

Actividad | #3 | Backup y Exportación Administracion de Base de Datos

Ingeniería en Desarrollo de Software

TUTOR: Miguel Ángel Rodríguez Vega

ALUMNO: Alejandra Ibarra

FECHA:11/02/2025

Indicé

Introducción…………………………………3

Descripción………………………………….3

Justificación………………………………….3

Desarrollo…………………………………….4

Conclusión…………………………………..

Referencias………………………………….

Introducción

La seguridad en el gestor de base de datos comienza por nuestra seguridad que abarca la autenticación que también se mencionaba en la actividad pasada, así como la autorización de usuarios frente a datos e instancias del servidor, también es importante crear un entorno seguro para el SQL en el cual debe incluir la seguridad en cada una de sus etapas de diseño, desarrollo e implementación del desarrollo del software y la base de datos.

Pero que es la autenticación esta nos refiere a un proceso de verificación de identidad de un usuario que quiera intentar acceder a una base de datos o a otra instancia de SQL y para esto también existen varias opciones como son:

* Autenticación de Windows: esta permite a los usuarios utilizar credenciales de inicio de sesión de Windows para que se les pueda otorgar el acceso.
* Autenticación de SQL: también conocida como autenticación mediante el inicio de sesión, este les permite a los usuarios ingresar un nombre de usuario y su contraseña en especifico para acceder

Descripción

Después se pasa a la autorización una vez que ya se haya identificado al usuario y se haya establecido su identidad, la autorización determina los permisos y los niveles de acceso que se les conceden a la base de datos o en la instancia de SQL, gracias a esto nos pueden garantizar que todos nuestros usuarios solo pueden acceder y manipular aquellos datos, pero es primordial primero la autenticación de cada uno de nosotros para poder tener el acceso.

En SQL nos proporciona unos roles basados que estos nos permiten agrupar y asignar permisos que son usados a cada grupo o usuario, algunos de estos roles ya también se encuentran predefinidos en SQL que nos incluyen los roles del administrador del sistema que también tienen privilegios completos y control total de la instancia. Un paso muy importante también es el respaldo local que nos ayuda a realizar copias de seguridad de nuestra base de datos como la que se realizo en esta actividad esto es fundamental para proteger la integridad y disponibilidad de los datos en caso de fallos del sistema.

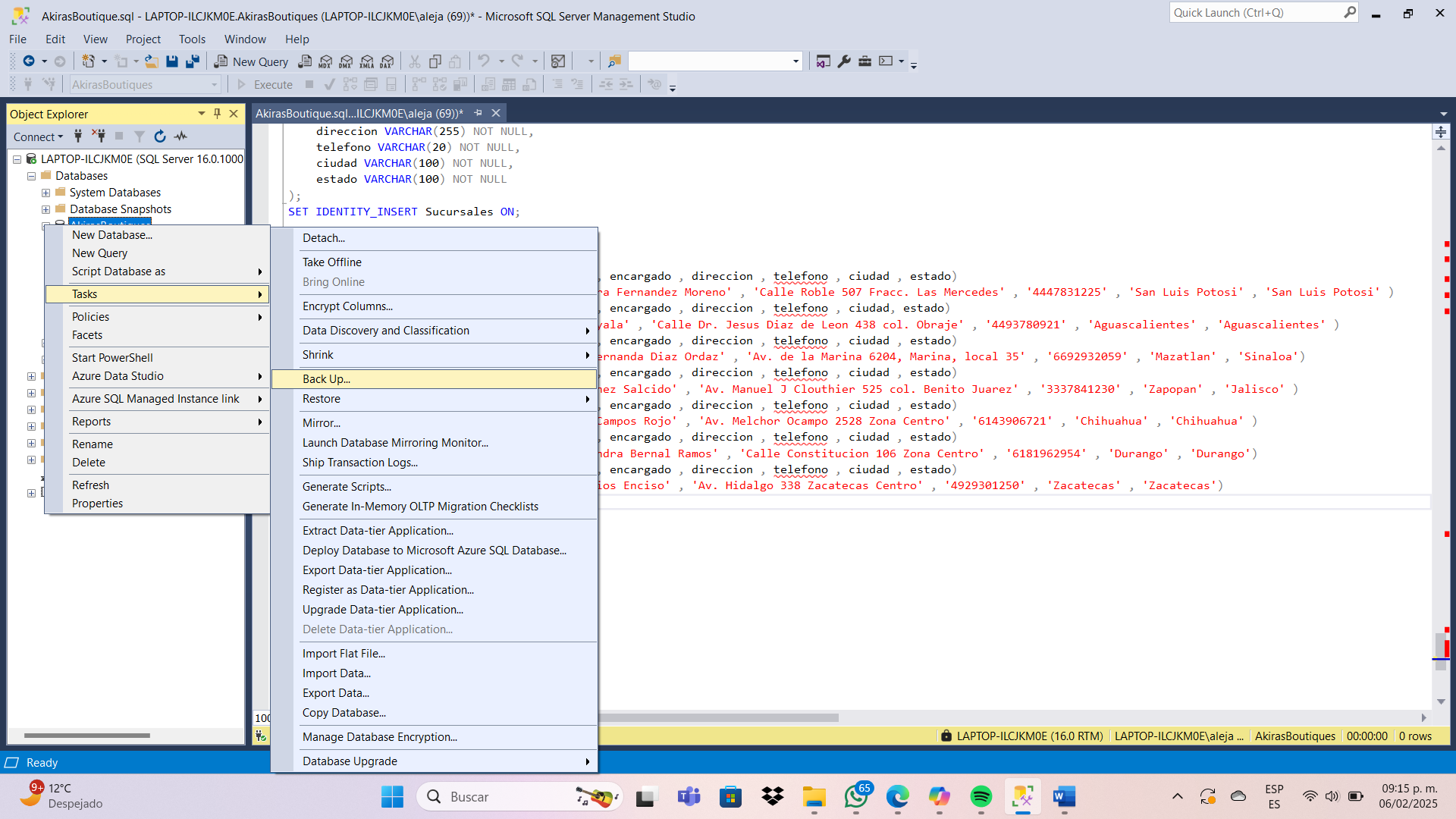
Justificación

El respaldo en la nube en este caso es necesario realizar un respaldo en nuestra nube de nuestra base de datos en la nube generalmente implica utilizar las herramientas y servicios específicos proporcionados por nuestro proveedor de la nube en la que se encuentra alojado en la base de datos. Los ataques de SQL son intentos malintencionados de explotar las vulnerabilidades en una aplicación o sistema que utilice una base de datos, estos ataques claro que cuentan con un objetivo que es acceder, manipular, o eliminar datos confidenciales almacenados en nuestra base de datos, que esta se considera una información muy importante y es vulnerable.

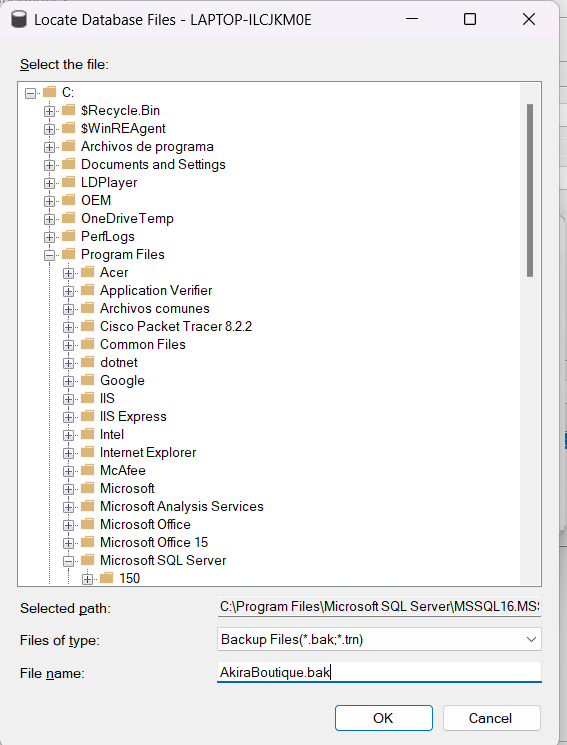
La inyección SQL es uno de los ataques mas comunes, los atacantes insertan un código malicioso en las entradas de una aplicación web con el fin de engañar al sistema y ejecutar ese código malicioso.

Desarrollo

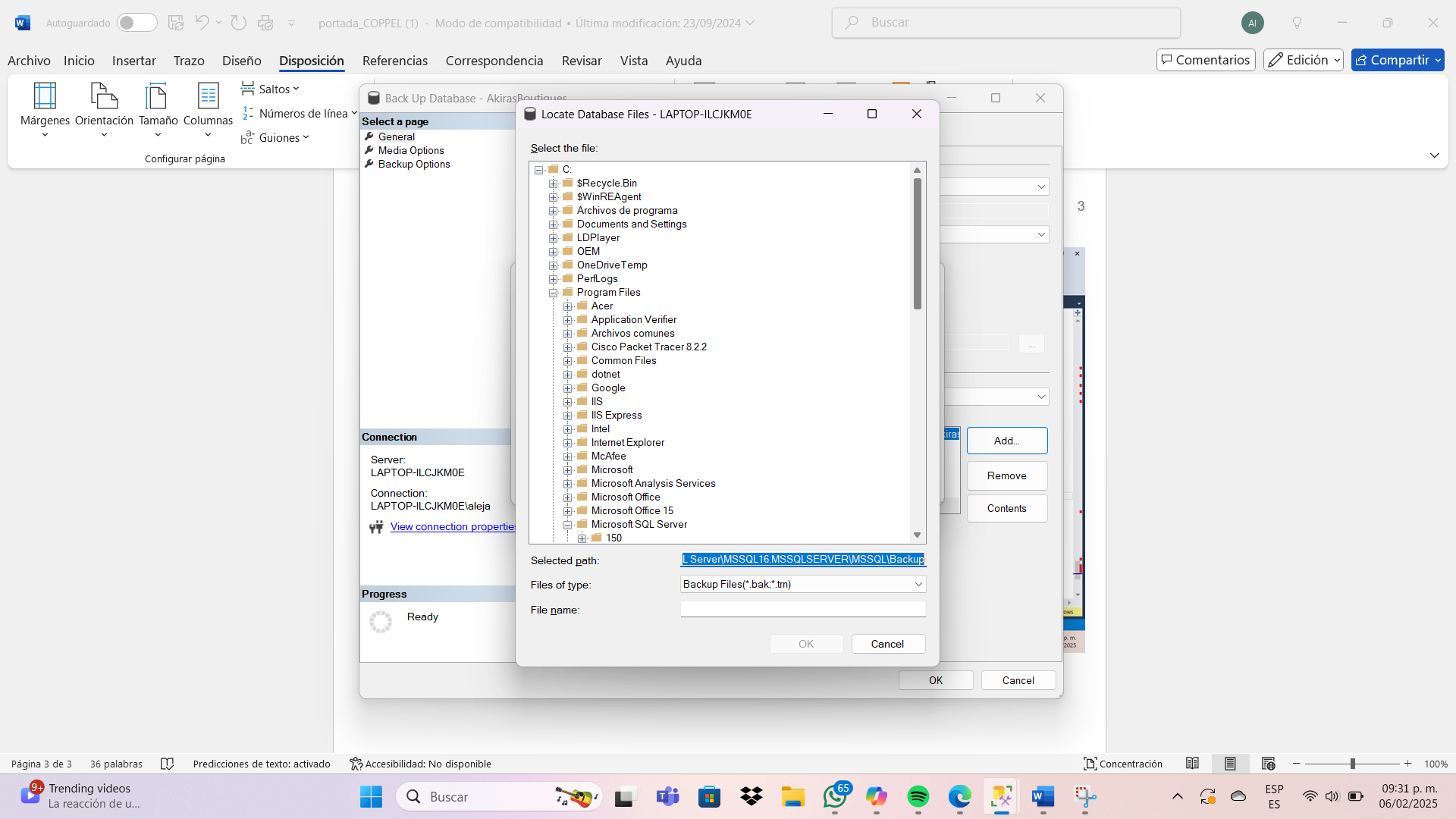
* Aquí vamos a comenzar a realizar el Back Up



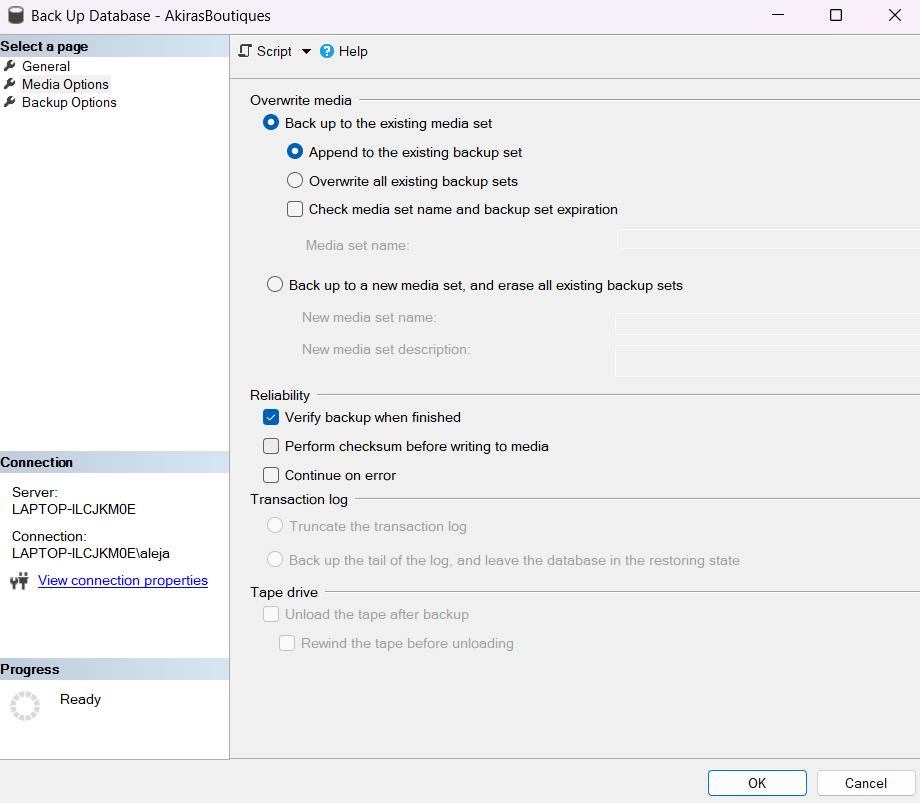
* Es esta pestaña nos está preguntando en donde lo guardaremos



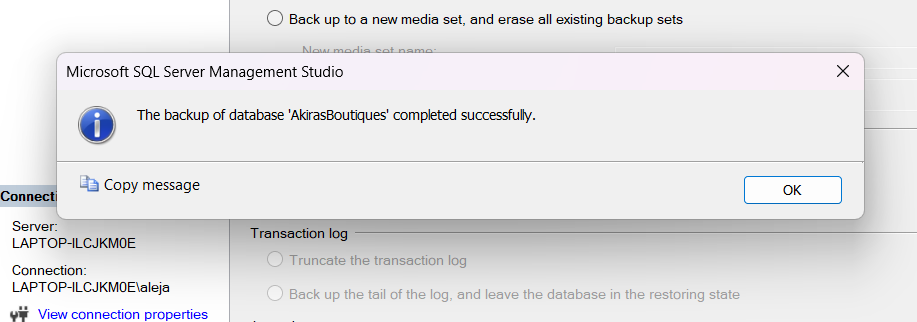
* Aquí se está realizando el segundo proceso de guardar, pero se le asignara un nombre para que se a más fácil encontrar e identificar



* En la siguiente pestaña se seleccionará la opción Verify backup y saldrá otra pestaña en la que nos dará un enlace que nos asegura que se realizó de forma correcta la verificación del backup



* Aquí arroja el menssaje de que ya quedo completado



BACKUP DATABASE [AkirasBoutiques] TO DISK = N'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Backup\AkirasBoutike.bak' WITH NOFORMAT, NOINIT, NAME = N'AkirasBoutiques-Full Database Backup', SKIP, NOREWIND, NOUNLOAD, STATS = 10

GO

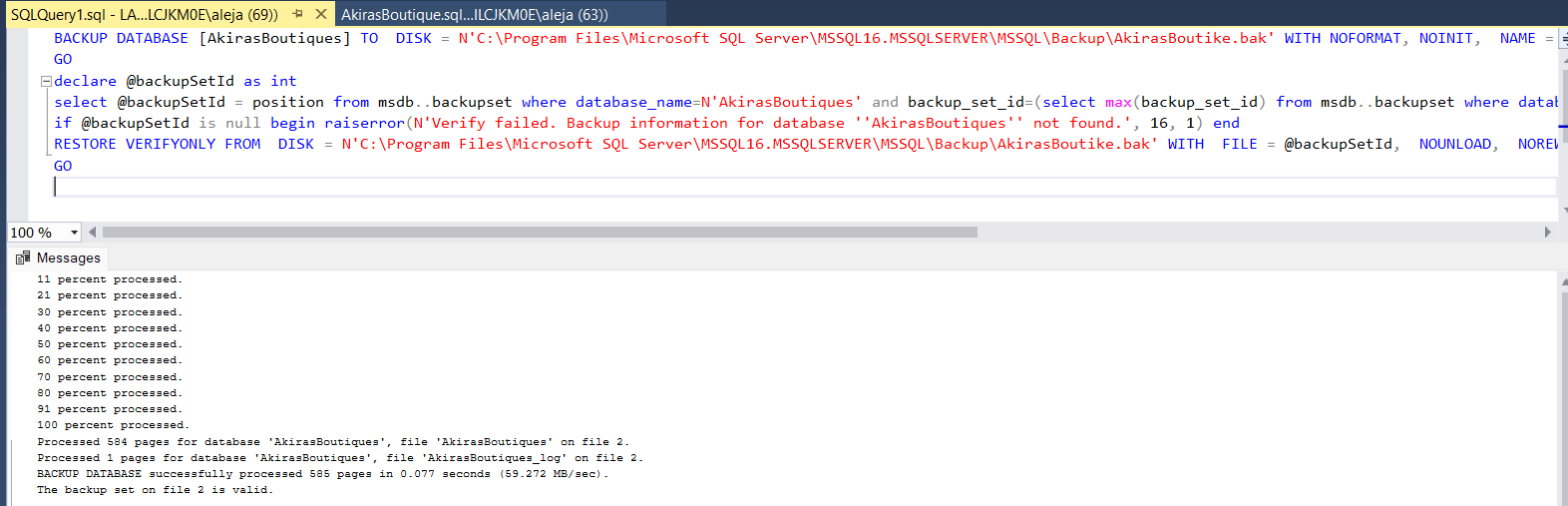
declare @backupSetId as int

select @backupSetId = position from msdb..backupset where database\_name=N'AkirasBoutiques' and backup\_set\_id=(select max(backup\_set\_id) from msdb..backupset where database\_name=N'AkirasBoutiques' )

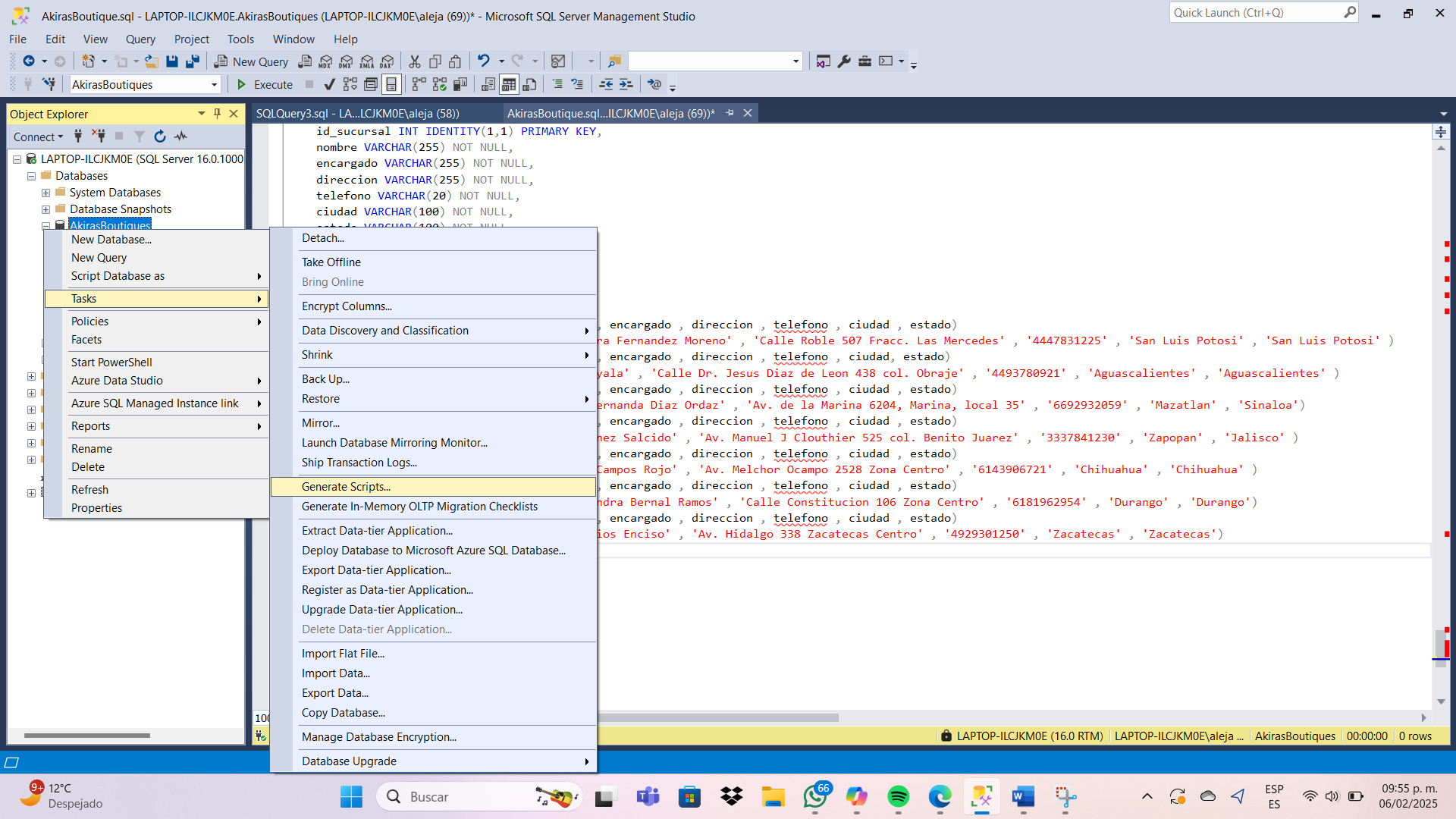
if @backupSetId is null begin raiserror(N'Verify failed. Backup information for database ''AkirasBoutiques'' not found.', 16, 1) end

RESTORE VERIFYONLY FROM DISK = N'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Backup\AkirasBoutike.bak' WITH FILE = @backupSetId, NOUNLOAD, NOREWIND

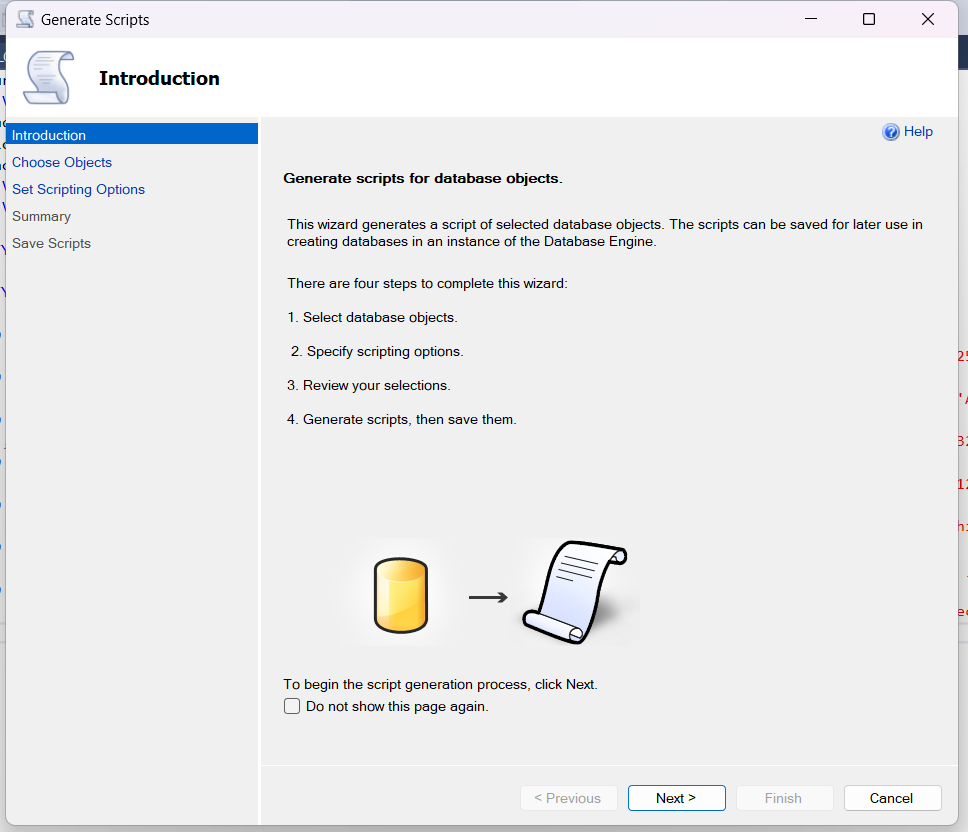
GO



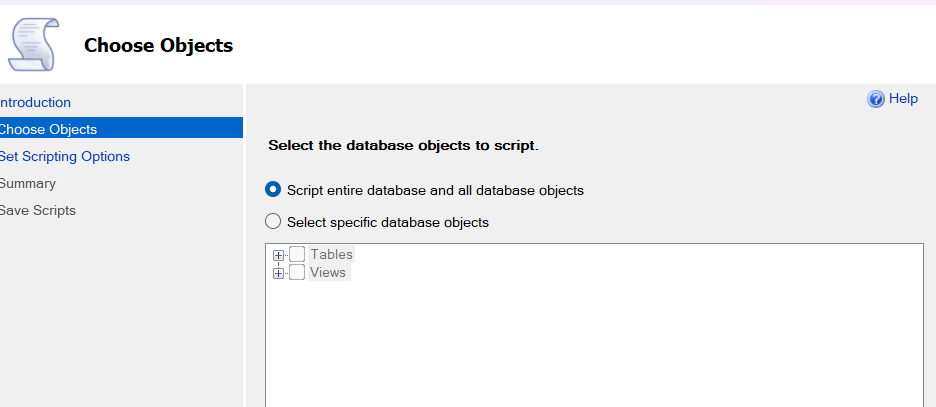
* Después de eso se genera el script de la base de datos



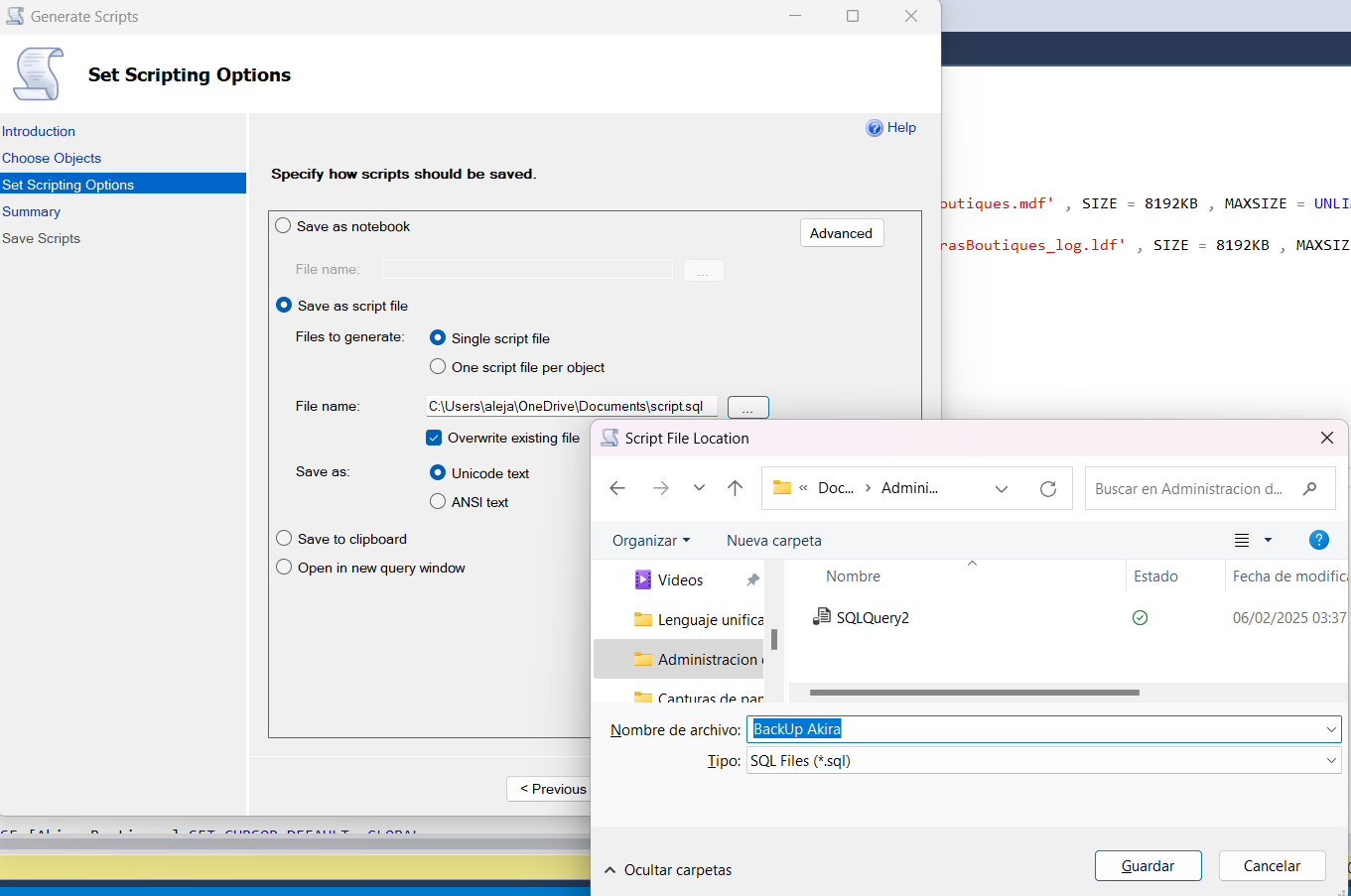
Este casi el último paso se genera un nuevo script donde se seleccionará los objetos específicos para su generación más adelante en una base de datos



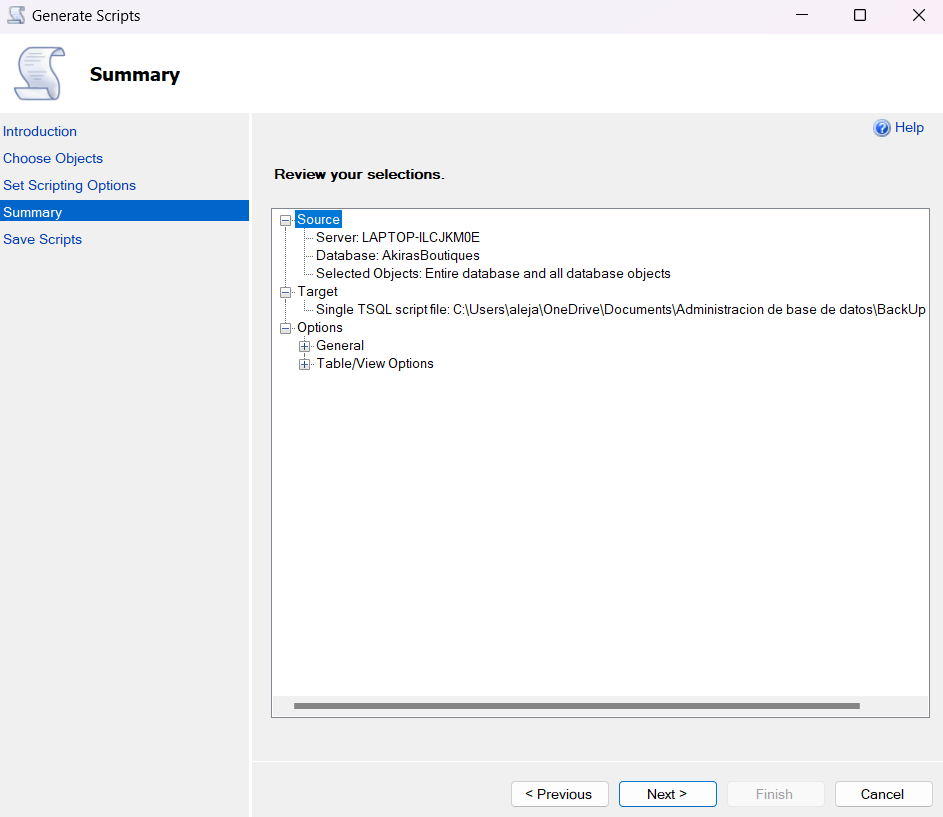
En este punto nos pregunta si solo seleccionaremos unos objetos en específico o toda la base de datos completa y en este caso se hizo completa



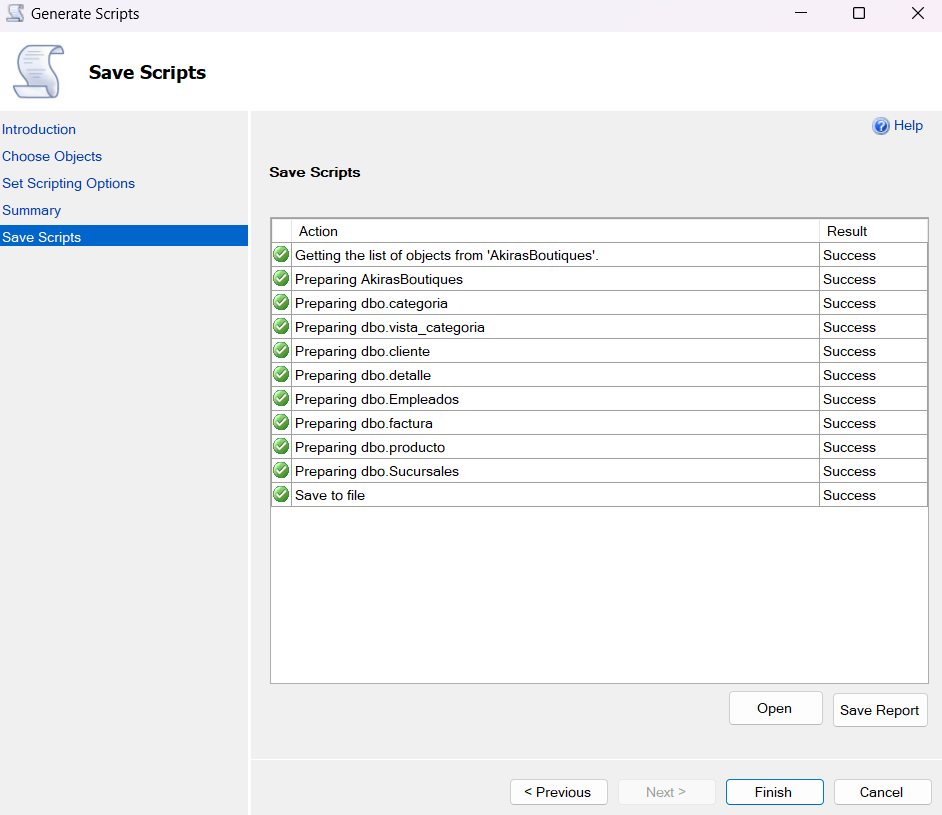
* Se guarda el archivo en la ruta que nosotros queramos



* Puntos de revisión



En este ultimo paso ya se completó, marcando así la lista de pasos que si se cumplieron para el Backup



Conclusión

Dentro de esta actividad se aprendió a realizar una copia de seguridad de nuestra base de datos, también adicional como entrar con el método de autenticación para que nosotros los que modificamos los datos, sinceramente si se tiene que pasar por bastantes filtros de seguridad para evitar una pérdida de datos.

También es importante conocer los métodos que los hackers pueden hacer como la encriptación de datos que se conoce como el intento de obtener acceso no autorizado a los datos encriptados almacenados en la base de datos, normalmente los ataques se centran en obtener la clave de acceso del cifrado sin tener la autorización adecuada o haber pasado por todos nuestros filtros de seguridad.

Un método también para poder evitar algún tipo de ataque es la encriptación que nos permite como su nombre lo dice encriptar columnas especificas que contienen datos sensibles, los datos se encriptan utilizando claves que se generan y que son gestionadas por nuestra base de datos.

Referencias