Seguridad e integridad de bases de datos

USB

Necesidad de seguridad

La seguridad de las bases de datos es una área amplia que abarca varios temas, entre ellos se encuentran los siguientes:

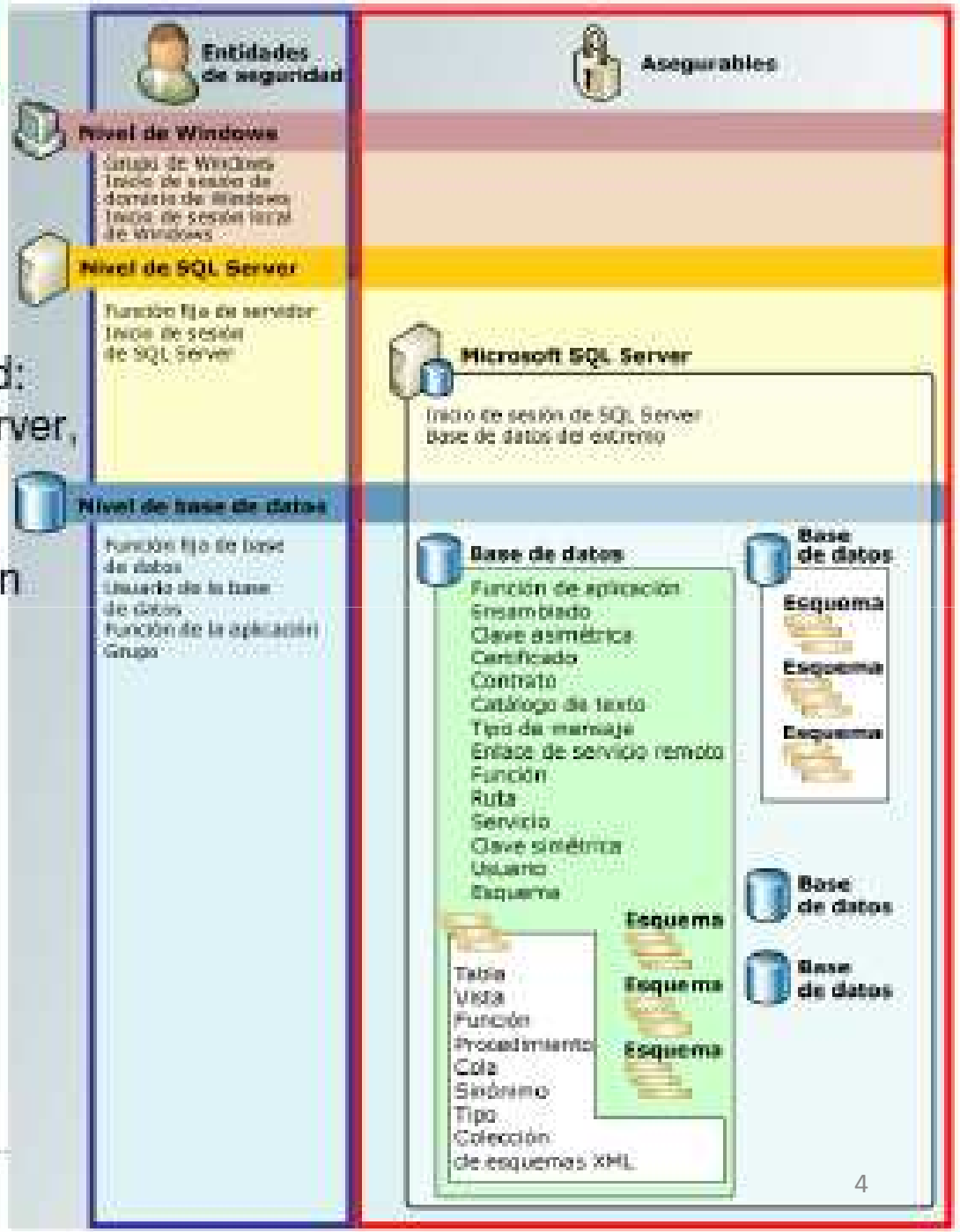
- Cuestiones éticas y legales relativas al derecho de tener acceso a cierta información
- Cuestiones de política a nivel gubernamental, institucional o corporativo, relacionadas con el tipo de información que no debe estar disponible para el publico
- Cuestiones relacionadas con el sistema, como los niveles del sistema en que deben manejarse diversas funciones de seguridad
- Las necesidades en las organizaciones de identificar múltiples niveles de seguridad y clasificar los datos y los usuarios según estos niveles

Modelo de seguridad en Sql Server

Jerarquía de Seguridad

Principals: entidades de seguridad: Usuarios windows, usuarios sql server, Usuarios de BD

Asegurables: recursos que pueden ser protegidos



4

Tipos de seguridad

En la actualidad se acostumbra hablar de dos tipos de mecanismos de seguridad en las bases de datos:

- Los **mecanismos de seguridad discrecionales se** usan para otorgar privilegios a los usuarios, incluida la capacidad de tener acceso a archivos, registros o campos de datos específicos en un determinado modo.
- Los **mecanismos de seguridad obligatorios sirven** para imponer igualdad de múltiples niveles clasificando los datos y los usuarios en varias clases (o niveles) de seguridad e implementando después la política de seguridad apropiada de la organización.

Control de acceso

- Un problema de seguridad común a todos los sistemas de computo es el de evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información o para efectuar cambios mal intencionados en una porción de la base de datos.
- El mecanismo de seguridad de un SGBD debe incluir formas de restringir el acceso al sistema como un todo. Esta función se denomina **control de acceso y se pone en practica** creando cuentas de usuarios y contraseñas para que el SGBD controle el proceso de entrada al sistema.

Cifrado de datos

- Otra técnica de seguridad es el **cifrado de datos, que** sirven para proteger datos confidenciales que se transmiten por satélite o por algún otro tipo de red de comunicaciones. El cifrado puede proveer protección adicional a secciones confidenciales de una base de datos.
- Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado que tenga acceso a los datos codificados tendrá problemas para descifrarlos, pero un usuario autorizado contara con algoritmos (o claves) de codificación o descifrado para descifrarlos.

Administrador de la Base de Datos

El administrador de bases de datos (DBA) es la autoridad central que controla un sistema de este tipo.

- El DBA tiene una cuenta privilegiada en el SGBD, a veces denominada cuenta del sistema, que confiere capacidades extraordinarias no disponibles para cuentas y usuarios ordinarios de la base de datos.
- El DBA ejecuta los siguientes tipos de acciones:
  - Creación de cuentas
  - Concesión de privilegios
  - Revocación de privilegios
  - Asignación de niveles de seguridad
- El DBA es el responsable de la seguridad global del sistema de base de datos.

Violaciones de la seguridad

- Entre las formas de acceso malintencionado se encuentran:
  - La lectura no autorizada de los datos (robo de información)
  - La modificación no autorizada de los datos
  - La destrucción no autorizada de los datos
- La **seguridad de las bases de datos se refiere a la** protección frente a accesos malintencionados. Para proteger la base de datos hay que adoptar medidas de seguridad en varios niveles:
  - Sistema de bases de datos
  - Sistema operativo
  - Red
  - Físico
  - Humano

Violaciones de la seguridad

- Debe conservarse la seguridad en todos estos niveles si hay que asegurar la seguridad de la base de datos. La debilidad de los niveles bajos de seguridad (físico o humano) permite burlar las medidas de seguridad estrictas de niveles superiores (base de datos).
- La seguridad dentro del sistema operativo se aplica en varios niveles, que van desde las contraseñas para el acceso al sistema hasta el aislamiento de los procesos concurrentes que se ejecutan en el sistema. El sistema de archivos también proporciona algún nivel de protección.

Autorizaciones

- Los usuarios pueden tener varios tipos de autorización para diferentes partes de la base de datos.
- Entre ellas están las siguientes:
  - La autorización de **lectura** permite la lectura de los datos, pero no su modificación.
  - La autorización de **inserción** permite la inserción de datos nuevos, pero no la modificación de los existentes.
  - La autorización de **actualización** permite la modificación de los datos, pero no su borrado.
  - La autorización de borrado permite el borrado de los datos.

Autorizaciones

Además de estas formas de autorización para el acceso a los datos, los usuarios pueden recibir autorización para modificar el esquema de la base de datos:

- La autorización de índices permite la creación y borrado de índices.
- La autorización de recursos permite la creación de relaciones nuevas.
- La autorización de alteración permite el añadido o el borrado de atributos de las relaciones.
- La autorización de eliminación permite el borrado de relaciones.

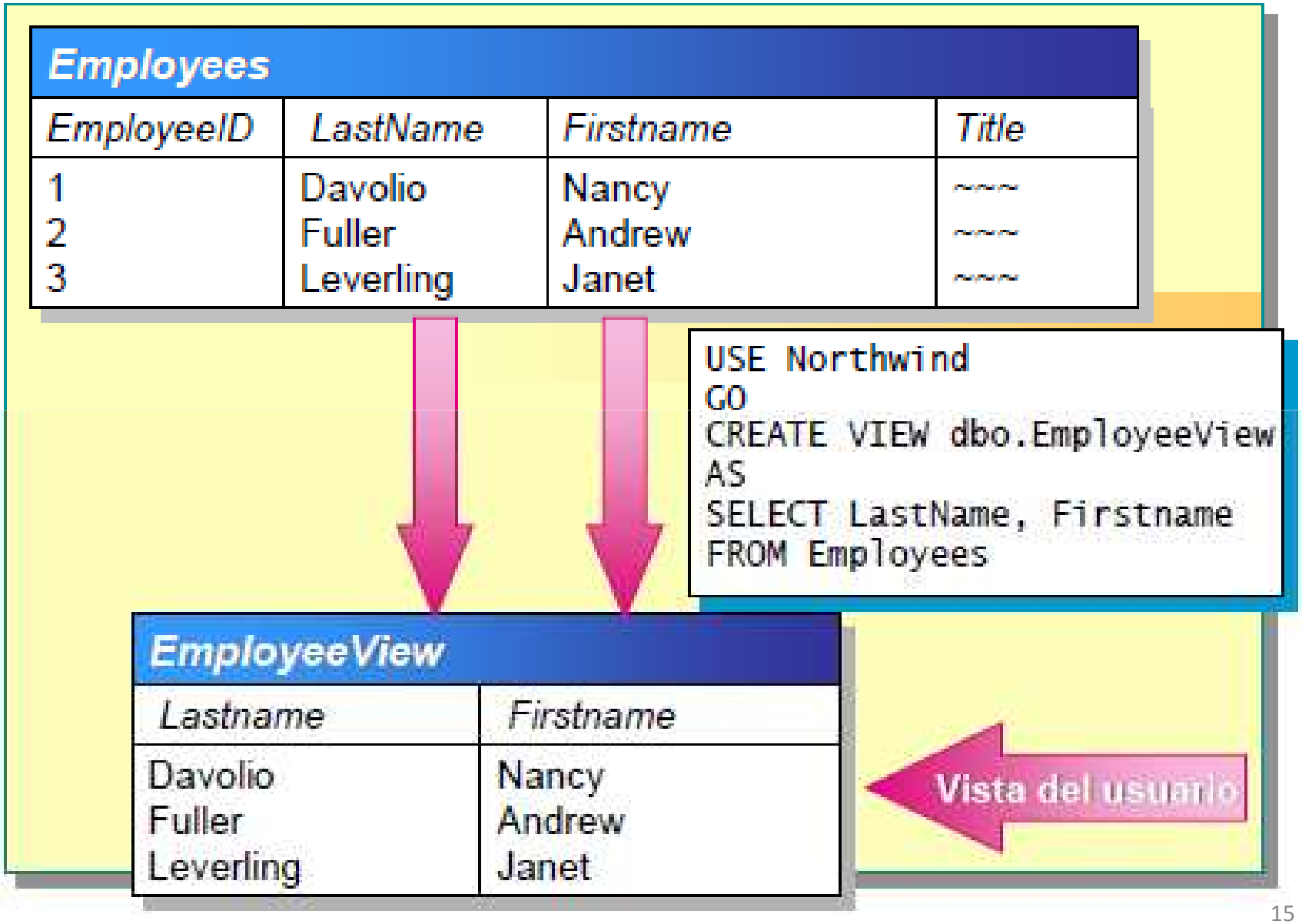
Estrategias de seguridad

- **Uso de vistas y funciones**
  - Dar permisos a vistas y funciones en lugar de a las propias tablas
  - Ocultan la complejidad de la BD
  - Permiten gestionar el acceso a nivel de columna
- **Uso de procedimientos almacenados**
  - Impiden operaciones incorrectas asegurando las reglas de negocio
  - Los usuarios no necesitan tener permiso para acceder a las tablas, solo permiso de ejecución de los procedimientos
  - Permiten establecer el nivel de seguridad más fino (contexto)

Vistas

- Una vista es una relación virtual.
- Una vista se puede construir realizando operaciones como las del álgebra relacional a partir de las relaciones base de la base de datos. Las relaciones base son aquellas que forman parte directa de la base de datos, las que se encuentran almacenadas físicamente.
- Estas proporcionan un poderoso mecanismo de seguridad, ocultando partes de la base de datos a ciertos usuarios. El usuario no sabrá que existen aquellos atributos que se han omitido al definir una vista.

Creación de vistas en sql server



Creación de vistas en sql server

- Una vista ofrece la posibilidad de almacenar una consulta predefinida como un objeto en una base de datos para usarse posteriormente.
- Las tablas consultadas en una vista se denominan *tablas base.* Algunos ejemplos habituales de vistas son los siguientes:
  - Un subconjunto de las filas o columnas de una tabla base.
  - Una unión de dos o más tablas base.
  - Una combinación de dos o más tablas base.
  - Un resumen estadístico de una tabla base.
  - Un subconjunto de otra vista o alguna combinación de vistas y tablas base.

Ejemplo

```
USE biblioteca
GO
CREATE VIEW dbo.VistaAutor
AS
SELECT Nombre, Nacionalidad
SELECT * from VistaAutor
FROM Autor
```

Resultados | Mensajes

	Nombre	Nacionalidad
1	Vitter David	USA
2	Saint Euxpery Antonie	Francia
3	Benedetti Mario	Ecuador

Creación de vistas en Posgresql

```
CREATE TABLE estudiante (nombre varchar(20), ci int8
PRIMARY KEY, edad int2);
```

nombre	ci	edad
María	17345678	17
Juan	12345657	20
Luis	23456923	19

```
CREATE VIEW mayoresedad AS SELECT * FROM estudiante
WHERE edad>18;
```

nombre	ci	edad
Juan	12345657	20
Luis	23456923	19

Encriptación de Datos

¿para qué?

- Evitar acceso a datos sensibles
- Evitar robo de copias de seguridad con datos sensibles

¿qué técnicas?

- Encriptación a nivel de columna
- Encriptación transparente (TDE), afecta a toda la BD

¿coste?

- Mayor sobrecarga y puede afectar al rendimiento
- Requiere una estrategia para la definición y mantenimiento de claves, passwords y certificados
- Por ello no debe considerarse para todos los datos y conexiones

Encriptación y autenticación

- Una técnica de seguridad es el cifrado de datos que sirve para proteger datos confidenciales que se transmiten por satélite o algún tipo de red de comunicaciones. Asimismo el cifrado puede proveer protección adicional a secciones confidenciales de una base de datos.
- Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado tendrá problemas para descifrar los datos codificados, pero un usuario autorizado contará con algoritmos para descifrarlos.

Encriptación de datos - Ejemplo

```
USE AdventureWorks2008R2;

--If there is no master key, create one now.
IF NOT EXISTS
    (SELECT * FROM sys.symmetric_keys
          WHERE symmetric_key_id = 101)
    CREATE MASTER KEY ENCRYPTION
      BY PASSWORD = 'Th15i$aS7riN&ofR@nD0m!T3%t'

select top 5 * from Sales.CreditCard
/*
CreditCardID CardType      CardNumber     ExpMonth ExpYear ModifiedDate
------------ ------------ ------------- -------- ------- ----------
1            SuperiorCard  33332664695310 11       2006    2007-08-30
2            Distinguish   55552127249722 8        2005    2008-01-06
3            ColonialVoice 77778344838353 7        2005    2008-02-15
4            ColonialVoice 77774915718248 7        2006    2007-06-21
5            Vista         11114404600042 4        2005    2007-03-05
*/
```

Control de Acceso

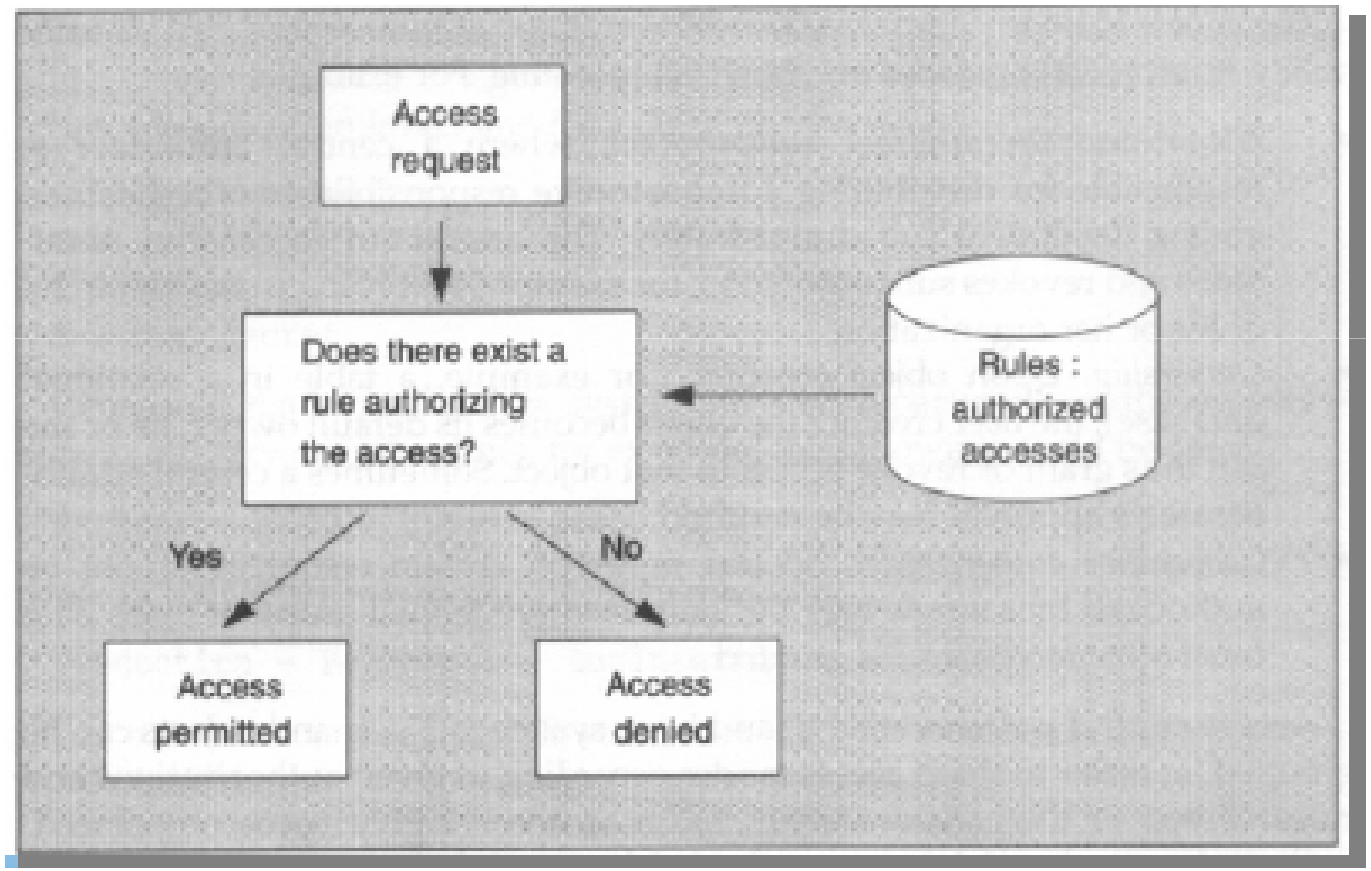
- Una BD para una empresa contiene grandes cantidades de información y usualmente tiene varios grupos de usuarios, la mayoría de estos usuarios necesitan acceder sólo a una pequeña parte de los datos.
- Por ello, un DBMS tiene dos enfoques principales para esto:
- **1.- Control de acceso discrecional: Previene de accesos** no autorizados a la base de datos y está basado en los derechos de acceso o privilegios y mecanismos para darle al usuario tales privilegios.
- **2. Control de acceso obligatorio**

Control de acceso discrecional

- Acceso discrecional es un modo de restringir el acceso a la información basado en privilegios. Dos niveles de asignación de privilegios:
- **Nivel de cuenta: En este nivel el administrador especifica los** privilegios particulares que tiene cada usuario, independiente de las tablas de la BD (CREATE TABLE, CREATE VIEW, ALTER, MODIFY, SELECT).
- **Nivel de relación: En este nivel se controlan los privilegios** para tener acceso cada relación o vista individual. Cada tabla de BD tiene asignada una cuenta propietario, que tiene todos los privilegios sobre esa tabla y se encarga de otorgarlos al resto de cuentas.

Control de acceso obligatorio

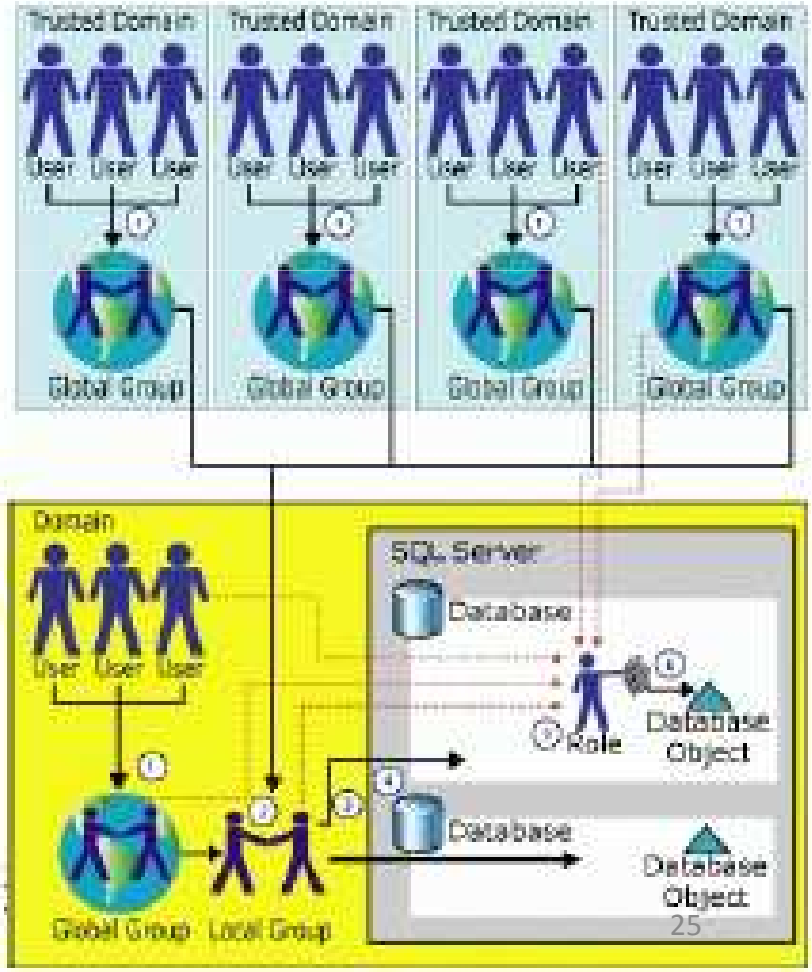
- Cerradas
- Abiertas



Inicios de sesión - Usuarios

- Modo de autentificación (acceso al servidor) **(Inicio de sesión: Login)**
  - Windows (S.O.)
  - Servidor SQL Server

- Acceso y gestión de una BD (autorización: User)
  - Permisos a
    - objetos de BD
    - ejecución de sentencias
  - Permisos a través de roles:
    - del servidor o de BD
    - definidos por el usuario



Concesión de permisos

```
GRANT { ALL [ PRIVILEGES ] }
    | permission [ ( column [ ,...n ] ) ] [ ,...n ]
    [ ON [ class :: ] securable ] TO principal [ ,...n ]
    [ WITH GRANT OPTION ] [ AS principal ]
```

- ALL : Esta opcion no concede todos los permisos posibles.

-Si el asegurable es una base de datos, "ALL" significa BACKUP DATABASE, BACKUP LOG, CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATE RULE, CREATE TABLE y CREATE VIEW.

- Si es una función escalar, "ALL" significa EXECUTE y REFERENCES.

- Si es una función con valores de tabla, "ALL" se refiere a DELETE, INSERT, REFERENCES, SELECT y UPDATE.

- Si es un proc. almacenado, "ALL" significa DELETE, EXECUTE, INSERT, SELECT y UPDATE.

- Si es una tabla o vista, "ALL" significa DELETE, INSERT, REFERENCES, SELECT y UPDATE.

- WITH GRANT OPTION: el usuario al que se le otorga permiso, puede a su vez, otorgárselo a otro.

Concesión de Permisos

- Permitir a los usuarios Maria, Juan y Marta crear bases de datos y tablas

```
GRANT CREATE DATABASE, CREATE TABLE
TO Maria, Juan, [Servidor\Marta]
```

- Permitir a María y a Juan, insertar, modificar y borrar en la tabla autores.

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

- Permitir a María actualizar el importe del préstamo.

```
GRANT UPDATE( importe ) ON prestamo
TO Maria
```

Revocación de permisos

```
REVOKE [ GRANT OPTION FOR ]
   {   [ ALL [ PRIVILEGES ] ]
         | permission [ ( column [ ,...n ] ) ] [ ,...n ] }
   [ ON [ class :: ] securable ]
   [TO | FROM } principal [ ,...n ]
   [ CASCADE] [ AS principal ]
```

- **GRANT OPTION FOR** : se quita al usuario la capacidad de dar o quitar permisos que le fueron concedidos por la cláusula WITH GRANT OPTION
- ***permiso***: SELECT, INSERT, DELETE, UPDATE, REFERENCES, EXECUTE, CREATE, etc.
- **CASCADE** : se quita el permiso al usuario/role y a los usuarios/roles a los que dio permiso, si se le concedió GRANT OPTION.
- **AS** : usuario o role que quita el permiso

Revocación de permisos - ejemplos

- Impedir a los usuarios Maria y Marta crear vistas en la BD activa.

```
REVOKE CREATE VIEW
TO Maria, [Servidor\Marta]
```

- Impedir que Maria ejecute la función "dameprecio".

```
REVOKE SELECT ON dbo.dameprecio
TO Maria
```

Denegar Permisos

Deniega un permiso a una entidad de seguridad. Evita que la entidad de seguridad herede permisos por su pertenencia a grupos o funciones. Su sintaxis es:

```
DENY { [ ALL [ PRIVILEGES ] ]
      | permission [ ( column [ ,...n ] ) ] [ ,...n ] }
  [ ON [ class :: ] securable ] TO principal [ ,...n ]
  [ CASCADE] [ AS principal ]
```

- ***permiso***: SELECT, INSERT, DELETE, UPDATE, REFERENCES, EXECUTE, CREATE, etc.
- **CASCADE** : Indica que el permiso se deniega para la entidad de seguridad especificada y para el resto de entidades de seguridad a las que ésta concedió el permiso. Es obligatorio cuando la entidad de seguridad tiene el permiso con GRANT OPTION.
- **AS** : usuario o role que quita el permiso