UNIVERSIDAD GERARDO BARRIOS

SM-CRU

Datos Generales	
Facultad	Ciencia y Tecnología
Asignatura	Administración de Base de Datos II
Docentes	Beatriz Amaya, Beatriz Zuniga, Gisela Espinoza Oscar Torres
No. de Unidad	2. SEGURIDAD DE LOS DATOS
Contenido a desarrollar	2.4 Seguridad de las bases de datos en entornos locales

Introduccion

Es importante desarrollar una política de seguridad orientada a proteger todos los activos de la organización. Un ABD es el responsable de definir esta política de seguridad en donde debe de establecer medidas para proteger las bases de datos de destrucción accidental o maliciosa o daños a la infraestructura de la base de datos. Además, si la organización es muy grande cada base de datos puede tener un administrador, denominado administrador de seguridad, que es responsable de implementar y mantener la política de seguridad de la base de datos. En esta sesión se pretende brindar los fundamentos teóricos y practicas sobre herramientas como keylogger, gestión de seguridad orientada a copias de respaldo, usuarios, roles y privilegios de las base de datos con el fin de establecer mecanismos de seguridad acordes a las exigencias tecnológicas del mundo actual.

Seguridad de las bases de datos en entornos locales

¿Qué es un keylogger?

¿Qué es una copia de respaldo de una base de datos?

¿Como crear sesiones de usuarios con privilegios en un DBMS?

Objetivo de la clase: Comprender los conceptos, herramientas e instrucciones de la seguridad de las bases de datos en entornos locales.

Keylogger:

Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado. Este software se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note. Además, un keylogger almacena los datos de forma local en el ordenador infectado y, en caso de que forme parte de un ataque mayor, permite que el atacante tenga acceso remoto al equipo de la víctima y registre la información en otro equipo. Aunque el término keylogger se usa, normalmente, para nombrar este tipo de herramienta maliciosas, existen también herramientas de vigilancia legítimas que usan las autoridades policiales y que funcionan de la misma forma que los keyloggers.

Entre los keyloggers mas comunes se tienen

1) **Keylogger Free : E**s capaz de registrar las pulsaciones de teclas, los datos del portapapeles y las direcciones del sitio sin la captura de pantalla, lo que está bien para las personas que no desean hacer capturas de pantalla. Hay un par de configuraciones de invisibilidad como la tecla de acceso directo oculto (por defecto, Ctrl + Shift + Alt + U), eliminando accesos directos del menú de inicio y la lista de desinstalación.

2) REFOG Keylogger Free: Es una compañía muy popular que ofrece una gama de Keylogger para el hogar, empresas y compañías, pero

desafortunadamente la versión gratuita es muy básica ya que la mayoría de las funciones importantes se han desactivado. La versión gratuita de REFOG keylogger solo puede controlar las pulsaciones de teclas, los sitios web visitados, el portapapeles, los programas ejecutados y las actividades de la computadora.

3) Revealer Keylogger Free: Es la segunda herramienta de supervisión más descargada en CNET Download.com. Es muy sensible y ligero en el uso del sistema. Puede grabar pulsaciones de teclas, admite múltiples idiomas, configuraciones de inicio, capacidad de ejecución con privilegios elevados, compatibilidad con teclas de acceso directo (por defecto, Ctrl + Alt + F9) y limpieza automática de registros, pero la captura de pantalla, opciones de entrega automatizada y características ocultas adicionales están deshabilitadas.

4) Real Free Keylogger: Es este software se define una contraseña para proteger el programa, de modo que solo tú puedas acceder a la configuración y ver los registros. Puedes configurar una tecla de acceso directo (por defecto Ctrl + Alt + X) para iniciar el programa cuando se está ejecutando en modo sigiloso. Viene con un programador para iniciar el registro automáticamente y los archivos de registro se pueden exportar como un archivo HTML.

Copias de respaldo: Las copias de respaldo proporcionan una importante solución para proteger datos críticos que están almacenados en bases de datos. Y para minimizar el riego de pérdida de datos, usted necesita asegurarse de que respalda sus bases de datos regularmente tomando en consideración los cambios aplicados a sus datos. Es una buena práctica probar sus copias de seguridad restaurando archivos de copias de seguridad al azar a un ambiente de pruebas y verificar que los archivos no estén corruptos. Además es ideal que las copias de respaldo se realicen diariamente para evitar perdida de información, dinero, clientes, etc.

Con las copias de respaldo si se dad un desastre normal de pérdida de datos, el DBA puede beneficiarse de copias de seguridad si hay un fallo de medios en uno de los discos o cualquier daño de hardware, un borrado o eliminación accidental aplicados por uno de los usuarios o usualmente copiar los datos desde un servidor a otro. Antes de programar el trabajo de copias de seguridad, se necesita tener una estimación de cuánto espacio de disco será usado por la copia de seguridad completa de la base de datos. También, usted necesita tener una estimación inicial del incremento en el tamaño de la base de datos, porque cuando este se incrementa las copias de seguridad completas requerirán más espacio de almacenamiento. Es mejor primero estimar cuándo espacio de disco requiere para su copia de seguridad completa. La operación de respaldo copia los datos en la base de datos al archivo de respaldo, este contiene sólo el espacio de datos usado sólo en su base de datos y no en la que no está siendo usada. El cual es usualmente más pequeño que el tamaño de la base de datos. Los DBMS ofrecen muchas formas de copias de respaldo, lo cual depende del modelo de recuperación de la base de datos, un DBA puede usar asistentes de los diferentes DBMS o Instrucciones que permitan realizar adecuadamente esta actividad. Como administrador de bases de datos, usted debería asegurarse de que cada base de datos es respaldada exitosamente y a tiempo.

¿Qué debería hacerse para asegurar que una base de datos es respaldada completamente a tiempo en tales casos?

Una idea posible para recuperarse de problemas de espacio y tiempo con respaldos de bases de datos es dividir la copia de seguridad en múltiples archivos y reducir el tiempo necesario para realizar las copias de seguridad y usar el espacio disponible en múltiples dispositivos. Lo que hace a este proceso más rápido es que usted tiene la habilidad de escribir a múltiples archivos al mismo tiempo y por tanto dividir la carga de trabajo usando múltiples hilos, así como teniendo archivos más pequeños que pueden ser movido a través de la

red o copiados al medio de respaldo. Otra ventaja de dividir la copia de seguridad en múltiples archivos es obtener un mejor rendimiento I/O. Una buena práctica es probar la copia de respaldo o múltiples archivos para verificar cuán rápido usted puede hacer que sus copias de seguridad funcionen y que es más fácil copiarla a una ruta de red o un dispositivo.

Crear sesiones de usuarios con privilegios en un DBMS

Un usuario es un nombre definido en la base de datos que puede conectarse a ella y acceder a determinada información según los permisos que tenga asignados por el administrador El objetivo de la creación de usuarios es establecer una cuenta segura y útil, que tenga los privilegios adecuados y los valores por defecto apropiados. Existen usuarios DBA, usuarios operadores y usuarios finales, este último puede ser interno o externo a la institución. Un usuario DBA tendrá asignado todos los privilegios de la base de datos, es el responsable de crear y asignar los privilegios a los demás usuarios, es decir es el que planifica la política de seguridad de las bases de datos.

Roles:

Los roles son los conjuntos de permisos. Estos conjuntos existen a tres niveles distintos: servidor, base de datos y aplicación. Los roles permiten agrupar los derechos y gestionar más fácilmente los diferentes usuarios y las conexiones. Siempre es preferible asignar los derechos a los roles y posteriormente asignar los roles a los usuarios. Con una estructura como esta, la adición y la modificación de permisos o de usuarios son más sencillas.

Nota : Si no está familiarizado con SQL Server, puede resultarle difícil determinar qué tipo de usuario quiere crear. En primer lugar, pregúntese lo siguiente: ¿tiene credenciales de inicio de sesión la persona o el grupo que necesita acceder a la base de datos? Los inicios de sesión en la base de datos maestra son habituales para las personas que administran SQL Server y para las personas que necesitan acceder a la mayoría de las bases de datos en la

instancia de SQL Server (o a todas). En este caso, creará un **usuario SQL con inicio de sesión**. El usuario de la base de datos es la identidad del inicio de sesión cuando está conectado a una base de datos. El usuario de la base de datos puede utilizar el mismo nombre que el inicio de sesión, pero no es necesario. En este tema se supone que ya existe un inicio de sesión en SQL Server. Una forma de crear un inicio de sesión es usando la siguiente instrucción en sql server:

create login entrada with password= '123'

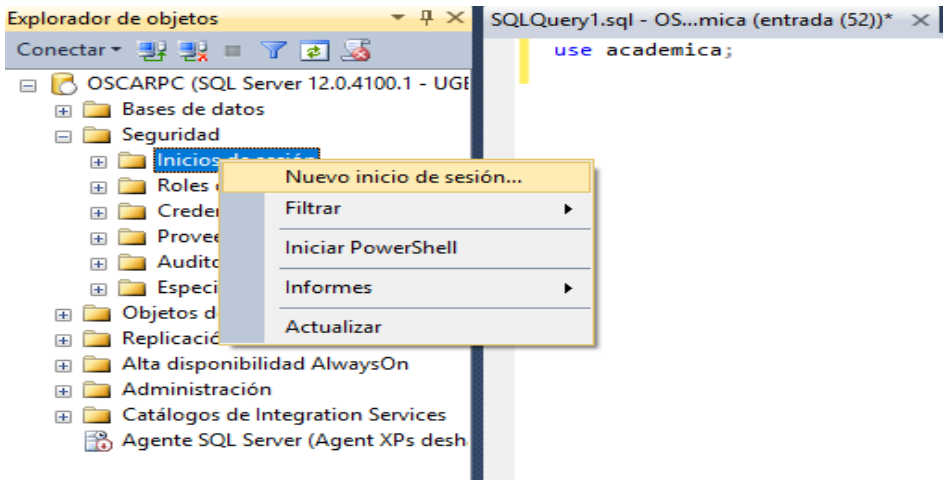
En esta sesión se desarrollara la siguiente practica usando el asistente de SQL Server

Practica: Crear sesiones, usuarios y asignar privilegios.

Requerimiento: SQL Server 2014 management studio, herramienta que deberá de instalar con anticipación y una vez instalado siga los siguientes pasos:

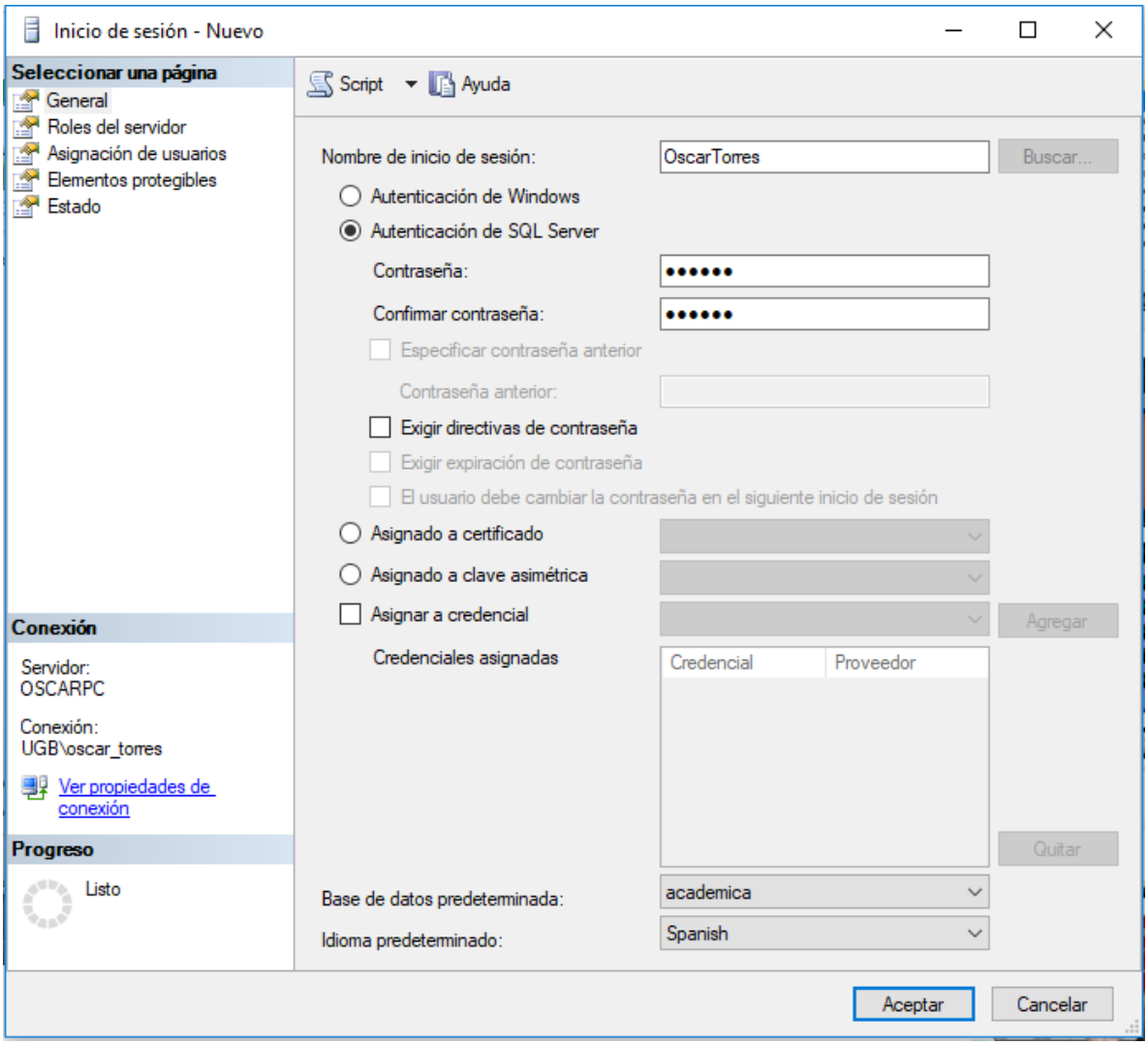
Paso 0: Cargue la herramienta y inicie sesión con el usuario principal.

Paso 1: Seleccione seguridad y luego de click derecho en inicio de sesión, después de click en "nuevo inicio de sesión", así como se observa en la siguiente imagen:

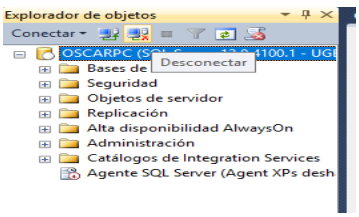


Paso 2: Escriba nombre de inicio de sesión, seleccione autenticación en SQL Server, escriba la contraseña, quite el chequeo "elegir directiva de

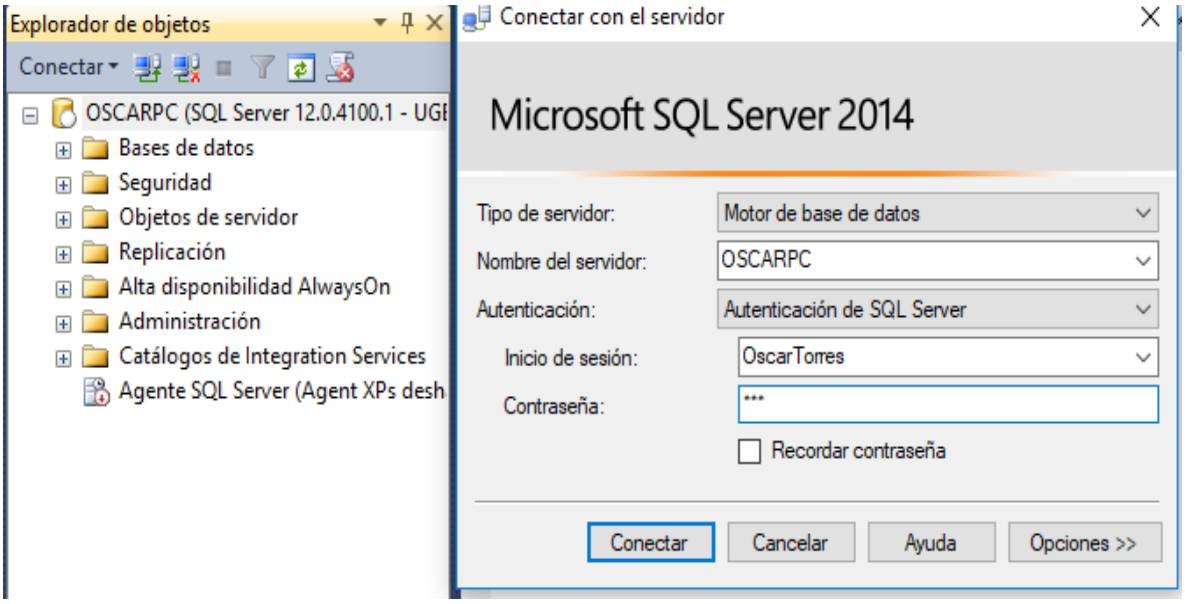
contraseña", seleccione la base de datos y de aceptar, así como se observa en la siguiente imagen:



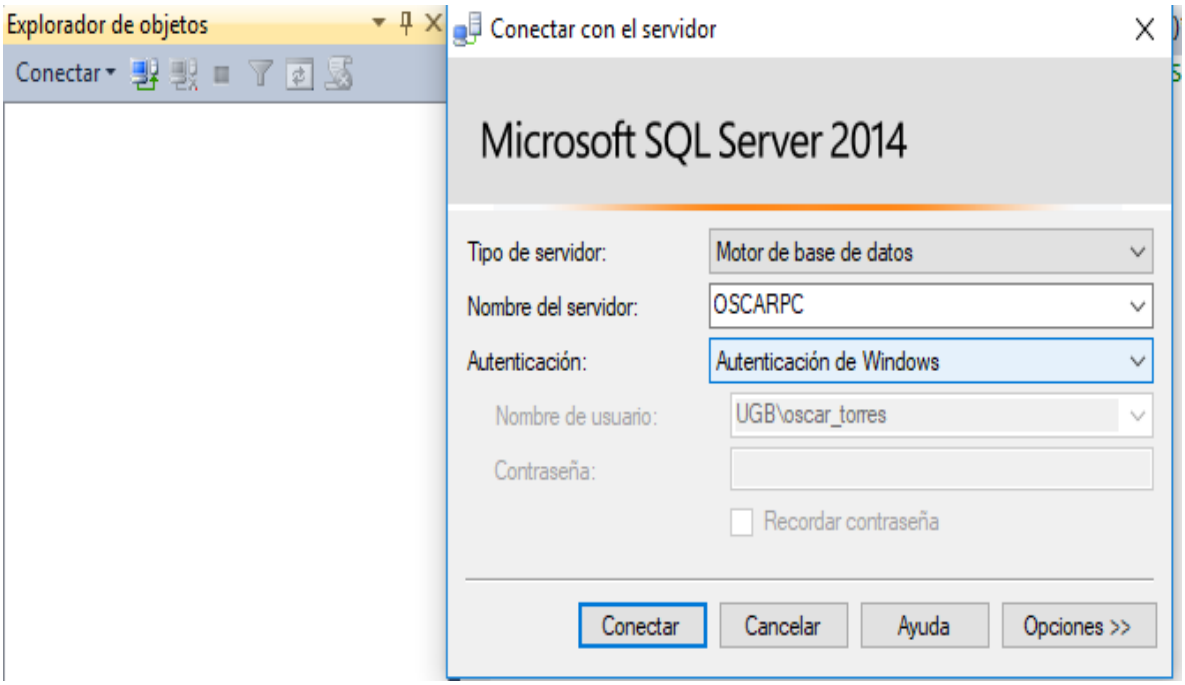
Paso 3: Cierre la sesión principal dando click en el icono de desconectar, así como se observa a continuación:



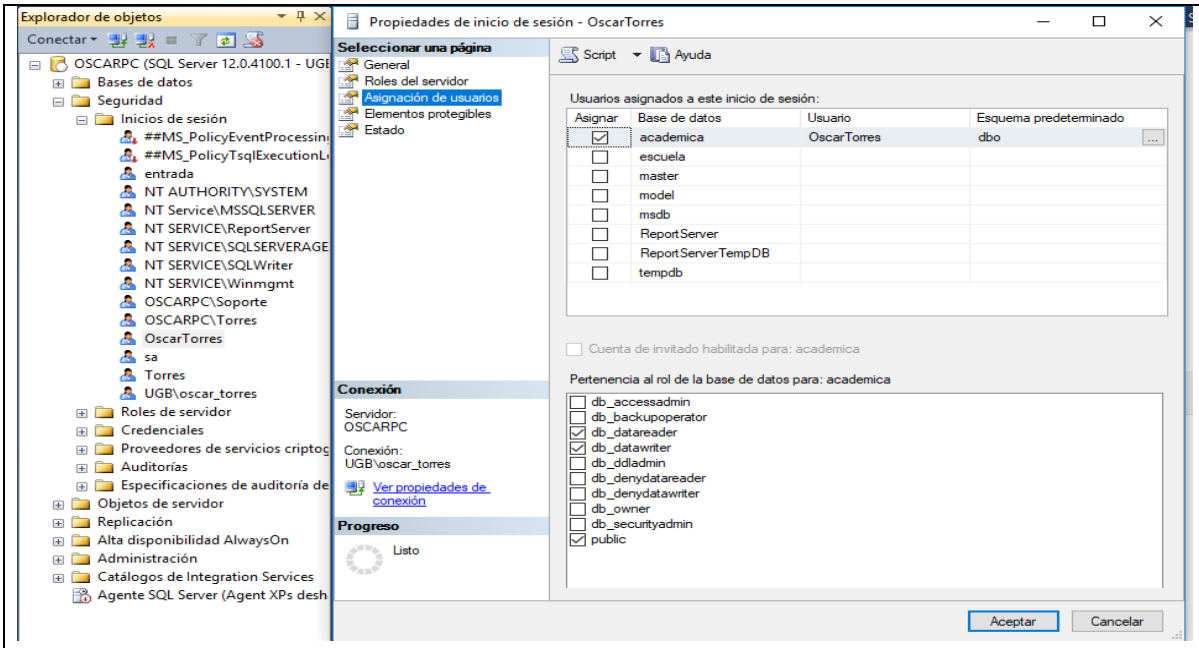
Paso 4: Inicie sesión con el nuevo usuario, ingrese inicio de sesión, contraseña y conectar, así como se observa en la siguiente imagen:



Paso 5: Cierre sesión creada e ingrese a sesión principal dando click en conectar, así como se observa en la siguiente imagen:



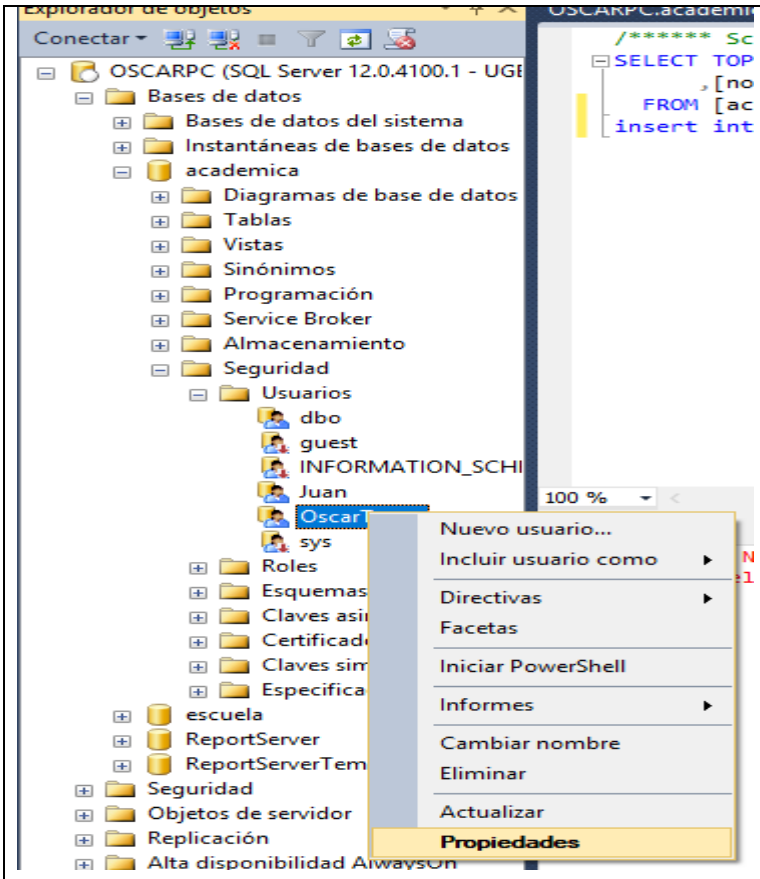
Paso 6: Asigne base de datos a usuario creado y privilegios de lectura, escritura y luego de click en aceptar, así como se observa en la siguiente imagen:



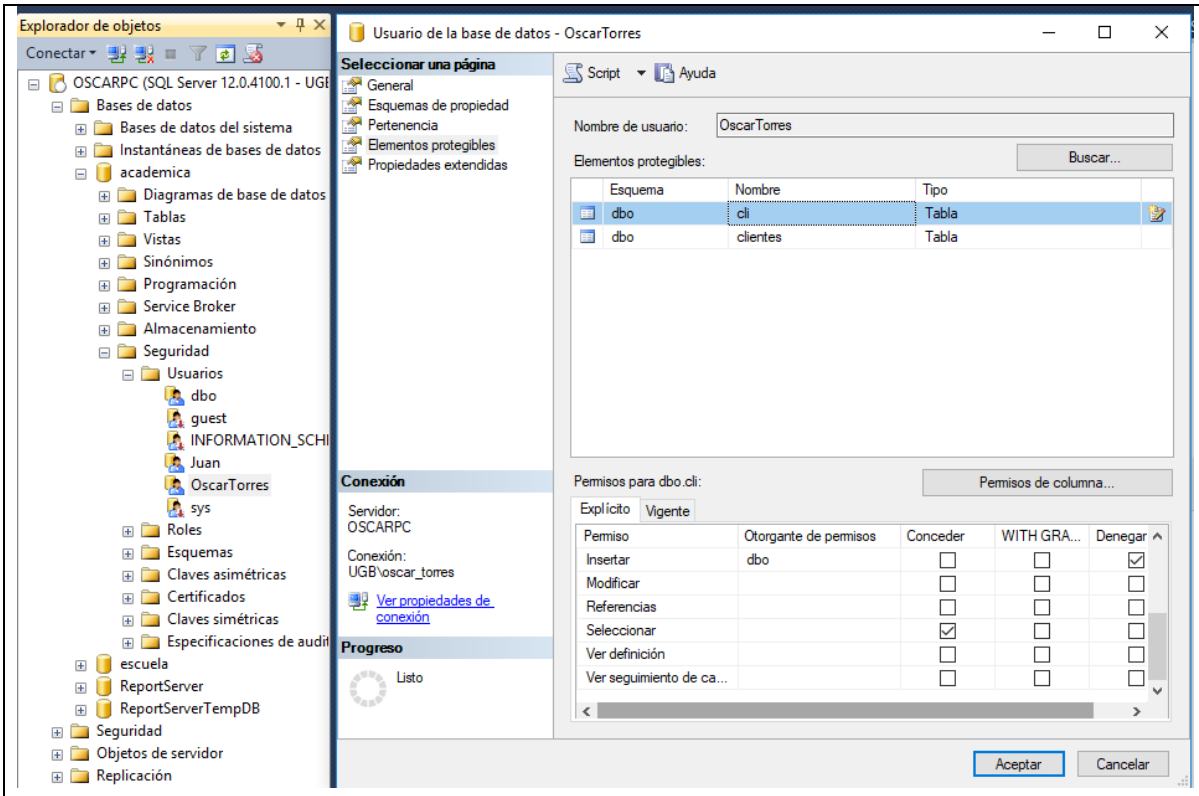
Nota: Si la persona o el grupo que necesita tener acceso a la base de datos no tiene credenciales de inicio de sesión y solo necesita tener acceso a una o a pocas bases de datos, cree un **usuario de Windows** o un **usuario SQL con contraseña**. También se denomina "usuario de base de datos independiente" y no está asociado con un inicio de sesión en la base de datos maestra. Se trata de una excelente opción si quiere mover fácilmente su base de datos entre instancias de SQL Server. Para usar esta opción en SQL Server , es necesario que un administrador habilite las bases de datos independientes para SQL Server, para crear un usuario asociado a un inicio de sesión puede escribir la siguiente instrucción

- create user oscar for login entrada with default_schema=dbo;

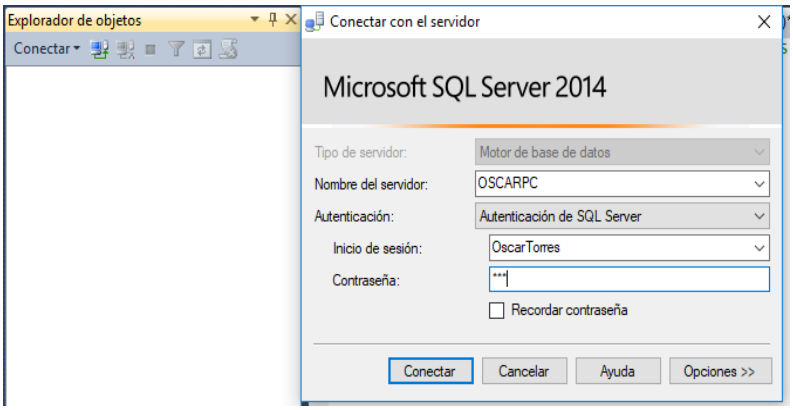
Paso 7: Para asignar privilegios sobre objetos de la base de datos, seleccione la base de datos, luego seguridad, usuarios, de click derecho sobre usuario creado y selecciones propiedades, así como se observa en la siguiente imagen:



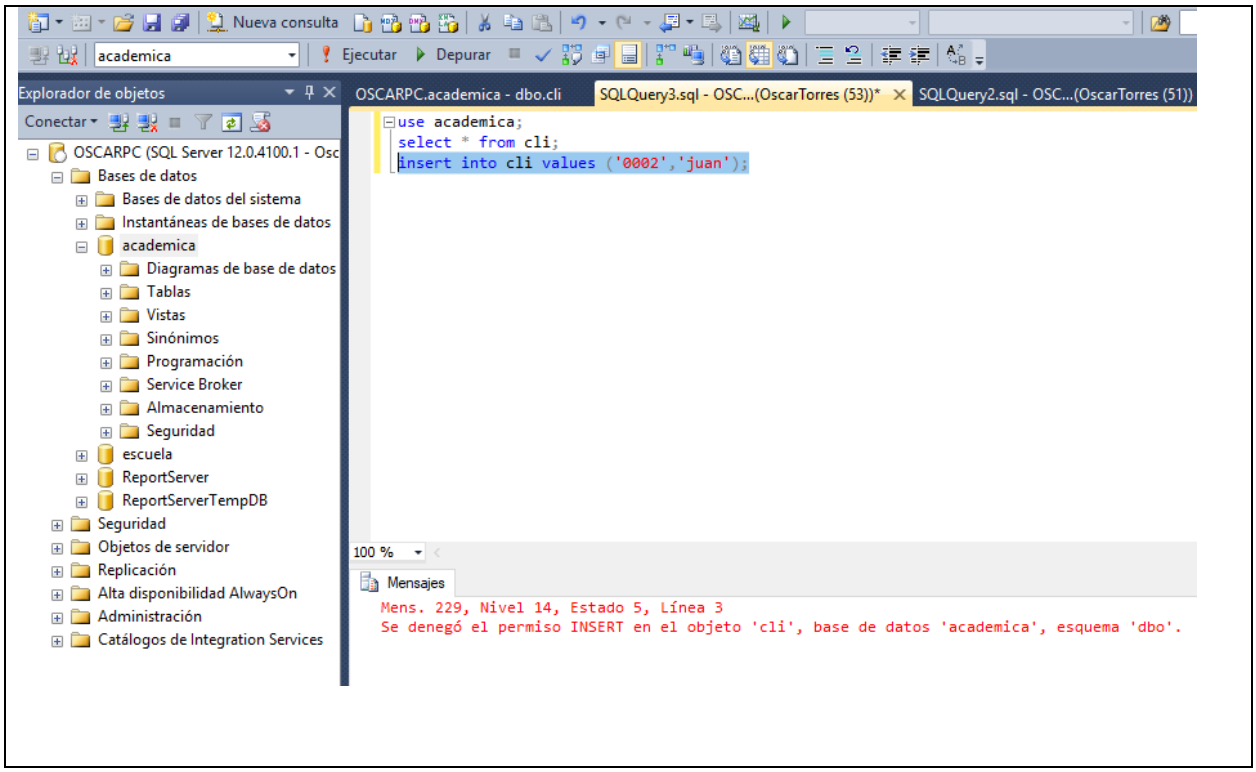
Paso 8: Aplique privilegios sobre los objetos, vaya a la opción marcada en azul "elementos protegidos", busque las tablas asignadas al usuario y en la parte inferior asigne el permiso "conceder" para seleccionar y "denegar" para insertar de la tabla llamada cli, así como se observa en la siguiente imagen:



Paso 9: Salir del usuario principal, e ingresar de nuevo con el usuario creado dando click en conectar, así como se observa en la siguiente imagen:



Paso 10: Pruebe los privilegios del usuario, seleccionado la base de datos, luego los datos de la tabla cli y tratando de insertar nuevos registros a la tabla, como se observa en la siguiente imagen:


Nueva consulta
academica
Ejecutar
Depurar
Explorador de objetos
Conectar
OSCARPC (SQL Server 12.0.4100.1 - Osc
Bases de datos
Bases de datos del sistema
Instantáneas de bases de datos
academica
Diagramas de base de datos
Tablas
Vistas
Sinónimos
Programación
Service Broker
Almacenamiento
Seguridad
escuela
ReportServer
ReportServerTempDB
Seguridad
Objetos de servidor
Replicación
Alta disponibilidad AlwaysOn
Administración
Catálogos de Integration Services
OSCARPC.academica - dbo.cli
SQLQuery3.sql - OSC...(OscarTorres (53))*
SQLQuery2.sql - OSC...(OscarTorres (51))
use academica;
select * from cli;
insert into cli values ('0002','juan');
100 %
Mensajes
Mens. 229, Nivel 14, Estado 5, Línea 3
Se denegó el permiso INSERT en el objeto 'cli', base de datos 'academica', esquema 'dbo'.

ACTIVIDAD DE EVALUACIÓN DE LA SEMANA	
Nombre de la Actividad	Plan de seguridad
Tipo de Actividad	Tarea
Tipo de Participación	Colaborativo
Instrucciones para la actividad	Después de dar lectura al contenido de la semana y participar activamente en la video conferencia, deberá: • Realizar actividad en clase designada por docente
Fecha de Entrega	Al final de clase práctica
Ponderación	Prácticas evaluadas (40% Laboratorio I)

RECURSOS COMPLEMENTARIOS		
Video	¿Qué es un Keylogger y cómo protegerme?	https://www.youtube.com/watch?v=gnbQDMKLMqY
Video	Respaldos (Backup) en SQL Server	https://www.youtube.com/watch?v=svpQow0wOcI
Video	Crear nuevo Usuario de Conexión	https://www.youtube.com/watch?v=GrH58D9Guuw&t=230s