Universidad Nacional de Ingeniería
Instituto de Estudio Superiores
Curso: Bases de Datos II / Docente: Ing. Pablo Argeñal
Guía de Laboratorio: Gestión de Seguridad en BD

Temas a desarrollar:

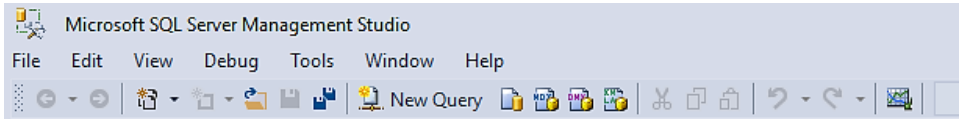
- Creación de Cuentas de acceso y Usuarios
- Concesión de permisos para acceso a objetos de BD a usuarios
- Concesión de permisos para creación de objetos de BD a usuarios
- Roles de Base de Datos
- Creación de Roles
- Roles de aplicación
- Administración por esquemas

Objetivo:

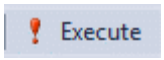
Implementar los diferentes comandos que se pueden utilizar para el acceso y creación de objetos programables en la base de datos.

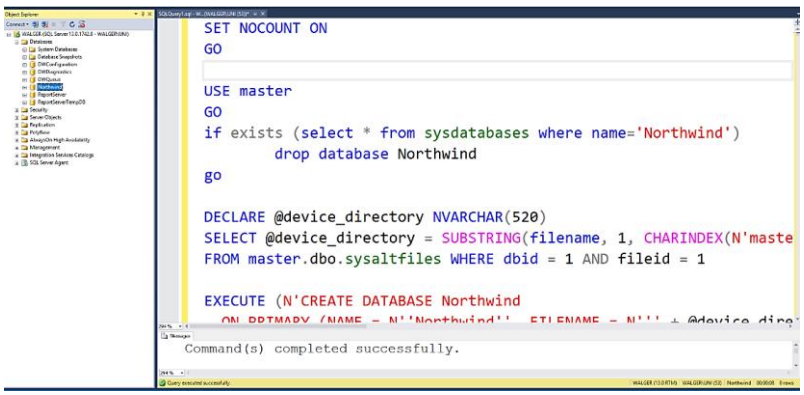
Requerimientos:

- Tener instalado la herramienta de Trabajo: SQL Server 2012 / 2014 / 2016 Versión Full o Express
- Una vez instalada la herramienta, instalar la BD Northwind con la que estaremos realizando las demostraciones, para instalar la BD siga los siguientes pasos:
  - ✓ Descargar el archivo **BD Northwind.txt** que se encuentra en la plataforma del curso en la pestaña Recursos.
  - ✓ En SQL Server en la parte superior, seleccionar New Query para abrir una consola de trabajo.



  - ✓ Pegar el código del archivo **BD Northwind.txt** en la consola y Ejecutar





Creación de Cuenta SQL y Cuenta Windows:

En SQL Server, los usuarios de la BD están asociados a una cuenta de acceso al servidor o login que bien podrá ser una cuenta SQL o cuenta de Windows. Las cuentas SQL estarán restringidas por usuario y password mientras que las cuentas de Windows podrán ser administradas mediante directorio activo y estarán supeditadas a un dominio, ambos tipos de cuenta inician el acceso de conexión con permisos mínimos.

```
Create login Acceso with password = 'sistemas123' -- Creación de Cuenta SQL
Create login [Servidor\UNI] from Windows -- Creación de Cuenta de Windows donde

 -- servidor es el dominio y UNI la cuenta de Windows
```

Una vez creada la cuenta, habrá que asignarle o crearle un usuario de BD para otorgarle el permiso de conexión, dicho usuario por cuestiones de seguridad inicia el acceso a la BD con privilegios mínimos al igual que las cuentas de acceso al servidor. Creación de usuario:

```
Create user Juan from login Acceso
```

Desarrollar una aplicación utilizando un enfoque basado en cuenta de usuario de privilegios mínimos constituye una parte importante de una estrategia de defensa exhaustiva contra las amenazas a la seguridad. Dicho enfoque garantiza que los usuarios siguen el principio de los privilegios mínimos y siempre inician sesión con cuentas de usuario limitadas. Las tareas administrativas se realizan utilizando roles fijos del servidor y el uso del rol fijo del servidor sysadmin será restringido.

Concesión de permisos para acceso a objetos de BD a usuarios

Las bases de datos pueden contener objetos como tablas, procedimientos, funciones entre otros, se puede conceder permisos de forma explícita para que los usuarios tengan acceso a ellos. Cada objeto susceptible de protegerse, tiene permisos que se pueden otorgar a una entidad de seguridad mediante instrucciones de permiso.

Para administrar los permisos de acceso a los objetos creados se utilizan básicamente los comandos DCL (Data Control Language) lenguaje de control de datos.

```
Grant -- Concede de acceso
Deny -- Denegación de acceso
Revoke -- Revocación de concesión o Denegación
```

Para realizar los Ejercicios Guiados deberá ingresar a la herramienta con una cuenta de con privilegios **Sysadmin** y ejecutar en consola los ejercicios.

Ejercicio 1: En este escenario crearemos un inicio de sesión llamado “Sistema”, dándole permiso de conexión en la BD Northwind, le daremos permiso de lectura, escritura y actualizado en todas las tablas.

1. Crear una cuenta de SQL

```
Create login Sistema with password = 'sistemas123'
```

2. Crear un Usuario en la BD Northwind llamado “Digitador” y asignarlo a la cuenta de acceso Sistema.

```
use Northwind
go
Create User Digitador from Login Sistema
```

3. Permiso de Lectura, escritura y actualizado en todas las tablas.

```
Grant select, insert, update on Database:: Northwind to Digitador
```

4. Acceda con la cuenta Sistema y verifique los permisos concedidos

Ejercicio 2: En este escenario revocaremos los permisos concedidos en el Ejercicio guiado 1 y solamente le daremos permiso de lectura en la tabla: Customers y Orders

1. Revocando los permisos concedidos:

```
Revoke select, insert, update on Database:: Northwind to Digitador
```

2. Asignando los nuevos permisos:

```
Grant select on Customers to Digitador
Grant select on Orders to Digitador
```

Otra forma de plantearlo:

```
Grant select on Object::Customers to Digitador
Grant select on Object:: Orders to Digitador
```

3. Para verificar los permisos del usuario en la BD.

```
use Northwind
go
sp_helprotect null, Digitador
```

4. Resultado de la consola al ejecutar el procedimiento `sp_helprotect`

Results | Messages

	Owner	Object	Grantee	Grantor	ProtectType	Action	Column
1	dbo	Customers	Digitador	dbo	Grant	Select	(All+New)
2	dbo	Orders	Digitador	dbo	Grant	Select	(All+New)
3	.	.	Digitador	dbo	Grant	CONNECT	.

Ejercicio 3: Siguiendo el escenario del ejercicio anterior, le daremos permisos de actualización en la tabla empleado.

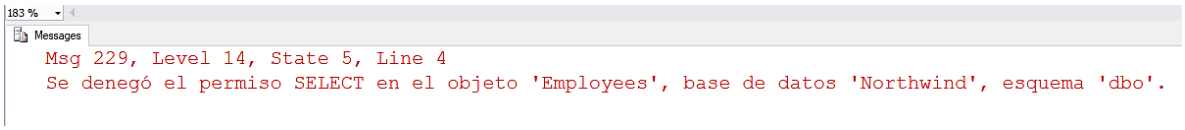
1. Permiso de Actualización en la tabla Empleado

   ```
   Grant update on Employees to Digitador
   ```

2. Ingrese con la Cuenta Sistema al gestor y ejecute la siguiente actualización en la tabla Employees:

   ```
   use Northwind
   go
   update Employees set Country = 'Nicaragua' where EmployeeID = 2
   ```

3. La herramienta mandará el siguiente error:

   Esto se debe porque no tiene permiso de selección en la tabla Employees, esto le impide ejecutar el comando `where` para realizar el filtro y actualizar el registro, para que finalmente pueda ejecutarlo entonces se le debe conceder el permiso de selección.

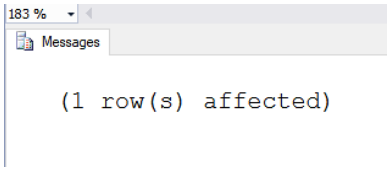
4. Concediendo permiso de selección en la tabla Employees:

   ```
   Grant select on Employees to Digitador
   ```

5. Ejecutar nuevamente la instrucción de actualizado.

   ```
   use Northwind
   go
   update Employees set Country = 'Nicaragua' where EmployeeID = 2
   ```

6. Confirmación de dato actualizado desde la consola de la cuenta Sistema.

Ejercicio 4: Siguiendo el escenario del ejercicio anterior, concédale permisos de ejecución en el procedimiento almacenado: `[dbo].[CustOrderHist]` y las vistas `[dbo].[Category Sales for 1997], [dbo].[Order Details Extended]`

1. Permiso en el procedimiento almacenado:

   ```
   Grant execute on [dbo].[CustOrderHist] to Digitador
   ```

2. Permiso en las vistas:

   ```
   Grant select on [dbo].[Category Sales for 1997] to Digitador
   Grant select on [dbo].[Order Details Extended] to Digitador
   ```

3. Revisar los permisos concedidos desde la consola de la cuenta sistema. Puede realizar la revocación para verificar que se revocó el permiso.

Propietario de Base de Datos

Cuando un inicio de sesión crea una base de datos, automáticamente se convierte en propietario de la base de datos en caso que no especifique un propietario. Dicho propietario utilizará el usuario dbo para realizar operaciones de las cuales no tendrá restricción. Es importante destacar este elemento dado que también pueden existir propietarios asignados desde el rol de base de datos db_owner, por lo tanto una base de datos puede tener más de un propietario. No se recomienda tener varios propietarios al mismo tiempo dado que pondría en riesgo la seguridad de la base de datos.

Ejercicio 5: Ahora crearemos un login de acceso llamado "Administrador" el cual convertiremos en propietario de la Base de Datos Northwind, esto le permitirá acceder la base de datos y administrar permisos a otros usuarios.

1. Creación del inicio de sesión Administrador

```
Create login Administrador with password = 'maestria2018'
```

2. Asignación de Propietario de la BD

```
use Northwind
go
Execute sp_changedbowner 'Administrador'
```

3. Ejecutar procedimiento para verificar el cambio

```
sp_helpdb Northwind
```

4. Resultado de la ejecución del procedimiento

Results | Messages

	name	db_size	owner	dbid	created	status	compatibility_level
1	Northwind	80.00 MB	Administrador	13	Mar 12 2018	Status=ONLINE, Updateability=READ_WRITE, UserAcc...	130

	name	fileid	filename	filegroup	size	maxsize	growth	usage
1	Northwind	1	C:\Program Files\Microsoft SQL Server\MSSQL13.MSS...	PRIMARY	8192 KB	Unlimited	65536 KB	data only
2	Northwind_log	2	C:\Program Files\Microsoft SQL Server\MSSQL13.MSS...	NULL	73728 KB	2147483648 KB	65536 KB	log only

Se observa en la ejecución del procedimiento que el owner es la entidad Administrador, lo interesante de este caso, es que no necesariamente la cuenta de inicio de sesión tuvo que tener un usuario para ser propietario, sino que directamente se le asigna el permiso.

Todos aquellos usuarios de base de datos con rol de propietario, propietario creador de la base de datos y aquellos inicios de sesión cuyo rol de servidor sea sysadmin, tendrán acceso pleno a todos los objetos de la base de datos utilizando como interfaz el usuario dbo. Tener presente que el usuario dbo[1] estará presente en todas las bases de datos.

[1] Dbo: Database owner – Propietario de Base de Datos

Herencia de Permisos

Ejercicio 6: En este escenario cambiaremos la autorización de propietario de northwind que tiene "Administrador" y se la asignaremos a la cuenta de Windows del sistema con sysadmin. Luego le daremos permisos sobre algunos objetos de la base de datos con la opción de heredar dichos permisos a otros usuarios.

1. Cambio de propietario de la BD Northwind a la cuenta de Windows.

```
use Northwind
go
Execute sp_changedbowner [SERVIDOR\UNI]
```

2. Creando el usuario de Administrador en la BD Northwind

```
use Northwind
go
Create user Principal from login Administrador
```

3. Asignación de Permisos de Selección en las tablas Employees y Customers con permisos de heredar sus permisos a otros usuarios con el comando `with grant option`.

```
Grant select on Customers to Principal with grant option
Grant select on Employees to Principal with grant option
```

   Revoque todos los permisos concedidos al usuario "Digitador", solo deje el permiso de conexión a la BD Northwind. Verifique los permisos concedidos ejecutando el procedimiento almacenado `sp_helprotect null, Digitador`

4. Ingrese a la herramienta con el Inicio de Sesión "Administrador" y conecte la consola con la BD Northwind, ahora la cuenta Administrador trabaja en Northwind con la cuenta de usuario llamada Principal.
5. Desde la cuenta Administrador conceda los permisos heredados al usuario "Digitador" en la BD Northwind

```
use Northwind
go
Grant select on Customers to Digitador
Grant select on Employees to Digitador
```

6. Conectarse con la cuenta Sistema en la BD Northwind y verificar que tiene los permisos concedidos por la cuenta de "Administrador".

Concesión de permisos para acceso a objetos de BD a usuarios

En esta sección trabajaremos los permisos para creación de objetos dentro de la base de datos. Tenemos que tener en cuenta la definición y el uso de los esquemas dentro de las bases de datos en SQL Server.

Los esquemas se definen como el ámbito de un objeto en la BD, a partir del esquema se puede crear los objetos y también se pueden administrar permisos.

Ejercicio 7: En este escenario concederemos permisos para crear objetos básicos como tablas, vista y procedimientos en la BD Northwind.

1. Crearemos un nuevo inicio de sesión llamado “Creador” con los permisos solicitados.

```
Create login Creador with password = 'maestria2018'
go
use Northwind
go
Exec sp_adduser Creador, creador  -- [2]
go
Grant create table to creador
Grant create view to creador
Grant create procedure to creador
```

2. Conectarse con el inicio de sesión “Creador” y conecte la BD Northwind. Dado que el usuario tiene por definición un esquema con su nombre, este podrá crear los objetos bajo dicho esquema. El esquema se crea automáticamente en la base de datos cuando se crea el usuario.

```
use Northwind
go
Create table creador.Persona(id int)
go
Create view creador.vistaClientes
as
Select * from Customers
go
Create procedure creador.Noclientes
as
Select count(*) from customers as Cantidad
```

3. Verificar en el explorador de objetos que los objetos han sido creados por el usuario.

[2] Sp_adduser: Procedimiento almacenado en master para agregar usuarios a bases de datos. Los nombres de usuarios pueden tener el mismo nombre que el inicio de sesión.

Ejercicio 8: Para esta práctica crearemos un esquema nuevo dentro de la Base de datos Northwind y asignaremos al usuario "Creador" como propietario de dicho esquema. Dado que tiene permisos de creación de tablas, vistas y procedimientos, podrá realizar objetos bajo este esquema.

1. Desde la cuenta de Windows con permisos sysadmin crearemos el esquema con nombre Reporte en la base de datos Northwind.

```
use Northwind
go
Create schema Reporte
```

2. Ahora asignaremos a la cuenta de usuario Creador como propietario del Esquema Reporte, esto le permitirá utilizar dicho esquema para crear objetos.

```
USE [Northwind]
GO
ALTER AUTHORIZATION ON SCHEMA::[Reporte] TO [creador][3]
GO
```

3. Desde la cuenta de usuario llamada Creador crearemos una vista utilizando el esquema Reporte.

```
Create view Reporte.ordenesxcliente
as
Select CustomerID,
count(*)  as Cantidad
from orders
Group by
CustomerID
```

Un dato interesante es que el usuario tiene permisos para crear la vista utilizando los diferentes objetos o tablas de la base de datos, pero no significa que pueda acceder a ellos. Si solamente ejecutamos la parte de la consulta, el gestor bloqueará debido a que no se tiene el permiso de selección en la tabla customers al igual si ejecutamos la selección de la vista creada. En ambos casos el gestor mandará el siguiente mensaje:

```
Messages
Msg 229, Level 14, State 5, Line 4
Se denegó el permiso SELECT en el objeto 'Orders', base de datos 'Northwind', esquema 'dbo'.
```

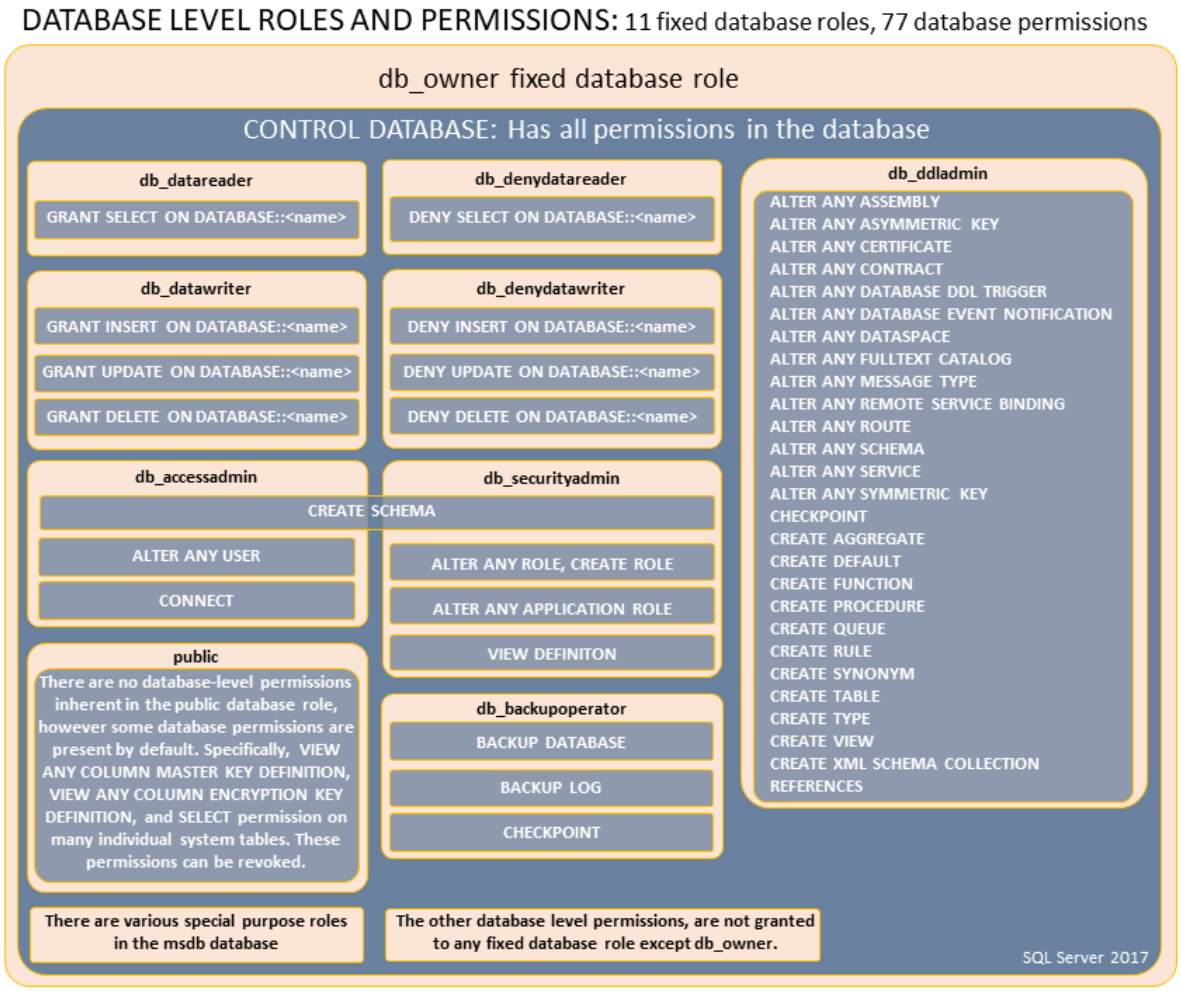
La seguridad en los gestores de bases de datos es muy compleja en algunos casos, se pueden visualizar los diferentes tipos de permisos que se pueden dar sobre objetos en el siguiente enlace.

[3] Directamente podemos crear el propietario en la creación del esquema.

```
Create schema Reporte authorization Creador
```

Roles de Bases de Datos

En la herramienta de estudio existen diferentes roles de bases de datos ya establecidos desde el momento de creación de la base de datos, estos roles no se pueden modificar pero si podemos personalizar la forma en que los usuarios harán uso de ellos, en la siguiente imagen se detallan los comandos que pueden ejecutar dichos roles.



[4]

La administración por roles ayuda a tener una mejor organización en cuento a las políticas de acceso seguro, creando un esquema simple y dinámico el cual puede ser asignado a todas las entidades que necesitan realizar una conexión al gestor de bases de datos.

[4] Imagen recopilada: Roles de Nivel de Base de Datos
https://docs.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles

En la tabla siguiente se muestran los roles fijos de base de datos y sus funcionalidades. Estos roles existen en todas las bases de datos. A excepción del rol de base de datos public, no se pueden cambiar los permisos asignados a los roles fijos de base de datos.

Nombre del rol fijo de base de datos	Descripción
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.[5]

[5] Tabla recopilada: Roles de Nivel de Base de Datos
https://docs.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles

Realizaremos demostraciones con algunos roles de BD

Ejercicio 9: En la consola con una cuenta sysadmin, asignar el rol **db_ddladmin** a la cuenta "creador" para realizar tareas de creación de objetos dentro de la base de datos.

1. Revocaremos todos los permisos que se le han concedido al usuario "creador" en la BD Northwind.

```
use Northwind
go
sp_helprotect null, creador
```

Results | Messages

	Owner	Object	Grantee	Grantor	ProtectType	Action	Column
1	.	.	creador	dbo	Grant	CONNECT	.
2	.	.	creador	dbo	Grant	Create Procedure	.
3	.	.	creador	dbo	Grant	Create Table	.
4	.	.	creador	dbo	Grant	Create View	.

2. Otorgar el rol de DB db_ddladmin

```
use Northwind
sp_addrolemember db_ddladmin, creador
```

3. Abrir una consola de trabajo con la cuenta de usuario "creador" en la BD Northwind y comprobar los permisos que han sido asignados con el rol de base de datos.

```
use northwind
go

Create table dbo.Prueba(id int)
```

4. Comprobar que el usuario no tiene permiso al acceso de registros a la tabla creada por el mismo.

```
Select * from Prueba
```

Messages

```
Msg 229, Level 14, State 5, Line 5
Se denegó el permiso SELECT en el objeto 'Prueba', base de datos 'Northwind', esquema 'dbo'.
```

Nota: Observar que aunque el usuario tiene permisos de creación de tablas, este no podrá acceder a los registros aunque la tabla sea creada por el mismo. Los permisos concedidos por db_ddladmin le permitirán ejecutar los comandos Alter y Drop en todos los objetos de la BD.

5. Personalizar los permisos concedidos al usuario creador negando la creación de vistas.

```
Deny create view to Creador
```

6. Confirmar que el permiso de creación de vistas ha sido denegado aunque este contemple el Rol de Base de Datos db_ddladmin

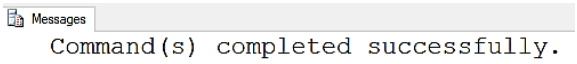
```
Create view creador.datosCliente
as
Select * from Customers
```

7. Revocar la negación al permiso de vistas

```
Revoke create view to Creador
```

8. Confirmar la creación de la vista dado que la Denegación ha sido revocada.

```
Create view creador.datosCliente
as
Select * from Customers
```



Ejercicio 10: Revocar el rol de base de datos db_ddladmin al usuario "Creador", conceder el rol de base de datos db_datareader que le dará permisos de lectura en todas las tablas de la base de datos.

1. Eliminar el rol al usuario "Creador"

```
use Northwind
go
sp_droprolemember db_ddladmin, creador
go
sp_addrolemember db_datareader, creador
```

2. Comprobar que el usuario "Creador" tiene permisos de selección en todas las tablas.
3. Eliminar los permisos de selección en la tabla Employees y Region

```
Deny Select on Employees to Creador
Deny select on Region to Creador
```

4. Comprobar que los permisos de selección han sido denegados.
5. Revisar los permisos y denegaciones asignadas al usuario.

```
sp_helprotect null, creador
```

	Owner	Object	Grantee	Grantor	ProtectType	Action	Column
1	dbo	Employees	creador	dbo	Deny	Select	(All+New)
2	dbo	Region	creador	dbo	Deny	Select	(All+New)
3	.	.	creador	dbo	Grant	CONNECT	.
4	.	.	creador	dbo	Grant	Create Procedure	.
5	.	.	creador	dbo	Grant	Create Table	.

```
sp_helplogins creador
```

	LoginName	DBName	UserName	UserOrAlias
1	Creador	Northwind	creador	User
2	Creador	Northwind	db_datareader	MemberOf

Creación de Roles

Ejercicio 10: Desde una cuenta Sysadmin, crear un rol de base de datos en Northwind llamado “Consulta” y asignar los permisos necesarios para visualizar todos los registros de las tablas, vistas y procedimientos almacenados.

1. Creación del Rol de Base de datos

```
Create Role Consulta
```

2. Asignación de permisos

```
Grant select on database:: Northwind to consulta
Grant Execute on database:: Northwind to consulta
```

3. Asignación del Rol “Consulta” al usuario de BD “Creador”

```
Execute sp_addrolemember Consulta, Creador
```

4. Confirmar en la consola de “Creador” que tiene los permisos concedidos por el rol.
5. Revisar los permisos y denegaciones asignadas al usuario.

```
sp_helplogins creador
```

	LoginName	SID	DefDBName	DefLangName	AUser	ARemote
1	Creador	0x28606A3537C0294C87F4D2F401F7F1A6	master	Español	yes	no

	LoginName	DBName	UserName	UserOrAlias
1	Creador	Northwind	Consulta	MemberOf
2	Creador	Northwind	creador	User
3	Creador	Northwind	db_datareader	MemberOf

Al ejecutar el procedimiento almacenado `sp_helplogins creador` se observa que el usuario “Creador” tiene membrecía con dos roles de base de datos.

6. Dado que el rol de base de datos “Consulta” tiene todos los permisos de acceso a lectura de todas las tablas, no es necesario que tenga asignado el rol db_datareader.

```
Use Northwind
go
Execute sp_droprolemember Consulta, Creador
```

Dado la distintas de formas acceso a los objetos de la BD procurar la no redundancia o duplicado de permisos como buena práctica de seguridad.

Roles de Aplicación

Un rol de aplicación es una entidad de seguridad de base de datos que permite que una aplicación se ejecute con sus propios permisos de usuario. Puede utilizar los roles de aplicación para permitir el acceso a datos específicos únicamente a aquellos usuarios que se conecten a través de una aplicación concreta. A diferencia de los roles de base de datos, los roles de aplicación no contienen miembros y están inactivos de manera predeterminada. Los roles de aplicación funcionan con ambos modos de autenticación. Los roles de aplicación se habilitan empleando **sp_setapprole**, que requiere una contraseña.

Ejercicio 11: Creación de un Rol de aplicación con permisos únicamente para modificar seleccionar, insertar y modificar la tabla **`[dbo].[Order Details]`** dicha tabla contiene los detalles de las órdenes realizadas por los usuarios, una vez ingresada no se puede modificar.

1. Desde una cuenta Sysadmin crearemos el rol de aplicación.

```
Create application role Actualiza_Detalle_Orden
with password = 'maestria2018'
```

2. Asignación de Permisos al rol de aplicación.

```
Grant select on [dbo].[Order Details] to Actualiza_Detalle_Orden
Grant update on [dbo].[Order Details] to Actualiza_Detalle_Orden
Grant insert on [dbo].[Order Details] to Actualiza_Detalle_Orden
```

3. Ingrese a la consola desde la cuenta “Creador” y active el rol

```
Execute sp_setapprole
Actualiza_Detalle_orden, 'maestria2018'
```

4. Asignar nuevos permisos al rol de aplicación y confirmar que el usuario puede ejecutarlos en tiempo real.

```
Grant select on [dbo].[Orders] to  Actualiza_Detalle_Orden
```

5. Confirmar que el usuario al activar el rol de aplicación suspende temporalmente todos los permisos que tiene asignado y obtiene únicamente los permisos concedidos por el rol de aplicación.

6. Para cancelar el rol de aplicación

```
sp_unsetapprole
```

7. Otra opción es desconectar el usuario del sistema y vuelva a conectar, observará que sus permisos anteriores han regresado.

Administración por Esquemas

Adicionalmente a los roles y permisos a discreción, tenemos la opción de administrar los accesos mediante los esquemas de la base de datos, esta forma de acceso es recomendable cuando tenemos objetos que pertenecen a un solo ámbito o contexto de trabajo, estará en dependencia del diseño de la base de datos y de como se concibe la política de acceso al sistema.

Para nuestro ejemplo utilizaremos la base de datos AdventureWorks2012 que está desarrollada bajo esquemas.

Ejercicio 12: Crear un usuario en la base de datos AdventureWorks2012 al inicio de sesión llamado "Creador", asignarle permiso de lectura en el esquema de "Production" y permisos de ejecución de procedimientos almacenados en el esquema dbo.

1. Creación del usuario en la Base de Datos AdventureWorks

```
use AdventureWorks2012
go
sp_adduser Creador, visitante
```

2. Asignación de permisos en el esquema de producción

```
Grant select on Schema :: Production to Visitante
```

3. Asignación de permisos sobre los procedimiento almacenados en el esquema

```
Grant execute on Schema :: dbo to Visitante
```

4. Acceder con la cuenta "Creador" a la base de datos AdventureWorks2012 y comprobar los permisos concedidos en base al esquema seleccionado.

5. Denegar el permiso de selección en la tabla products

```
Deny select on production.Product to Visitante
```

6. Al igual que la administración por roles, si deseamos denegar un acceso concedido ya sea por rol o esquema, entonces aplicamos el comando `Deny`

7. Revocar los permisos concedidos por el esquema y revocar la negación en la tabla product

```
Revoke select on Schema :: Production to Visitante
Revoke execute on Schema :: dbo to Visitante

Revoke select on production.Product to Visitante
```

8. Revisar en la cuenta "Creador" que el usuario ya no cuenta con los permisos.

ORIENTACIÓN DE EJERCICIOS A REALIZAR

- Descargar el archivo de nombre “Archivos BD” que se encuentra en la pestaña recursos de la primera semana en la plataforma.
- El archivo contiene una nueva versión de la BD Northwind por lo que tendrá que sustituirla en caso que la tenga instalada.
- Listar los usuarios huérfanos de la base de datos.
- Presentar mediante procedimiento o consulta descubra las concesiones y negaciones que tienen dichos usuarios huérfanos.
- Revocar todas las concesiones y negaciones que tienen los usuarios huérfanos de la BD.
- Reorganizar los objetos de la BD bajo los siguientes esquemas:

Esquema	Propietario	Objetos
Sales	dbo	[dbo].[Orders] [dbo].[Order Details]
Customer	dbo	[dbo].[Customers] [dbo].[CustomerCustomerDemo] [dbo].[CustomerDemographics]
Supplier	ObjetosAdmin	[dbo].[Suppliers] [dbo].[Products] [dbo].[Shippers] [dbo].[Territories] [dbo].[Region]
Product	ObjetosAdmin	[dbo].[Products] [dbo].[Categories]
Person	ObjetosAdmin	[dbo].[Employees] [dbo].[EmployeeTerritories]
Procedures	ObjetosAdmin	[dbo].[CustOrderHist] [dbo].[CustOrdersDetail] [dbo].[CustOrdersOrders] [dbo].[Employee Sales by Country] [dbo].[Sales by Year] [dbo].[SalesByCategory] [dbo].[Ten Most Expensive Products]

- Crear un rol de Base de datos en Northwind llamado “Auditoria” con las siguientes asignaciones:
    - ✓ Permisos de lectura en todos los esquemas de la Base de datos.
    - ✓ Permisos de ejecución en todos los procedimientos almacenados.
    - ✓ Permisos de creación de vista en el nuevo esquema Sales.

- Crear un inicio de sesión llamado “Auditor” exigiendo el cambio de contraseña para la primera conexión.
- Crear un usuario dentro de northwind llamado “Revisor” y asignarlo al inicio de sesión “Auditor” con el rol “Auditoria”.

Considere un escenario donde se necesita crear un acceso para realizar operaciones de gestión de pedidos, con las siguientes condiciones:

- ✓ Ingresar órdenes con detalles
- ✓ Visualizar órdenes
- ✓ Buscar y visualizar clientes potenciales para gestionar órdenes.

Proponga y configure el acceso que cumpla con las condiciones, considere un ambiente multi usuario.

Establecer Falso o Verdadero:

(En ambos casos, explique o demuestre el procedimiento para validar su respuesta)

- Los usuarios que han recibido permisos para crear tablas, pueden crear tablas en los esquemas de su propiedad.
- Los usuarios al ser creados tienen por defecto el rol public.
- Se pueden asignar permisos al rol de base de datos public.
- Los usuarios con With grant Option no pueden heredar permisos a usuarios con rol db_datareader.
- Un inicio de sesión puede tener más de un usuario siempre y cuando tenga un nombre.distino en la misma base de datos.
- El rol de Servidor Datawriter solo permite permisos de escritura y actualizado.
- Un esquema puede tener más de un propietario.
- Se puede borrar un usuario cuando no propietario de un esquema.
- El rol de BD db_BackupOperator no permite realizar backup del log de transacciones.
- El rol db_ddladmin permite le permite al usuario crear vistas con objetos a los que no tiene permiso de acceso.
- El rol db_owner no puede crear backup de la base de datos.
- Para borrar los permisos de un usuario que ha heredado a otros usuarios se utiliza CASCADE.
- Se puede denegar el permiso de selección a un objeto que es propiedad del usuario.
- Db_SecurityAdmin puede denegar y conceder accesos a todos los usuarios de la base de

datos.

- Cuando se agrega un objeto a un esquema que es propiedad del usuario, este podrá borrarlo o modificarlo.
- Db_Securityadmin puede crear usuarios y asignarlos a cuentas de acceso.
- Pueden existir usuarios sin login
- SetupAdmin permite administrar SQL Server Agent
- Securityadmin puede ingresar a todas las bases de datos
- Securityadmin puede borrar esquemas y crear nuevos esquemas
- Securityadmin puede cambiar los permisos de propiedad de un esquema (Transferirlos)
- Bulkadmin puede administrar la función Bulk Insert
- Al revocarle los permisos de un usuario no se revokan los heredados
- db_owner puede administrar dispositivos de almacenamiento sp_addumpdevice