CURSO BASE DE DATOS 2

(#14) SEGURIDAD

Grupo N3G/N3C REM

BIENVENIDAS / BIENVENIDOS

A/P Jorge Mario Benitez Ruiz,
DSI
Jorge.Benitez@fi365.ort.edu.uy

- **Inicio puntual 19:30 hs.**
- **Es deseable CAMARA ENCENDIDA y**
- **Se recomienda MICROFONO en Mute al Inicio**

Seguridad en los SGBD

Seguridad en las bases de datos ofrece protección contra:

- Revelación no autorizada (confidencialidad)
- Alteración no autorizada (integridad)
- Destrucción intencional o involuntaria

Protección dirigida a dos tipos de usuarios:

- Los que no tienen derechos de acceso
- Los que tienen derechos limitados a ciertas acciones

Seguridad en los SGBD

Objetivos

Integridad:

Sólo los usuarios autorizados deberían tener acceso para modificar datos.

Disponibilidad:

Los datos deben estar disponibles para usuarios y programas de actualización autorizados.

Confidencialidad:

Protección de los datos de su revelación no autorizada.

Seguridad en los SGBD

Elementos que pueden ser protegidos

Granularidad

- **Un atributo de una tupla.**
- **Un conjunto de columnas.**
- **Una tupla individual.**
- **Un conjunto de tuplas de una relación.**
- **Una relación en particular.**
- **Un conjunto de relaciones.**
- **La base de datos completa**

Seguridad en los SGBD

La sintaxis para la creación de un usuario en T-SQL es la siguiente:

```
/* Se crea el LOGIN en el SGBD */
CREATE LOGIN Jorge
            WITH PASSWORD = 'ORTdb2';

/* Se crea el usuario partiendo del LOGIN */
USE MiBase;
GO
CREATE USER Profesor FOR LOGIN Jorge;
```

```
CREATE LOGIN LoginName WITH PASSWORD = 'Pass1LoginName' MUST_CHANGE,
    DEFAULT_DATABASE = Northwind ,CHECK_EXPIRATION =  ON,
    CHECK_POLICY =  ON --OFF
```

Seguridad en los SGBD

GRANT

Concede permisos para una tabla, vista, función o procedimiento almacenado

Por ejemplo:

```
GRANT SELECT ON dbo.Tabla TO Profesor;
```

Seguridad en los SGBD

- **Select, Update**
  - **Tablas, Vistas, Columnas**
- **Insert, Delete**
  - **Tablas, Vistas**
- **Execute**
  - **Stored Procedures, Funciones**
- **View Definition**
  - **Procedures, Tablas, Vistas, Sinónimos,..**
- **Alter**
- **Control**

Seguridad en los SGBD

Cada **usuario** tiene ciertos privilegios, y dentro de esos privilegios podemos hablar de:

privilegios de sistema: son los que nos dan derecho a realizar ciertas operaciones sobre objetos de un tipo especificado.

privilegios sobre objetos: estos privilegios nos permiten realizar cambios en los datos de los objetos de otros usuarios

Cuando **creamos un usuario** es necesario **darle privilegios**, de lo contrario no podría realizar ninguna acción.

Seguridad en los SGBD

Server-Level,

- **sysadmin**
  - **pueden hacer todo**
- **serveradmin**
  - **cambiar configuraciones de la instancia, shutdown**
- **securityadmin**

Database-Level permissions

- **processadmin**
  - **terminar procesos**
- **dbcreator**
  - **create, alter, drop, restore**
- **public**
  - **todos los logins pertenecen a este rol**
- **sp_srvrolepermission 'sysadmin'**

Seguridad en los SGBD

Conceder el permiso SELECT para una tabla

En el siguiente ejemplo, se concede el permiso **SELECT** al usuario Profesor para la tabla dbo.Empleados de la base de datos Empresa.

```
USE Empresa
GRANT SELECT ON dbo.empleados TO Profesor
```

Seguridad en los SGBD

Control de Acceso Discrecional – Ejemplos -

- GRANT INSERT, SELECT ON Atletas TO Homero

  Homero puede insertar y seleccionar tuplas de Atletas

- GRANT DELETE ON Atletas TO Entrenador WITH GRANT OPTION

  Entrenador puede borrar tuplas de Atletas y autorizar borrados a otros usuarios.

- GRANT UPDATE (categoría) ON Atletas TO Organizador

  Organizador puede actualizar solamente la categoría en las tuplas de Atletas.

- GRANT SELECT ON VistaAtletasVeteranos TO Juan, Ivan, Ines

  Juan, Ivan e Ines NO pueden consultar directamente la tabla Atletas

- **REVOKE**: cuando un privilegio le es revocado al **usuarioX**, también le es revocado a los que lo obtuvieron solamente de usuarioX

Seguridad en los SGBD

La sentencia para privilegios sobre los objetos es la siguiente:

```
GRANT {privilegio_objeto[,privilegio_objeto]...| all
ON [usuario.]objeto}
TO {usuario|rol| public [,{usuario|rol|public} ...]
          [with grant option];
```

Seguridad en los SGBD

Mientras que la sentencia para crear privilegios de sistema es la siguiente:

GRANT {privilegio|rol} [,privilegio|rol}, ...]
TO {usuario|rol| public [,{usuario|rol|public} ...]
[with admin option];

Seguridad en los SGBD

En ambos caso se utiliza la sentencia revoke para suprimir privilegios, cambiando la sintaxis.

Para los privilegios de sistema:

revoke {privilegio|rol} [,privilegio|rol}] ...
from {usuario|rol|public} [,usuario|rol|public}] ...;

Para los privilegios de objetos:

revoke {privilegio[,privilegio] ... | all [privileges]}
on [usuario.]objeto
from {usuario|rol|public}[,{usuario|rol|public}]...;

Seguridad en los SGBD

Por ejemplo:

Si desea dar permisos :
SELECT, **INSERT**, **UPDATE** y **DELETE**

sobre una tabla llamada **CLIENTES** al usuario abd88 se debe ejecutar:

GRANT select,insert,update,delete **ON** **clientes** **TO** abd88;

Seguridad en los SGBD

Por ejemplo:

Si desea dar permisos de consulta en una tabla (clientes) a todos los usuarios:

GRANT select **ON** clientes **TO** public;

Seguridad en los SGBD

Por ejemplo:

Para eliminar los privilegios de borrado al usuario abd88:

REVOKE delete **ON** clientes **TO** abd88;

Seguridad en los SGBD

Por ejemplo:

Si se tiene la función **sf_buscar** y le quiere dar permisos de ejecución al usuario **abd88** :

GRANT execute **ON** **sf_buscar** **TO** **abd88**;

Seguridad en los SGBD

Por ejemplo:

Sintaxis :

revoke execute on object from user;

Si se quiere quitar los privilegios de ejecución sobre la función **sf_buscar** al usuario abd88:

revoke execute on sf_buscar from abd88;

Si se desea quitar los privilegios de ejecución a todos los usuarios:

revoke execute on sf_buscar from public;

Base de datos 2

UNIVERSIDAD ORT
Uruguay

T-SQL
Seguridad / ROLES

Seguridad en los SGBD

Autorización basada en ROLES

CREATE ROLE <nombre rol> [**WITH ADMIN** <quien>]

Roles pueden ser asignados a usuarios o a otros roles <a-quien>

Seguridad en los SGBD

ROLES

Un rol es un conjunto de permisos que recibe un nombre común y facilita la tarea de dar permisos a los usuarios.

Para crear un rol tan solo tenemos que escribir lo siguiente:
CREATE ROLE nombre_rol;

En el siguiente ejemplo se crea el rol de nombre vendedores que es propiedad del usuario Profesor

```
CREATE ROLE vendedores AUTHORIZATION Profesor
```

Seguridad en los SGBD

ROLES

En el siguiente ejemplo:

se crea un **rol** y, a continuación, se concede el permiso **EXECUTE** al rol en el procedimiento **spVentas** de la **base de datos Empresa**.

```
USE Empresa;
CREATE ROLE newrole ;
GRANT EXECUTE ON spVentas TO newrole ;
```

Seguridad en los SGBD

ROLES

En el siguiente ejemplo, muestra como agregar y/o borrar usuarios a un ROL

```
CREATE ROLE Ventas;

ALTER ROLE Ventas ADD MEMBER pedro;

ALTER ROLE Ventas DROP MEMBER pedro;
```

Seguridad en los SGBD

Trabajar con ROLES

```
create role todos_vendedores;

grant select, update on ventas to todos_vendedores;
grant select on facturas to todos_vendedores;

grant todos_vendedores to juan, maria, jose;
```

Base de datos 2

UNIVERSIDAD ORT
Uruguay

T-SQL
VIEWs (VISTAS) / Seguridad
Practico 6 (ej.5 a 9)

UNIVERSIDAD ORT
Uruguay