**AaronAndal**

**M02 - Base de datos**

**Objetivos y funcionalidades de los SGBD**

1. **Posibilitar las consultas no predefinidas de cualquier complejidad**

Los usuarios que tienen acceso a un Sistema de Gestión de Base de Datos han de poder plantearse un sistema de consulta sobre los datos almacenados.

El SGBD tiene que ser capaz de responder por sí mismo a la consulta, sin necesidad de recorrer a alguna aplicación externa.

Antiguamente cuando no existían las base de datos ni los gestores habían dos posibilidades

1. Un listado secuencial de todos los datos y seleccionar manualmente las que interesan.
2. Escribir el código fuente de un programa para resolver una cuestión, compilarlo y ejecutarlo.

Actualmente, están capacitados para interpretar directamente las consultas expresadas habitualmente cómo sentencias formuladas en el lenguaje de consulta SQL. Además los SGBD del mercado deben de alcanzar una serie de objetivos y ofrecer determinadas funcionalidades.

1. **Garantizar la independencia física y la independencia lógica de los datos**

Hay que garantizar la máxima independencia física de los datos respecto a los procesos de los usuarios. Se tienen que poder llevar a cabo todo tipo de cambios tecnológicos de índole física para mejorar el rendimiento, sin tener que modificar ni las consultas a la BD ni las aplicaciones que acceden a ella.

De la misma forma también se debe asegurar la independencia lógica de los datos, esto implica que las modificaciones en la base de datos no impida la ejecución normal de los procesos de los usuarios.

1. **Evitar o solucionar los problemas derivados con la redundancia**

La repetición de los datos hoy en día se ha considerado como algo negativo, ya que conlleva a un coste de almacenamiento innecesario. Los discos duros cada día son más caros pero suben más su capacidad y rendimiento.

La repetición de los datos puede ser peligrosa y que cuando se actualizan pueden perder la integridad de los datos. Quiere decir que una pequeña modificación puede alterar los datos y su coherencia.

La **redundancia** consiste en la repetición indebida de los datos. Se incremente los riesgos de pérdida de integridad.

Los SGBD han de permitir al diseñador de la BD la repetición de datos.

El objetico de los SGBD es garantizar la actualización correcta de todos los datos ahí donde estén duplicadas de forma automática.

Otro tipo se llama **datos derivados**, que trata de datos almacenados en la base de datos, que en realidad son el resultado de los cálculos hechos con otros datos presentes en la misma BD.

Los datos derivados también pueden ser aceptables y conllevan a una repetición evidente de algunos datos.

1. **Proteger la integridad de los datos**

A demás de **redundancia**, hay muchos otros motivos que puedes hacer perder la consistencia de los datos como las siguientes:

* Los errores humanos
* Las diferencias de los algoritmos de las aplicaciones.
* Las averías de los soportes físicos de almacenamiento.
* Las transacciones incompletas como consecuencia de las interrupciones de suministramiento eléctrico.
* Los SGBD tienen que proteger la integridad de las BD de cada uno de los casos. Por esto disponemos:
* Las reglas de integridad (restricciones),
* Los sistemas de restauración basados en copias de seguridad.

Mediante las **reglas de integridad**, el sistema valida automáticamente ciertas condiciones en producirse una actualización de datos, y la autorización si se cumple, o deniega el permiso en caso contrario.

Las reglas de integridad pueden ser de dos tipos:

* **Restricciones del modelo**: Las reglas insertadas al modelo de datos que utiliza el SGBD. El sistema los incorpora predefinidas.
* **Restricciones de usuario**: Son regalos definidas por el usuario de la BD y sirve para modelar aspectos específicos del mundo real.

Los SGBD también proporcionan herramientas para realizar periódicamente **copias de seguridad de los datos** que permiten restaurar los datos dañados y retornarlos a un estado consistente.

1. **Permitir la concurrencia de usuarios**

Uno de los objetivos fundamentales de todo SGBD es posibilitar de manera eficiente el acceso simultáneo por parte de muchos usuarios.

Hemos de considerar dos tipologías de acceso concurridos, con problemáticos bien diferenciadas:

* **Acceso de consulta de datos**:Podrían provocar problemas de rendimiento, derivados por soportes físicos disponibles o proporcionar herramientas de copias de seguridad.
* **Acceso de modificación de datos**: Las actualizaciones de los mismos datos pueden causar problemas de interferencia que tengan como consecuencia la aparición de datos erróneos y la pérdida de la integridad de la BD.

Para tratar correctamente los problemas derivados de la concurrencia de usuarios, los SGBD utilizan fundamentalmente dos técnicas: **las transacciones y los bloqueos**.

Un **intercambio o transacción** consiste en un conjunto de operaciones simples que deben ejecutarse como una unidad.

Las operaciones de una transacción nunca se han de ejecutar a medias. Si por algún motivo no se ha podido ejecutarlas correctamente. Automáticamente los cambios no se guardarán.

Aunque también se puede dar la situación en que diferentes transacciones quieran acceder a la BD a la vez. En esos casos, aunque la transacción se considere correcta no se podrá garantizar la consistencia de los datos.

Un **bloqueo** consiste en impedir el acceso a determinados datos durante el tiempo en que sean utilizados por un intercambio.

Los bloqueos provocan esperas y pausas, pero las nuevas versiones de diferentes SGBD del mercado se esfuerzan a minimizar estos efectos negativos.

1. **Contribuir a la seguridad de los datos.**

La seguridad de los datos hace referencia a su confidencialidad. El acceso a los datos no tiene que ser libre sino que con precaución se tiene que vigilar.

Los SGBD tienen que permitir definir autorizaciones de auditoría para el acceso a las bases de datos. Estableciendo permisos diferentes en función de las características del usuario/grupos.

Hay 4 niveles de SGBD:

* Nivel global de toda la BD
* Nivel de entidad
* Nivel de atributo
* Nivel de tipo de operación

Estos mecanismos de seguridad requieren que cada usuario se pueda identificar con sus credenciales. La forma más habitual es la utilización de nombre de usuario y contraseña. Aunque hay otros métodos de identificación.

Las técnicas de encriptación permiten almacenar la información utilizando códigos secretos que no permiten el acceso con facilidad a los datos. Para ello la persona necesita saber el código secreto.

La encriptación puede disminuir el acceso a los datos ya que conlleva a la utilización de algoritmos adicionales. Es conveniente optimizar y encriptar las contraseñas.