

Antes de crearse las bases de datos integrada, se usaban sistemas de procesamiento de archivos, y los datos que usaban los programas de aplicación de una organización se almacenaban en archivos separados. Por lo general, un departamento que necesitaba un programa de aplicación trabajaba con el departamento de procesamiento de datos de la organización para crear especificaciones tanto para el programa como para los datos necesarios para él. Con frecuencia los mismos datos se recopilaban y almacenaban de manera independiente mediante varios departamentos dentro de una organización, pero no se compartían. Cada aplicación tenía sus propios archivos de datos que se creaban de manera específica para la aplicación, y estos pertenecían al departamento para el que se escribía la aplicación. El enfoque de base de datos integrada tiene muchas ventajas:

1. Compartir datos

La base de datos pertenece a toda la organización. El ABD gestiona los datos, pero estos no pertenecen a algún individuo o departamento. Por ende, la organización tiene el control sobre los datos que necesita para dirigir su negocio. Muchos usuarios pueden tener autorización para acceder al mismo trozo de información. La autorización para acceder a los datos la otorga el ABD, no otro departamento.

2. Control de redundancia

Cuando se almacena en una base de datos, la información se integra de modo que múltiples copias de los mismos datos no se almacenan a menos que sea necesario. Se permite alguna redundancia limitada para mantener las conexiones lógicas entre los ítems de datos o para mejorar el rendimiento. Para poner un caso, en el ejemplo de universidad que se discutió en la sección 1.2, la ID del estudiante aparecía tanto en la tabla Student como en la tabla Enroll. El sistema de gestión de la base de datos “sabe acerca” de dicha repetición. Una base de datos de ordinario no tiene múltiples copias de registros enteros, a

diferencia de un sistema de archivos, donde distintos departamentos podían tener duplicados de archivos enteros.

3. Consistencia de datos

Un efecto de eliminar o controlar la redundancia es que los datos son consistentes. Si un ítem de datos aparece solo una vez, cualquier actualización a su valor necesita realizarse solo una vez, y todos los usuarios tendrán acceso al mismo nuevo valor. Si el sistema tiene cierta redundancia controlada, cuando recibe una actualización a un ítem que aparezca más de una vez con frecuencia puede realizar actualizaciones en cascada. Esto significa que automáticamente actualizará cada ocurrencia de dicho ítem, lo que mantiene consistente a la base de datos. Por ejemplo, si se cambia la ID de un estudiante en la tabla Student, los registros Enroll para dicho estudiante se actualizarán para mostrar la nueva ID en forma automática.

4. Estándares de datos mejorados

El ABD, que es responsable del diseño y mantenimiento de la base de datos para satisfacer las necesidades de todos los usuarios, define y refuerza los estándares de toda la organización para la representación de datos en la base de datos. En esta categoría se incluyen reglas como el formato de todos los ítems de datos, convenciones acerca de nombres de datos, estándares de documentación, frecuencia de actualizaciones, procedimientos de actualización, frecuencia de respaldos, procedimientos de respaldos y uso permitido de la base de datos. Por ejemplo, el ABD puede elaborar una regla para que las direcciones se almacenen en un formato particular. En Estados Unidos, una convención puede ser que, para los nombres de los estados, se usen abreviaturas con dos letras. La base de datos se puede configurar de modo que cualquier otra representación se rechace. En otros países, las zonas postales pueden definirse con base en cierto número de caracteres.

5. Mejor seguridad de datos

Los datos en la base de datos de una organización son un valioso recurso corporativo que **se debe proteger de mal uso intencional o accidental**. La seguridad de datos es la protección de la base de datos de acceso no autorizado por personas o programas que puedan hacer mal uso o dañar los datos. Un sistema de base de datos permite la definición y fortalecimiento de restricciones de seguridad en varios niveles. **Todo acceso autorizado a la base de datos es a través del DBMS**, que puede requerir que los usuarios pasen a través de procedimientos de seguridad o usar contraseñas para obtener acceso a la base de datos. Para eliminar la posibilidad de que un usuario pase por un lado del DBMS y obtenga acceso a los datos en forma ilegal, **el DBMS puede encriptar los datos antes de almacenarlos**. Entonces, cuando un usuario autorizado debe recuperar datos, **se desencryptarán automáticamente**. Los datos recuperados en cualquiera otra forma aparecerán en su forma encriptada. Los usuarios autorizados pueden no estar al tanto de la encriptación de datos. A cada usuario se le proporciona una vista de una porción predefinida de la base de datos. Por ejemplo, en una universidad, la oficina de admisión puede tener acceso a cierta información del personal docente, como la tabla Faculty **en el ejemplo anterior, pero no a ítems como el salario**. En la vista se incluyen descripciones de los ítems de datos a los que se permite el acceso del usuario, y el tipo de acceso permitido, ya sea sólo recuperación, actualización o borrado de registros existentes, o inserción de nuevos registros. **Si un usuario intenta acceder a un ítem que no está incluido en su vista, o intenta una operación no autorizada, el DBMS automáticamente registra la ID del usuario en una bitácora (log) de seguridad que está disponible al ABD**.

6. Integridad de datos mejorada

Algunos sistemas de gestión de base de datos permiten al ABD definir restricciones de integridad: **reglas de consistencia que la base de datos debe obedecer**. Estas restricciones se aplican a ítems dentro de un registro

(restricciones intra-registro) o a registros que se relacionan mutuamente (restricciones inte-registro), o pueden ser restricciones generales del negocio. Por ejemplo, en los registros de clase, puede haber una regla de que el número de estudiantes inscritos en una clase nunca supere algún máximo de inscripción permitido. Otra regla puede ser que la ID del personal docente en un registro de clase deba corresponder a una ID de personal docente real en un registro de personal docente. El DBMS es responsable de nunca permitir la inserción, el borrado o la actualización de un registro que viole una restricción de integridad.

7. Equilibrio de los requisitos en conflicto

Cada departamento o usuario individual tiene necesidades de datos que pueden estar en conflicto con los de otros usuarios. El ABD está al tanto de las necesidades de todos los usuarios y puede tomar decisiones acerca del diseño, uso y mantenimiento de la base de datos que proporcionen las mejores soluciones para la organización como un todo. Estas decisiones por lo general favorecen las aplicaciones más importantes, posiblemente a costa de las menos vitales.

8. Desarrollo más rápido de nuevas aplicaciones

Una base de datos bien diseñada proporciona un modelo preciso de las operaciones de la organización. Cuando se propone una nueva aplicación, es probable que los datos requeridos ya estén almacenados en la base de datos. Si es así, el DBMS puede proporcionar datos en la forma requerida por el programa. El tiempo de desarrollo se reduce porque no se necesita una fase de creación de archivos para la nueva aplicación, como ocurría cuando se usaban los sistemas de procesamiento de archivos.

9. Mejor accesibilidad de datos

Además de proporcionar datos para los programas, la mayoría de los sistemas de gestión de base de datos permiten acceso interactivo a los usuarios.

Proporcionan lenguajes de consulta que permiten a los usuarios plantear preguntas ad hoc (La frase "ad hoc" es un término latino que significa literalmente "para esto.") y obtener la información deseada.

10. Economía de escala

Cuando todos los requisitos de datos de la organización se satisfacen mediante una base de datos en lugar de muchos archivos separados, el tamaño de la operación combinada proporciona muchas ventajas. La porción del presupuesto que de ordinario se asignaría a varios departamentos para sus costos de diseño, almacenamiento y costos de datos, se puede combinar, lo que posiblemente resulte en un costo total más bajo. Los recursos combinados se pueden usar para desarrollar un sistema más sofisticado y poderoso que cualquier departamento podría costear en forma individual, lo que proporciona características no disponibles en un entorno de procesamiento de archivos. El tiempo de programador que ordinariamente se dedicaría al diseño de archivos y la escritura de programas para acceder a ellos se puede emplear en la mejora de la base de datos. Cualquier mejora a la base de datos beneficia a muchos usuarios.

11. Más control sobre la concurrencia

Si a dos usuarios se les permite ingresar a datos simultáneamente, y al menos uno de ellos actualiza datos, es posible que interfieran uno con el otro. Por ejemplo, si ambos intentan realizar actualizaciones, una actualización se puede perder, porque el segundo puede sobrescribir el valor grabado por el primero. Si las actualizaciones tienen la intención de ser acumulativas, este es un serio problema. La mayoría de los sistemas de gestión de bases de datos integradas tienen sub-sistemas para controlar concurrencia, de modo que las transacciones no se pierdan o desempeñen de manera incorrecta.

12. Mejores procedimientos de respaldo y recuperación

En un entorno de base de datos, los registros de la base de datos por lo general se respaldan (copian) de manera regular, acaso por la noche. Para mantener seguro el respaldo, se usa una cinta u otro medio. Conforme se realizan transacciones, cualquier actualización se registra en una bitácora (log) de cambios. Si el sistema fracasa, cinta y log se usan para llevar la base de datos al estado en que estaba justo antes de la falla. Por tanto, el sistema se auto-recupera.