Práctica 6
Objetivo: Seguridad

Se desea crear un sistema para proteger la seguridad de las cuentas de usuario de un sistema.

La tabla sobre la que se almacenan las cuentas de usuario tiene la siguiente estructura:

```
CREATE TABLE AccountsTable
  (id Int not null primary key,
   userCode nvarChar(20) not null,
   userPassword VarBinary(200) not null,
   name NvarChar(30) not null,
   apellido1 NvarChar(30) not null,
   apellido2 nvarChar(30) not null,
   accountNumber VarBinary(200))
```

Paso 1: Crear el entorno de desarrollo y pruebas

Para crear el entorno para el desarrollo de la solución se debe de crear una base de datos llamada 'cuentasusuarios' y en ella crear la tabla anterior.

Paso 2: Sistema de encriptación

Sobre la base de datos del paso anterior se desea implementar un sistema de seguridad con las siguientes características:

1- Debe de almacenar encriptados el userPassword y accountNumber, para ello se debe construir un procedimiento que añada una nueva cuenta con todos sus datos y almacene encriptados los valores de ambos atributos. El procedimiento debe utilizar una clave simetrica para realizar este proceso. Para esto es necesario (ver http://msdn.microsoft.com/es-es/library/aa337557(v=sql.90).aspx para sintaxis) (Algunos ejemplos: http://gerardoramosun.wordpress.com/2007/04/29/encripcion-de-datos-con-sql-server-2005/):
   a. Crear una Database Master Key (DMK).
   b. Crear un certificado llamado en la base de datos 'cuentaUsuarios' con fecha de caducidad 31 de diciembre de 2022.
   c. Crear un una clave simétrica 'seguridadusuariossimetrica' y protegerla con el certificado anterior.
2- Se debe de crear otro procedimiento que tome como entrada un código de usuario y retorne en un parámetro de salida el número de cuenta corriente sin encriptar.

Paso 3: Uso y pruebas de los procedimientos

Los usuarios que deban acceder a la información protegida de esta tabla deberan hacerlo a través de un rol específico. Para ello es necesario crear un nuevo rol en la base de datos y llamarlo 'datosSensibles'. Hay que implementar en la base de datos la seguridad necesaria para que sea posible utilizar los procedimientos desarrollados a los usuarios que se incluyan en el rol indicado. Para ello es necesario:

a) Crear un rol 'datosSensibles' y asignarle a este rol la posibilidad de consultar, insertar,modificar y borrar datos en la tabla accountsTable.
b) Dar el permiso de ejecución de ambos procedimentos al 'rol datossensibles'.

c) Dar el permiso de 'control on certificate' al certificado creado en el paso anterior al rol 'datossensibles'
d) Dar el permiso 'references on symmetric key' a la clave simétrica creada en el paso anterior al rol 'datossensibles'

Paso 4: Prueba del sistema

Para probar el sistema es preciso que a través de un nuevo usuario sea posible probar ambos procedimientos. Para ello es necesario:

a) Crear un nuevo inicio de sesión en el servidor
b) Crear un usuario de BD en la base de datos 'cuentausuarios' y asignarle el inicio de sesión creado en el punto anterior.
c) Asignar el rol 'datosSensibles' a este *user*.
d) Conectarse con este usuario en la B.D. 'cuentausuarios'
e) Probar a insertar una nueva cuenta en la tabla.
f) Probar a obtener la cuenta corriente.

Paso 5: Proteger la tabla mediante disparadores

Es preciso evitar el borrado de la tabla, para ello es necesario implemetar un disparador que evite el borrado de la tabla y de las filas de la tabla.

Paso 6: Establecer auditoria

Mediante el sistema de auditoría de SQL Server (AUDIT), es preciso implementar una auditoría completa de los accesos a la tabla (inserciones, borrados, consultas y actualizaciones). Una guía de uso en http://eliasnegrete.wordpress.com/2010/02/03/lo-nuevo-auditoria-en-sql-server-2008/

Paso 7: Proteger los datos de la tabla.

Implementar un sistema de auditoría que para cualquier cambio en la información de la tabla se almacenen los valores antes y despues de las filas afectadas.