TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE CIUDAD MADERO

Creación de roles en la base de datos AdventureWorks 2019

Alumno: Alonso Palafox Miguel Ángel

Núm. De control: 22070280

Carrera: Ingeniería en Sistemas Computacionales

Docente: Fernando Manzanares González

Materia: Administración de Base de Datos

HORA: 16:00 – 17:00 HRS

PERIODO: ENERO – JUNIO 2025

Introducción

Este reporte detalla el proceso de creación de roles personalizados dentro de la base de datos OLTP (*Online Transaction Processing*) AdventureWorks2019 utilizando Microsoft SQL Server. La finalidad principal de esta actividad fue aplicar los conceptos de control de acceso a través de roles, una práctica esencial en la administración de bases de datos para garantizar la seguridad, integridad y confidencialidad de la información.

La creación de roles permite agrupar usuarios con funciones similares dentro de una organización y asignarles permisos específicos sobre las tablas que requieren, lo cual facilita la administración y evita otorgar más privilegios de los necesarios. En este proyecto se diseñaron e implementaron distintos roles con niveles de acceso diferenciados sobre tablas como Sales.Customer, HumanResources.Employee y Person.EmailAddress, simulando escenarios reales de uso dentro de un sistema empresarial.

Roles creados

Para esta actividad, se crearon tres roles con el fin de ejemplificar distintos niveles de acceso y responsabilidades dentro de la base de datos AdventureWorks2019. Cada uno de estos roles fue diseñado para cubrir necesidades específicas de usuarios en áreas clave como atención al cliente y recursos humanos. Los permisos fueron otorgados con base en los principios de seguridad y control de privilegios mínimos, permitiendo realizar únicamente las operaciones necesarias según el perfil de cada usuario.

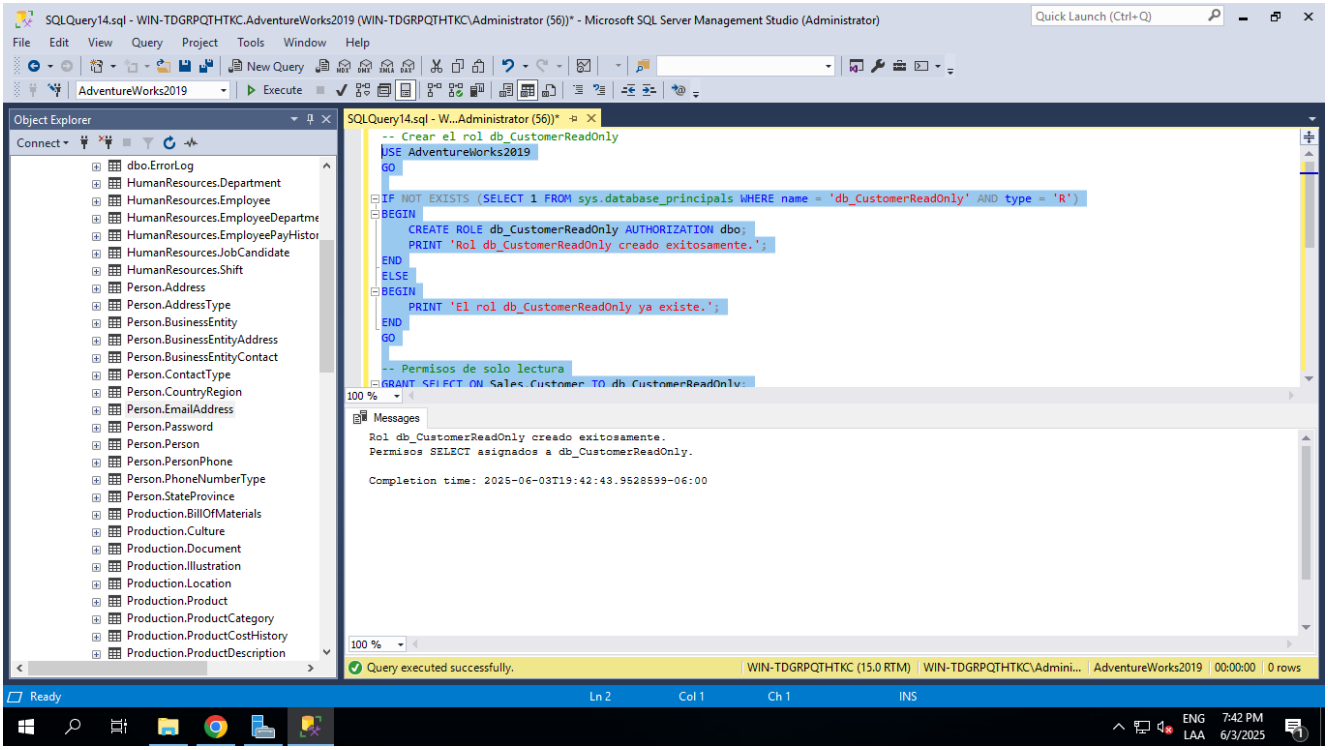
Los roles creados son los siguientes:

- db_CustomerReadOnly: acceso de solo lectura a información de clientes.
- db_CustomerService: acceso de lectura y actualización a datos de clientes.
- db_EmployeeManager: acceso de lectura y actualización a información de empleados.

A continuación, se describe el propósito de cada rol y los permisos asignados a las tablas correspondientes.

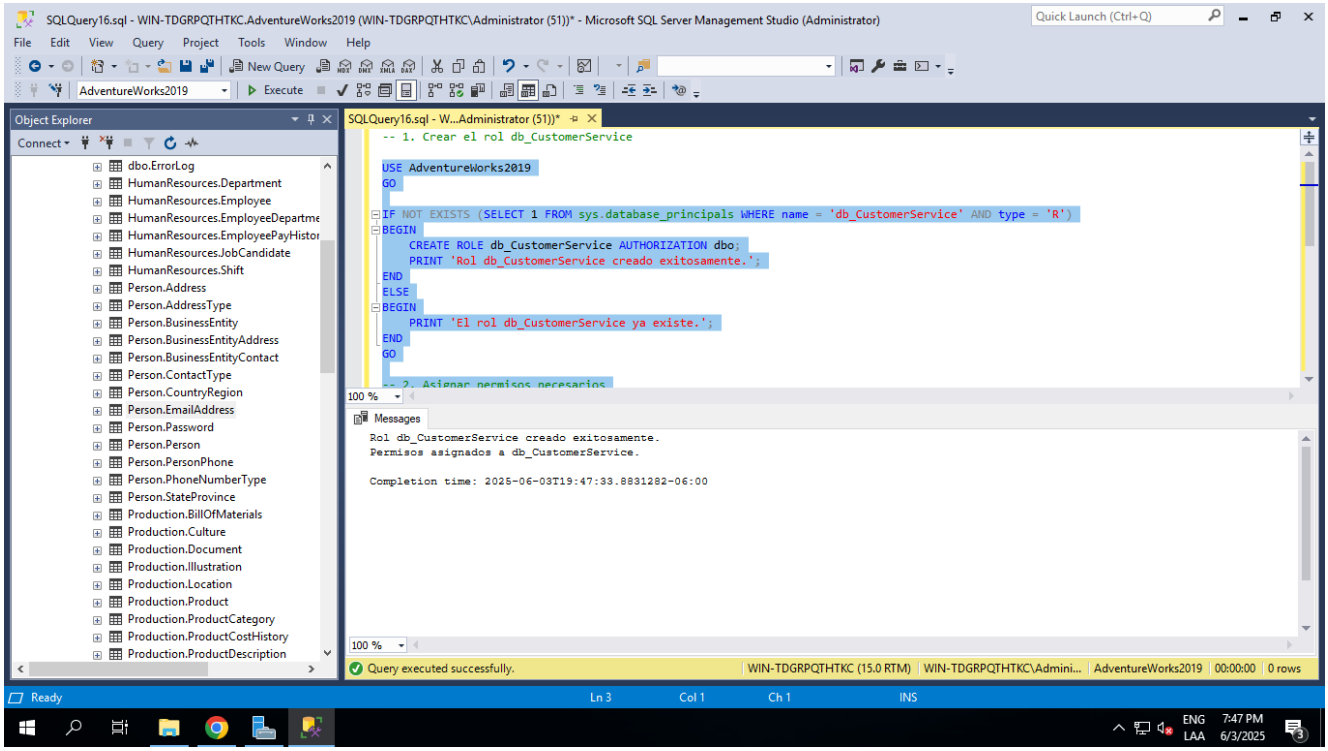
Rol: db_CustomerReadOnly

Descripción: Este rol está destinado a usuarios que requieren únicamente visualizar información de clientes. Es ideal para personal de análisis o auditoría que necesita revisar datos sin riesgo de modificaciones. Se otorgaron permisos SELECT sobre la tabla [Sales].[Customer] y las tablas relacionadas [Person].[Person], [Sales].[Store] y [Sales].[SalesTerritory].



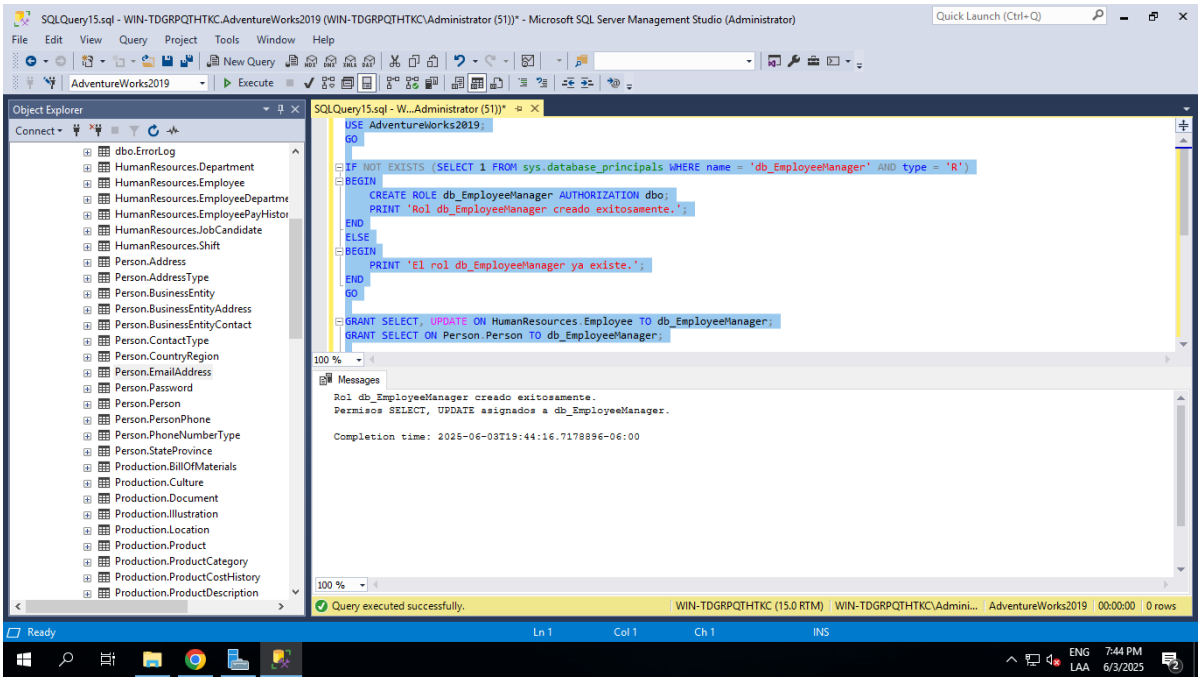
Rol: db_CustomerService

Descripción: Pensado para personal de servicio al cliente o soporte, este rol permite consultar y actualizar información de clientes, sin permitir la eliminación o inserción de registros. Esto permite mantener actualizada la base de datos sin comprometer la integridad de los datos históricos.

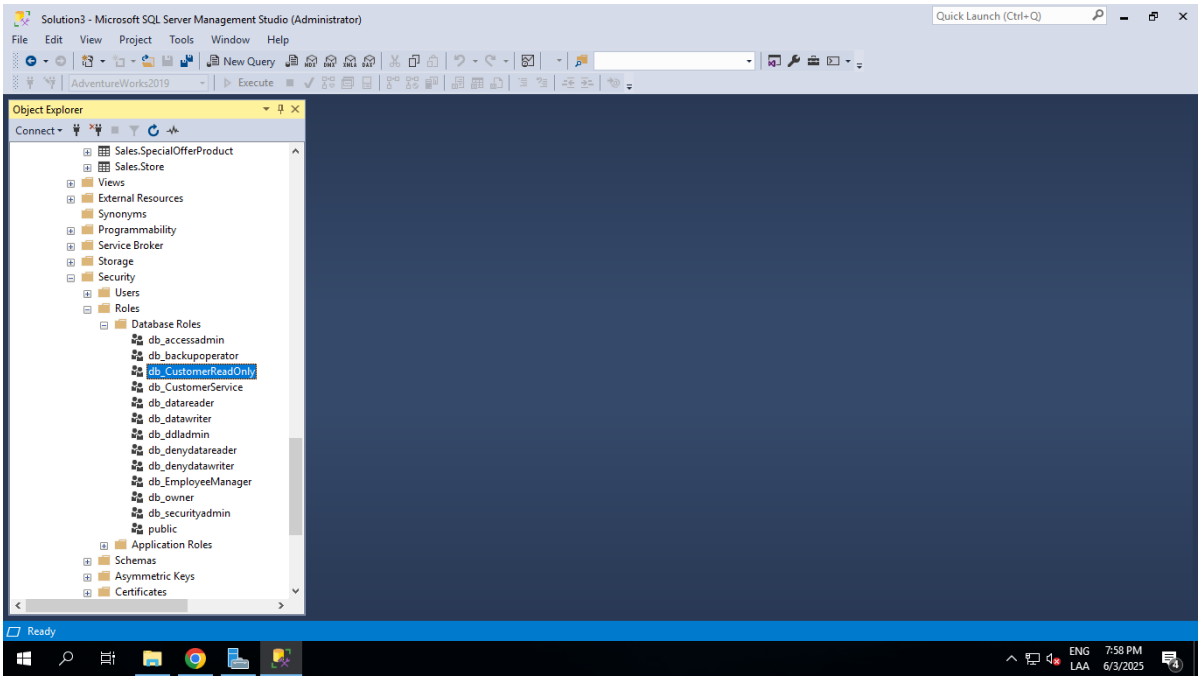


Rol: db_EmployeeManager

Descripción: Rol otorgado a supervisores de personal o recursos humanos que necesitan consultar y modificar datos de empleados. Tienen acceso de lectura y escritura sobre la tabla [HumanResources].[Employee], lo cual permite actualizar puestos, horas disponibles, estatus, etc., pero sin capacidad para eliminar registros o crear nuevos empleados.



Evidencia de la creación de los roles:



Conclusión

La implementación de roles dentro de la base de datos AdventureWorks2019 permitió aplicar de forma práctica los conceptos clave de la administración de seguridad en entornos de bases de datos. A través de la creación de roles con distintos niveles de acceso, fue posible demostrar cómo se puede controlar de manera efectiva qué usuarios tienen permiso para consultar, modificar o administrar los datos según su función dentro de una organización.

Esta estrategia no solo mejora la organización y el mantenimiento del sistema, sino que también fortalece la protección de la información, evita accesos no autorizados y promueve la integridad de los datos. En entornos reales, el uso adecuado de roles es una práctica recomendada para cumplir con políticas de seguridad, normativas internas y estándares profesionales de gestión de datos.

La actividad evidenció la importancia de establecer permisos personalizados como una medida proactiva de seguridad y administración, contribuyendo a un entorno más ordenado, eficiente y seguro.