SEGURIDAD EN BASES DE DATOS

Tareas de Administración que permiten el manejo de Seguridad

Seguridad en Bases de Datos.

- Cada DBMS entre sus funciones principales incorpora mecanismos de seguridad de manera a permitir el acceso controlado a la información contenida en las bases de datos. Conceptualmente podemos clasificar en 2 (dos):
  - Acceso Identificado de Usuarios al SGBD y a las Bases de Datos administradas por el mismo.
  - Administración de Permisos de los Usuarios (Roles, Grupos, Owner, Usuario)

Acceso Identificado de Usuarios al SGBD.

- Para ingresar al SGBD se debe contar con credenciales (login), en algunos DBMS las credenciales se integran con el Sistema Operativo (Ej. Microsoft SQL Server).
- Existen predefinidos roles de administración del SGBD, por defecto en una instalación se encuentra disponible el System User o System Administrator (por sus siglas *sa*).
- El login permite el acceso al SGBD solamente, para el acceso a las Bases de Datos se deben crear usuarios que correspondan a un login.

Roles Predefinidos en el SGBD.

- System User o System Administrator (sa): tiene definidas todas las operaciones de administración del SGBD, creación de Bases de Datos, Logins, Parámetros de Configuración, entre otras opciones.
- System Security Officer (SSO): tiene a su cargo la administración de usuarios (creación, modificación, cambios de clave).
- Operator: tiene a su cargo la tarea de administración de las copias de seguridad.
- Cada DBMS incorpora otros roles predefinidos de acuerdo a las funciones que tiene incorporadas, ej: Technical support, Replication, Monitor, Web Services.

Administración de Permisos.

- Cada base de datos tiene un propietario Owner (dbo por sus siglas en ingles), el System Administrator cuando accede a una base de datos tiene este privilegio asignado por defecto.
- Se puede crear nuevos usuarios y asignarles el privilegio de propietario de una base de datos, este usuario tendrá las opciones de crear objetos y administrar los permisos de los mismos a otros usuarios.

Administración de Permisos.

- Los usuarios que no tienen los privilegios de System Administrator u Owner de la base de datos, deben contar con los privilegios necesarios para manipular los datos de los objetos creados.

  GRANT (SELECT | INSERT | UPDATE | DELETE | EXECUTE) ON (OBJETO) TO (USUARIO)

- Así también se pueden revocar los privilegios:

  REVOKE (SELECT | INSERT | UPDATE | DELETE | EXECUTE) ON (OBJETO) FROM (USUARIO)

Administración de Permisos.

- Además de los roles que estan predefinidos en el SGBD, se pueden crear nuevos Roles que agrupen a distintos usuarios de acuerdo a una función determinada, ejemplo: Cajeros, Vendedores, Funcionarios.
- Los permisos de acceso a los objetos se asignan al ROL, posteriormente se asocian los Usuarios a cada ROL y los permisos son “heredados”, de esta manera se optimiza la administración de los permisos.

Administración de Permisos.

- El System Administrator o el Database Owner pueden asignar permisos para creación de objetos en la base de datos.

  GRANT CREATE (TABLE|PROCEDURE|FUNCTION) TO USUARIO

- La administración de la seguridad de los objetos creados por estos usuarios puede realizarse por el System Administrator, el DBO o bien el owner del objeto.

Administración de Permisos.

- Un mecanismo para asegurar la manipulación de objetos que contienen información sensible es crear procedimientos almacenados o funciones que accedan a los datos de estas tablas y otorgar el privilegio de EXECUTE.
- De esta manera los usuarios no podrán manipular la información (sentencias INSERT, UPDATE,DELETE) , solo podrán acceder a través de la ejecución del procedimiento.

Seguridad en Bases de Datos.

- Mecanismos de autenticación:

http://msdn.microsoft.com/es-es/library/bb669066%28v=vs.110%29.aspx

- Roles de Servidor y Bases de Datos:

http://msdn.microsoft.com/es-es/library/bb669078%28v=vs.110%29.aspx

- Autorización y permisos

http://msdn.microsoft.com/es-es/library/bb669084%28v=vs.110%29.aspx