Síntesis conceptual

Grado: Administración de sistemas informáticos en red
Asignatura: Administración de Sistemas Gestores de Bases de Datos
Unidad: 4. Seguridad

Resumen

- Las tareas necesarias para garantizar la seguridad desde el primer momento posterior a la instalación del SGBD deben estar enfocadas en asegurar la confidencialidad de la información y la integridad de los datos. El administrador de base de datos debe conocer las herramientas que el SGBD tenga disponibles para gestionarlas.

- Las políticas de seguridad implementadas sobre el SGBD pueden ser activas o pasivas. Las primeras son medidas preventivas llevadas a cabo de forma proactiva, con el objetivo de prevenir fallos en el SGBD. Se deben gestionar los usuarios y permisos, definición de esquemas externos y la encriptación de la información. También se gestionará la concurrencia, transacciones y restricciones. Las pasivas se dan cuando fallan las primeras, se deben buscar las posibles causas de los fallos e incorporar mecanismos para que no se repitan. Las auditorías ayudarán a la investigación de los fallos, mientras que, en lo referente a la integridad, se recurrirá a los mecanismos de respaldo y recuperación.

- La encriptación de la información se puede realizar en dos modos: explícitamente mediante funciones o aplicando cifrado transparente. Hay dos tipos de funciones de cifrado explícito, las que permiten descifrar la información posteriormente y que garantizan la confidencialidad y aquellas en las que no se requiere descifrar la información (Hash, MAC), se suelen utilizar para validación (contraseñas o firmas).

- La auditoría es una medida de seguridad pasiva a la que se suele recurrir cuando se han detectado ciertas anomalías que deben ser investigadas.

- La definición de restricciones (valores fuera de rango, claves primarias y foráneas, etc.) y la gestión de transacciones para controlar la concurrencia, son herramientas que vienen en la mayoría de SGBD,

- Por razones de administración, el DBA, podrá inhabilitar temporalmente las restricciones,

- Las transacciones concurrentes pueden generar problemas de integridad de varios tipos: lectura sucia, lectura no repetible o lectura fantasma. Los bloqueos son mecanismos de aislamiento para evitar problemas de integridad, pero a su vez, pueden generar problemas de interbloqueo.

- El estándar SQL define cuatro niveles de aislamiento para gestionar los problemas de concurrencia e interbloqueos: lectura no confirmada, lectura confirmada, lectura

repetible y serializable. Debe buscarse el equilibrio entre garantizar la integridad y la agilidad del sistema.

- Las sentencias del lenguaje de control de transacciones (TCL) son commit (confirmación de transacción) y rollback (deshacer la transacción). El registro de transacciones se guarda en el cuaderno de bitácora.

- Las funciones de copias de seguridad y restauración, junto con el cuaderno de bitácora, van a permitir garantizar la recuperación de los datos y restauración del sistema en caso de fallo.

- La LOPD establece como catalogar la información a tratar y los niveles de seguridad que hay que aplicar en cada categoría. El DBA tiene la responsabilidad de garantizar el cumplimiento de la ley en lo referente al SGBD, planificando y ejecutando las medidas de seguridad tales como: políticas de copias de seguridad y restauración (simulacros, soportes, tipos de copia, etc.), integridad, auditoría, encriptación, etc.

Conceptos fundamentales

- **Encriptación transparente (TDE):** Método de encriptación para garantizar que los ficheros de la base de datos se guardan encriptados, así como las comunicaciones se cifran. Todo ello sin que el usuario tenga que intervenir explícitamente.

- **Auditoría:** Medida de seguridad pasiva a la que se recurre normalmente cuando ha ocurrido algún tipo de anomalía. Casi todos los SGBD definen mecanismos para llevarla a cabo.

- **Restricciones:** Mecanismo del SGBD que define el tipo de datos y los valores que pueden tomar ciertos campos. Los más comunes son: nulidad, claves (primaria, foránea, única, valores por defecto, verificación o restricción de rango y disparadores).

- **Interbloqueos (deadlocks):** problemas que pueden ocurrir en una base de datos cuando dos transacciones están bloqueando recursos que ambas necesitan, quedando ambas atrapadas.

- **Aislamiento:** es una característica de los sistemas de gestión de bases de datos relacionales que aísla las transacciones individuales de las demás, de forma que los cambios realizados por una transacción no son visibles a otras transacciones hasta que la primera se haya completado.

- **LOPD:** Ley Orgánica de Protección de datos.

Procesos fundamentales

Utilización de funciones del paquete DBMS_CRYPTO.
Configuración del cifrado TDE en Oracle.
Exportación e importación de datos con los comandos exp/imp de Oracle.