Seguridad en Sistemas de Bases de Datos

Corresponde ahora discutir acerca de la importancia de la seguridad de la información dentro del ciclo de vida de una base de datos.

Como parte del diseño físico y de cara a la implementación de una base de datos es necesario establecer con claridad las especificaciones y los mecanismos que permitan asegurar la integridad y disponibilidad de los datos. Se discutirán aquí los riesgos a los que están expuestos los sistemas de bases de datos y las armas de las que disponemos para prevenirlos. Y por supuesto haremos uso de los mecanismos de seguridad lógica que proveen los SGBD.

Con el estudio de esta unidad, esperamos que usted adquiera la capacidad de proponer mecanismos que permitan garantizar la confidencialidad, integridad y disponibilidad de la base de datos.

Para la implementación de seguridad de acceso a nivel del SGBD continuaremos trabajando con el SGBD Oracle.

1. Panorámica de la seguridad en sistemas de bases de datos

Es necesario definir todas las medidas que hagan falta para asegurar que la base de datos no se vea afectada ni en su contenido, ni en su accesibilidad. Por ello, es importante que se implementen mecanismos que permitan evitar ataques externos (acciones preventivas), y si ocurrieren poder identificar el origen y sus responsables (acciones correctivas).

La seguridad de los datos implica garantizar que la información almacenada en una base datos, que se registra, actualiza y explora por canales autorizados (por ejemplo: a través de los sistemas de información institucionales), no sufra pérdida ni alteraciones fraudulentas, y que pueda ser accedida y extraída en cualquier momento sin inconvenientes.

Los sistemas de bases de datos, al igual que muchos sistemas computacionales, están expuestos a muchas amenazas que podrían vulnerar ese estado deseado de los datos. Es decir, podrían existir vías por las cuales agentes externos no deseados pueden atacar y afectar la operación normal de una base de datos. Debemos tener claro cuáles son esas amenazas y cuáles son las herramientas que disponemos para prevenirlas.

La operación de la base de datos podría alterarse, sea por una afectación directa sobre el servidor donde se ha implementado el SGBD, o indirectamente a través las aplicaciones que acceden a los datos.

Por lo tanto, la seguridad de los datos debe analizarse principalmente desde dos perspectivas:

- Seguridad de la base de datos.
- Seguridad de las aplicaciones.

En la *seguridad de la base de datos*, entiéndase aquella inherente al servidor de bases de datos, que incluye el motor de base de datos (SGBD) y su plataforma de implementación. La *seguridad de las aplicaciones*, en cambio se analiza bajo la perspectiva de que una aplicación podría ser un punto de acceso indirecto a la base de datos. Entonces, un agente mal intencionado podría atacar la base de datos, accediendo directamente al servidor, o, indirectamente a través de las aplicaciones que gestionan la información. Otra vía de ataque puede ser por intercepción a nivel de la red de datos.

2. Seguridad de la base de datos

Comprende 3 aspectos principales:

- Confidencialidad
- Integridad
- Disponibilidad.

La *confidencialidad* se refiere a la necesidad de que el acceso a la información se realice solo por vías autorizadas. Es decir, se debe evitar que personas o agentes no autorizados puedan visualizar y/o alterar los datos.

La *integridad* implica asegurar que la información almacenada en la base de datos, sea completa, consistente y de calidad.

La *disponibilidad* refiere a garantizar el acceso a la base de datos, en todo momento que lo requiera la organización.

2.1. Confidencialidad

Implica, impedir el acceso a los datos a personal o agentes no autorizados. Pues no toda la información que una empresa almacena en sus bases de datos, es pública; hay mucha información reservada. Incluso internamente dentro de la propia organización, sus funcionarios dependiendo de su rol, perfil y cargo podrán o no acceder a cierta información.

Para esto existen varios mecanismos que se pueden implementar:

a) Acceso físico.
b) Acceso lógico (autenticación y asignación de privilegios).
c) Vistas en base de datos.
d) Vistas de usuario en aplicaciones.
e) Cifrado.
f) Otros.

Acceso físico

A nivel físico, se debe restringir el acceso al servidor de base de datos solo a personal autorizado, que normalmente es el DBA. Para ello es necesario que el equipo servidor esté ubicado en un lugar seguro, y que existan adecuados mecanismos de control de acceso físico a ese sitio.

Acceso lógico

A nivel lógico se requiere controlar el acceso a la base de datos a través de mecanismos de autenticación provistos por el propio SGBD, o a través de otros servicios de directorio basados en el *Protocolo Ligero de Acceso a Directorios* (LDAP, por sus siglas en inglés). Normalmente todo SGBD permite la asignación de credenciales (usuario y contraseña) para permitir el acceso de una persona o sistema. La autenticación abre la puerta principal, es decir permite establecer una conexión con la base de datos, pero no necesariamente permite acceder a los objetos de esta.

Adicionalmente se requiere que el usuario tenga privilegios, que son los permisos que se asignan a un usuario internamente dentro del SGBD, y que permiten establecer a cuáles objetos puede acceder y las

operaciones que puede ejecutar sobre esos objetos. Por ejemplo, la aplicación web de consulta de notas de la UTPL, tiene acceso a la base de datos del Sistema Académico, únicamente a ciertas tablas relacionadas a las notas, pero únicamente con permisos de lectura.

Para facilitar esta tarea los SGBD permiten por ejemplo la creación de perfiles de usuario y/o roles, los cuales permiten agrupar usuarios bajo una misma categoría y con los mismos privilegios.

	En el Entorno Virtual de Aprendizaje revise el recurso "**Práctica seguridad Oracle**". Que es una práctica guiada sobre la creación de usuarios y asignación de privilegios en Oracle.

Vistas en base de datos

Podemos crear vistas a nivel de base de datos que permitan acceder solo a una porción de los datos. Y asignar privilegios para que ciertos usuarios puedan acceder solo a la vista y no a las tablas origen.

Vistas de usuario en aplicaciones

Las aplicaciones de usuario final también conllevan el control de confidencialidad. De hecho, son las que implementan las vistas de usuario. De manera que, al autorizarle al usuario de la aplicación a acceder solo a ciertas funcionalidades, indirectamente le están restringiendo el acceso solo a ciertos datos.

2.2. Integridad

La integridad de la base de datos debe estar asegurada, es decir, hay que garantizar la calidad de los datos. Implica que la información debe ser completa, correcta y consistente.

Por ejemplo, en el caso de una tabla PERSONAS, no debería ocurrir que:

- Dos personas tengan el mismo número de identificación.
- Exista una persona de la que no se conozca su nombre.
- Existen personas asociadas a un código de nacionalidad que no exista en el catálogo NACIONALIDADES.
- Se produzcan alteraciones fraudulentas de los datos (desde orígenes desconocidos, en horarios no previstos y/o por agentes no autorizados).

Para evitar problemas de integridad de esta índole, hay dos mecanismos que implementan los SGBD: el control de restricciones de integridad y la gestión de transacciones.

Control de restricciones de integridad

Es necesario que, al construir la base de datos, y específicamente al traducir el modelo lógico al SGBD, ***todas*** las restricciones de integridad que impone el negocio sean implementadas; sea a nivel del SGBD (mediante DDL o Triggers) o a nivel de las aplicaciones. Esto ya se mencionó en la unidad 2, pero es importante recalcarlo.

Como sabemos a nivel de SQL mediante DDL, son 5 tipos de restricciones de integridad que se pueden implementar:

- Integridad de entidades (PRIMARY KEY)

- Integridad referencial (FOREIGN KEY)
- Claves alternativas (UNIQUE KEY)
- Campos obligatorios (NOT NULL)
- Validación de dominio (CHECK)

Otras restricciones se pueden implementar usando Triggers, por ejemplo:

- La empresa solicita que ningún usuario ni aplicación pueda registrar transacciones pasadas las 21h00.
- Actualización automática de campos derivados.
- Control de cardinalidades máximas distintas a N o *.

Y el resto de las restricciones que no se puedan implementar mediante el SGBD, las debería controlar la aplicación.

Gestión de transacciones

Otra vía por la que pueden generarse inconsistencias en la base datos es cuando se registran transacciones (por ejemplo, una factura de venta), que involucran a dos o más tablas. Si no se gestionan correctamente podría ocurrir que ante un fallo del sistema la transacción quede parcialmente registrada (solo se registra la cabecera de la factura y no los ítems), lo que sería una grave inconsistencia.

Así mismo se podrían producir inconsistencias durante la ejecución concurrente de transacciones. Es decir, cuando muchos usuarios acceden y actualizan la base de datos simultáneamente (por ejemplo, varias cajas de un supermercado registrando facturas al mismo tiempo). Sin el adecuado control, ello podría conllevar a modificaciones erróneas o sobre escrituras de los datos.

Felizmente, los SGBD incorporan un componente para realizar este tipo de control y garantizar la integridad de los datos luego de ejecutarse una transacción o varias transacciones simultáneamente. Si recuerda, en la arquitectura del sistema de base de datos (figura 1.5 del texto básico) dentro del gestor de almacenamiento existe un componente llamado *gestor de transacciones*, que es el encargado de planificar la ejecución de transacciones de manera que nunca afecte a la consistencia de los datos.

El tema de la gestión de transacciones y control de concurrencia se estudia en detalle en la unidad 5.

2.3. Disponibilidad

La disponibilidad implica asegurar que la base de datos esté disponible de forma permanente y con un adecuado desempeño.

Es una parte importante de la seguridad, busca evitar al máximo **Downtimes** de la base de datos. Para lo que es necesario considerar medidas como:

- Definir políticas de respaldo y recuperación.
- Definir protocolos de recuperación ante desastres.
- Implementar redundancia a nivel de almacenamiento (RAID).
- Implementar redundancia a nivel eléctrico.
- Implementar replicación.
- Mantener servidores de respaldo.

3. Seguridad de las aplicaciones

Las aplicaciones al ser el intermediario entre los usuarios finales y la base de datos constituyen un punto crítico para la seguridad de los datos. Pues, si no están debidamente validadas, podrían terminar siendo la puerta de entrada "trasera" a la base de datos. Pudiendo producirse accesos indebidos por causas tan simples como que a un usuario le roben o adivinen sus credenciales, hasta algo más complejo como es la inyección de SQL a través de los formularios de las aplicaciones.

Son muchos son los riesgos a los que está expuesta una base de datos e igualmente muchos los mecanismos para combatirlos. Especial atención merece el cifrado de datos que actualmente se implementa en aplicaciones web (HTTPS), en especial para asegurar la información que viaja a través de internet.

En la Tabla 1, Coronel et al. (2011), nos presenta una lista muy completa de las posibles amenazas (vulnerabilidades) a las que está expuesta una base de datos, y un conjunto de medidas que se suelen tomar para proteger los datos de esos riesgos, revíselas con atención.

Tabla 1. Vulnerabilidades de seguridad y medidas relacionadas
Fuente: Coronel et al., 2011, p.630
Elaborado: Encalada, E.

Componente del sistema	Vulnerabilidad de seguridad	Medidas de seguridad
Personal	• El usuario establece una contraseña en blanco. • La contraseña es corta o incluye fecha de nacimiento. • El usuario deja la puerta abierta todo el tiempo. • El usuario deja la información de nómina en la pantalla durante largos períodos de tiempo.	• Aplicar directivas de contraseñas complejas. • Utilizar autenticación multinivel. • Utilice pantallas de seguridad y protectores de pantalla. • Educar a los usuarios sobre los datos sensibles. • Instalar cámaras de seguridad. • Utilice cerraduras de puerta automáticas.
Estación de trabajo y servidores	• El usuario copia los datos en una unidad de flash. • La estación de trabajo es utilizada por múltiples usuarios. • Un fallo de corriente bloquea el ordenador. • Personal no autorizado puede usar la computadora. • Datos sensibles se almacenan en una computadora laptop. • Datos perdidos por disco duro/laptop robados. • Daños físicos en los equipos • Se produce un desastre natural.	• Utilice directivas de grupo para restringir el uso de unidades flash. • Asigne derechos de acceso de usuario a las estaciones de trabajo. • Instale fuentes de alimentación ininterrumpidas (UPS). • Agregue bloqueos de seguridad a los equipos. • Implementar un interruptor "muerto" para laptops robadas. • Cree y pruebe los planes de respaldo y recuperación de datos. • Redundancia a nivel de discos (RAID). • Implementar un servidor de respaldo. • Asegurar el sistema contra desastres naturales, usar estrategias de co-localización.
Sistema operativo	• Ataques de desbordamiento de espacio de almacenamiento temporal • Ataques de virus • Ataques de gusanos • Ataques de denegación de servicios • Caballos de Troya • Aplicaciones de spyware (espías) • Violadores de contraseñas	• Aplicar parches y actualizaciones de seguridad del sistema operativo. • Aplicar parches del servidor de aplicaciones. • Instalar software antivirus y antispyware. • Imponga rastros de auditoría en los equipos. • Realice copias de seguridad periódicas del sistema. • Instale sólo aplicaciones autorizadas. • Utilice directivas de grupo para evitar instalaciones no autorizadas.
Aplicaciones	• Errores de aplicación; desbordamiento de espacio de almacenamiento temporal	• Pruebe extensamente los programas de aplicación. • Construir salvaguardias en el código.

	• Inyección SQL, secuestro de sesión, etc. • Vulnerabilidades de la aplicación; codificación cruzada, entradas no validadas • Ataques por correo: correo basura, suplantación de identidad, etc. • Correos de ingeniería social	• Realice extensas pruebas de vulnerabilidad en aplicaciones. • Instalar lectores de spam y software antivirus para sistemas de correo electrónico. • Utilice técnicas de codificación segura (vea www.owasp.org). • Educar a los usuarios sobre los ataques de ingeniería social.
Red	• Detección de IP • Detectores de paquetes • Ataques de hackers • Borrar contraseñas en red	• Instale firewalls. • Utilizar redes privadas virtuales (VPN). • Utilice sistemas de detección de intrusos (IDS). • Utilice el control de acceso a la red (NAC). • Vigilancia de actividad en red.
Datos	• Partes de datos están abiertos a todos los usuarios. • Se puede acceder a los datos de forma remota. • Los datos se pueden eliminar desde un recurso compartido.	• Implementar seguridad de sistema de archivos. • Implementar la seguridad de acceso compartido. • Use el permiso de acceso. • Cifrar los datos a nivel del sistema o de la base de datos.

Es muy importante que usted en su rol de DBA sepa evaluar y tener presente los posibles riesgos a los que se puede enfrentar y de acuerdo con el contexto de implementación en el que este participando sepa proponer medidas que reduzcan la probabilidad de ocurrencia.

Es responsabilidad del DBA, implementar todas las medidas para garantizar

- la disponibilidad de la base de datos (en tiempo y en rendimiento).
- la integridad de los datos.
- la integridad de los equipos.
- la no alteración indebida de los datos.
- la no fuga de información.

Actividades propuestas:

1. Realice un mapa mental donde se sinteticen los aspectos de seguridad, las amenazas y los mecanismos de prevención.

2. Asuma que usted es el DBA en una institución bancaria; que acciones y mecanismos implementaría para asegurar la disponibilidad de la base de datos. Un banco exige una disponibilidad 24x7.

.-