Seguridad II

Control de acceso

Control de acceso

Definimos control de acceso como conjunto de funciones del SGBD para asegurar que los accesos del sistema estan de acuerdo con las reglas establecidas por la política de protección fijada para el modelo de negocio.

Control de acceso

El control de acceso se puede considerar que está formado por dos componentes:

1. Políticas de acceso: definen los principios por los cuales se autoriza un usuario o se deniega el acceso específico a la base de datos.

Control de acceso

2. Mecanismos de seguridad: formados por todos aquellos procedimientos que se aplicarán a aquellas consultas con el objetivo que los usuarios cumplan con los principios anteriores.

Privilegios

El control de acceso discrecional permite que un usuario tenga diferentes derechos de acceso sobre diferentes objetos.

Privilegios

Para un programador es más sencillo decir lo que puede hacer un usuario que no decir lo que no puede hacer, por esa razón los lenguajes soportan la definición de autoridades y no de restricciones.

Estas autoridades se definen en cuatro componentes

Privilegios

1.- Nombre: la autoridad será registrada en el catálogo bajo este nombre.

2.- uno o más privilegios especificados (GRANT en SQL)

3.- la varrel a la que se aplica la autoridad

Privilegios

4.- uno o más usuarios a quienes se van a otorgar los privilegios especificados sobre la varrel especificada

Registros de auditoría

Es importante no dar por hecho que el sistema de seguridad es perfecto, en bases de datos donde la información es valiosa o los procesos que se realizan son de nivel crítico para la integridad, un registro de auditoría es necesario.

Auditorías

La auditoría corresponde a un conjunto de mecanismos para saber quien ha hecho el qué.

Se utilizan para los siguientes casos:

- La investigación sospechosa
- Monitorización de actividades específicas.

Auditorías

El sistema de auditorías tiene que permitir:

Auditoría de sentencias: indica cuando y quien ha utilizado el tipo de sentencia concreta.

Auditoría de objetos: es sistema auditará cada vez que se haga una operación sobre un objeto determinado.

Auditorías

Auditar sentencias sobre objetos, una versión combinada de las dos anteriores.

Auditar usuarios o grupos.

Registros de auditoría

un registro de auditoría es un archivo o una BD especial en la que el sistema lleva automáticamente la cuenta de todas las operaciones realizadas por los usuarios sobre los datos.

Control de acceso obligatorio

Los controles obligatorios son aplicables a las bases de datos en que los datos tienen una estructura de clasificación bastante estática y rígida, como puede ser caso de determinados ambientes militares o gubernamentales.

Control de acceso obligatorio

cada objeto de datos tiene un nivel de clasificación, el cual puede ser:

1. Secreto máximo (TS: top secret)
2. Secret (S)
3. Confidencial (C)
4. No clasificado (U: unclassified)

Control de acceso obligatorio

cada usuario tiene un nivel de acreditación (las mismas de clasificación).

Por lo tanto, se imponen las reglas de Bell-LaPadula, estas reglas son:

Control de acceso obligatorio

1. un sujeto puede puede ver un objeto si y solo si la clasificación del sujeto es mayor que la clasificación del objeto.
2. Un sujeto puede modificar un objeto si su nivel de acreditación es igual que el nivel de clasificación del objeto.

Administrador y seguridad.

Por lo que se refiere a la seguridad las funciones del administrador incluye:

1. Definición de esquema: El administrador crea el esquema original de la BD, escribe el conjunto de instrucciones de definición de datos.

Administrador y seguridad.

2. Definición de la estructura y del método de acceso: referente al software cliente utilizado y las diferentes actividades relacionadas con el almacenaje y la recuperación utilizando diferentes estandards

Administrador y seguridad.

3. Modificación del esquema y la organización física. Los administradores de la BD hacen cambios en el esquema y la organización física para reflejar las necesidades cambiantes dentro de la organización o hacer modificaciones físicas para mejorar el rendimiento

Administrador y seguridad.

4. Concesión de autorización para el acceso a los datos. Concesión de diferentes tipos de autorizaciones a diferentes usuarios según los criterios establecidos por la empresa.

Administrador y seguridad.

5. Mantenimiento rutinario: actividades como
   A. Copia de seguridad periódica.
   B. Asegurarse que hay espacio en disco para el almacenamiento de los datos.
   C. supervisar tareas y la no degradación del rendimiento.