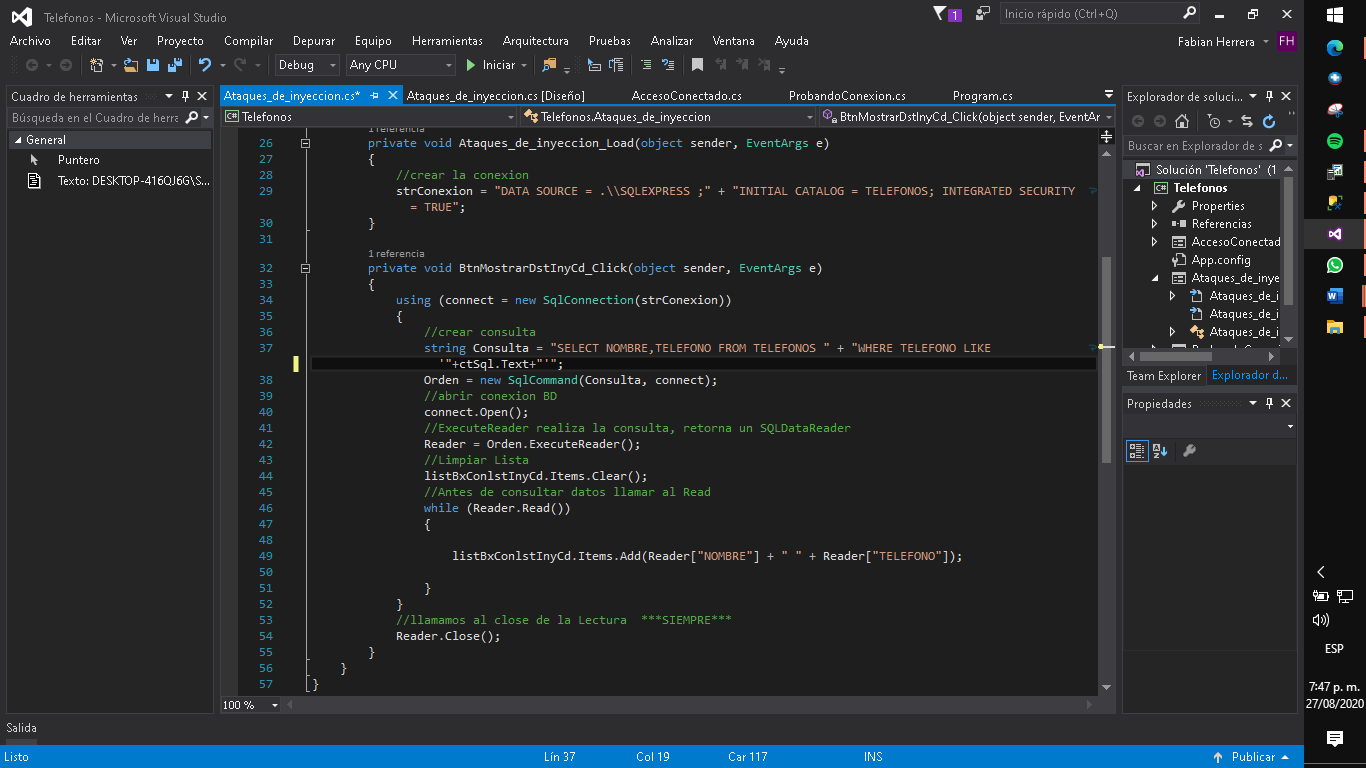
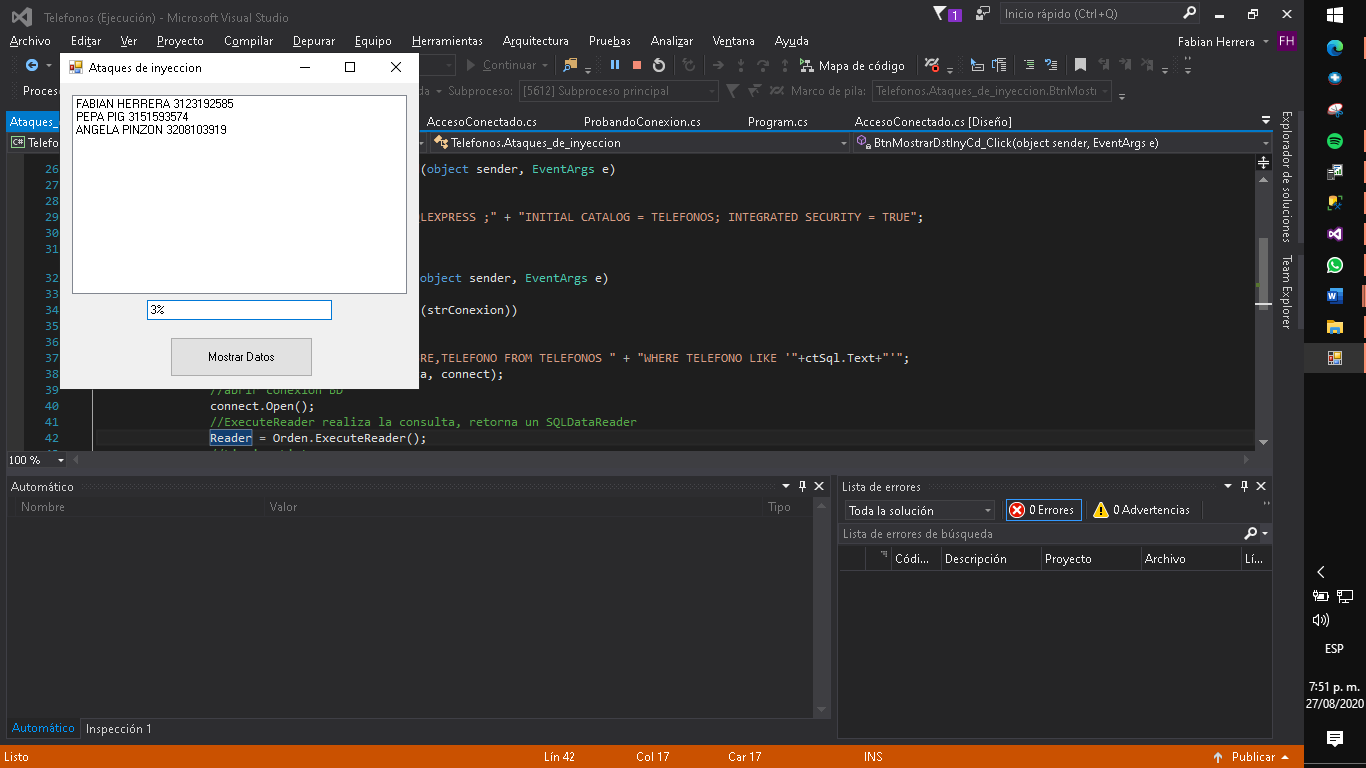
**Inyección de Código SQL**

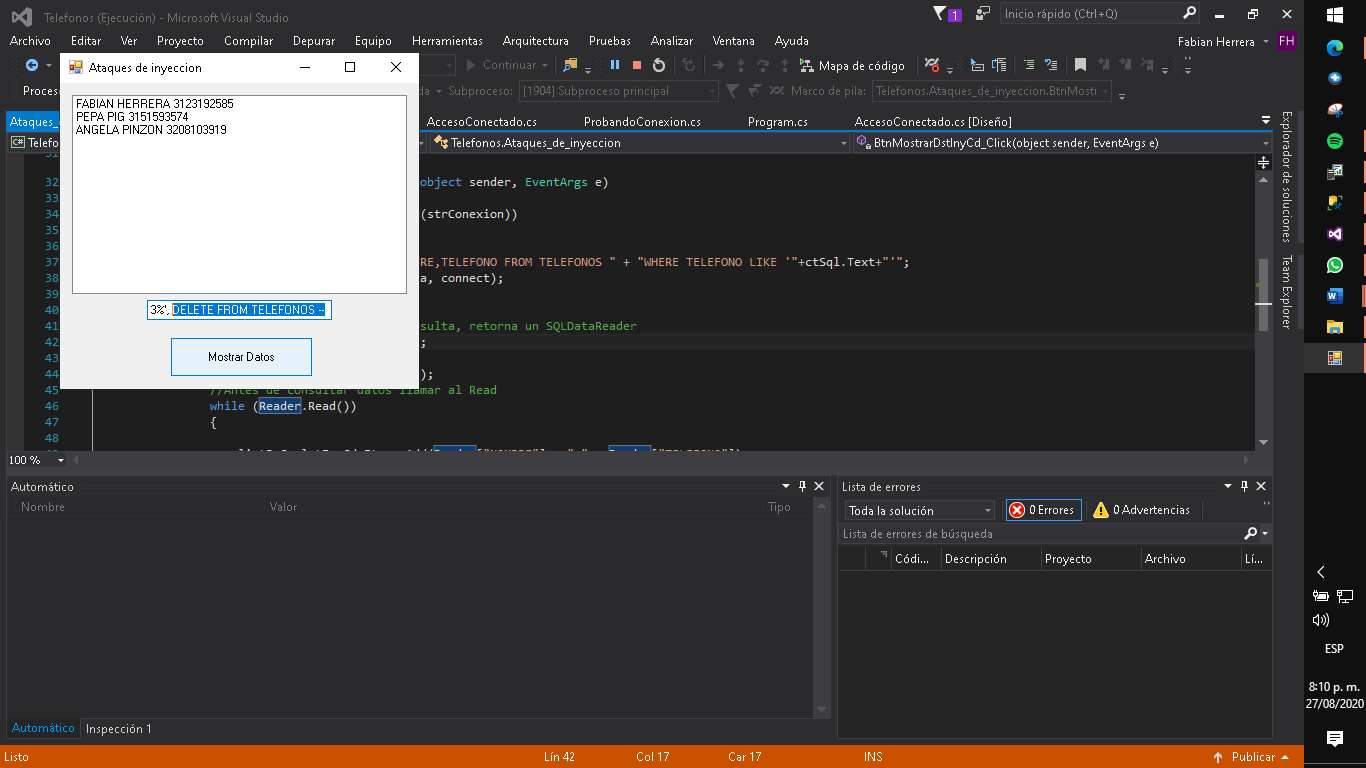
* Vulneración a la integridad de datos habilitada



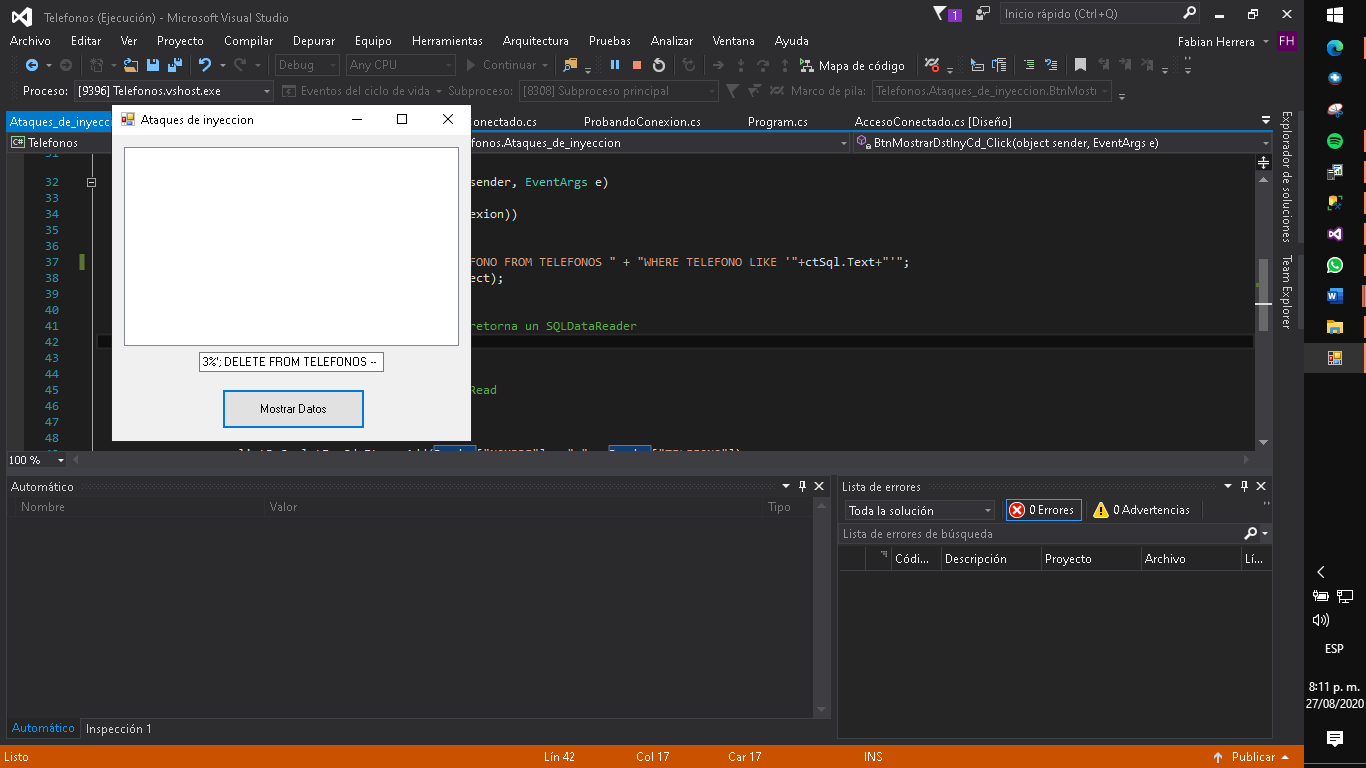
* Ejecución de filtro 3%, el cual gracias a la instrucción LIKE de SQL muestra todos los datos que inicien con el numero 3 en el campo TELEFONO



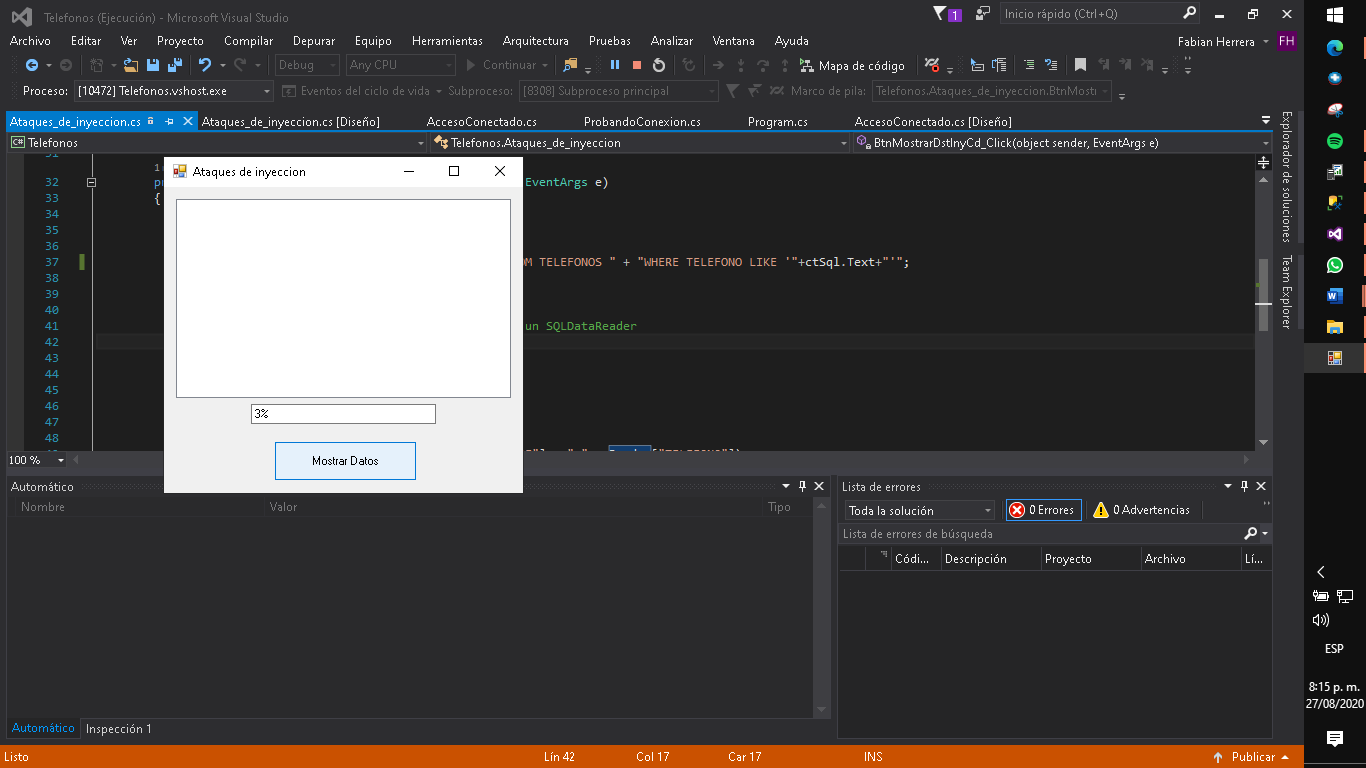
* inyección de código '; DELETE FROM TELEFONOS --, el cual borra todos los datos almacenados en la tabla



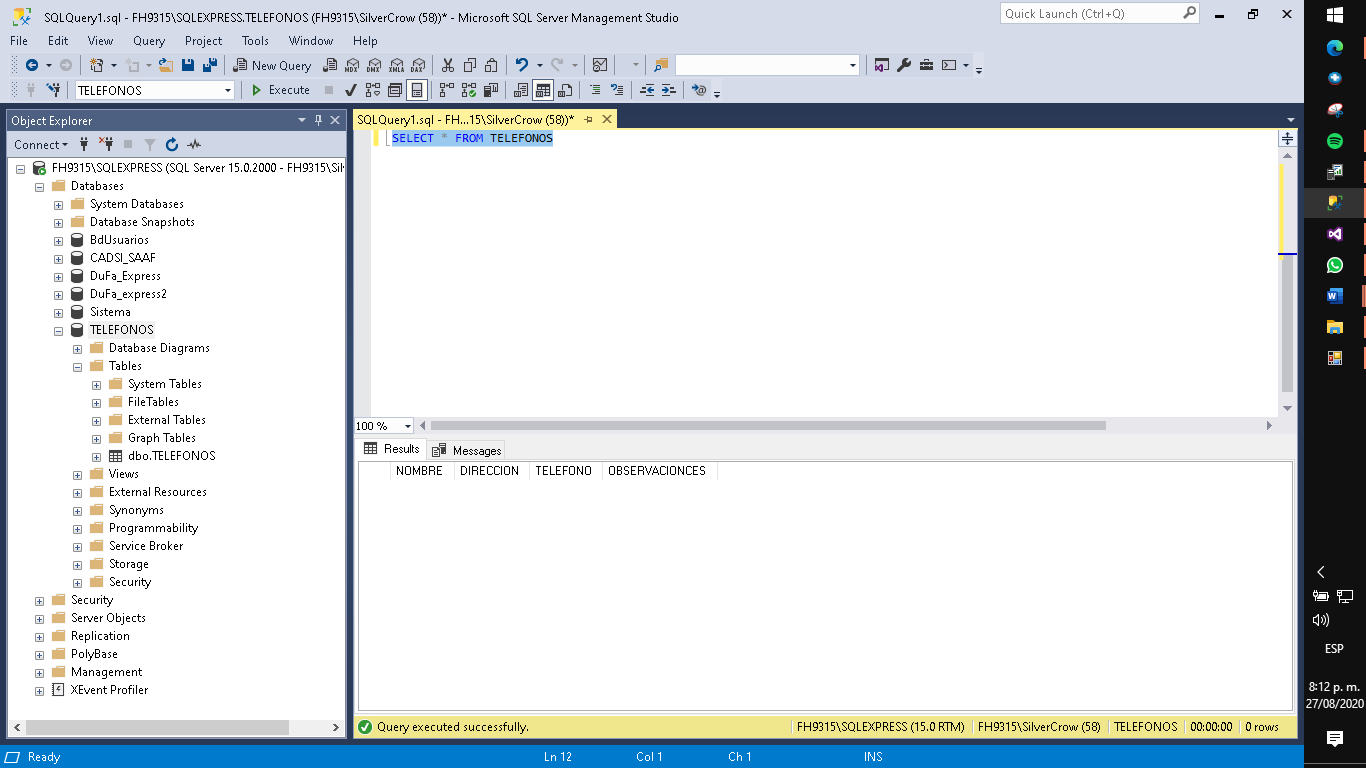
* Resultado, información de la Base de Datos eliminada



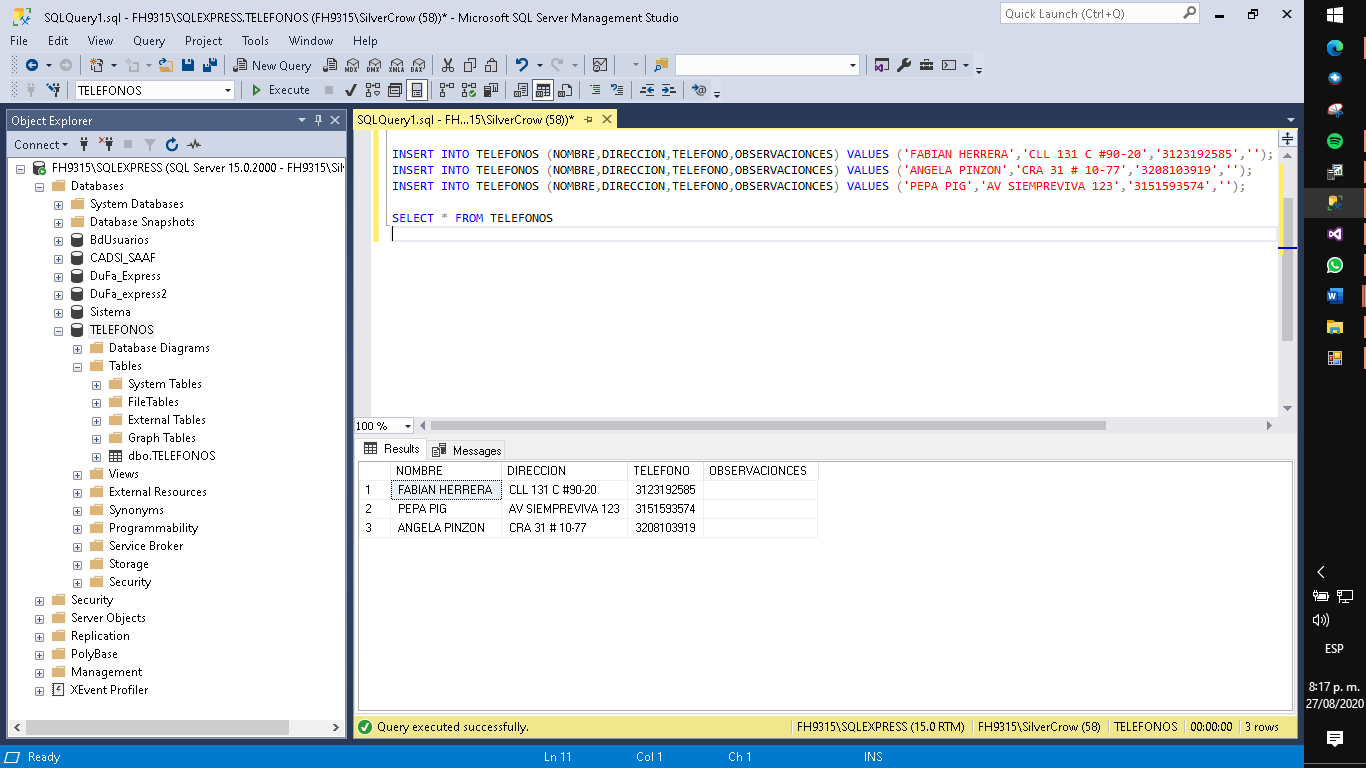
* Confirmación de datos Eliminados por medio de la aplicación aplicando el filtro 3%



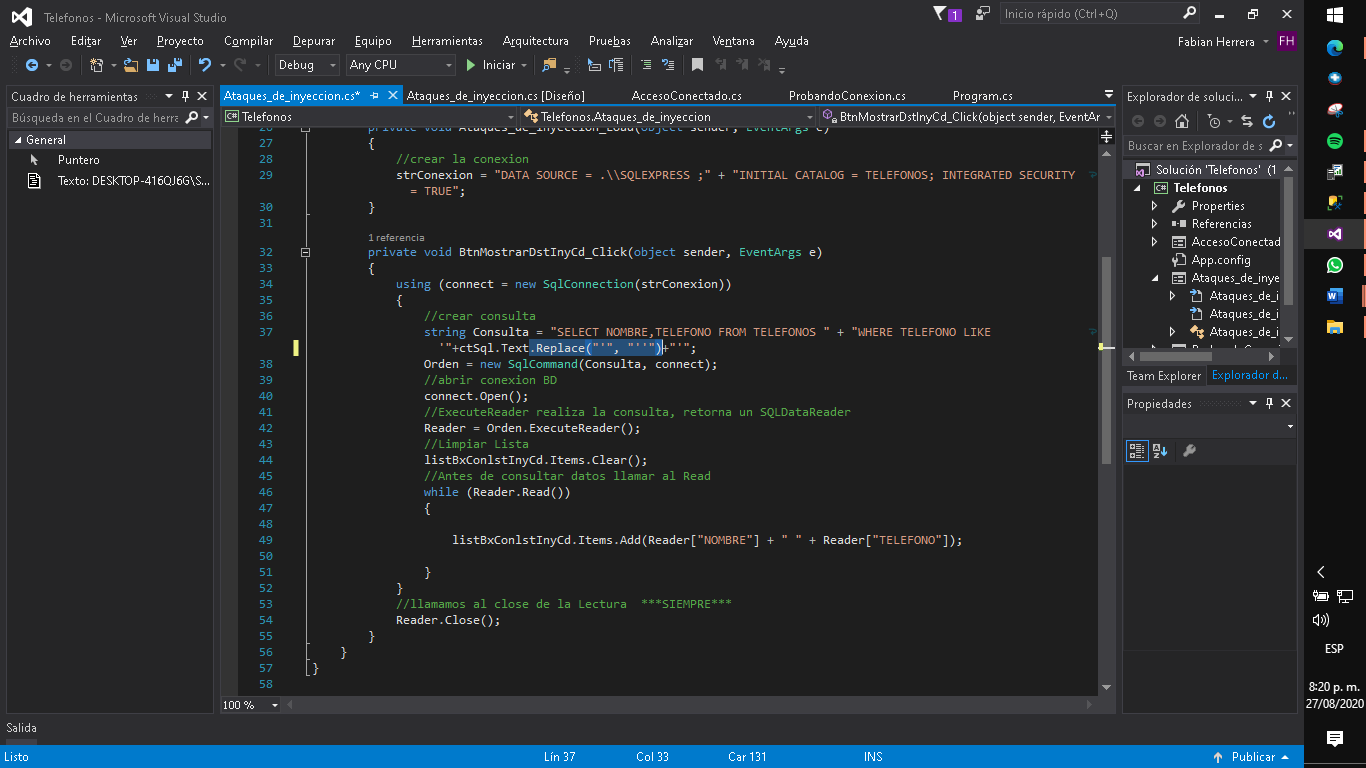
* Confirmación de datos Eliminados de la tabla en SQL server por medio del comando SELECT \* FROM TELEFONOS, Lo cual arroja una tabla vacía ya que los datos fueron eliminados.



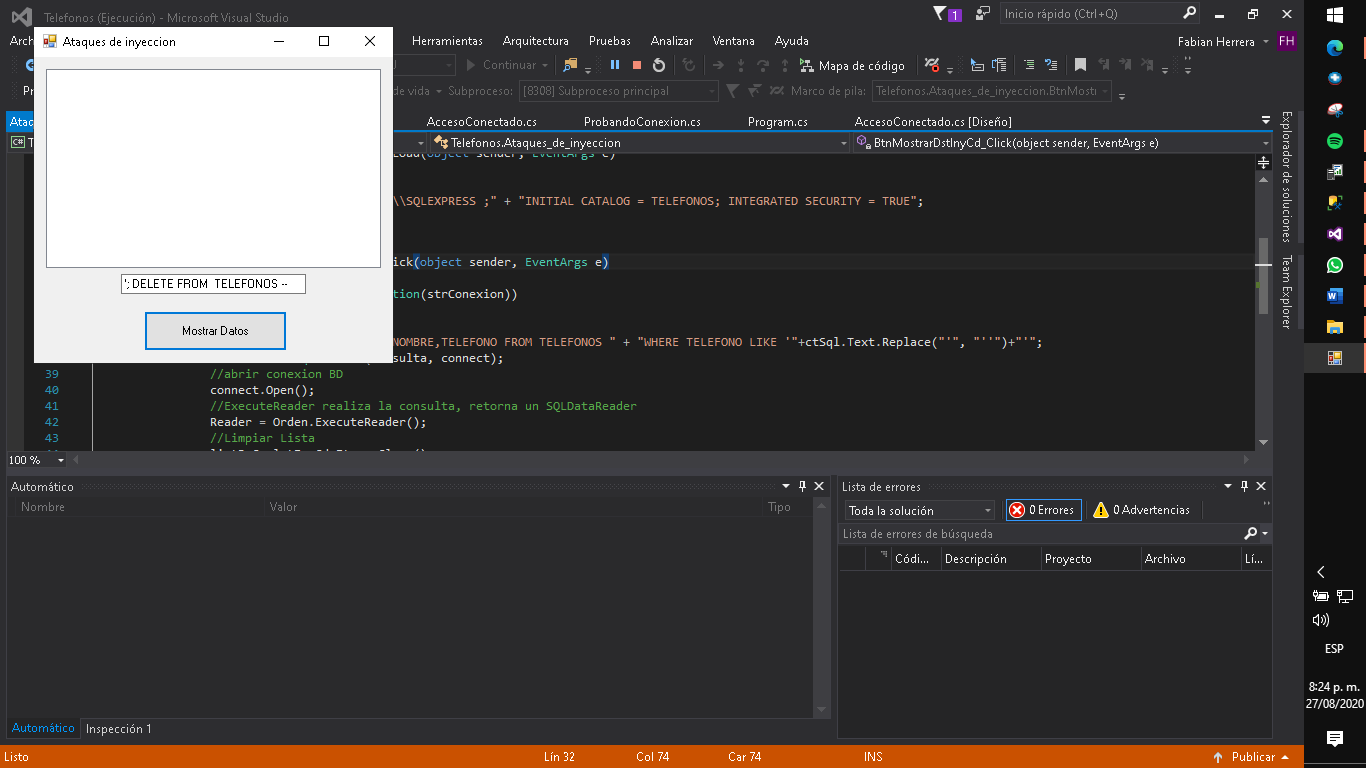
* Nuevos registros en la BD



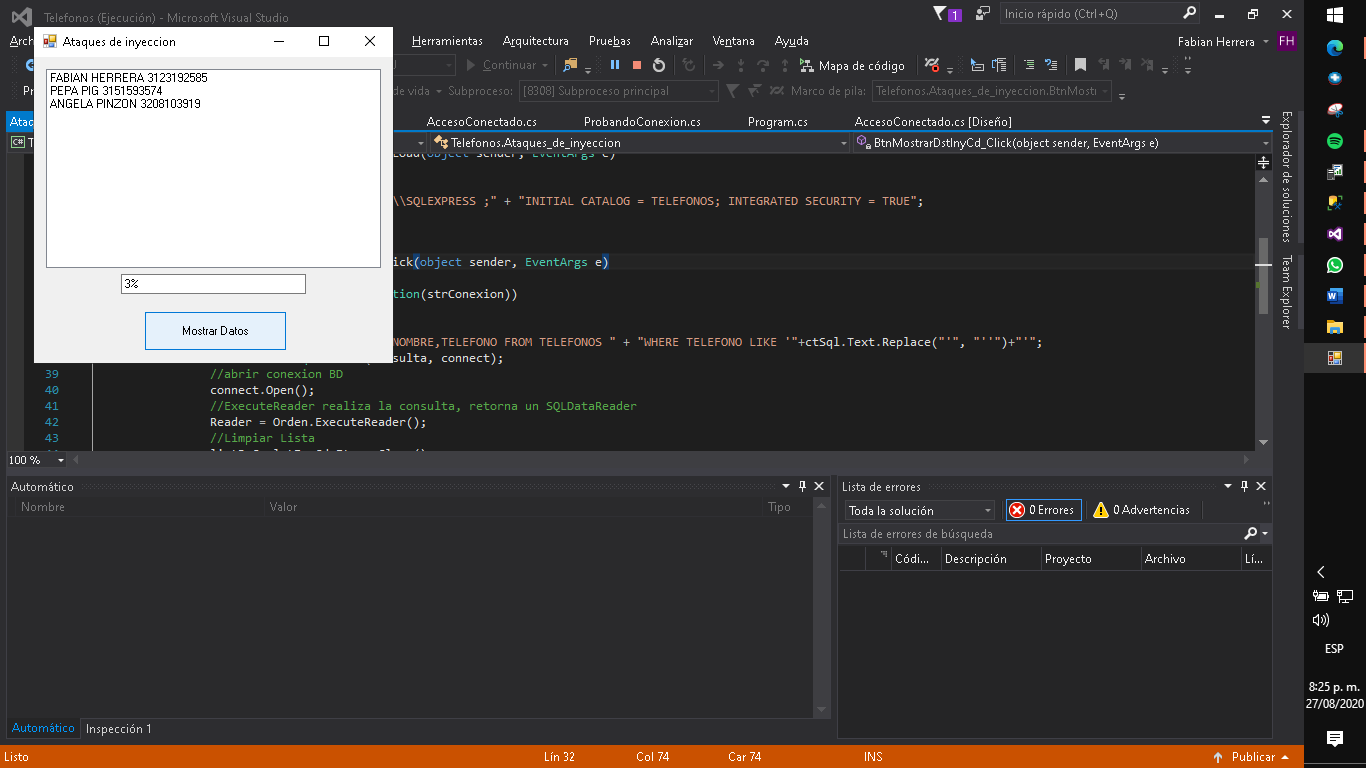
* Se añade seguridad en el campo para combatir vulnerabilidad *.Replace("'", "''")*



* La ejecución de '; DELETE FROM TELEFONOS – aparentemente realizo cambios en la base de datos



* Sin embargo los datos siguen existiendo en la base de datos ya que los caracteres ‘ o ‘’, fueron parametrizados para no ser tomados en cuenta por la aplicación, denegando la manipulación e integridad de la Base de datos.



* Algunos registros de SQL server profiler sobre las interacciones con la base de datos, Cabe tener en cuenta que algunos registros repetidos fueron almacenados en el informe de trazabilidad dadas las pruebas realizadas antes de las evidencias.

