Bases de Datos

Tema 04. Administración de Bases de datos

Marta Elena Zorrilla Pantaleón

Rafael Duque Medina

DPTO. DE MATEMÁTICAS, ESTADÍSTICA Y COMPUTACIÓN

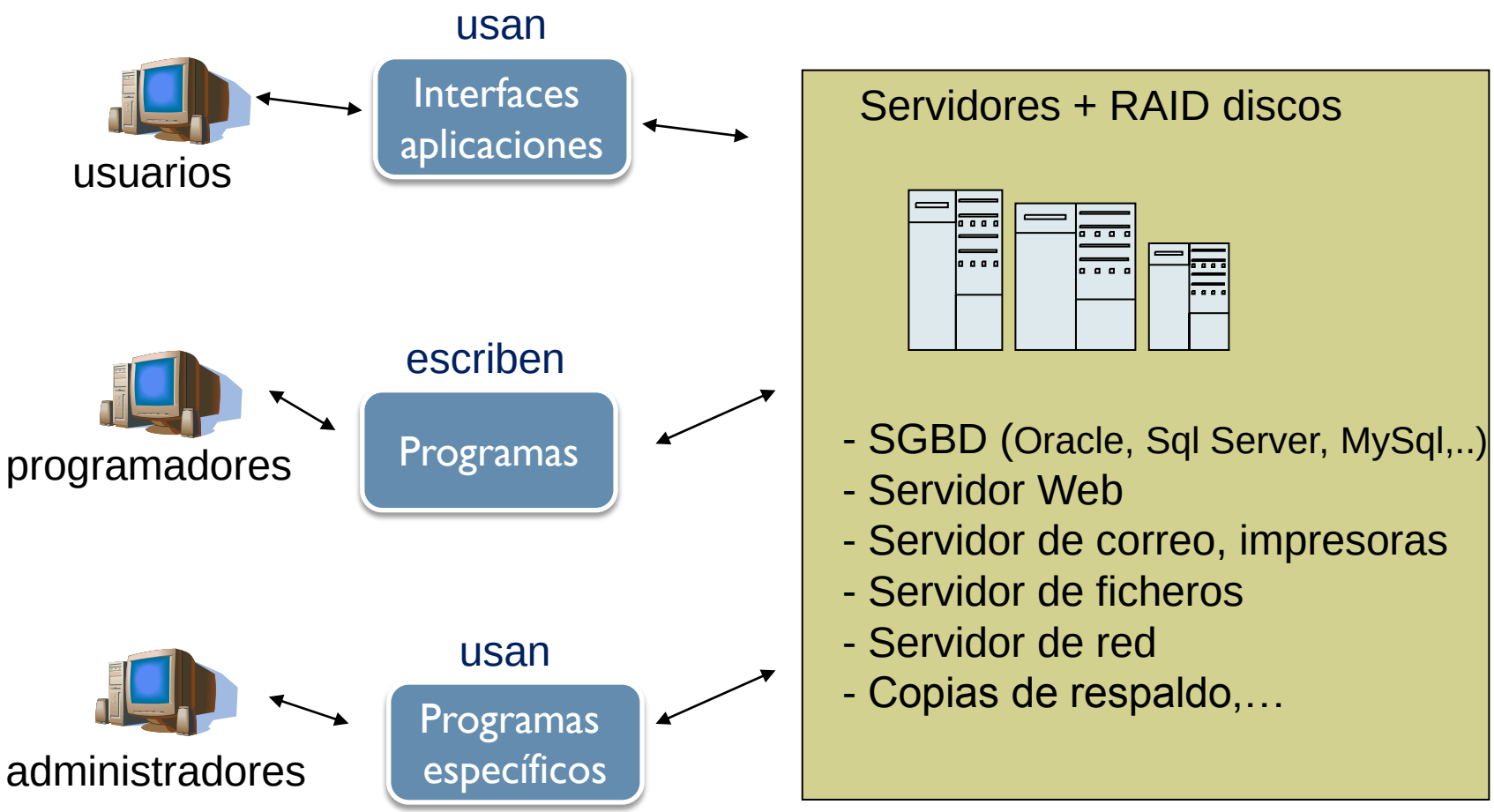
Tabla de contenido

- Arquitectura del Servicio de Informática de una Organización
  - Usuarios y tareas
  - Funciones del administrador de BD y del administrador de datos.
- Herramientas de administración de BD
  - Catálogo de BD e Information Schema.
- Seguridad en BD
  - Introducción
  - Problemas de seguridad
  - Mecanismos de seguridad
  - Seguridad a nivel de aplicación de BD

Lectura recomendada

- Cap. 23. Elmasri, R., Navathe, S.B., Fundamentos de Sistemas de Bases de Datos, 3ª; edición, Pearson Education, 2008
- Cap. 3 y 4. Pons, O. et al. Introducción a las bases de datos. Paraninfo. 2007
- Cap. 3. Piattini, M., Marcos, E., Calero, C., Vela, B. Tecnología y diseño de bases de datos. Ra-ma, 2006.
- Task of a database administrator. http://download.oracle.com/docs/cd/B28359_01/server.111/b28310/dba002.htm

Arquitectura del Servicio de Informática de una Organización



Tipos de Usuarios

- Usuarios normales – invocan programas de aplicación que se han escrito previamente
  - Ej. acceso a BD en la Web (cuentas bancarias, carritos de la compra, gestión universitaria, etc.)
- Programadores – escriben programas que embeben las llamadas a la BD o a otros sistemas de información. Utilizan herramientas DRA (.Net, Powerbuilder, VB, Jbuilder, eclipse…)
- Administradores (depende del tamaño de la organización) :
  - De Bases de Datos
  - De Sistemas y seguridad
  - De Red
  - Etc.

Administrador de Sistemas

- Responsable del mantenimiento de un sistema informático existente.

- Sus responsabilidades generalmente incluyen:
  - Realizar copias de seguridad.
  - Actualizar el sistema operativo y configurar los cambios.
  - Instalar y configurar el nuevo hardware y software.
  - Agregar, borrar y modificar información de las cuentas de usuarios, restablecer contraseñas, etc.
  - Responder consultas técnicas.
  - Responsable de la seguridad.
  - Responsable de documentar la configuración del sistema.
  - Resolución de problemas.
  - Configuración óptima del sistema.
  - Implantación de Planes de Recuperación ante Desastres (PRD).

Administrador de red

- Responsables del mantenimiento y configuración de la red

- Tareas:
  - Despliegue, mantenimiento y monitoreo del engranaje de la red: switches, routers, cortafuegos, etc.
  - Asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios.
  - Vigilar el uso eficiente de la red
  - Realizar el diseño y seguridad de la red

Administrador de BD (DBA)

- Responsable del correcto funcionamiento del SGBD a nivel técnico. Debe mantener la integridad, la seguridad y la disponibilidad de los datos del sistema.
- Tareas:
  - Instalar, configurar y actualizar SGBD
  - Administrar el respaldo y la recuperación de BDs
  - Monitorizar el rendimiento y espacio de almacenamiento del SGBD
  - Sintonización (tunning) → eficiencia
  - Seguridad y privacidad. Definir política de seguridad de acceso a datos (usuarios, roles, certificados,..).
  - Resolver problemas técnicos
  - Establecer normas y procedimientos para controlar la seguridad y la integridad de los datos (reglas para la definición de schemas, procedures, triggers, etc.)
  - Ayudar a los programadores y diseñadores de BD a utilizar eficientemente las capacidades del gestor de base de datos.
  - **Nota**: El diseño lógico y físico de las bases de datos a pesar de no ser obligaciones de un administrador de bases de datos, es a veces parte del trabajo (generalmente el paso de lógico a físico). Esas funciones, por lo general, están asignadas a los analistas/diseñadores de bases de datos.

Administrador de Datos (DA)

- Responsable de la planificación y coordinación de las fuentes de datos de la organización

- Tareas:
  - Proporciona control centralizado sobre los datos
    - Definición de datos (nombre, contenido, formato, dominio,…)
    - Integración de datos
    - Determinar la fuente fidedigna de dónde se ha de tomar el dato
  - Coordina la integridad, seguridad, privacidad y control de los datos
  - Comunicarse con gerentes del negocio y con los técnicos para identificar nuevas necesidades y planificar su desarrollo.

- Generalmente es un experto en diseño de BD y conocedor del negocio

DA vs DBA

- **Administradores de Datos:**
  - Las responsabilidades de los DA se centran en el desarrollo de los procedimientos y las políticas generales para el Sistema de Información (SI).
  - Están muy involucrados en las primeras etapas del ciclo de vida del SI, desde la planificación de la BD hasta el diseño lógico.

- **Administradores de Bases de Datos:**
  - Los DBA interactúan con el sistema y con los usuarios y suelen tener responsabilidades más bien técnicas.
  - Juegan un papel primordial en la planificación y el desarrollo de BD y en la formación de los usuarios. Están más relacionados con las fases de diseño de la aplicación y el diseño físico de la base de datos, así como con el mantenimiento operacional.

Herramientas de Admón. de BD

- Generalmente gráficas, aunque los DBA escriben habitualmente scripts en SQL para realizar tareas repetitivas (generar cuentas de usuario, asignar permisos, etc.) usando para ello el **catálogo** de la BD
- **Editor SQL**
  - Editor textual y gráfico para escribir sentencias SQL
  - Permiten conocer el plan de ejecución de consultas
- **Herramienta para la Configuración del servidor:**
  - Administrar los servicios asociados al Gestor
  - Configurar los protocolos de red utilizados por el Gestor
  - Administrar la configuración de conectividad de red de los equipos cliente
- **Generador de trazas** (seguimiento de eventos)
  - Captura y guarda datos acerca de cada evento en un archivo o en una tabla para analizarlos posteriormente. P.ej., supervisar el entorno de producción para ver qué procedimientos almacenados, consultas, etc. afectan negativamente al rendimiento (depurar aplicaciones cliente, procesos batch,…),

Herramientas de Admón. de BD (y 2)

- **Optimizador**:
  - Analiza la forma en que se procesan las consultas en las bases de datos especificadas por el usuario y, a continuación, recomienda la forma en que se puede mejorar el rendimiento del procesamiento modificando las estructuras de diseño físico tales como índices, vistas indizadas y particiones.

- **Monitor de actividad**: permite determinar el volumen y los tipos generales de actividad en el sistema, por ejemplo:
  - Transacciones.
  - Usuarios conectados actualmente en una instancia y la última instrucción ejecutada.
  - Bloqueos activos.

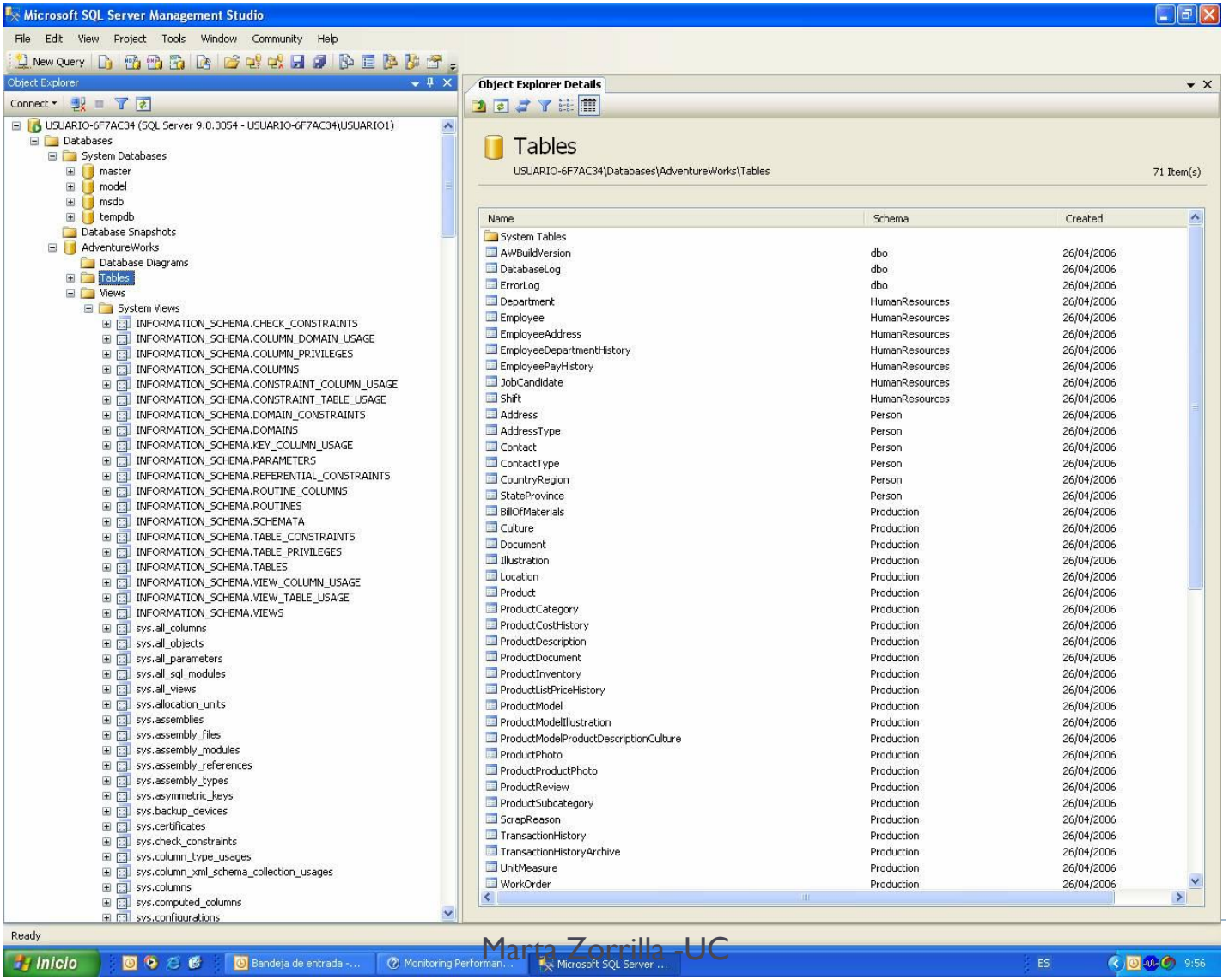
Catálogo del SGBD

- El catálogo del sistema constituye el núcleo de todo SGBD. Es una BD para almacenar los esquemas o descripciones de las BDs que el SGBD mantiene.
- Cada una de las BDs se describe por los datos almacenados en el catálogo (metadatos).
- El catálogo contiene una descripción del esquema lógico de la base de datos, del esquema interno, de los esquemas externos o vistas y de las correspondencias entre los esquemas en los diferentes niveles.
- Además, contiene información que utilizan módulos específicos del SGBD (optimización de consultas, seguridad y autorización...)
- El admón. de SGBD debe conocer y dominar la estructura del catálogo para escribir scripts que le permitan automatizar tareas (gestionar permisos, revisar restricciones, controlar el crecimiento de los índices, etc.)

Catálogo e Information Schema

- Información sobre los datos
  - Vistas del Catálogo
    - muestran metadatos que describen los objetos de una instancia del Gestor (databases, users, procedures,…)
  - Information Schema:
    - vistas que proporcionan información (metadatos) sobre todos los objetos de datos almacenados en una BD en concreto. Recogido en SQL99 y ampliado en SQL2003.
    - A pesar de ello, cada gestor lo implementa de forma propietaria (catálogo).
    - No todos los gestores lo implementan

Information_schema vs catálogo (SQL Server 2008)



Catálogo en SQL Server 2008

- Las vistas **INFORMATION_SCHEMA** se incluyen en cada base de datos. Cada vista de esquema de información contiene metadatos para todos los objetos de datos almacenados en esa base de datos en concreto.
- Las **tablas base** del sistema son las tablas subyacentes que almacenan los metadatos para una base de datos específica.
- La base de datos **master** es especial al respecto porque contiene algunas tablas adicionales que no se encuentran en ninguna de las demás bases de datos.
- La base de datos **master** registra toda la información de sistema. Dentro de esta información se incluyen los metadatos de todas las instancias, como las cuentas de inicio de sesión, los servidores vinculados y la configuración del sistema. Asimismo, master es la base de datos que registra la existencia de las demás bases de datos, la ubicación de los archivos de las bases de datos y la información de inicialización de SQL Server.

Seguridad en BD

- Los datos son un recurso valioso para las organizaciones, por lo que se han de establecer políticas de seguridad para garantizar su **confidencialidad**, su **integridad** y su **disponibilidad**
  - **Confidencialidad**. No desvelar datos a usuarios no autorizados. Comprende también la privacidad (protección de datos personales).
  - **Disponibilidad**. La información debe estar accesible.
  - **Integridad**. Permite asegurar que los datos no han sido falseados.
- El término 'seguridad en la BD' engloba a cualquier mecanismo que proteja a la base de datos frente a amenazas intencionadas o accidentales.
- La seguridad no se aplican únicamente a los datos almacenados en las propias bases de datos, sino también a otras partes del sistema que pueden afectar directamente a la propia base de datos y al transporte de los datos. Por esa razón la seguridad en la base de datos es una técnica que abarca tanto el hardware, el software, las personas y los datos.

Seguridad en BD (y 2)

- Por ello hay que establecer medidas de seguridad a varios niveles:
  - **Físico**. Los equipos informáticos deben protegerse contra los fallos físicos (cortes de red, discos redundantes,..).
  - **Humano**. Todos los usuarios deben estar bien identificados y autorizados.
  - **Sistema operativo**. Un sistema operativo débil podría permitir un acceso no autorizado.
  - **Red**. Dado que muchas bases de datos permiten accesos remotos la seguridad a nivel de red es muy importante.
  - **Sistema de gestión de base de datos**. Dado que sus usuarios pueden tener diferentes privilegios de acceso, el SGBD debe asegurarse de que éstos se cumplen.

Problemas de seguridad en BD

- El robo y el fraude
  - No afecta solo al entorno de la BD, si no a toda la organización. Son personas y por ello se deben reducir las oportunidades que estos sujetos puedan tener para llevar a cabo tales delitos.
  - El robo y el fraude no significa directamente que se produzca una alteración en los datos, si no que se produce una clara pérdida de confidencialidad y privacidad.
- Pérdida de confidencialidad y privacidad
  - Confidencialidad hace referencia a la necesidad de mantener en secreto ciertos datos críticos para la organización, mientras que privacidad hace referencia a la necesidad de proteger datos acerca de las personas (LOPD).
- Pérdida de integridad.
  - Se refiere a la aparición de datos inválidos o corrompidos.
  - Para minimizarlo, se ha de tener un buen diseño de BD, definir planes de mantenimiento de los datos y del sistema, así como realizar un correcto uso de las transacciones.

Mecanismos de seguridad

- Para minimizar todos estos problemas los gestores de BD proveen diversos mecanismos aunque estos hay que complementarlos con buenas prácticas para la construcción de aplicaciones y una adecuada seguridad a nivel de red (cortafuegos, permisos a recursos, etc.).
- Los gestores de BD ofrecen:
  - Protección de acceso al gestor
  - Control de acceso discrecional a los objetos de la BD
  - Recuperación ante fallos (checkpoints, backup)
  - Cifrado de datos
    - Algunos gestores ofrecen la posibilidad de cifrar los ficheros de datos siendo el gestor quien descifre, almacenar datos encriptados por medio de APIs o utilidades ofrecidas por el gestor.
    - Supone mayor sobrecarga y puede afectar al rendimiento, por eso hay que delimitar qué se encripta
    - Para la transferencia de datos por la red se puede hacer uso de protocolos seguros (Secure Sockets Layer, Secure Shell, IPSec)

Mecanismos de seguridad (y 2)

- Protección de acceso
  - El proceso de autentificación es el que verifica que cualquier usuario que entra en un sistema es quien dice ser.
  - Generalmente se establece a través de un nombre de usuario y una contraseña
  - Métodos de autentificación:
    - Autentificación a través de la base de datos
    - Autentificación mediante el sistema operativo
    - Autentificación a través de una red. Es posible realizar una autentificación contra una base de datos utilizando SSL (Secure Sockets Layer) o un servicio independiente (Kerberos o Radius, p.ej.)

Mecanismos de seguridad (y 3)

- Control de acceso Discrecional
  - Los privilegios discrecionales otorgan o revocan privilegios o permisos a los usuarios y/o roles sobre los distintos objetos de la BD (schema, view, table, procedure,…)
  - Para otorgar y revocar privilegios se utilizan dos sentencias SQL, Grant y Revoke (según SQL-2003).

```
GRANT <privilegios> TO <usuario> [ { <coma> <usuario> }... ]
[ WITH HIERARCHY OPTION ]
[ WITH GRANT OPTION ]
[ GRANTED BY [CURRENT_USER | CURRENT_ROLE]]
```

```
REVOKE
[GRANT OPTION FOR | HIERARCHY OPTION FOR ] <privilegios>
FROM <usuario> [ { <coma> < usuario> }... ]
[ GRANTED BY [CURRENT_USER | CURRENT_ROLE]]
```

Mecanismos de seguridad (y 3)

- Para otorgar o revocar permisos:
  - A nivel de sistema, el usuario debe tener el privilegio "ADMIN OPTION"
  - A nivel de objeto, se debe ser el propietario del objeto, o que el propietario del mismo le haya otorgado privilegios sobre él con la cláusula "WITH GRANT OPTION"
  - Sobre cualquier objeto que se otorgue un permiso, se puede utilizar la opción WITH HIERARCHY para extender esos permisos a sus objetos (tabla a columnas, p.ej.).
  - GRANT OPTION FOR : quita al usuario la capacidad de dar o quitar permisos que le fueron concedidos por la cláusula WITH GRANT OPTION. Lo mismo ocurre con HIERARCHY OPTION FOR
- Los privilegios más habituales son en:
  - Tablas/Vistas: Select , Insert , Update, Delete, References, Alter, Index
  - Columna: References, Insert, Update
  - Funciones: Select
  - Procedimientos: Execute

Mecanismos de seguridad (y 4)

- Ejemplos

```
GRANT INSERT, UPDATE, DELETE ON tbl_autores TO Maria, Juan
```

```
GRANT UPDATE( col_importe ) ON tbl_compra TO Maria
```

```
REVOKE SELECT ON fun_dameprecio FROM Maria
```

```
REVOKE EXECUTE ON proc_actu_precios FROM Maria
```

Mecanismos de seguridad (y 5)

- Grant y Revoke también permiten definir autorizaciones a nivel de rol

```
GRANT <rol> [ { <coma> <rol> }... ]
TO <rol/usuario> [ { <coma> <rol/usuario> }... ]
[ WITH ADMIN OPTION ]
[ GRANTED BY [CURRENT_USER | CURRENT_ROLE]]
```

```
REVOKE [ ADMIN OPTION FOR ] <rol> [ { <coma> <rol> }... ]
FROM <rol/usuario> [ { <coma> <rol/usuario> }... ]
[ GRANTED BY [ CURRENT_USER | CURRENT_ROLE]]
```

  - Cláusula "WITH ADMIN OPTION" permite a un usuario/rol agregar, eliminar o cambiar los roles de los demás usuarios o roles
  - EJ.: **GRANT** rol_alumno **TO** Maria

Mecanismos de seguridad (y 6)

- Limitaciones de seguridad en Gestor BD
  - No se puede establecer privilegios a nivel de fila (p. ej. cada alumno sólo vea sus notas). Aunque hay extensiones para proporcionar control de acceso en el nivel de las filas y para trabajar con gran número de usuarios aún no están normalizadas.
  - Una estrategia es utilizar vistas para restringir la información, con ellas se consigue que el usuario/programa no interactúe directamente con la base de datos.
  - También el uso de funciones y procedimientos almacenados ayuda a garantizar la seguridad pues los usuarios/programas no necesitan tener permiso para acceder a las tablas, solo permiso de ejecución de los procedimientos y/o funciones. Además, si están bien programados, impiden operaciones incorrectas asegurando las reglas de negocio.

Mecanismos de seguridad (y 7)

- Recuperación ante fallos
  - Otro aspecto importante es realizar copias de seguridad, ya que ante cualquier inconveniente, como fallo de lectura en un disco, problema hardware en el servidor, accesos indeseados al sistema… puede ser necesario recuperar los datos en la última situación estable en el mismo u otro servidor.
  - Medios
    - Copias de seguridad (back-up).
      - Periódicamente se deben hacer copias y guardarlas en lugar seguro. Estas deben basarse en copias completas (por ej. cada semana) e incrementales (cada día o fracción) para facilitar la recuperación y no hacer caer el rendimiento del gestor con copias frecuentes.
    - Registro histórico (log).
      - El log se ha de almacenar en un disco distinto a los datos de forma que este no se pierda a no ser que el fallo sea catastrófico.
      - También se debe realizar copia de seguridad de él, de forma que se pueda restaurar la base de datos desde su último backup hasta última situación estable antes del fallo.

Seguridad a nivel de aplicación de BD

- Otro aspecto importante para asegurar las BD es impedir o salvaguardar su acceso y uso malintencionado a través de las aplicaciones de usuario. Para ello se debe:
  - Encriptar la información de conexión (usuario – passwd – servidor) generalmente disponible en los ficheros de configuración de las aplicaciones
  - Monitorizar los usuarios que se conectan a la BD y desde qué IP
  - Ofuscar el código fuente de la aplicación para evitar que los intrusos averigüen información sobre la estructura de la base de datos, o información de autentificación
  - Evitar la inyección SQL, esto es, construir consultas como concatenación de textos introducidos por el usuario y disponibles en la aplicación. Utilizar consultas parametrizadas

Inyección SQL (Ejemplo)

CODIGO DE LA APLICACIÓN

```
var ciudad;
 ciudad = Request.form ("ciudad")
var sql = "SELECT * FROM Pedidos
        WHERE ciudad = '" + ciudad + "'";
```

USUARIO 'NORMAL'

Introduce "Valencia" en el formulario

La consulta enviada al gestor es:

```
SELECT * FROM pedidos WHERE ciudad = 'Valencia'
```

USUARIO MALICIOSO

Introduce la siguiente sentencia en el formulario:

Valencia' ; DROP TABLE Pedidos

La consulta enviada al servidor es:

```
SELECT * FROM Pedido WHERE ciudad = 'Valencia';
DROP TABLE Pedidos
```