



Unidad 3

Seguridad en bases de datos

UTPL
UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Agenda

- Introducción
- Objetivos de seguridad
- Amenazas y contramedidas
- Monitoreo y auditoria
- Papel del DBA en seguridad
- Gestión del acceso de usuarios
- Respaldo y recuperación



Introducción

- La seguridad de los datos debe analizarse principalmente desde dos perspectivas:
 - Seguridad de la base de datos.
 - Seguridad de las aplicaciones.
- Conlleva 3 objetivos principales:
 - Confidencialidad
 - Integridad
 - Disponibilidad

Introducción

- **Confidencialidad:**
 - Se refiere a la necesidad de que el acceso a la información se realice solo por vías autorizadas.
- **Integridad:**
 - Implica asegurar que la información almacenada en la base de datos, sea completa, consistente y de calidad.
- **Disponibilidad**
 - Refiere a garantizar el acceso a la base de datos, en todo momento que lo requiera la organización.

Confidencialidad

- Implica impedir el acceso a los datos a personal o agentes no autorizados.
- Control de acceso físico
 - Mecanismos de control para acceso a físico a DataCenter
 - Hardware e instalaciones (ubicación, respaldos, climatización)
 - Sistema de red y comunicaciones
 - Uso de firewalls
 - Políticas y protocolos de seguridad internos

Confidencialidad

- Control de autenticación
 - Seguridad a nivel de usuarios, control de acceso a través de usuario y contraseña.
 - Requiere sistema autenticación (BD o LDAP)
- Control de autorizaciones
 - Perfiles de usuario, roles
 - Privilegios
 - Objetos (tablas, vistas, procedimientos almacenados, etc)
 - Operaciones (DML, DDL, ejecutar, etc)
- El control de autenticación abre puerta principal, mientras que el control de autorizaciones abre puertas internas (confidencialidad).

Confidencialidad

- Uso de mecanismos de cifrado (encriptación) de los datos
- Utilización de vistas de usuario

Los mecanismos para garantizar la confidencialidad también se pueden implementar a nivel de aplicación



Integridad

- Se debe garantizar la calidad de los datos.
 - Implica que la información debe ser completa, correcta y consistente.
 - Control de restricciones de integridad
 - Integridad de entidades (PRIMARY KEY)
 - Integridad referencial (FOREIGN KEY)
 - Claves alternativas (UNIQUE KEY)
 - Campos obligatorios (NOT NULL)
 - Validación de dominio (CHECK)
- 
- DDL**

Integridad

- Todas las restricciones deben estar controladas, a nivel de base de datos (DDL, triggers) y a nivel de aplicación (lo que no se pueda a nivel de base de datos).
- Integridad a nivel de transacciones
 - Ej 1: evitar que al registrar una venta únicamente se registre la cabecera y no los ítems, ni se actualice inventario
 - Ej 2: Evitar que al realizar una transferencia de una cuenta A a una cuenta B, solamente se registre el débito y no la acreditación.
 - **Control de transacciones**

Disponibilidad

- La disponibilidad es una parte importante de la seguridad, que busca evitar al máximo DownTimes de la base de datos.
- La disponibilidad implica que se debe garantizar la operación continua del servicio de la base de datos de acuerdo a lo requerido por el negocio.
- Por ejemplo: disponibilidad 24x7x365 implica que la base de datos no puede dejar de operar ni un solo momento.
- No solo es operación continua, implica también garantizar el rendimiento adecuado del servicio.

Disponibilidad

- Para garantizar la continuidad del servicio la palabra claves es “redundancia”.
- Algunos de los mecanismos son:
 - Redundancia a nivel de almacenamiento (RAID)
 - Redundancia a nivel eléctrico
 - Servidores de respaldo
 - Planes y protocolos de recuperación ante desastres
 - Políticas de respaldo y recuperación

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Amenazas y contramedidas

- Todo sistema está expuesto a amenazas que atentan su normal funcionamiento. Igual pasa con un SGBD.
- Es necesario entonces identificar con antelación todas las posibles amenazas que pueden afectar la operación de nuestra base de datos.
- Y por cada amenaza debemos establecer acciones que permitan contrarrestarlas (contramedidas).
- Por ejemplo, ante la amenaza de un fallo en el hardware de nuestro servidor una contramedida puede ser: contar con un servidor de respaldo.

Amenazas y contramedidas

Amenazas

Amenaza / Vulnerabilidad	Objetivo de seguridad en riesgo
Fallos de hardware	Disponibilidad
Fallos en mecanismos de control de acceso físico	Confidencialidad, Integridad
Fallos de comunicaciones (red)	Disponibilidad
Fallos de energía	Disponibilidad
Falta de capacitación de usuarios finales	Integridad
Suplantación de identidad (Phishing)	Confidencialidad
Denegación de servicios (DoS)	Disponibilidad
Implantación de Malware	Integridad, Disponibilidad
Entrada ilegal por parte de un hacker	Confidencialidad, Integridad

Amenazas y contramedidas

Contramedidas

Objetivo de seguridad	Mecanismo de seguridad
Confidencialidad	<p>Control de acceso físico a instalaciones.</p> <p>Control de acceso lógico (autenticación y autorización).</p> <p>Uso de mecanismos de cifrado de los datos.</p> <p>Uso de vistas de datos.</p> <p>Uso de firewalls.</p>
Integridad	<p>Implementación de restricciones de integridad.</p> <p>Gestión de transacciones y control de concurrencia.</p> <p>Copias de seguridad (respaldos).</p>
Disponibilidad	<p>Redundancia en almacenamiento secundario (RAID).</p> <p>Redundancia eléctrica.</p> <p>Servidores de respaldo.</p> <p>Protocolos de recuperación ante desastres.</p> <p>Segmentación de redes.</p> <p>Copias de seguridad (respaldos).</p>

Amenazas y contramedidas

- Revisar documento complementario **“Seguridad en Sistemas de Bases de Datos”**. En el apartado “Seguridad de las aplicaciones” se muestra una tabla de vulnerabilidades y medidas asociadas.



Monitoreo y auditoría

Monitorización de seguridad

- Se deben acumular evidencias que permitan auditar la operación de la base de datos.
- Conexiones y operaciones deben quedar registradas:
 - Log a nivel de aplicaciones
 - Log a nivel de base de datos
- Contenido de un log de base de datos:
 - Operación realizada (SELECT, INSERT, UPDATE, etc.)
 - Terminal o maquina desde donde se ejecutó la operación
 - Usuario que ejecutó la operación
 - Fecha y hora
 - Base de datos, tablas y campos afectados
 - Valor anterior
 - Valor nuevo (en caso de UPDATE)

Monitoreo y auditoría

Auditoría

- Ocurre cuando hay sospecha de alteración indebida de los datos, o cuando las políticas de seguridad de la organización lo determinan.
- Implica
 - analizar los logs de la base de datos y de la aplicación
 - revisar configuración de cuentas y permisos
 - inclusive revisar la seguridad física de acceso a servidores.
- Ayuda a descubrir causas o responsables de anomalías en los datos.

Monitoreo y auditoría

Auditoría

- En sistemas que ya están en producción, los datos NUNCA deberían actualizarse directamente en la base de datos por los usuarios.
- La gestión y acceso a los datos se debe realizar a través de las aplicaciones.
- El DBA es el primer responsable si la causa de anomalías son huecos de seguridad.

Papel del DBA en seguridad

- Autoridad central de la base de datos
- Maneja las cuentas de administración de la base de datos (sys, system, root, sa, postgres)
- Responsable de definir perfiles de usuario, crear cuentas, asignar privilegios.
- Responsable de monitorear el acceso.
- Responsable de asegurar la disponibilidad.

Respaldo y recuperación

- Implica obtener en almacenamiento terciario (cintas, discos externos, etc.) una copia de los datos almacenados en la base de datos.
- Garantiza la no pérdida de datos en caso de fallo o pérdida de datos por otro motivo.
- También permiten recuperar información para procesos de auditoría.
- Periódicamente se debe ensayar la recuperación de la base de datos, para validar tanto los respaldos como el procedimiento de recuperación.

Respaldo y recuperación

Tipos de respaldo

- **Respaldo completo:** Copia completa de la base de datos
- **Respaldo incremental:** Respalda los cambios desde la última fecha de respaldo.
- **Respaldo en frío:** Se detiene la base de datos para obtener los respaldos.
- **Respaldo en caliente:** Se obtienen mientras la base de datos está operativa.
- **Respaldo concurrente:** Mientras los usuarios están trabajando en la base datos.
- **Respaldo lógico:** Volcado de los datos en archivo de respaldos
- **Respaldo físico:** Se respaldan los archivos físicos.

Respaldo y recuperación

- Los respaldos deben estar debidamente etiquetados.
- Deben haber multiples réplicas del mismo respaldo almacenados en lugares diferentes.
- El acceso físico a los respaldos debe estar protegido.
- En muchos casos se contratan servicios de empresas aseguradoras.

Material complementario

- Complementariamente en el curso están disponibles los siguientes recursos:
 - **Documento “Seguridad en sistemas de bases de datos”**: describe los 3 aspectos de la seguridad, y las vulnerabilidades a las que esta expuesta una base de datos
 - **Documento “Oracle Controlling User Access”**: Guía Oracle sobre gestión de usuarios y permisos.
 - **Documento “Práctica guiada seguridad Oracle”**: Guía paso a paso en la configuración de usuarios, roles, y permisos en Oracle.