicializar replicación streaming.
Los roles que son superuser pueden pasarse todas las verificaciones.
Un rol usado para replicación streaming debe tener permiso login.

```
CREATE ROLE nombre REPLICATION LOGIN;
```

Privilegio ***password***

Significa que el método de autenticación del cliente requiere del uso de una contraseña cuando se conecte a la base de datos.
La contraseña de la base de datos es independiente de la del OS.

```
CREATE ROLE nombre PASSWORD ‘contraseña’;
```

# Usuarios y Roles

## Atributos de Role

Privilegio ***inherit***

Determina cuando un role hereda los privilegios de un role del cual es miembro. *Noinherit* sólo permite usar la instrucción *SET ROLE.*
Si no se especifica, por defecto se asume *inherit.*

CREATE ROLE ***nombre*** INHERIT;

Privilegio ***connection limit***

Especifica cuántas conexiones concurrentes puede hacer el rol, por defecto el valor es -1 que significa que no hay límite.
La transacciones y las conexiones en segundo plano no suman.

CREATE ROLE ***nombre*** CONNECTION LIMIT ***numero;***

# Usuarios y Roles

## Atributos de Role

Privilegio ***valid until***

Determina la fecha y hora en la cual la contraseña del role deja de ser válida.
Si se omite esta opción, la contraseña no tendrá caducidad.

CREATE ROLE ***nombre*** VALIS UNTIL ***timestamp***;

Privilegio ***in role | in group***

Asigna una nueva membresía del role en los roles listados y que ya existen con anterioridad.
No hay opción de agregar el role como administrados (se usa *grant*)

CREATE ROLE ***nombre*** IN ROLE ***role;***
CREATE ROLE ***nombre*** IN GROUP ***role;***

# Usuarios y Roles

## Atributos de Role

Privilegio ***role | user***

Lista uno o más roles existentes que serán adicionados como miembros del nuevo role.
Crea un nuevo role como grupo.

CREATE ROLE ***nombre*** ROLE ***roles***;

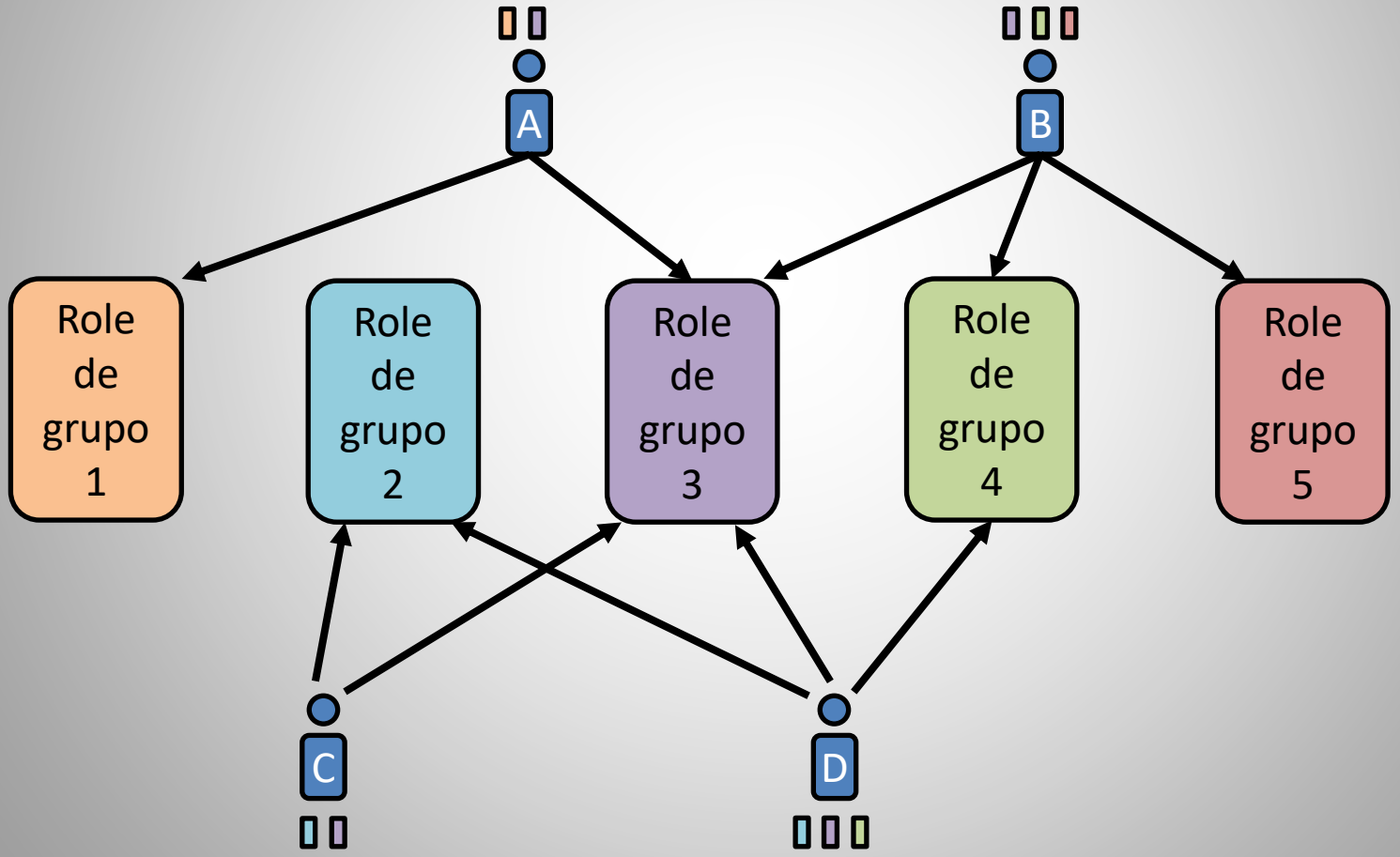
Privilegio ***admin***

Es como la cláusula *role*, pero los roles invocados se agregan al nuevo role con la opción *admin,* dándoles derecho de otorgar membresías en éste role a otros.

CREATE ROLE ***nombre*** ADMIN ***role;***

# Usuarios y Roles

## Membresías de Role



# Usuarios y Roles

## Membresías de Role

Se crea el role de grupo primero, usualmente sin el privilegio login.

CREATE ROLE ***nombre_grupo***;

Se crea el role de usuario con el privilegio login.

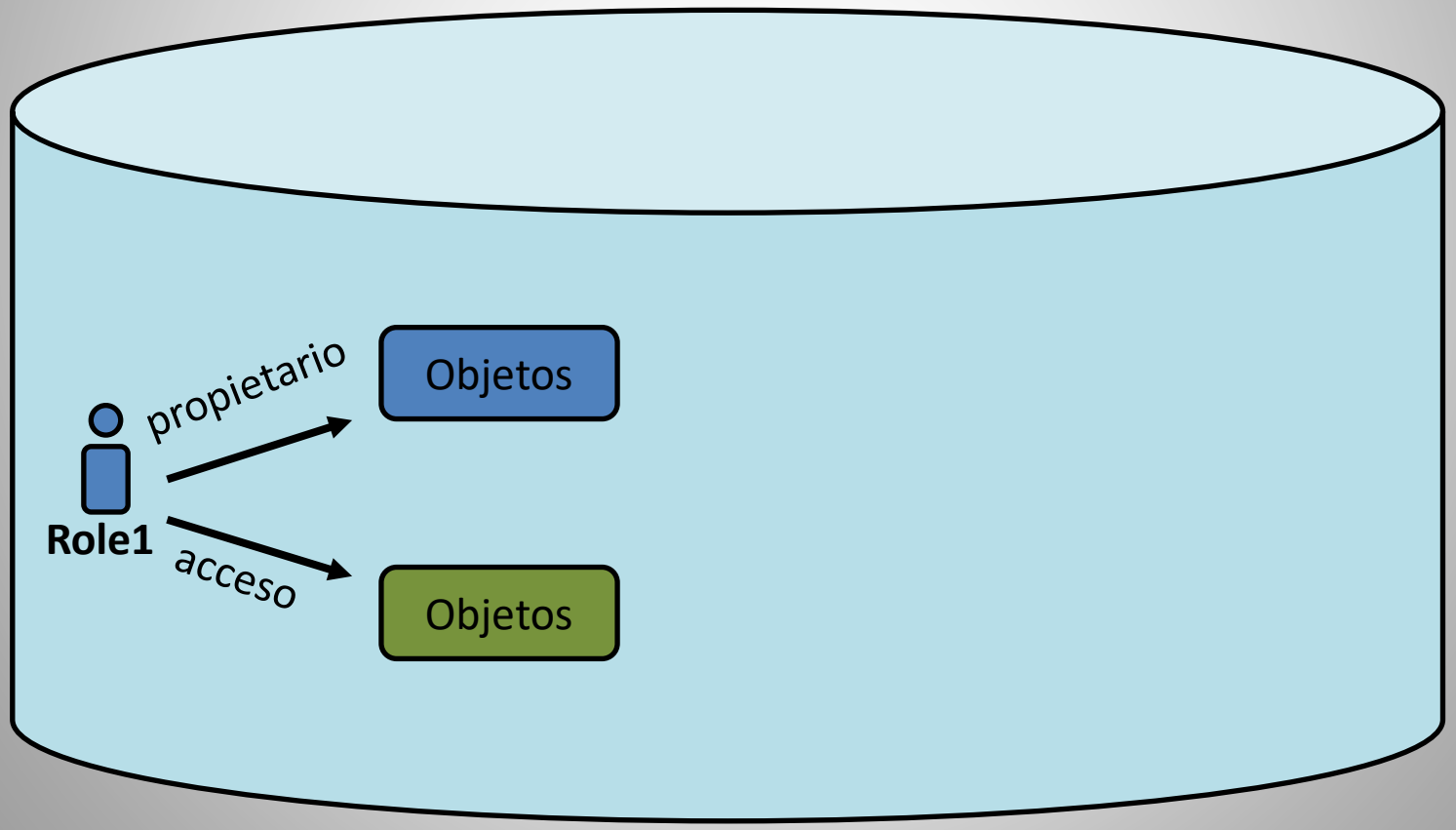
CREATE ROLE ***nombre_usuario*** PASSWORD ***'contraseña'***;

Se concede o revoca la membresía del usuario al grupo

GRANT ***nombre_grupo*** TO ***nombre_usuario;***
REVOKE ***nombre_grupo*** FROM ***nombre_usuario;***

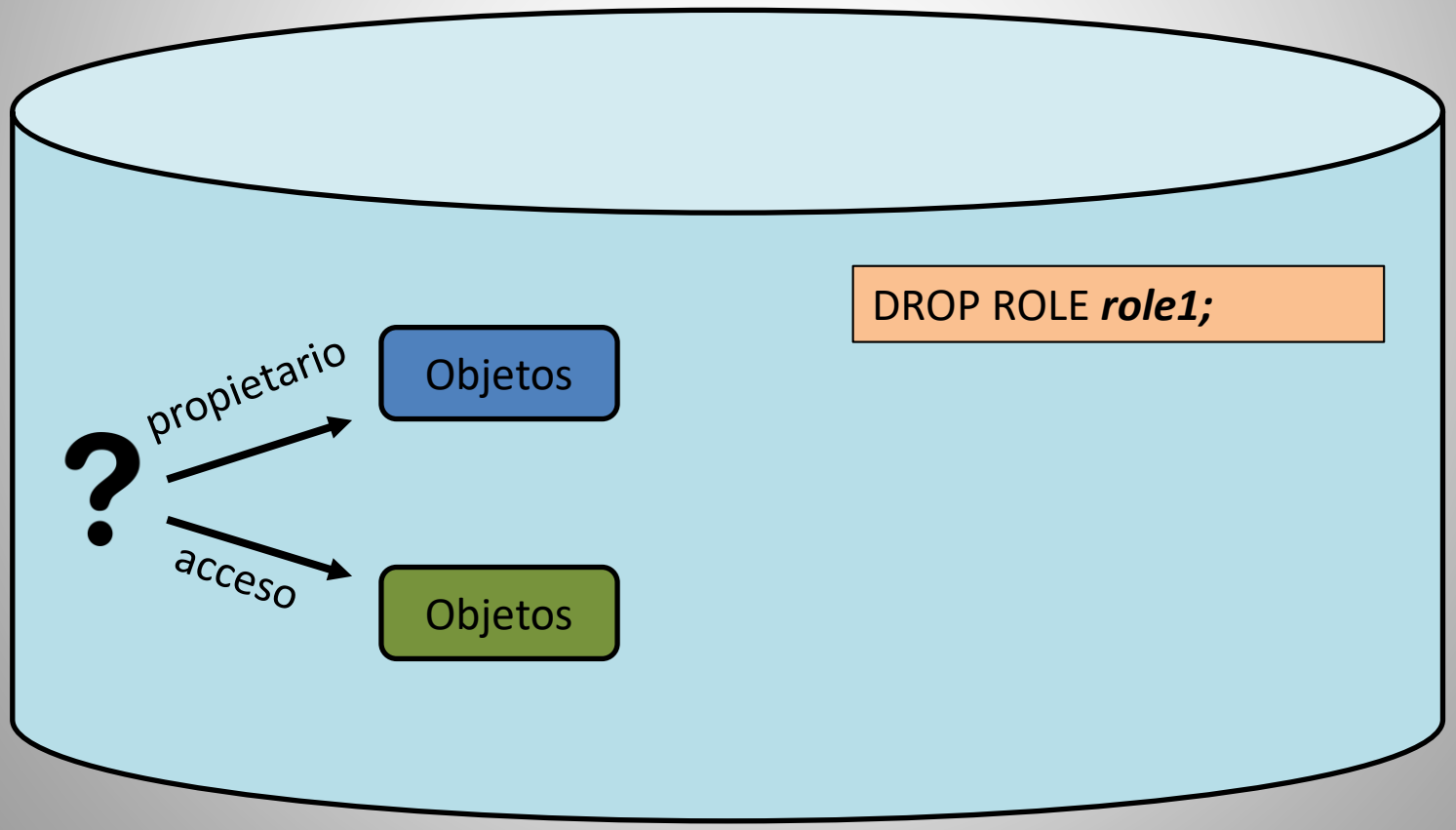
# Usuarios y Roles

## Borrado de Role



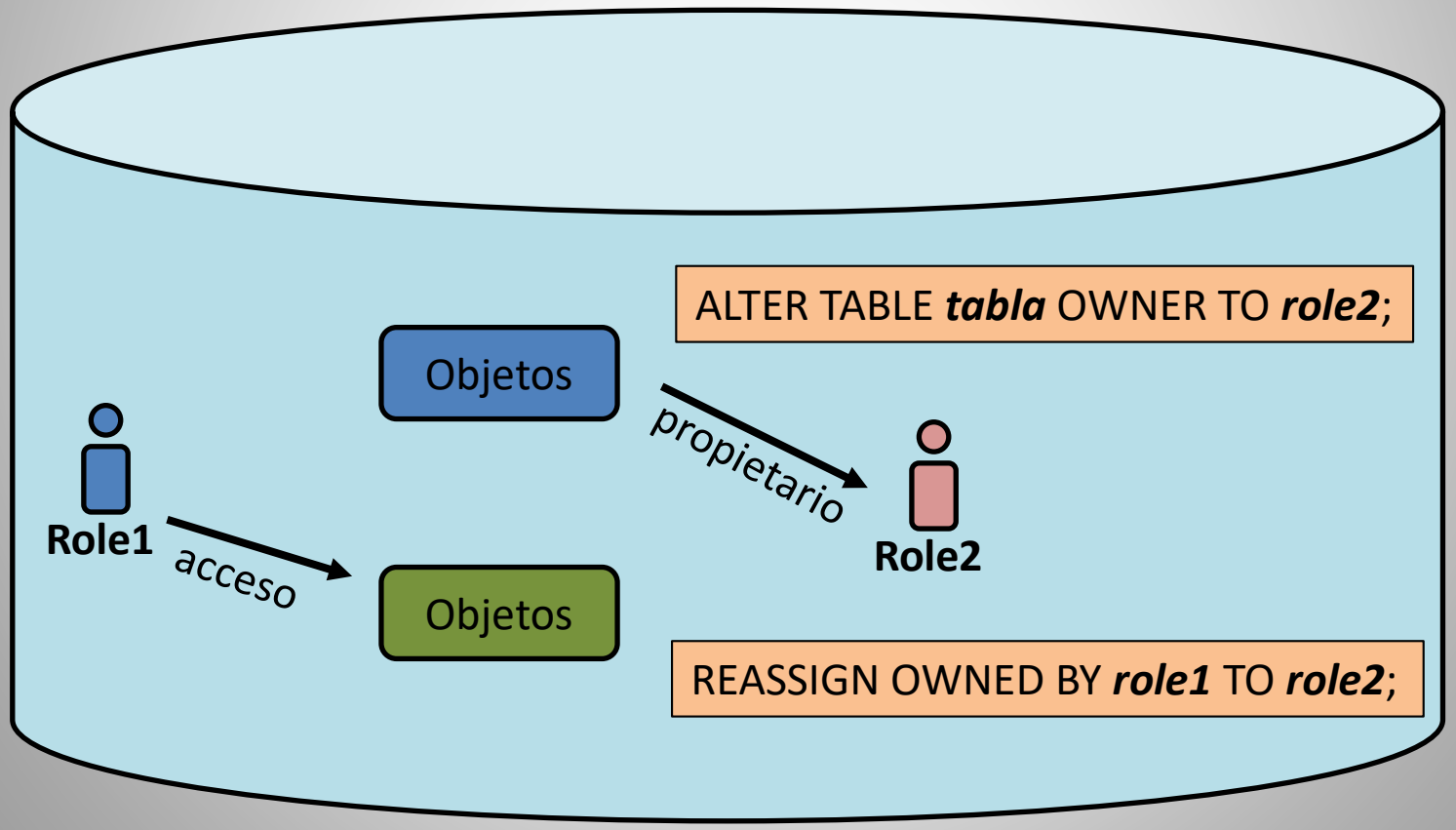
# Usuarios y Roles

## Borrado de Role



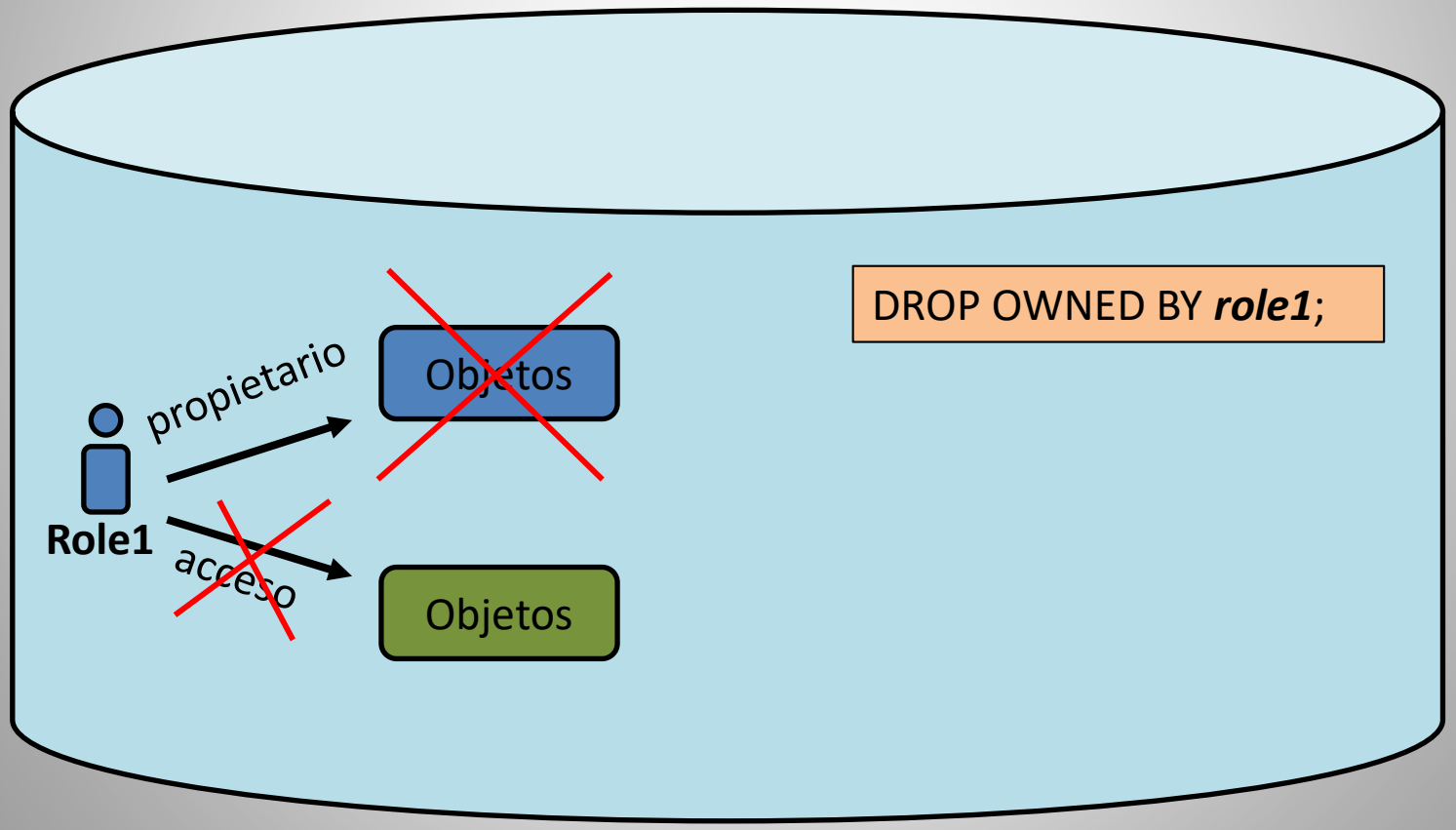
# Usuarios y Roles

## Borrado de Role



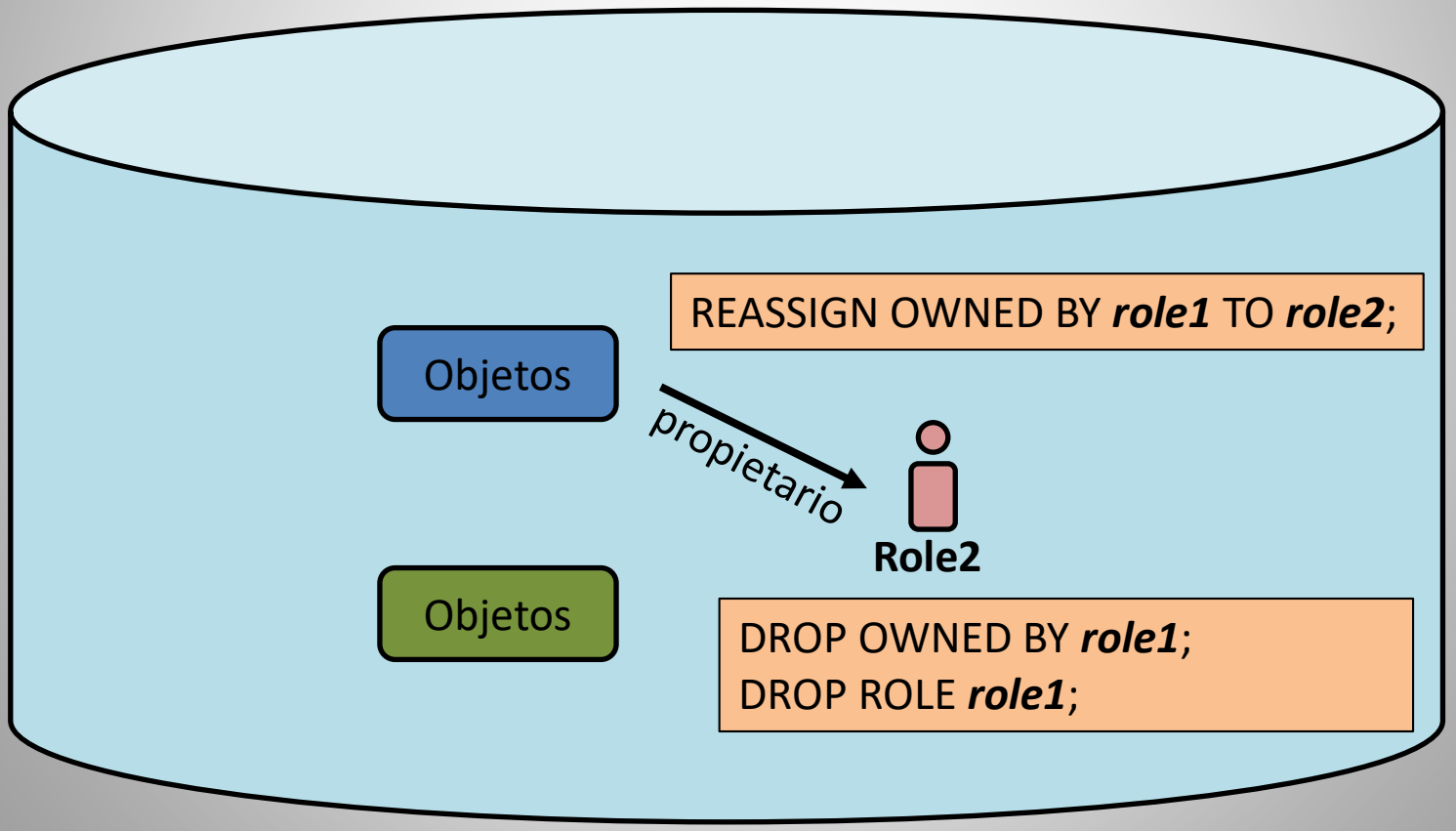
# Usuarios y Roles

## Borrado de Role

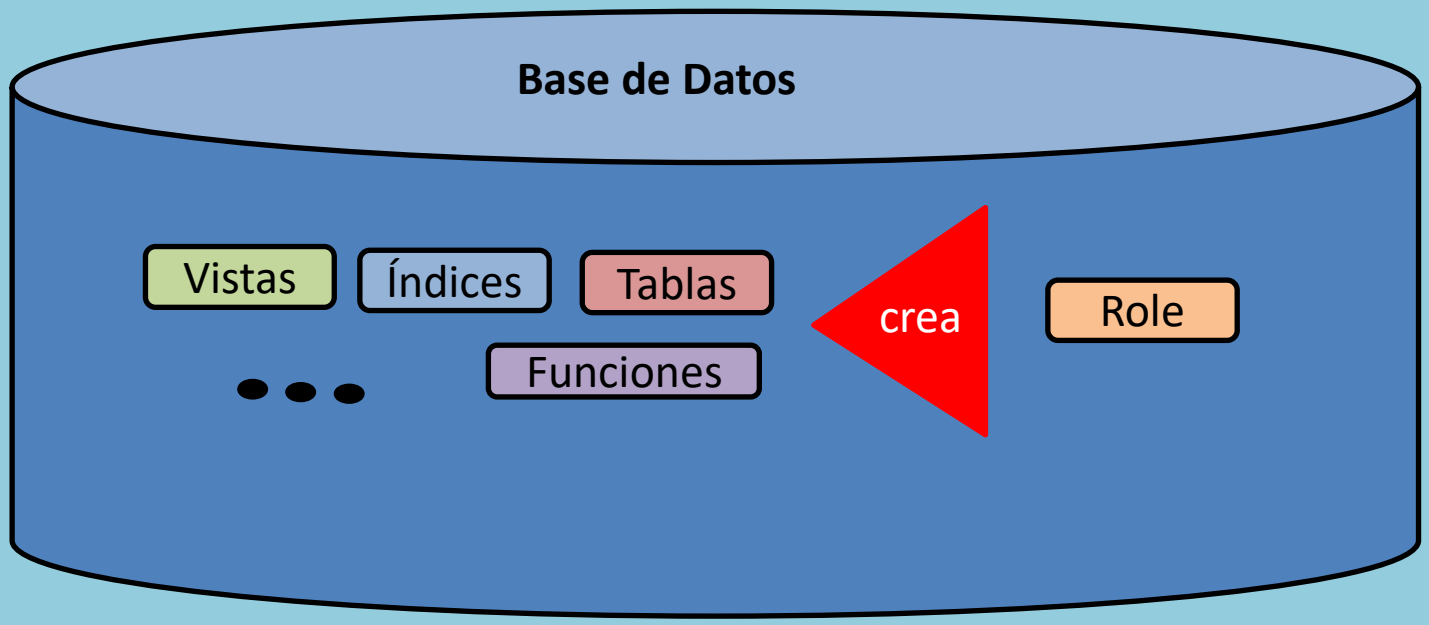


# Usuarios y Roles

## Borrado de Role

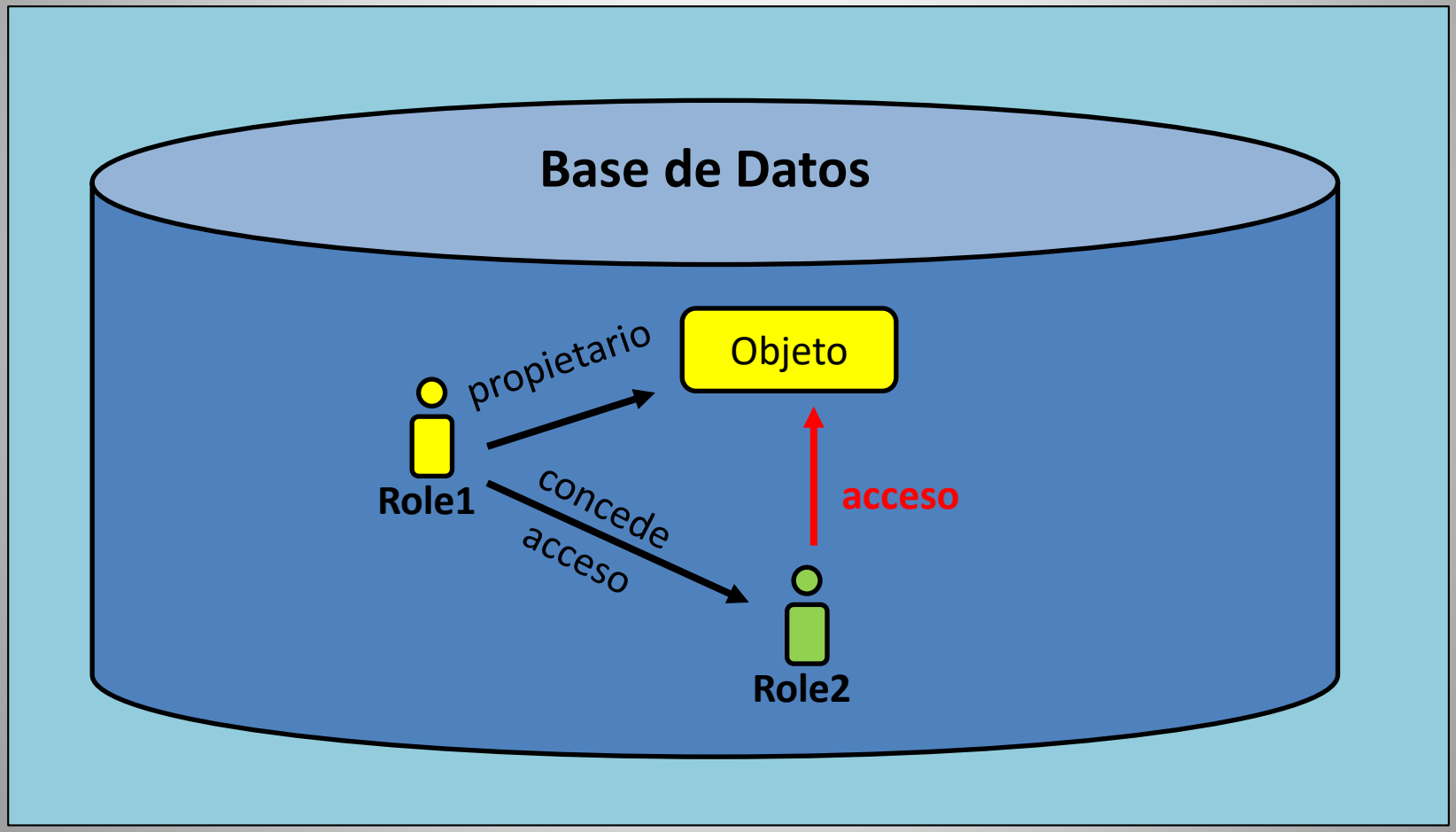


# Privilegios



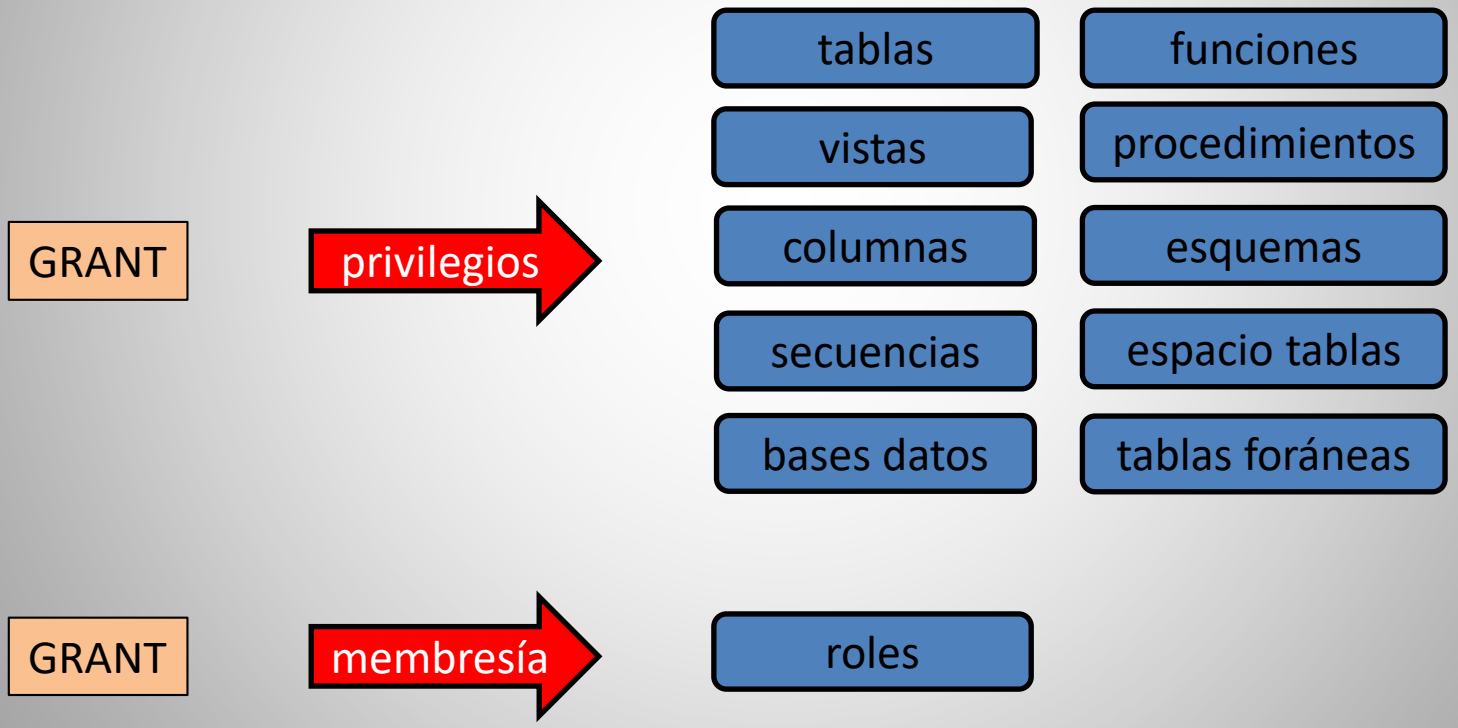

El role es propietario de todos los objetos que crea, y es el único que tiene acceso a ellos

# Privilegios



# Privilegios

La instrucción GRANT tiene dos variantes básicas



# Privilegios

La instrucción GRANT para conceder privilegios a tablas

```
GRANT { { SELECT | INSERT | UPDATE | DELETE | TRUNCATE | REFERENCES | TRIGGER }
      [, ...] | ALL [ PRIVILEGES ] }
      ON { [ TABLE ] table_name [, ...]
      | ALL TABLES IN SCHEMA schema_name [, ...] }
      TO role_specification [, ...] [ WITH GRANT OPTION ]

GRANT { { SELECT | INSERT | UPDATE | REFERENCES } ( column_name
      [, ...] )
      [, ...] | ALL [ PRIVILEGES ] ( column_name [, ...] ) }
      ON [ TABLE ] table_name [, ...]
      TO role_specification [, ...] [ WITH GRANT OPTION ]
```

Donde *role_specification* puede ser [GROUP] role_name, PUBLIC, CURRENT_USER, SESSION_USER

# Privilegios

PUBLIC es usado en la instrucción GRANT para conceder privilegios a todos los roles.

WITH GRANT OPTION es usado en la instrucción GRANT para conceder privilegios los roles que los recibieron para también conceder privilegios a otros roles. Pero nunca pueden conceder más privilegios de los que tienen.

GRANT INSERT ON ***tabla*** TO PUBLIC;
GRANT INSERT, UPDATE ON ***tabla*** TO ***role2***;
GRANT ALL ON ***tabla*** TO ***role3*** WITH GRANT OPTION;
GRANT SELECT (***campo1, campo3***) ON ***tabla*** TO ***role4***;

# Privilegios

Para el conceder acceso a tablas, es posible que también sea necesario conceder acceso a los esquemas donde se encuentran esas tablas.

De forma parecida, al momento de crear una tabla, si se requiere usar un dominio, se puede también conceder acceso al dominio particular

```
GRANT { USAGE | ALL [ PRIVILEGES ] }
   ON DOMAIN domain_name [, ...]
   TO role_specification [, ...] [ WITH GRANT OPTION ]
```

```
GRANT { { CREATE | USAGE } [, ...] | ALL [ PRIVILEGES ] }
   ON SCHEMA schema_name [, ...]
   TO role_specification [, ...] [ WITH GRANT OPTION ]
```

GRANT USAGE ON SCHEMA ***esquema*** TO ***role***;

# Privilegios

La instrucción REVOKE revoca los privilegios a tablas concedidos a los roles

```
REVOKE [ GRANT OPTION FOR ]
    { { SELECT | INSERT | UPDATE | DELETE | TRUNCATE | REFERENCES | TRIGGER }
    [, ...] | ALL [ PRIVILEGES ] }
    ON { [ TABLE ] table_name [, ...]
    | ALL TABLES IN SCHEMA schema_name [, ...] }
    FROM { [ GROUP ] role_name | PUBLIC } [, ...]
    [ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
    { { SELECT | INSERT | UPDATE | REFERENCES } ( column_name [, ...] )
    [, ...] | ALL [ PRIVILEGES ] ( column_name [, ...] ) }
    ON [ TABLE ] table_name [, ...]
    FROM { [ GROUP ] role_name | PUBLIC } [, ...]
    [ CASCADE | RESTRICT ]
```

# Privilegios

Cuando CASCADE se especifica en la instrucción REVOKE revoca los privilegios a tablas concedidos a los roles especificados, y también a los roles que ellos concedieron privilegios.

Cuando GRANT OPTION se especifica en la instrucción REVOKE revoca sólo los privilegios concedidos con la opción de GRANT OPTION, no los demás privilegios. Si no se especifican, se revocan todos.

Cuando se revocan privilegios sobre una tabla a un role, automáticamente se revocan los privilegios que tenga también sobre las columnas de la misma tabla.

Un role sólo puede revocar los privilegios que llegó a conceder a otros roles

# Privilegios

REVOKE INSERT ON ***tabla*** FROM PUBLIC;

REVOKE INSERT, UPDATE ON ***tabla*** FROM ***role2***;

REVOKE ALL ON ***tabla*** FROM ***role3*** WITH GRANT OPTION;

REVOKE SELECT (***campo1, campo3***) ON ***tabla*** FROM ***role4***;

# Bibliografía

Anón. s. f. «PostgreSQL: Documentation: 12: PostgreSQL 12.2 Documentation». (https://www.postgresql.org/docs/12/index.html).