

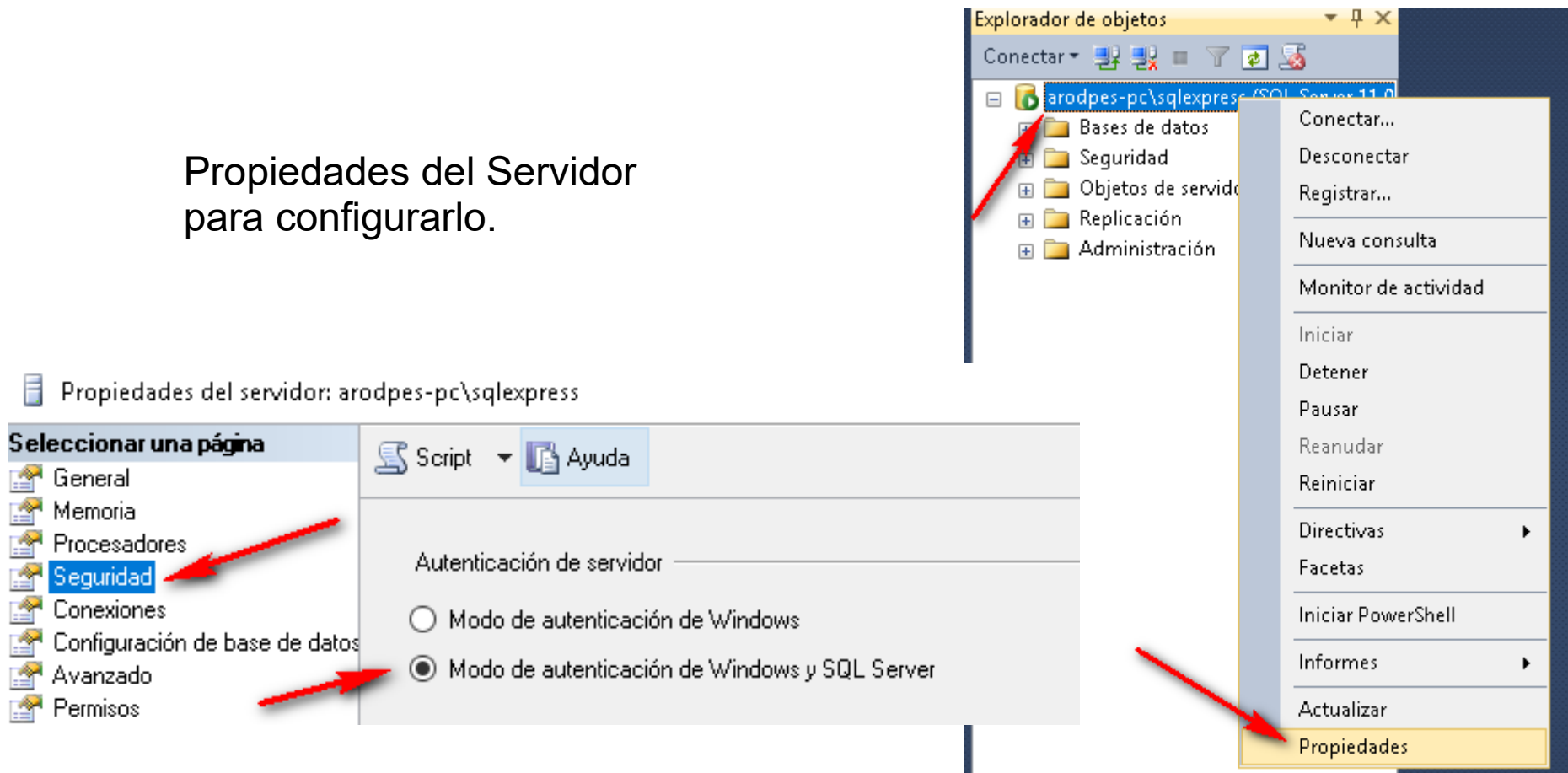
Usuarios SQL Server

Tipo de gestión de seguridad en SQL Server:

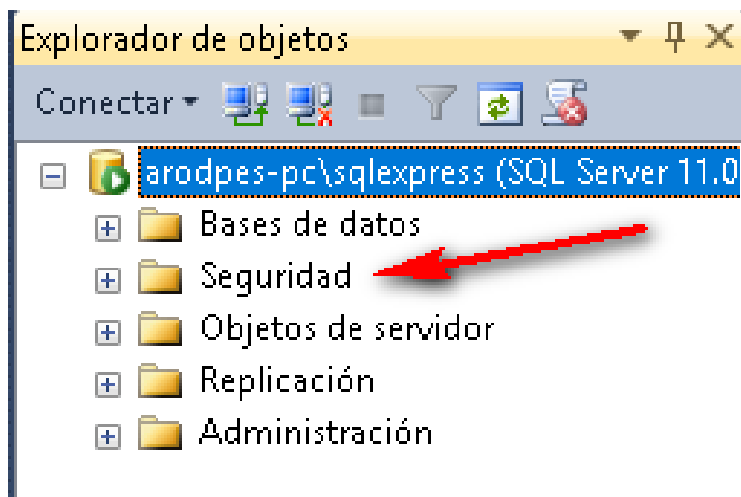
- Inicios de sesión Windows, gestionados por el Sistema Operativo mediante el Directorio activo.
- Inicios de sesión gestionados por el propio SQL Server

Se recomienda el primero, porque la gestión de los usuarios del SO es más eficiente, pero para las pruebas es mejor el otro.

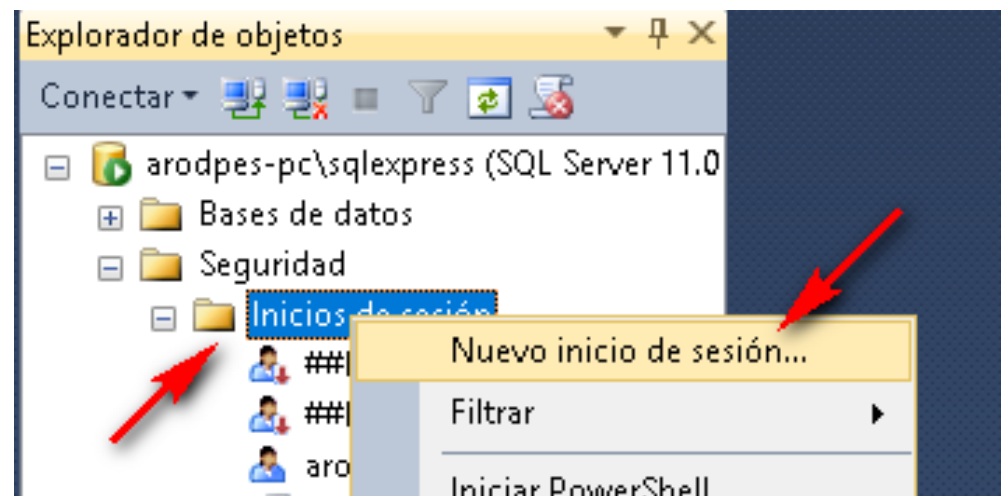
Propiedades del Servidor para configurarlo.



Generaremos un inicio de sesión que nos permitirá acceder al Gestor.



Click en Seguridad del Sistema.
Botón derecha en Inicios de sesión



Inicio de sesión - Nuevo

Seleccionar una página

- General
- Roles del servidor
- Asignación de usuarios
- Elementos protegibles
- Estado

Script Ayuda

Nombre de inicio de sesión: usuario2017 Buscar..

☐ Autenticación de Windows

☒ Autenticación de SQL Server

Contraseña:

Confirmar contraseña:

☐ Especificar contraseña anterior

Contraseña anterior:

☐ Exigir directivas de contraseña

☐ Exigir expiración de contraseña

☐ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

☐ Asignado a certificado

☐ Asignado a clave asimétrica

☐ Asignar a credencial

Credenciales asignadas

Credencial	Proveedor
------------	-----------

Agregar

Base de datos predeterminada: master

Idioma predeterminado: <predeterminado>

Quitar

Conexión

Servidor: arodpes-pc\squlexpress

Conexión: ARODPES-PC\arodpes

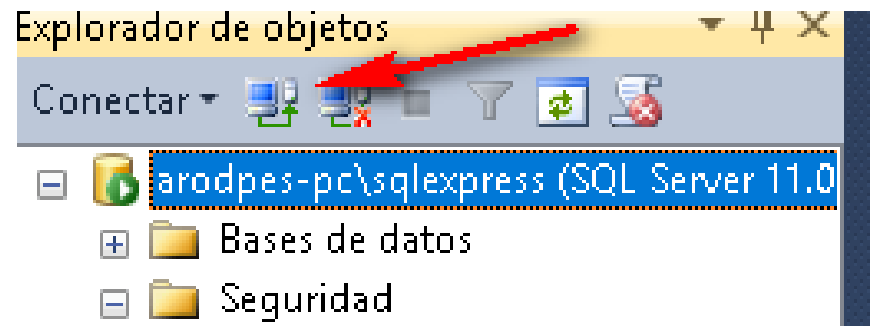
[Ver propiedades de conexión](#)

Progreso

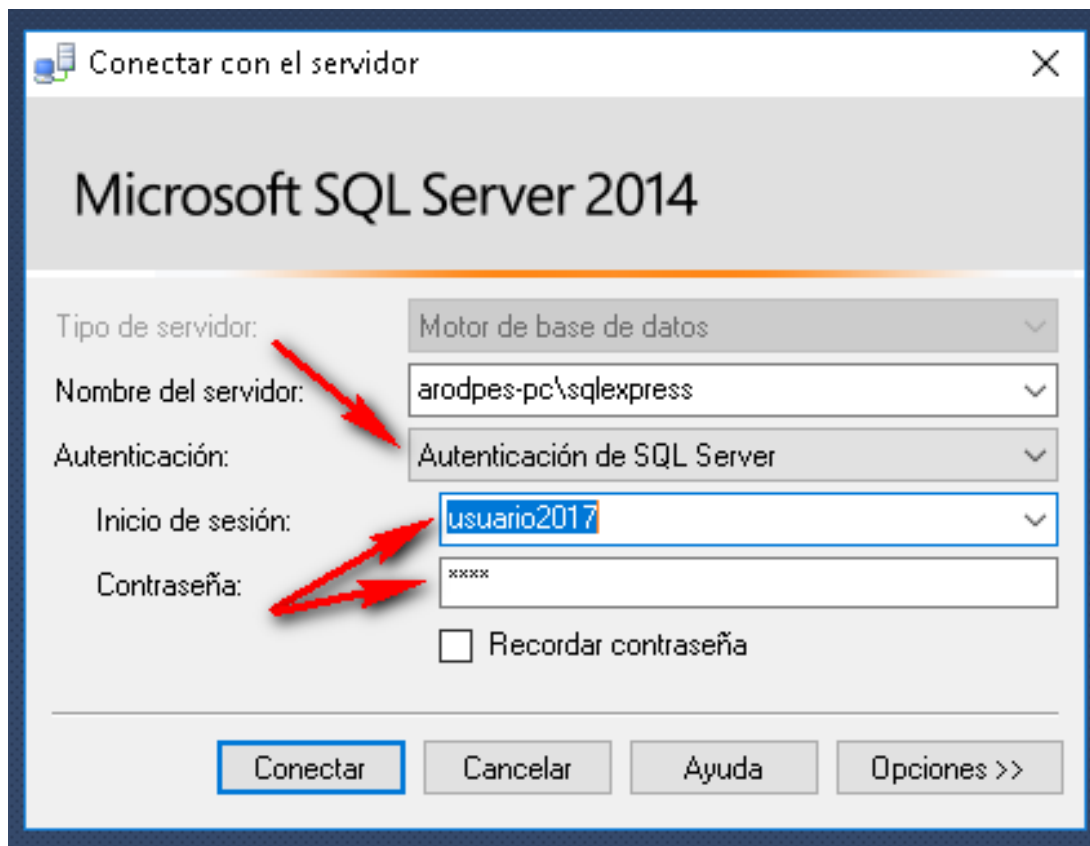
Listo

Damos nombre de inicio de sesión y clave. Quitamos las directivas de contraseña para facilitar la prueba, aunque no lo haríamos en un sistema en producción. Debemos fijarnos en que podemos asignar la BD por defecto, que será master si no indicamos otra.

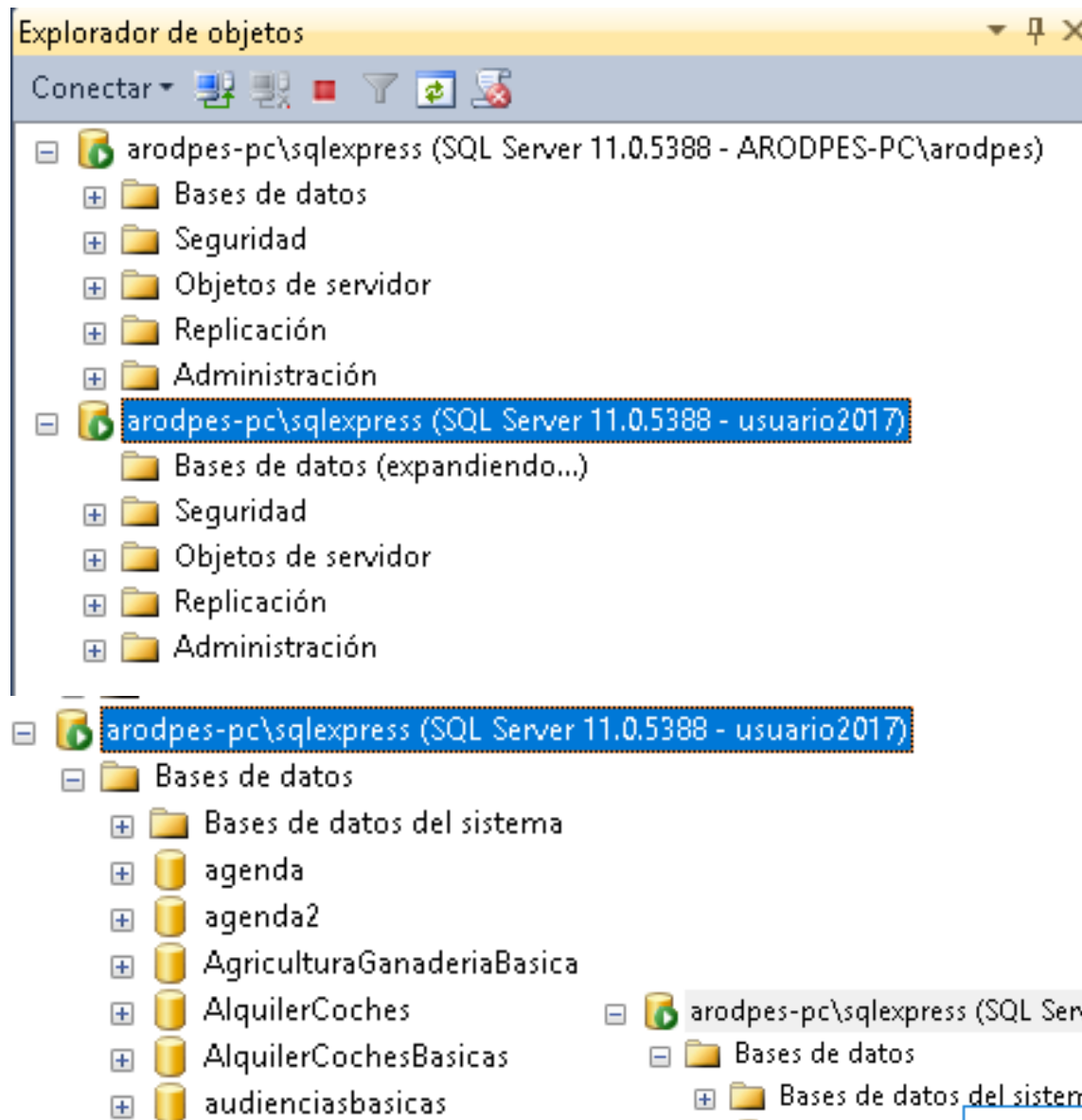
Con este inicio de sesión ya podemos probar acceder al sistema



Haciendo click en el icono abrimos otra conexión en el sistema con la misma instancia de Management Studio



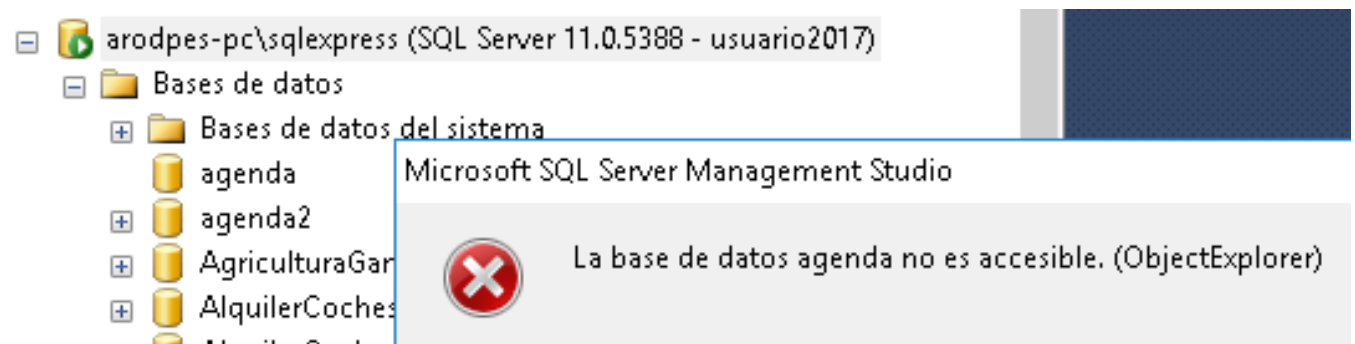
Elegimos Autenticación de SQL Server y colocamos el inicio de sesión y la clave

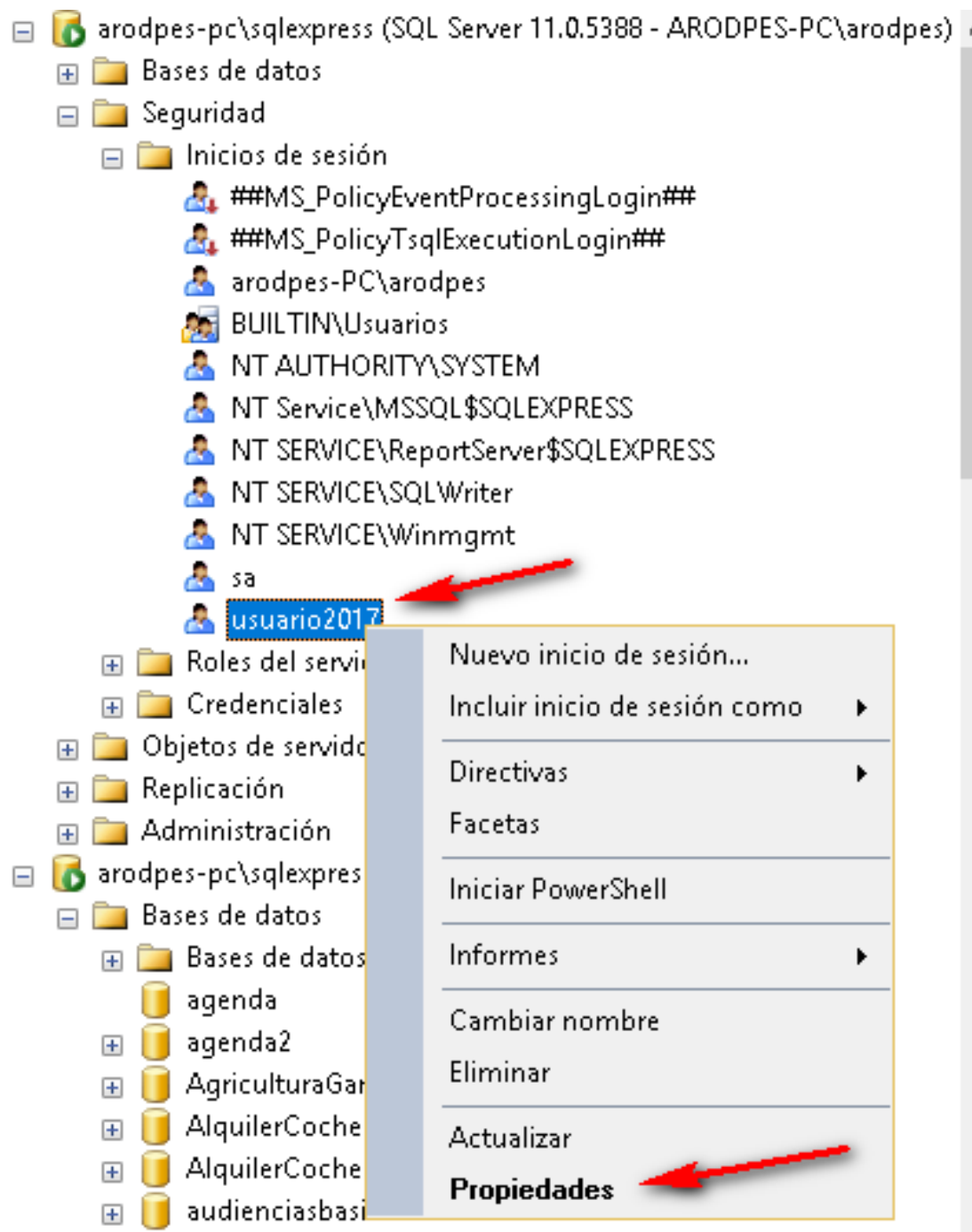


Tendremos dos conexiones, una como administrados y la otra con el inicio de sesión generado

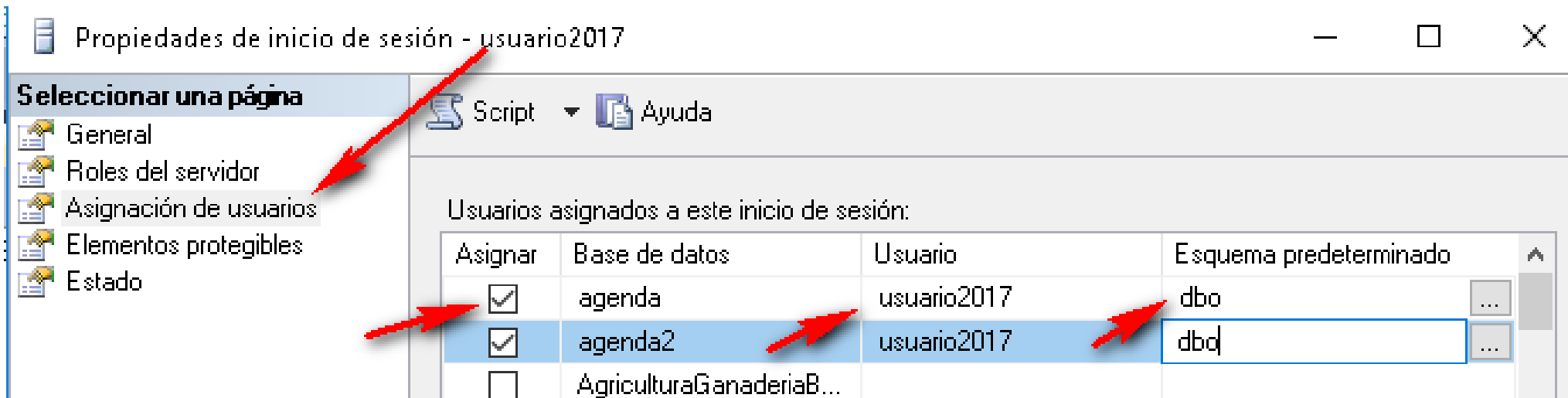
Podremos ver el nombre de las BD del servidor...

Pero dará error al intentar acceder a ellas





Estudiamos las propiedades del inicio de sesión...

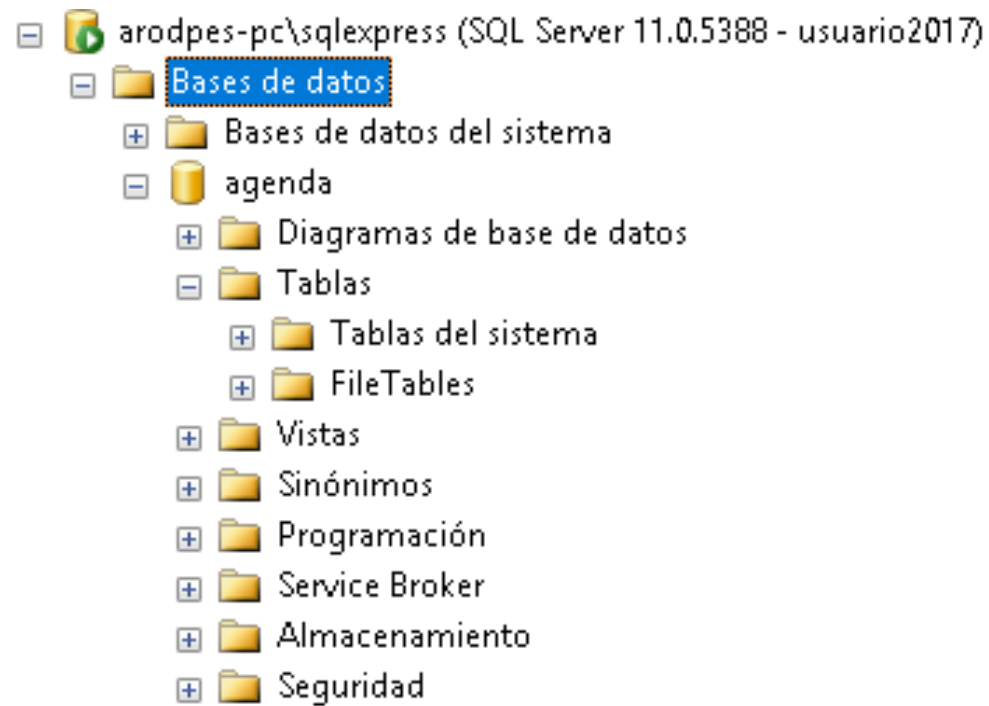


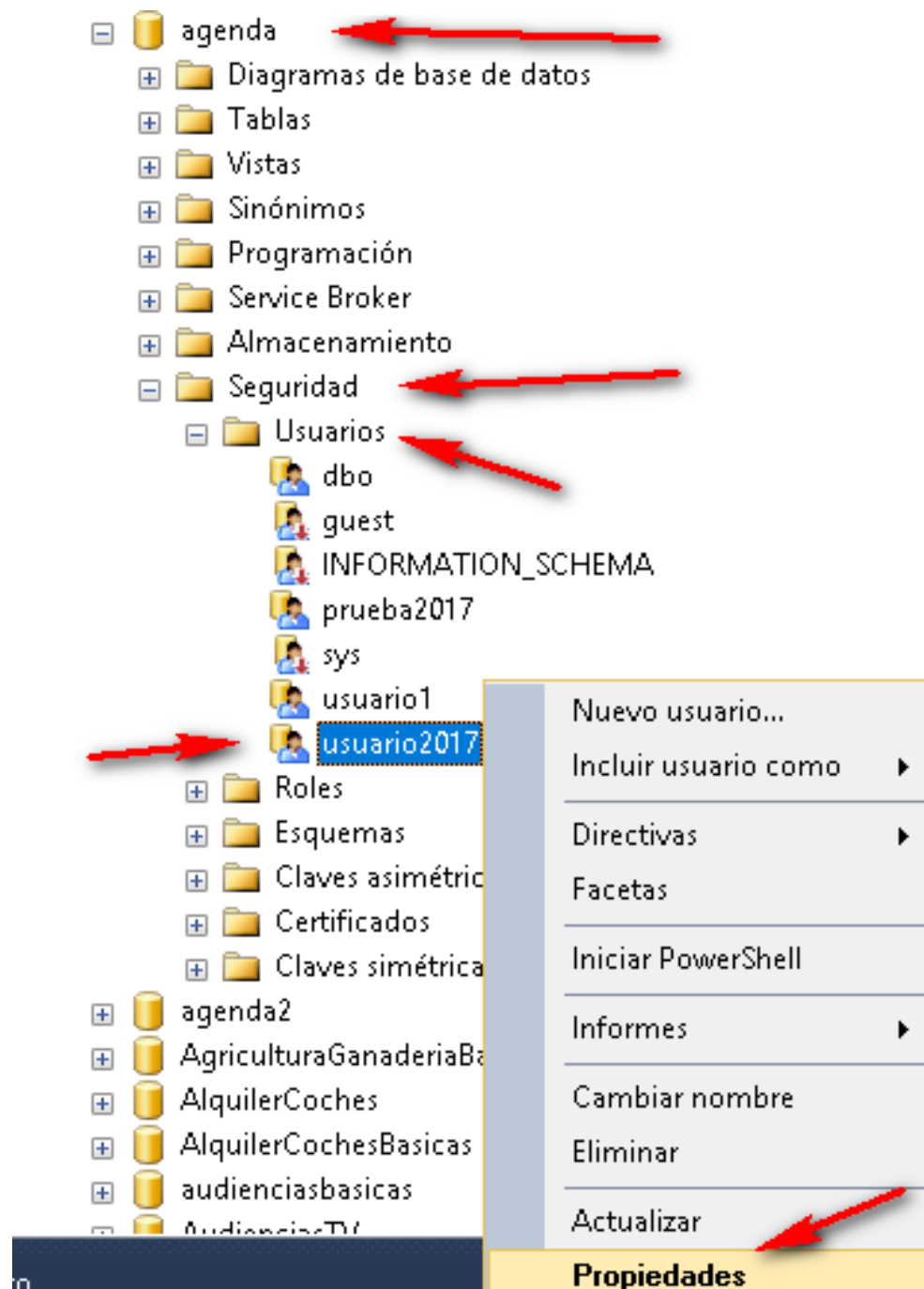
Cada inicio de sesión se debe asignar a un usuario de cada BD. Suele mantenerse el nombre.

El usuario es el que definirá cómo se accede a la BD.

Marcaremos el asignar, por defecto llama al usuario igual que al inicio de sesión y le indicamos el esquema (lo normal es dbo, data base owner, el propietario de la base de datos).

Con esto conseguiremos que no nos de error al acceder a la BD pero no podremos ver los objetos que tiene.










Ahora vamos a acceder a la seguridad del usuario de la BD agenda, para especificar lo que puede realizar.


Asignando al usuario el rol de base de datos:

En el ejemplo asignamos el rol db_datareader al usuario2017 en la BD agenda, con lo que podrá leer y sólo leer los objetos de la BD.

 Usuario de la base de datos - usuario2017

Seleccionar una página

 General
 Esquemas de propiedad
 Pertenencia
 Elementos protegibles
 Propiedades extendidas

Script  Ayuda

Pertenencia al rol de la base de datos:

Miembros del rol

<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input checked="" type="checkbox"/>	db_datareader
<input type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin

Comprobamos.

- [-] arodpe-pc\sqlexpress (SQL Server 11.0.5388 - usuario2017)
 - [-] Bases de datos
 - + Bases de datos del sistema
 - [-] agenda
 - + Diagramas de base de datos
 - [-] Tablas
 - + Tablas del sistema
 - + FileTables
 - + clase.Personas
 - + dbo.Personas
 - + otro.Personas
 - + otronuevo.Personas

Podemos ver las tablas.

Y ver su contenido

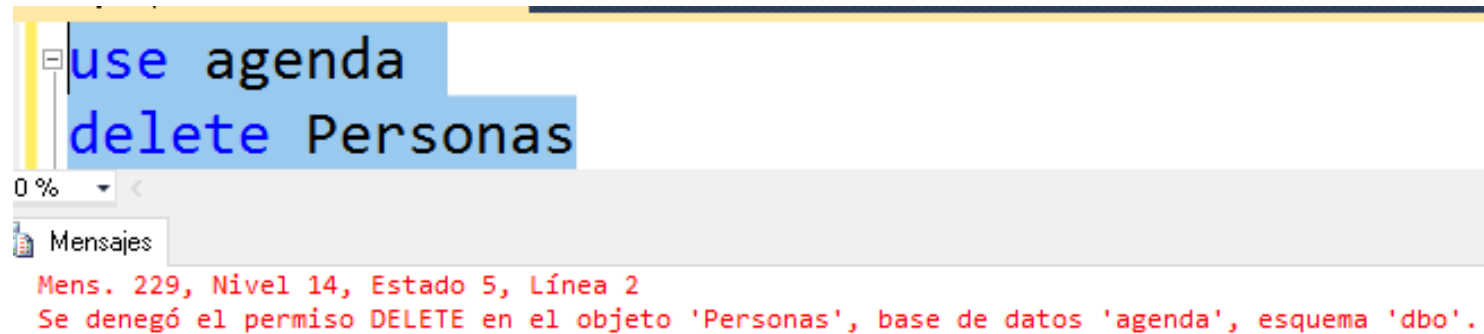
```
use agenda
select idpersona,nombre,apellidos
FROM Personas
```

00 %

Resultados Mensajes

	idpersona	nombre	apellidos
1	1	Juan	Hernández Pérez
2	2	María	Fernández Hernández
3	3	Marta	Pérez Rodríguez
4	4	José	González González
5	5	Antonia	Pérez González

No deja borrar el contenido

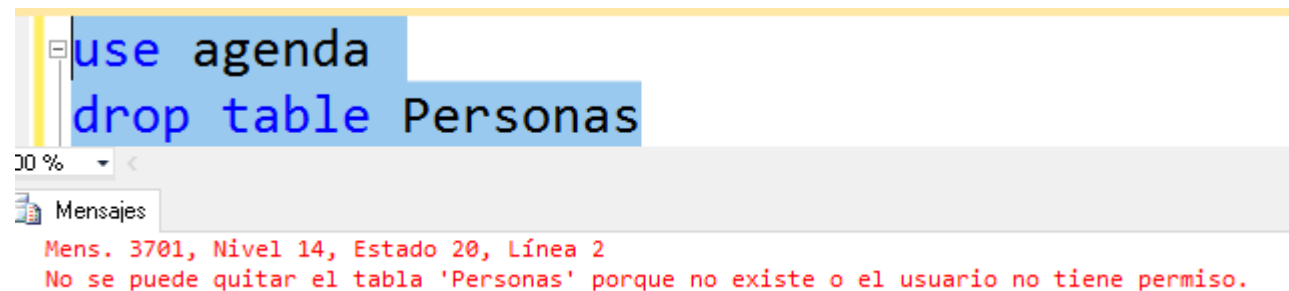


The screenshot shows the SQL Server Enterprise Manager interface. The left pane displays the 'Mensajes' (Messages) folder. The main pane shows a red error message: 'Mens. 229, Nivel 14, Estado 5, Línea 2' followed by 'Se denegó el permiso DELETE en el objeto 'Personas', base de datos 'agenda', esquema 'dbo'.' The background of the main pane is light blue, and the text 'use agenda' and 'delete Personas' is visible in a darker blue font.

```
use agenda
delete Personas
```

Mens. 229, Nivel 14, Estado 5, Línea 2
Se denegó el permiso DELETE en el objeto 'Personas', base de datos 'agenda', esquema 'dbo'.

No deja eliminar el objeto



The screenshot shows the SQL Server Enterprise Manager interface. The left pane displays the 'Mensajes' (Messages) folder. The main pane shows a red error message: 'Mens. 3701, Nivel 14, Estado 20, Línea 2' followed by 'No se puede quitar el tabla 'Personas' porque no existe o el usuario no tiene permiso.' The background of the main pane is light blue, and the text 'use agenda' and 'drop table Personas' is visible in a darker blue font.

```
use agenda
drop table Personas
```

Mens. 3701, Nivel 14, Estado 20, Línea 2
No se puede quitar el tabla 'Personas' porque no existe o el usuario no tiene permiso.

Podemos precisar los permisos

Accediendo a las propiedades del usuario de la BD podremos añadir o quitar permisos de acceso.

Buscar objetos del tipo... Tabla

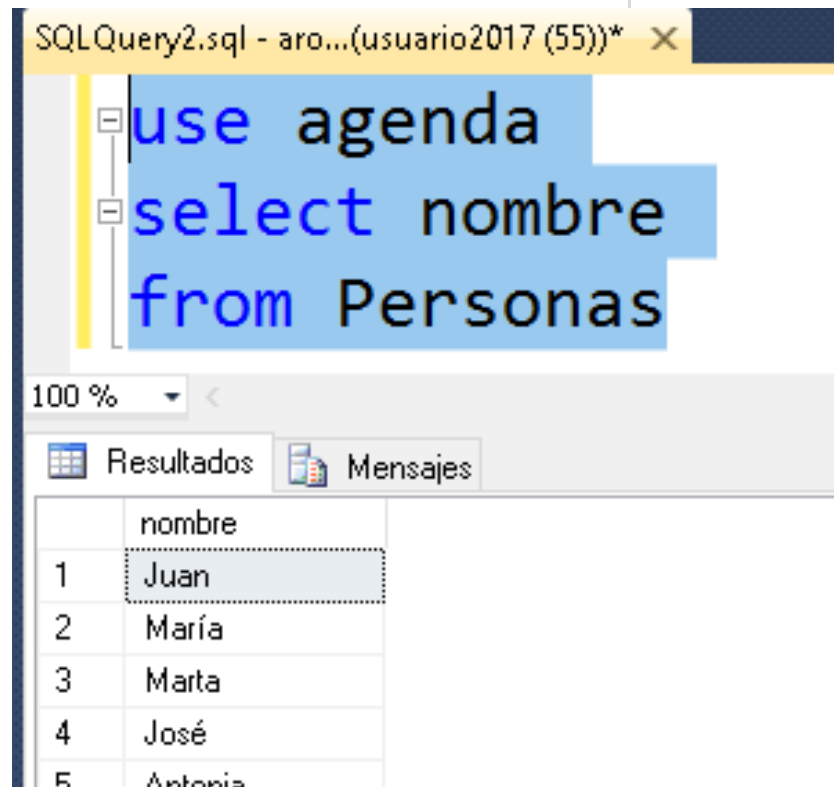
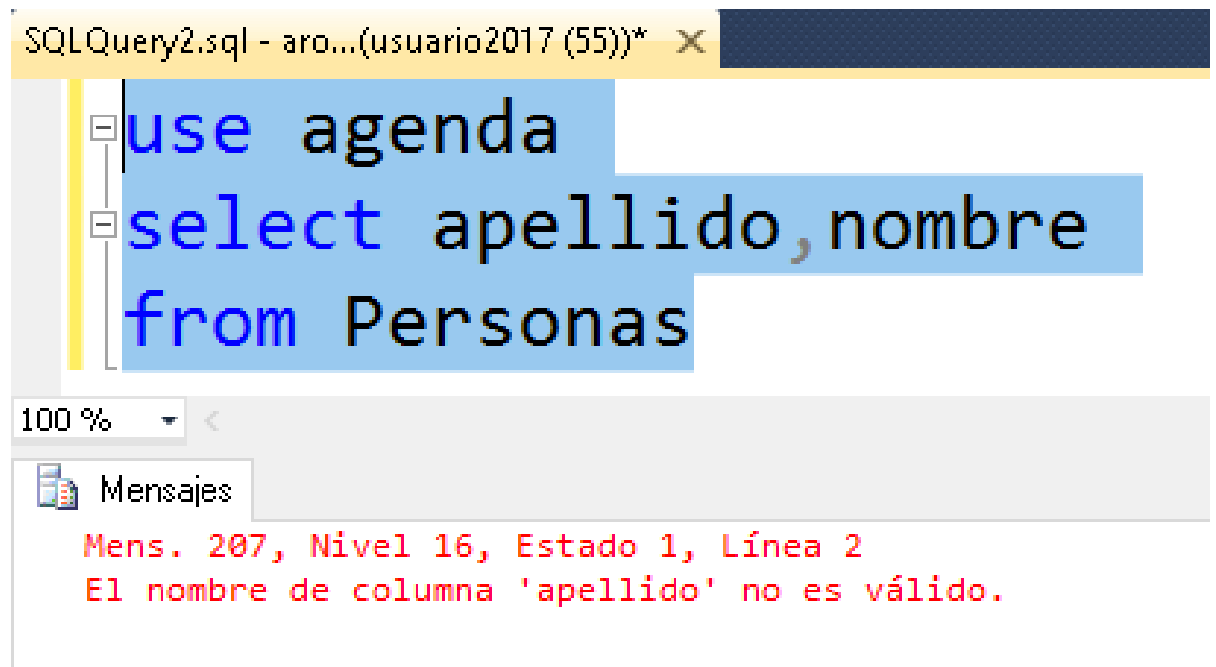
The screenshot shows the 'usuario2017' user properties window in SQL Server Enterprise Manager. The 'General' tab is selected, showing the user name 'usuario2017'. The 'Elements to protect' section shows a list of objects, with 'dbo.Personas' selected. A red arrow points to the 'dbo.Personas' row in the table.

The 'Permissions for dbo.Personas' section shows the 'Column Permissions' dialog box. The 'Entity' is 'usuario2017', the 'Grantor' is 'dbo.Personas', and the 'Permission' is 'Actualizar'. The 'Column Permissions' table shows the 'Deny' checkbox checked for the 'apellidos' column.

Esquema	Nombre	Tipo
clase	Personas	Tabla
dbo	Personas	Tabla
otro	Personas	Tabla
otro nuevo	Personas	Tabla

Nombre de columna	Conceder	WITH GRA...	Denegar
apellidos	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
idPersona	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nombre	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

La columna apellido no se puede usar en el select



La columna nombre sola sí se permite

Roles de base de datos

Nombre del rol fijo de base de datos	Description
db_owner	Los miembros del rol fijo de base de datos db_owner pueden realizar todas las actividades de configuración y mantenimiento en la base de datos y también pueden quitar la base de datos en SQL Server. (En Base de datos SQL y Almacenamiento de datos SQL, algunas actividades de mantenimiento requieren permisos a nivel de servidor y los roles db_owners no las pueden realizar).
db_securityadmin	Los miembros del rol fijo de base de datos db_securityadmin pueden modificar la pertenencia a roles y administrar permisos. Si se agregan entidades de seguridad a este rol, podría habilitarse un aumento de privilegios no deseado.
db_accessadmin	Los miembros del rol fijo de base de datos db_accessadmin pueden agregar o quitar el acceso a la base de datos para inicios de sesión de Windows, grupos de Windows e inicios de sesión de SQL Server .
db_backupoperator	Los miembros del rol fijo de base de datos db_backupoperator pueden crear copias de seguridad de la base de datos.

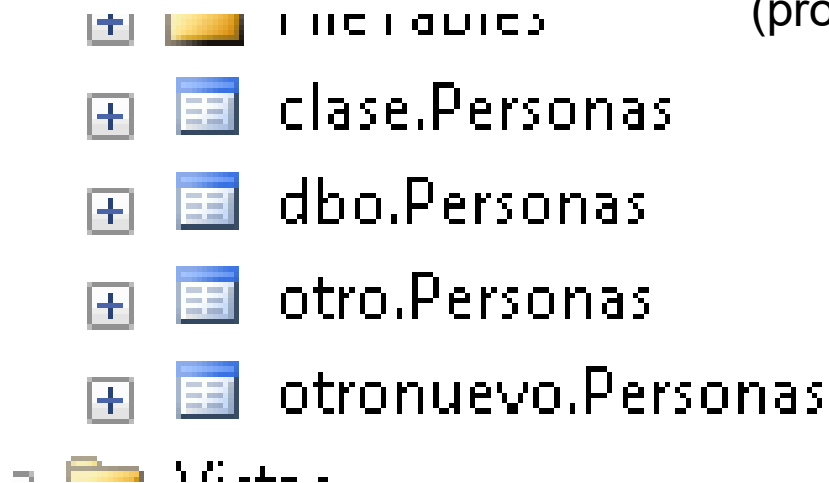
db_ddladmin	Los miembros del rol fijo de base de datos db_ddladmin pueden ejecutar cualquier comando del lenguaje de definición de datos (DDL) en una base de datos.
db_datawriter	Los miembros del rol fijo de base de datos db_datawriter pueden agregar, eliminar o cambiar datos en todas las tablas de usuario.
db_datareader	Los miembros del rol fijo de base de datos db_datareader pueden leer todos los datos de todas las tablas de usuario.
db_denydatawriter	Los miembros del rol fijo de base de datos db_denydatawriter no pueden agregar, modificar ni eliminar datos de tablas de usuario de una base de datos.
db_denydatareader	Los miembros del rol fijo de base de datos db_denydatareader no pueden leer datos de las tablas de usuario dentro de una base de datos.

Roles de Servidor

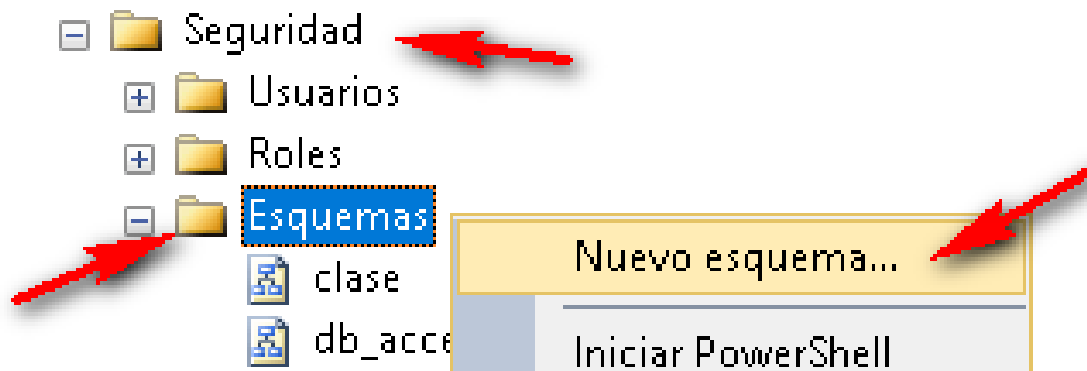
Rol fijo de nivel de servidor	Descripción
sysadmin	Los miembros del rol fijo de servidor sysadmin pueden realizar cualquier actividad en el servidor.
serveradmin	Los miembros del rol fijo de servidor serveradmin pueden cambiar las opciones de configuración en el servidor y cerrar el servidor.
securityadmin	<p>Los miembros del rol fijo de servidor securityadmin administran los inicios de sesión y sus propiedades. Administran los permisos de servidor GRANT, DENY y REVOKE. También pueden administrar los permisos de nivel de base de datos GRANT, DENY y REVOKE si tienen acceso a una base de datos. Asimismo, pueden restablecer contraseñas para inicios de sesión de SQL Server.</p> <p>** Nota de seguridad ** La capacidad de conceder acceso a Motor de base de datos y configurar los permisos de usuario permite que el administrador de seguridad asigne la mayoría de los permisos de servidor. El rol securityadmin se debe tratar como equivalente al rol sysadmin .</p>
processadmin	Los miembros del rol fijo de servidor processadmin pueden finalizar los procesos que se ejecutan en una instancia de SQL Server.

setupadmin	Los miembros del rol fijo de servidor setupadmin pueden agregar y quitar servidores vinculados mediante instrucciones de Transact-SQL. (Es necesaria la pertenencia a sysadmin cuando se usa Management Studio).
bulkadmin	Los miembros del rol fijo de servidor bulkadmin pueden ejecutar la instrucción BULK INSERT.
diskadmin	El rol fijo de servidor diskadmin se utiliza para administrar archivos de disco.
dbcreator	Los miembros del rol fijo de servidor dbcreator pueden crear, modificar, quitar y restaurar cualquier base de datos.
public	<p>Cada inicio de sesión de SQL Server pertenece al rol público de servidor. Cuando a una entidad de seguridad de servidor no se le han concedido ni denegado permisos específicos para un objeto protegible, el usuario hereda los permisos concedidos al rol pública para ese elemento. Solo asigne los permisos públicos en cualquier objeto cuando desee que el objeto esté disponible para todos los usuarios. No puede cambiar la pertenencia en public.</p> <p>Nota: public se implementa de manera diferente que otros roles. Pero se pueden conceder, denegar o revocar permisos desde public.</p>

Esquema de la BD

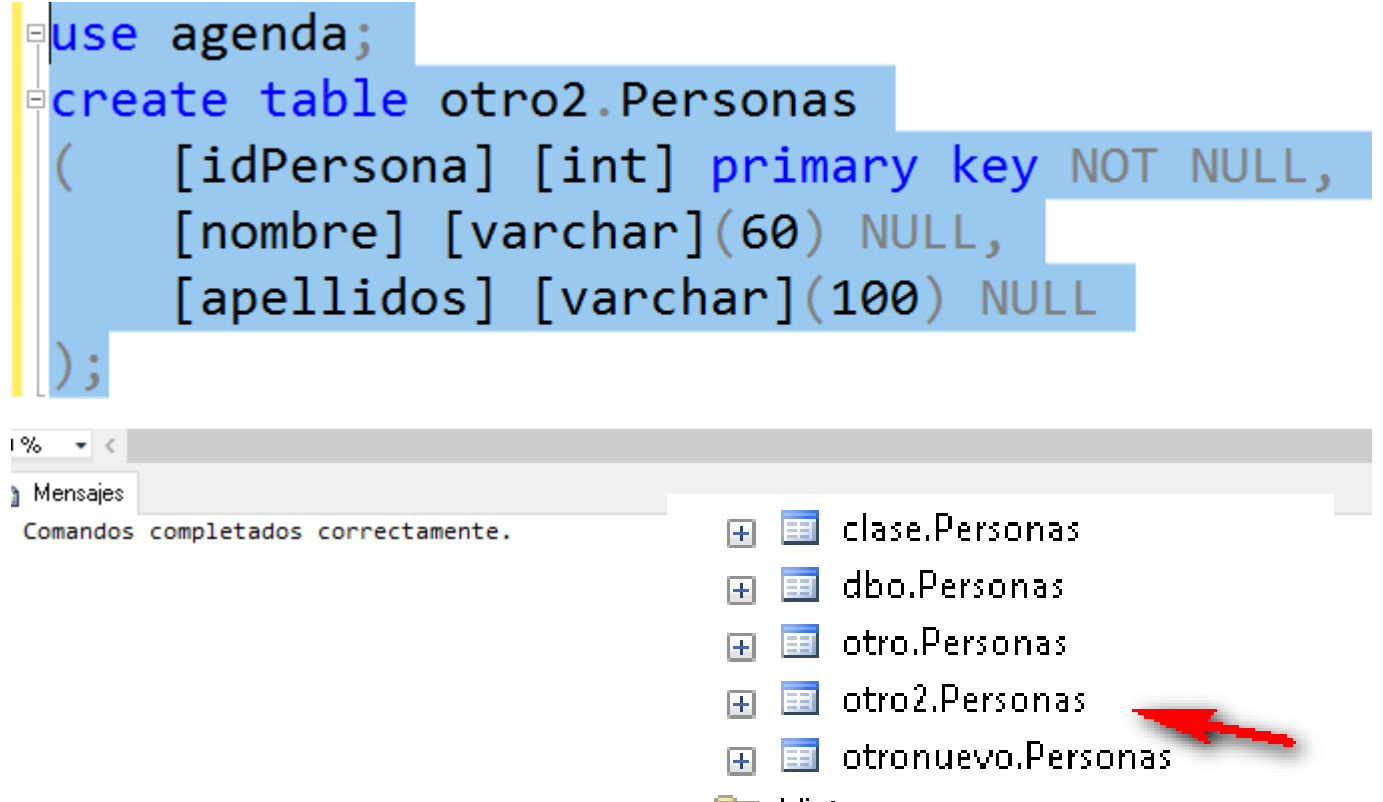


Estructura para organizar las tablas.
Funcionan como carpetas en la BD.
Podemos asignar a cada usuario qué esquema tiene por defecto.
El normal es dbo que proviene de la definición de data base owner (propietario de la base de datos).



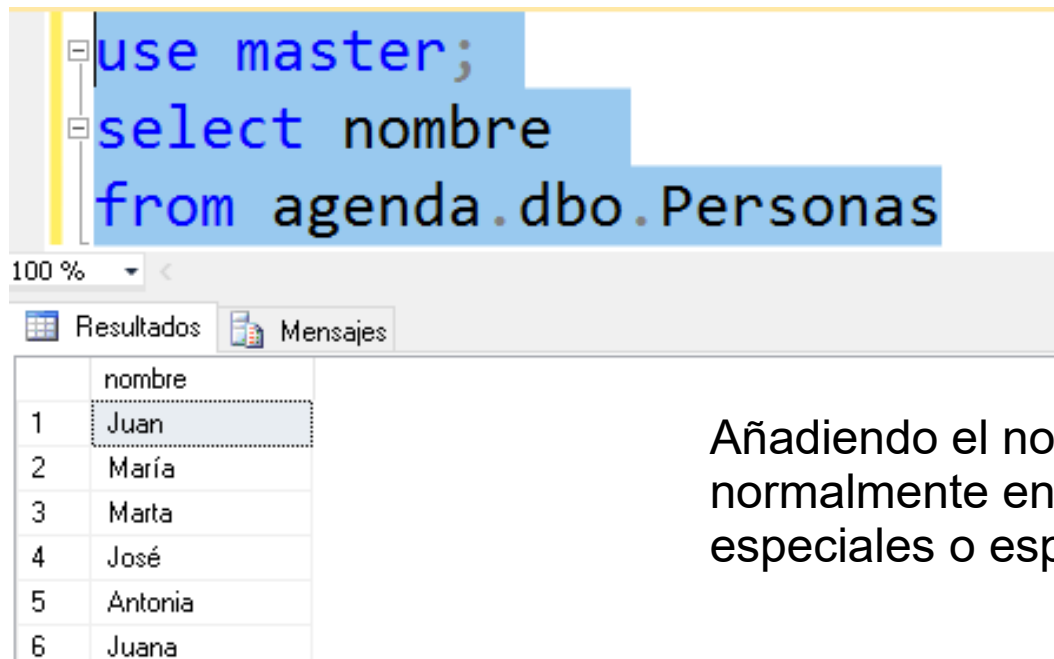
Podemos crear nuevos esquemas

Podremos entonces crear tablas, incluso con el mismo nombre en el rol creado.



Nombre completo de una tabla:

BaseDeDatos.Eschema.Tabla



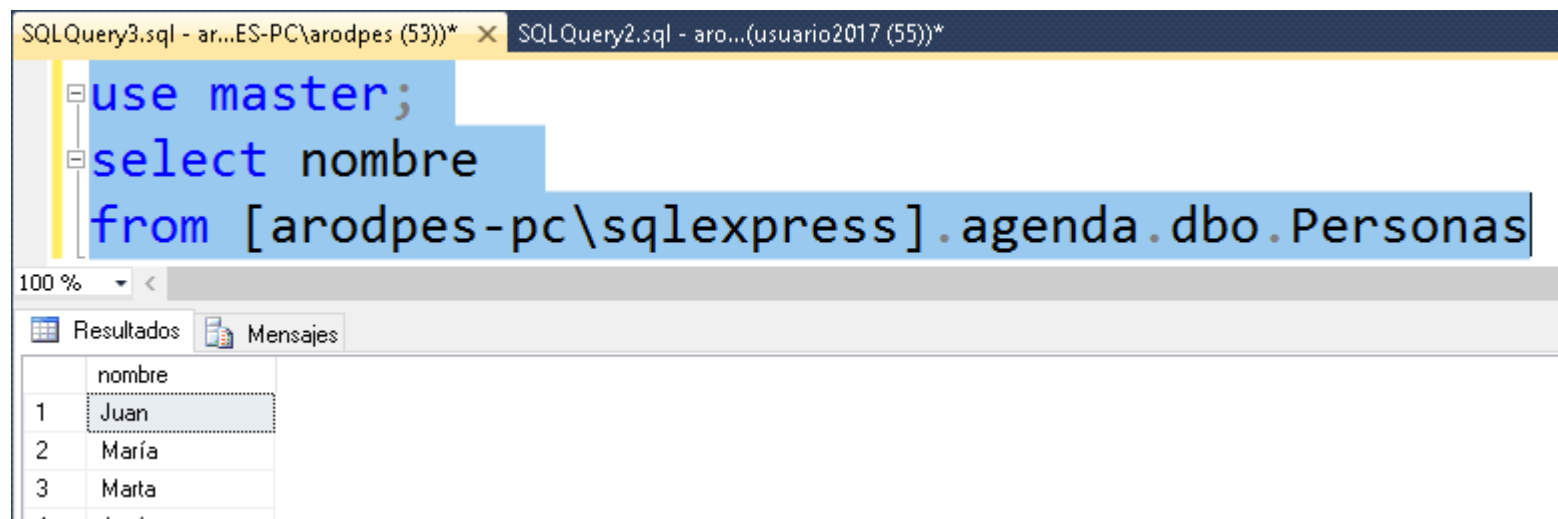
The screenshot shows a SQL query window with the following text:

```
use master;  
select nombre  
from agenda.dbo.Personas
```

Below the query window is a results grid showing the output of the query:

	nombre
1	Juan
2	María
3	Marta
4	José
5	Antonia
6	Juana

Añadiendo el nombre del servidor al principio, normalmente entre corchetes si tiene caracteres especiales o espacios en blanco



The screenshot shows a SQL query window with the following text:

```
use master;  
select nombre  
from [arodpes-pc\sqlexpress].agenda.dbo.Personas
```

Below the query window is a results grid showing the output of the query:

	nombre
1	Juan
2	María
3	Marta
4	José
5	Antonia
6	Juana

Gestión de inicios de sesión y usuarios de BD mediante sentencias.

Crear inicio de sesión de SQL Server

```
create login alvaro2 with password = '1234',  
check_policy = off;
```

Microsoft SQL Server 2014

Tipo de servidor: Motor de base de datos

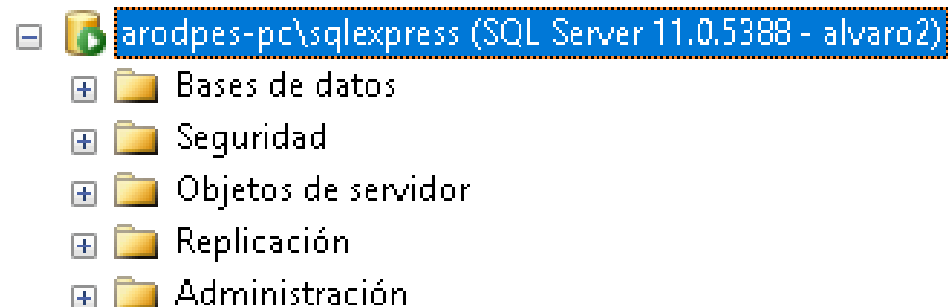
Nombre del servidor: arodpes-pc\squlexpress

Autenticación: Autenticación de SQL Server

Inicio de sesión: alvaro2

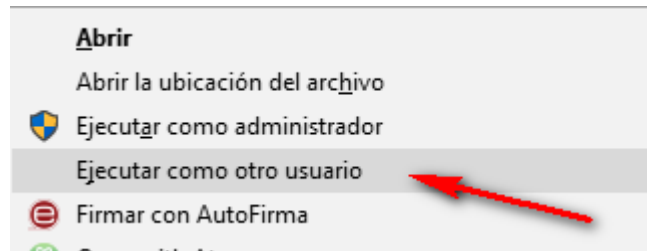
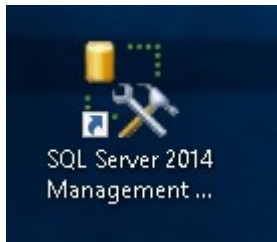
Contraseña:

☐ Recordar contraseña



Crear inicio de sesión de usuario Windows

```
CREATE LOGIN [arodpes-PC\alvaro] FROM WINDOWS;  
GO
```



Shift y Botón derecho sobre acceso directo

Seguridad de Windows

Ejecutar como otro usuario

Escriba las credenciales que se usarán para C:\Program Files (x86)\Microsoft SQL Server\120\Tools\Binn\ManagementStudio\Ssms.exe.

Dominio: ARODPES-PC

[Más opciones](#)

Aceptar Cancelar

Conectar con el servidor

Microsoft SQL Server 2014

Tipo de servidor: Motor de base de datos

Nombre del servidor: arodpes-PC\squlexpress

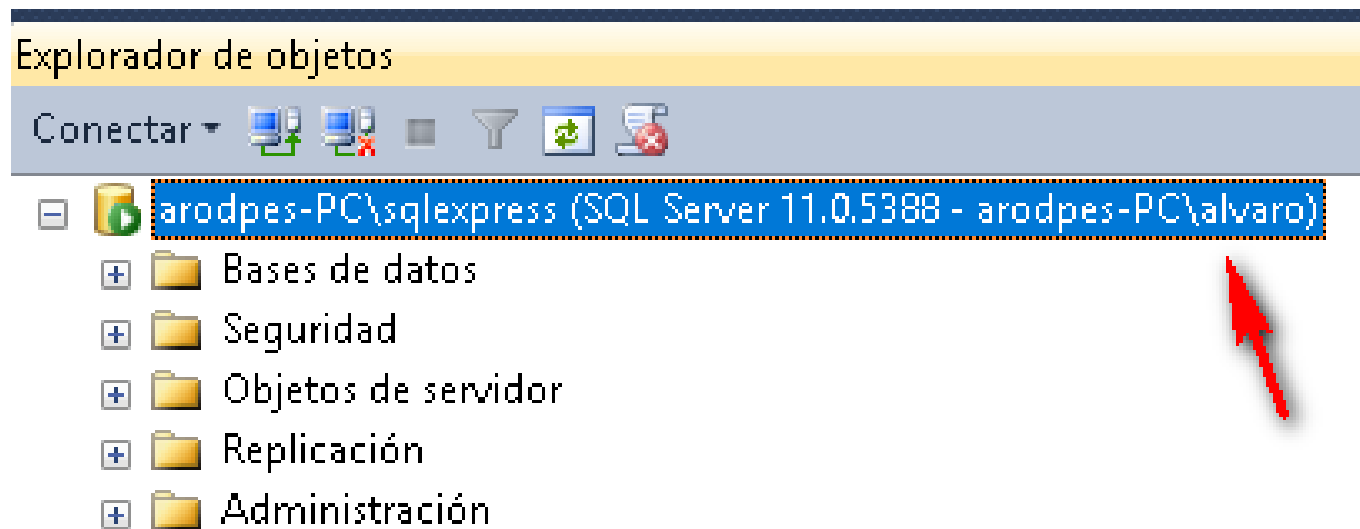
Autenticación: Autenticación de Windows

Nombre de usuario: arodpes-PC\alvaro

Contraseña:

☐ Recordar contraseña

Conectar Cancelar Ayuda Opciones >>



Podemos borrar los login con drop login

Además podremos activarlos o desactivarlos:

```
alter login alvaro2 enable;  
go
```

```
alter login alvaro2 disable;  
go
```



```
use master
```

```
go
```

```
select * from sys.server_principals;
```

```
go
```

Tabla con entidades de seguridad del servidor: logins, roles,...

 Resultados  Mensajes			
	name	principal_id	sid
1	sa	1	0x01
2	public	2	0x02
3	sysadmin	3	0x03
4	securityadmin	4	0x04
5	serveradmin	5	0x05
6	setupadmin	6	0x06
7	processadmin	7	0x07
8	diskadmin	8	0x08
9	dbcreator	9	0x09
10	bulkadmin	10	0x0A

Inicios de sesión SQL

```
use master|
go
select * from sys.sql_logins;
go
```

Resultados		Mensajes					
	name	principal_id	sid	type	type_desc	is_disabled	password_hash
1	sa	1	0x01	S	SQL_LOGIN	0	0x020062E8B418CB507
2	##MS_PolicyTsqlExecutionLogin##	257	0xFB5428192C68DE479445435923D3CE58	S	SQL_LOGIN	1	0x0200FCE508901EC7A
3	##MS_PolicyEventProcessingLogin##	273	0x446912BCC3681B409A98B45B269A3493	S	SQL_LOGIN	1	0x0200CF76D47BC6464
4	usuario2017	290	0x8B5FCACBF3C3BE4CBDE628699F355C2A	S	SQL_LOGIN	0	0x02005E9C1CDFE4104
5	alvaro2	291	0xAB08903651F8B14D8F5EE453FE01C19C	S	SQL_LOGIN	0	0x0200B8550259334DF



```
use master
```

```
go
```

```
select * from sys.server_principals;
```

```
go
```

Tabla con entidades de seguridad del servidor: logins, roles,...

 Resultados  Mensajes			
	name	principal_id	sid
1	sa	1	0x01
2	public	2	0x02
3	sysadmin	3	0x03
4	securityadmin	4	0x04
5	serveradmin	5	0x05
6	setupadmin	6	0x06
7	processadmin	7	0x07
8	diskadmin	8	0x08
9	dbcreator	9	0x09
10	bulkadmin	10	0x0A

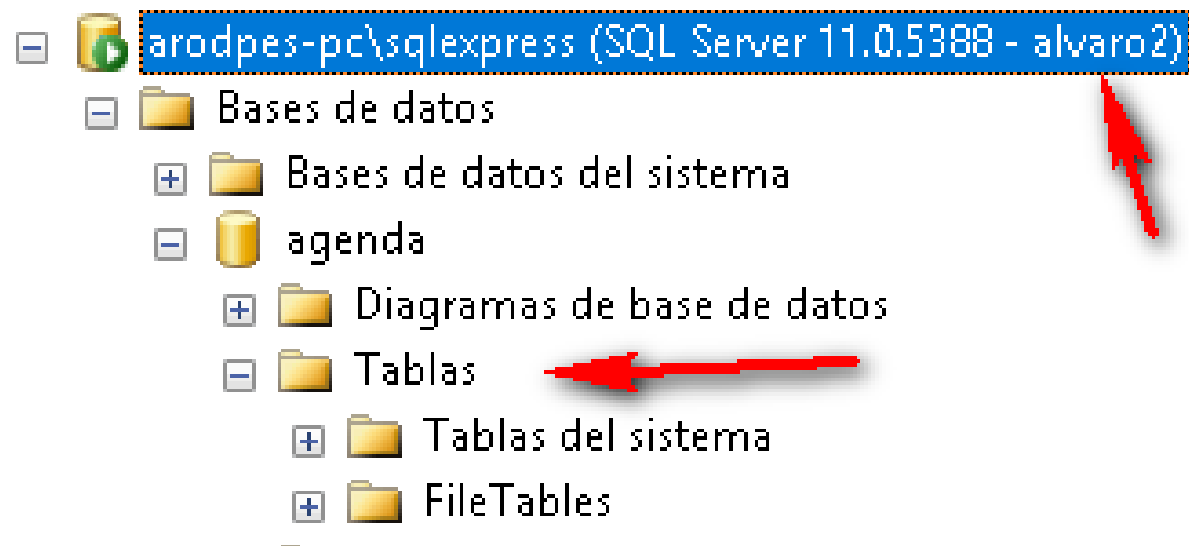
Crear usuario de la BD y asignarlo a un inicio de sesión

```
use agenda
```

```
go
```

```
create user alvaro2 for login alvaro2  
with default_schema=dbo;
```

```
go
```



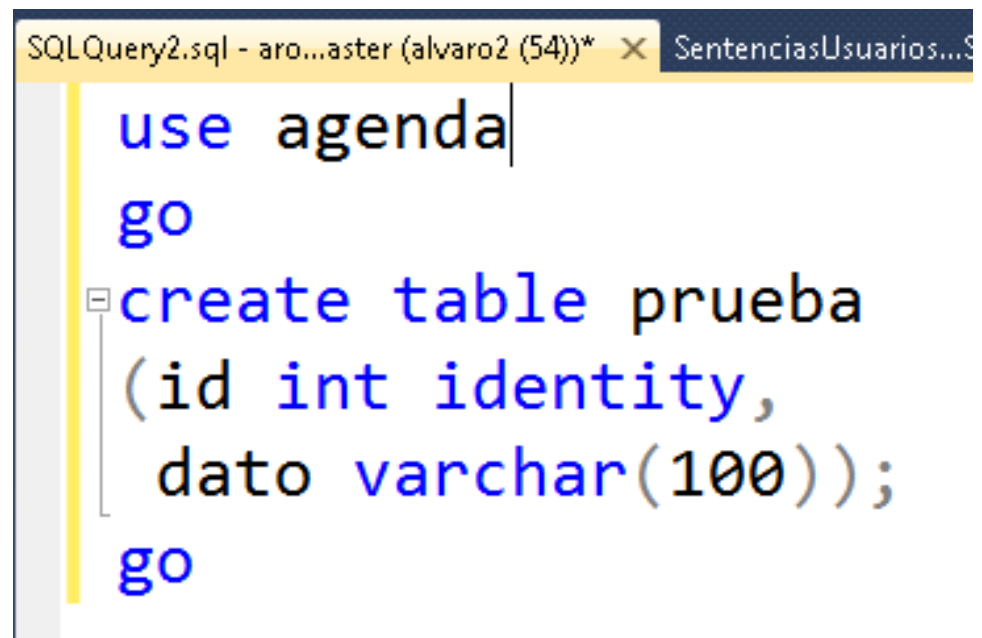
Falta asignar permisos o rol de base de datos para poder actuar sobre las tablas.

Asignando rol de BD

```
exec sp_addrolemember 'db_datareader','alvaro2';  
go|
```

Dar permisos

```
use agenda;  
go  
grant create table to alvaro2;  
go
```



The screenshot shows a SQL query editor window with a yellow title bar. The title bar contains the text "SQLQuery2.sql - aro...aster (alvaro2 (54))*" followed by a close button (X) and another tab labeled "SentenciasUsuarios...S". The editor area has a light gray background and a yellow vertical line on the left. The SQL script being edited is as follows:

```
use agenda  
go  
create table prueba  
(id int identity,  
  dato varchar(100));  
go
```


GRANT ALL/CREATE, DELETE, INSERT, REFERENCES, SELECT, UPDATE, EXECUTE
esquema.OBJETO (Columna1, Columna2,...)

TO Usuario

WITH GRANT OPTION (Puede transferir los permisos)

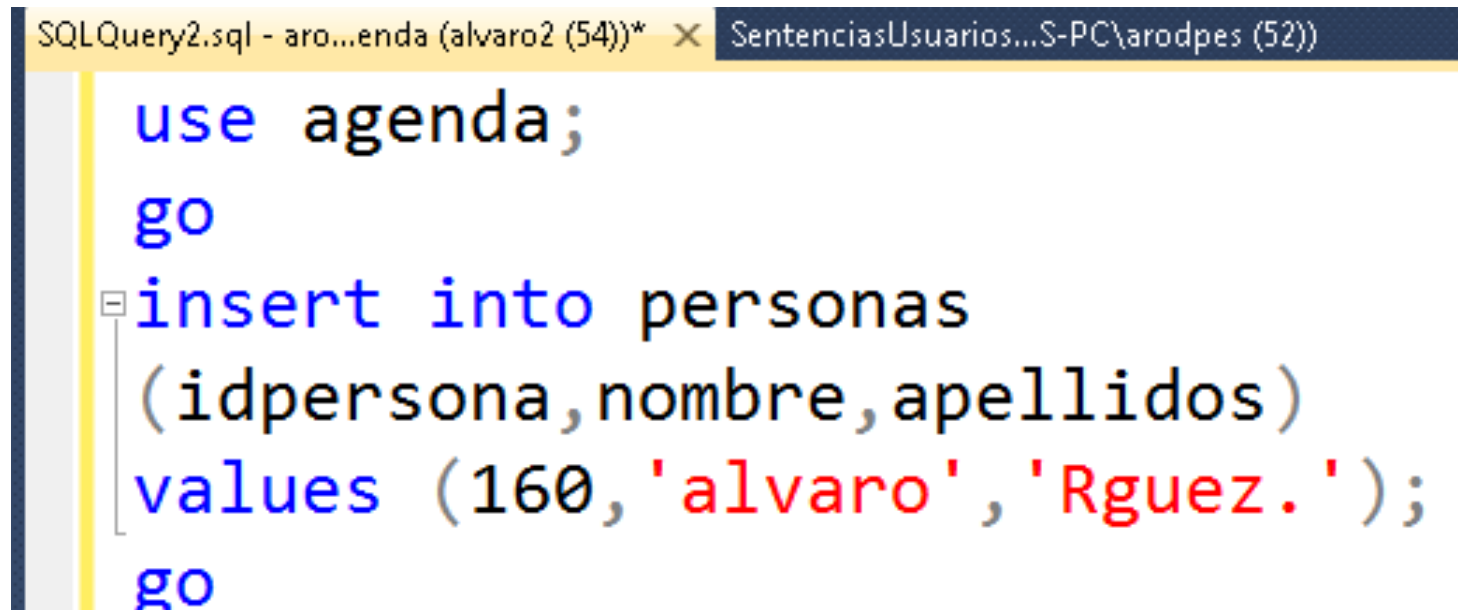
**Dar
permiso**

```
use agenda;
```

```
go
```

```
grant insert on personas to alvaro2;
```

```
go
```



The screenshot shows a SQL query editor window with two tabs: 'SQLQuery2.sql - aro...enda (alvaro2 (54))*' and 'SentenciasUsuarios...S-PC\arodpes (52)'. The script in the editor is as follows:

```
use agenda;  
go  
insert into personas  
  (idpersona,nombre,apellidos)  
values (160,'alvaro','Rguez.');
```

DENY ALL/CREATE, DELETE, INSERT, REFERENCES, SELECT, UPDATE, EXECUTE
esquema.OBJETO (Columna1, Columna2,...)

TO Usuario

WITH GRANT OPTION (Puede transferir los permisos)

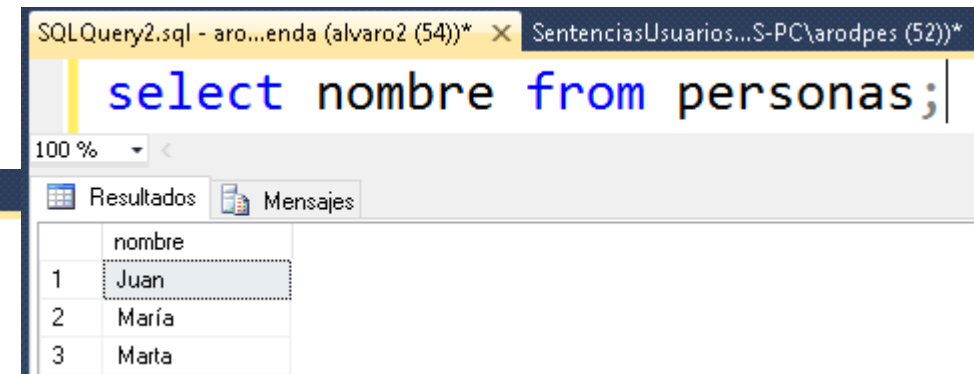
**Denegar
permiso**

```
use agenda;
```

```
go
```

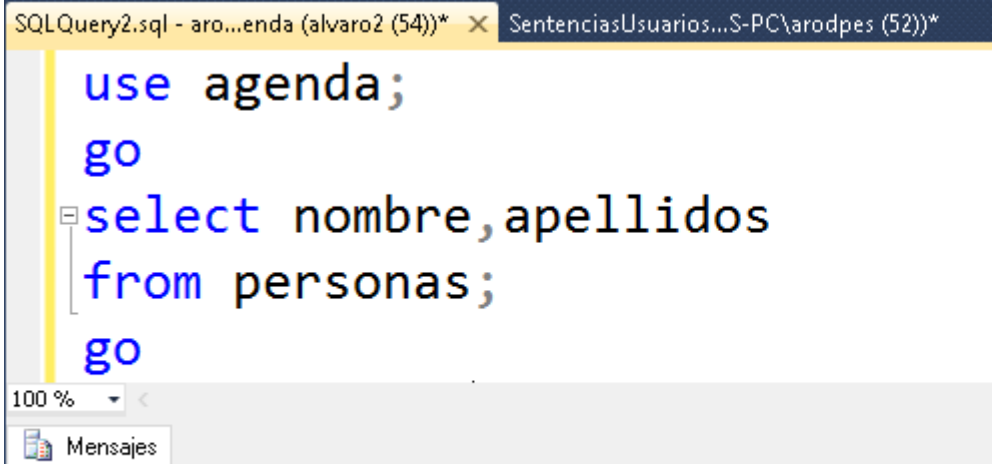
```
deny select on personas(apellidos) to alvaro2;
```

```
go
```



The screenshot shows two windows from SQL Server Enterprise Manager. The top window, titled 'SQLQuery2.sql - aro...enda (alvaro2 (54))*', contains the SQL query: `select nombre from personas;`. The bottom window, titled 'SentenciasUsuarios...S-PC\arodpes (52))*', shows the 'Resultados' (Results) tab with a table of data. The table has two columns: 'nombre' and an index column. The data rows are: 1 Juan, 2 María, and 3 Marta.

	nombre
1	Juan
2	María
3	Marta



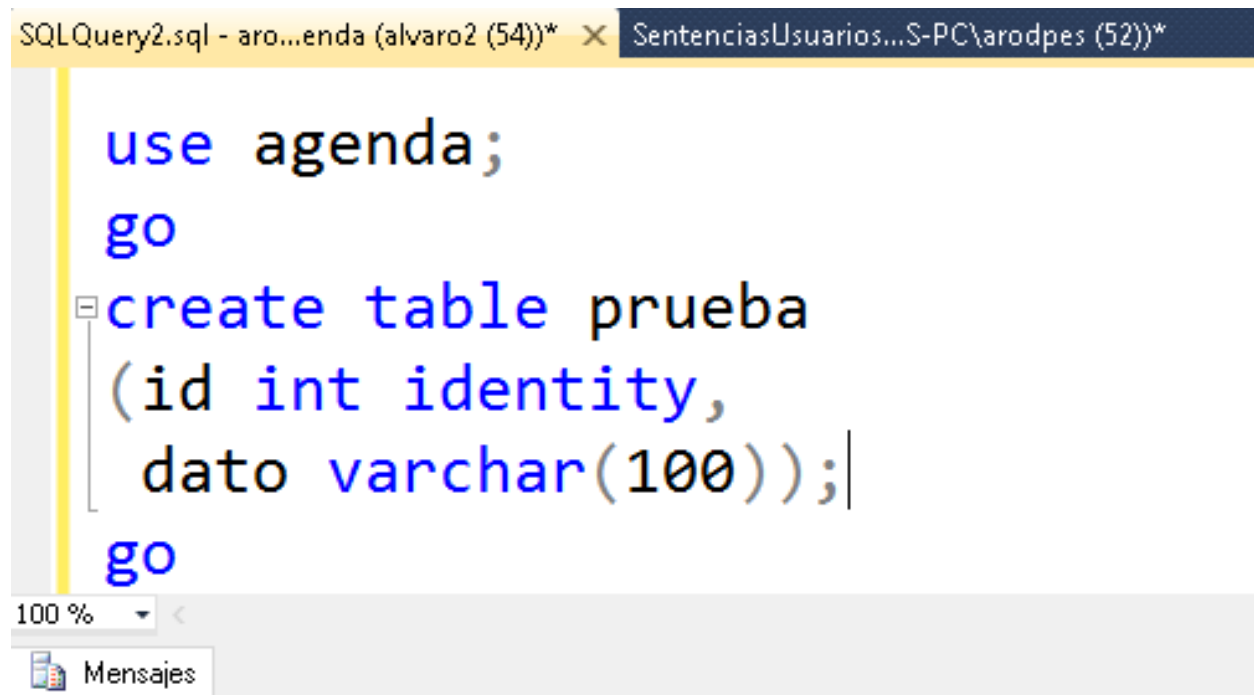
The screenshot shows two windows from SQL Server Enterprise Manager. The top window, titled 'SQLQuery2.sql - aro...enda (alvaro2 (54))*', contains the SQL query: `use agenda;`, `go`, `select nombre,apellidos`, `from personas;`, and `go`. The bottom window, titled 'SentenciasUsuarios...S-PC\arodpes (52))*', shows the 'Mensajes' (Messages) tab with an error message.

Mensajes
Mens. 230, Nivel 14, Estado 1, Línea 17 Se denegó el permiso SELECT en la columna 'apellidos' del objeto 'Personas', base de datos 'agenda', esquema 'dbo'.

REVOKE ALL/CREATE, DELETE, INSERT, REFERENCES, SELECT, UPDATE, EXECUTE
esquema.OBJETO (Columna1, Columna2,...)
TO Usuario

**Quitar
permiso
dado antes**

```
use agenda;  
go  
revoke create table to alvaro2;  
go|
```



The screenshot shows a SQL query editor window with two tabs: 'SQLQuery2.sql - aro...enda (alvaro2 (54))*' and 'SentenciasUsuarios...S-PC\arodpes (52))*'. The active tab contains the following SQL code:

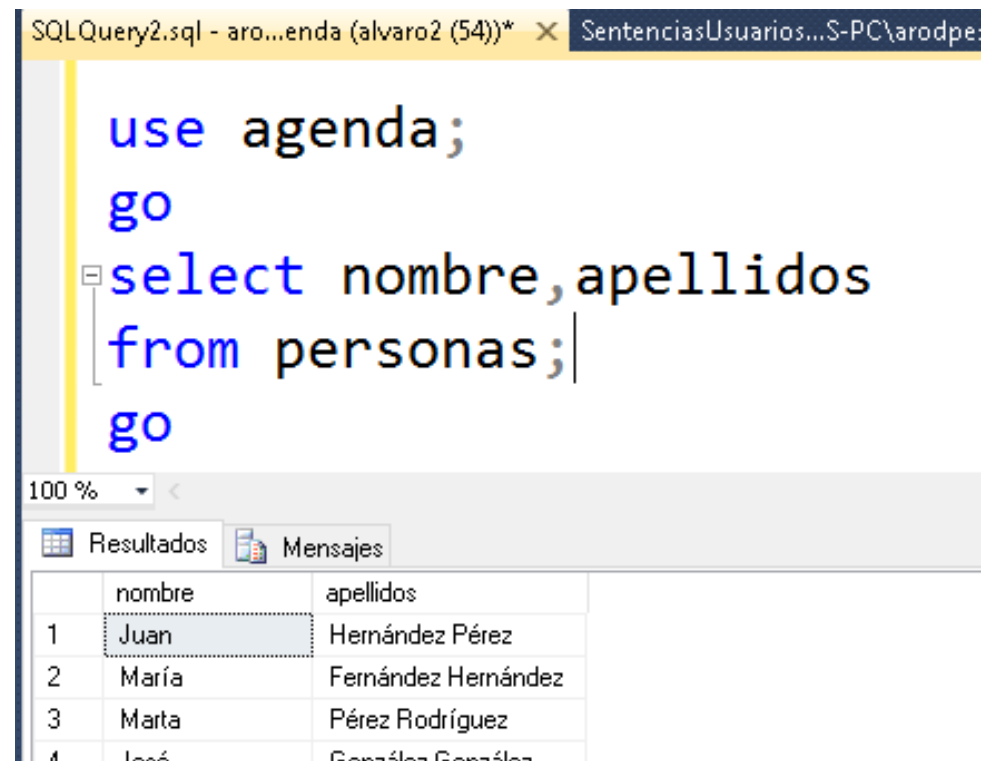
```
use agenda;  
go  
create table prueba  
(id int identity,  
  dato varchar(100));  
go
```

Below the code editor, there is a status bar showing '100 %' and a 'Mensajes' (Messages) icon.

Mens. 262, Nivel 14, Estado 1, Línea 25
Se ha denegado el permiso CREATE TABLE en la base de datos 'agenda'.

```
use agenda;  
go  
revoke select on personas(apellidos) to alvaro2;  
go
```

**También sirve para anular
denegación de permiso**



The screenshot shows a SQL Server Enterprise Manager interface. The top pane displays a query window titled 'SQLQuery2.sql - aro...enda (alvaro2 (54))*'. The query text is:

```
use agenda;  
go  
select nombre,apellidos  
from personas;  
go
```

The bottom pane shows the 'Resultados' (Results) tab, displaying a table with 4 rows and 2 columns: 'nombre' and 'apellidos'. The data is as follows:

	nombre	apellidos
1	Juan	Hernández Pérez
2	María	Fernández Hernández
3	Marta	Pérez Rodríguez
4	Isa	González González