Módulo 9.
Seguridad en Bases de Datos
La seguridad en una base de datos

Francisco Medina López

C O A P A

Contenido

1. **Introducción**
2. Problemas de seguridad en bases de datos
3. Integridad de datos
4. Control de acceso
5. Arquitecturas de seguridad
6. Mejores prácticas

[Introducción] ¿Por qué es importante?

- Una base de datos con un bajo nivel de seguridad compromete no solamente a la base de datos misma, sino también al sistema operativo y a otros sistema relacionados.

- Para proteger el acceso a la información sensible y a los activos digitales de una organización.

[Introducción] ¿Por qué es importante?

- Los sistemas de bases de datos son sistemas extremadamente complejos y con gran dificultad para *configurar* y *asegurar*.

La protección del sistema operativo y de los servicios de red en un servidor de bases de datos tiene una importancia crítica.

- Las bases de datos son la *base* de los nuevos negocios electrónicos, de los sistemas de planeación empresarial de recursos(ERP) y de otros sistemas críticos de negocios.

[Introducción] Aspectos de seguridad

- Secrecía y confidencialidad
- Precisión, integridad y autenticidad
- Disponibilidad y recuperabilidad

[Introducción] Aspectos de seguridad

- Secrecía y confidencialidad
  - Los datos deben ser protegidos de *liberación* no autorizada
    - Mediante recuperación directa o inferencia lógica
    - Mediante lectura de usuarios no autorizados
- Precisión, integridad y autenticidad
  - Los datos deben ser protegidos de modificación accidental o maliciosa (considerando incluso la inserción de datos falsos o la destrucción de los mismos)
  - El origen de los datos debe ser verificable

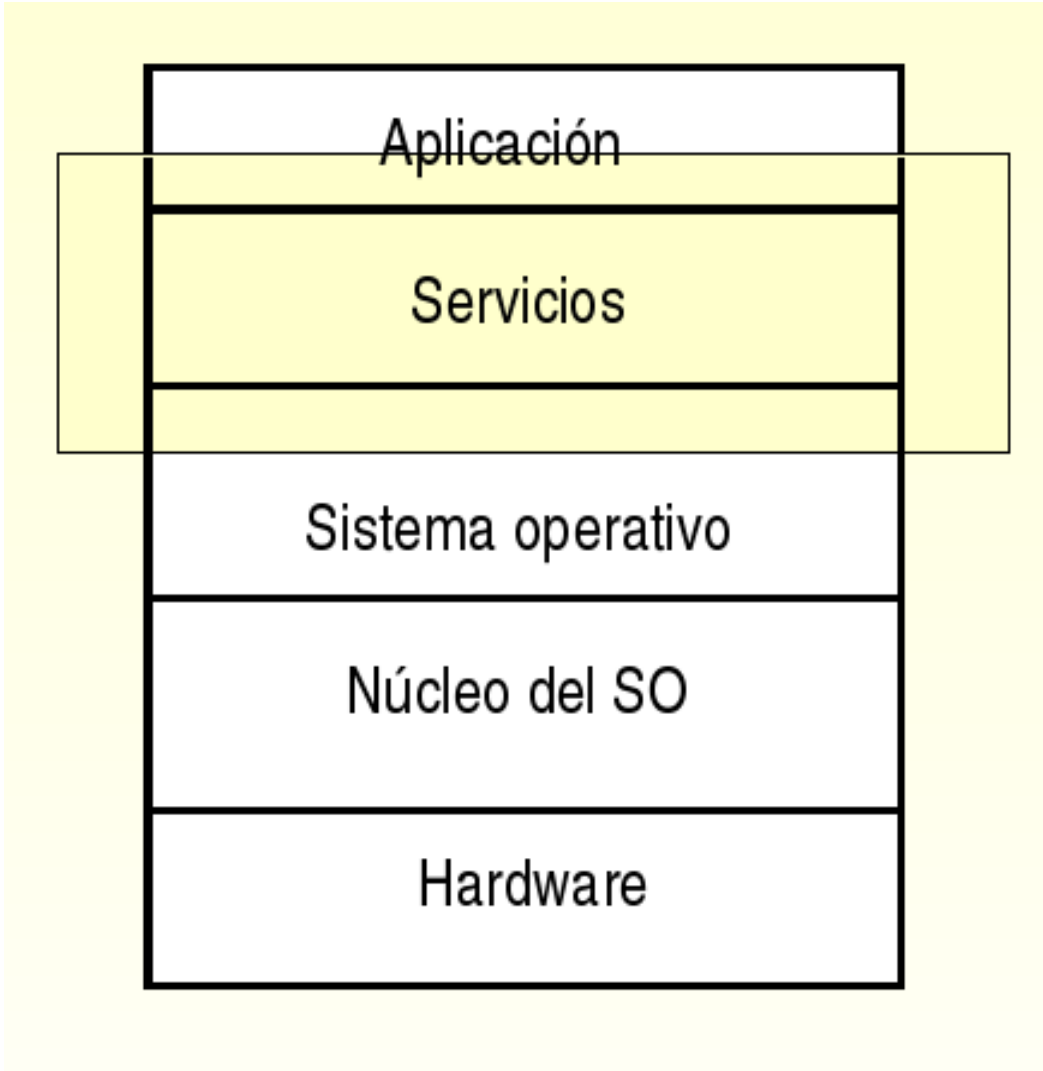
[Introducción] Aspectos de seguridad

- Disponibilidad y recuperabilidad
  - Los sistemas de bases de datos deben mantenerse operando y recuperarse en caso de pérdida de datos.

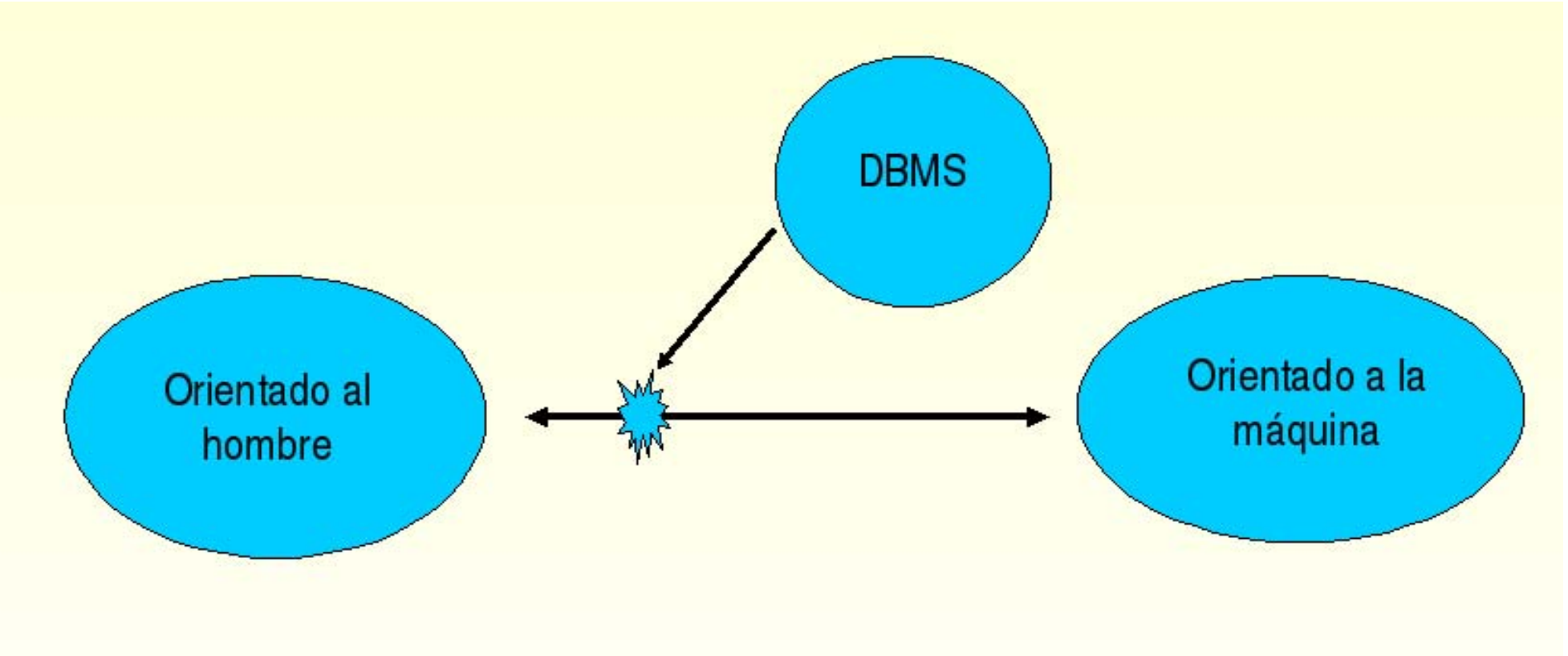
[Introducción] Problemas de seguridad

- La seguridad en bases de datos comprende medidas para evitar:
  - Liberación inapropiada de información (pérdida de secrecía o confidencialidad)
  - Modificación inapropiada de datos (pérdida de integridad)
  - Negación de servicio (pérdida de disponibilidad)
  - Robo o fraude

[Introducción] Alcance de un dba



[Introducción] Alcance de un dba



Contenido

[Problemas de seguridad] Amenazas

- Un manejador de base de datos debe proteger sus datos de:
  - Accidentes, por ejemplo errores de captura o de programación.
  - Uso malicioso de la base de datos.
  - Fallas de hardware o software que corrompen datos.

- Tipos de Amenazas

  - Accidentales o no fraudulentas (sin voluntad de causar daño):

  - Accidentes o desastres naturales
  - Errores o bugs en hardware o software
  - Errores humanos

  – **Intencionales** o fraudulentas (con voluntad explicita de causar daño)

  - Involucran a dos tipos de usuarios:
    - Usuarios autorizados que abusan de sus privilegios y autoridad.
    - Agentes hostiles

[Problemas de seguridad] Consecuencias

- Liberación inapropiada de información
- Modificación inapropiada de datos
- Negación de servicio

[Problemas de seguridad] Requerimientos

- Los requerimientos mínimos necesarios que debe cumplir cualquier programa que se diga RDBM son:
  - Autenticación de usuarios
  - Protección de acceso impropio
  - Integridad de la base de datos
  - Administración y protección de datos sensibles
  - Registro de eventos y auditoría

[Problemas de seguridad] Requerimientos

1. Autenticación de Usuarios
   - Necesidad de identificar de forma única a los usuarios de la base de datos.
   - Puede ser realizada por:
     - Sistema operativo
     - DBMS
2. Protección de acceso impropio
   - Permitir acceso a los objetos de la BD solamente a usuarios autorizados
   - Problemática: *Granularidad* más fina que en el caso de los sistemas operativos

3. Integridad fisica
   - Sistema de respaldo y recuperación
   - Uso de un log o *journal*
   - Instrucciones especiales para aplicar operaciones o cancelarlas
     - Con puntos de inicio y de control *(commit)*

[Problemas de seguridad] Requerimientos

4. Administración y protección de datos sensibles
   - Datos sensibles:
     - Datos que no deben ser hechos públicos
   - Factores que pueden hacer sensibles a los datos:
     - Inherentemente sensible
     - El valor mismo debe protegerse (sea declarado sensible o no)
     - Proviene de una fuente sensible
     - Debe protegerse la fuente de la que procede
     - Se ha declarado sensible
     - Se derivan de un registro o un atributo sensible

[Problemas de seguridad] Valor de la info.

- Puede haber bases de datos:
  - Solamente con datos sensibles
  - Solamente con datos públicos
  - Con ambos tipos de datos

Contenido

[Integridad de datos] Definición

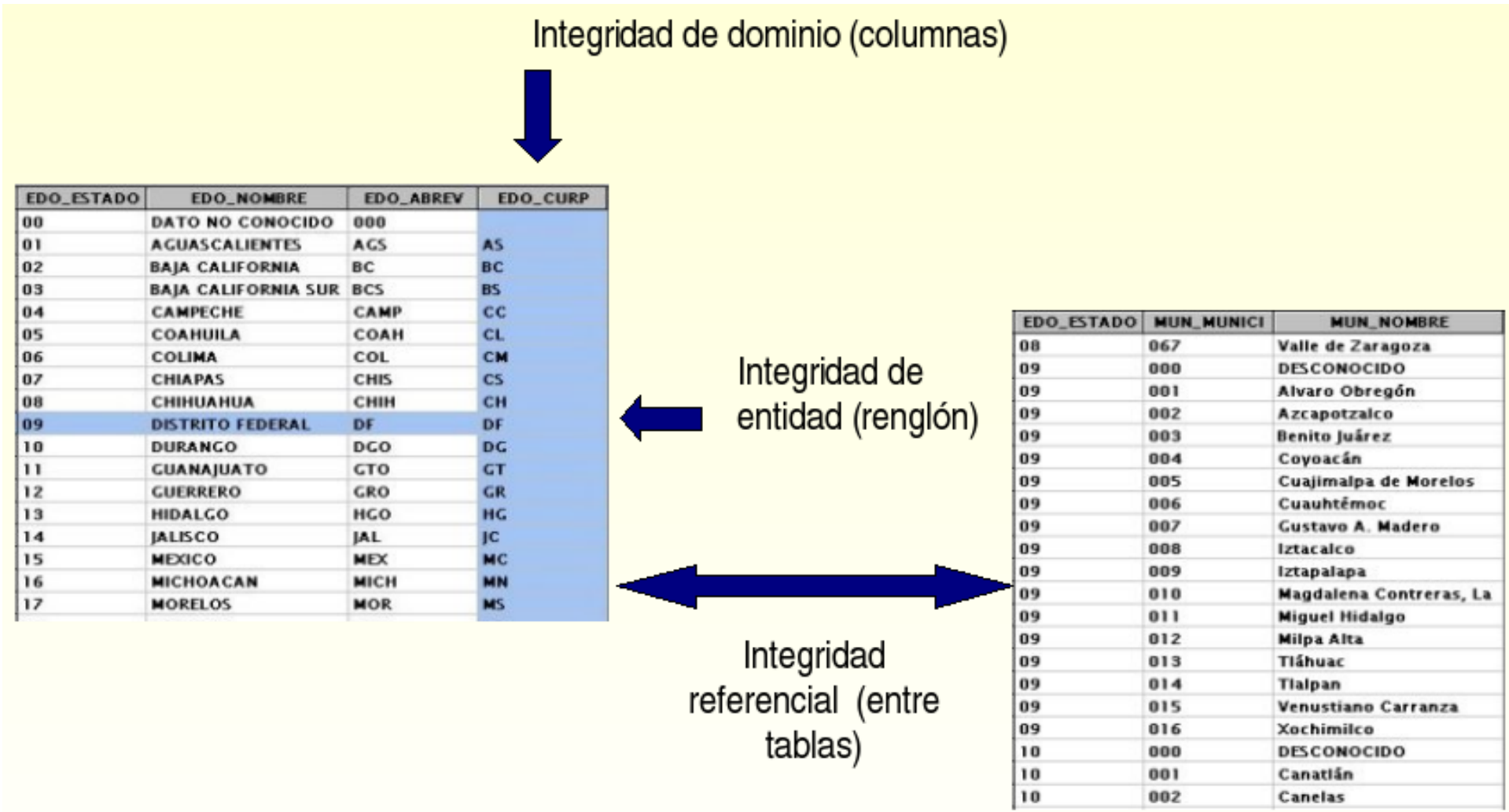
- Expectativa de calidad de datos.
  - Los datos tienen integridad si su calidad alcanza o supera los requerimientos de calidad que los usuarios *esperan* de ellos.
- Protección contra la modificación ***impropia*** de datos.
- Protección contra la modificación ***no autorizada*** de los datos.

- Integridad de dominio
  - Requiere que un conjunto de valores sean válidos para una columna y especifica si se permiten valores nulos. Se implementa mediante la verificación de validez y se puede forzar restringiendo el tipo de datos, formato o rango de valores permitidos en una columna.

- Integridad de entidad
  - Requiere que todos los renglones de una tabla tengan un identificador único, conocido como llave primaria. El valor de una llave primaria puede cambiarse dependiendo del nivel de integridad requerido entre la llave primaria y otras tablas.

- Integridad referencial
  - Asegura que las relaciones entre la llave primaria (en una tabla referenciada) y las llaves foráneas (en una tabla referenciante) siempre se mantenga.
  - Un renglón en una tabla referenciada no puede ser borrado y si un una llave foránea hace referencia a ese renglón, tampoco la llave primaria puede modificarse.

[Integridad de datos] Tipos de integridad



EDO_ESTADO	EDO_NOMBRE	EDO_ABREV	EDO_CURP
00	DATO NO CONOCIDO	000	
01	AGUASCALIENTES	AGS	AS
02	BAJA CALIFORNIA	BC	BC
03	BAJA CALIFORNIA SUR	BCS	BS
04	CAMPECHE	CAMP	CC
05	COAHUILA	COAH	CL
06	COLIMA	COL	CM
07	CHIAPAS	CHIS	CS
08	CHIHUAHUA	CHIH	CH
09	DISTRITO FEDERAL	DF	DF
10	DURANGO	DGO	DG
11	GUANAJUATO	GTO	GT
12	GUERRERO	GRO	GR
13	HIDALGO	HGO	HG
14	JALISCO	JAL	JC
15	MEXICO	MEX	MC
16	MICHOACAN	MICH	MN
17	MORELOS	MOR	MS

EDO_ESTADO	MUN_MUNICI	MUN_NOMBRE
08	067	Valle de Zaragoza
09	000	DESCONOCIDO
09	001	Alvaro Obregón
09	002	Azcapotzalco
09	003	Benito Juárez
09	004	Coyoacán
09	005	Cuajimalpa de Morelos
09	006	Cuauhtémoc
09	007	Gustavo A. Madero
09	008	Iztacalco
09	009	Iztapalapa
09	010	Magdalena Contreras, La
09	011	Miguel Hidalgo
09	012	Milpa Alta
09	013	Tláhuac
09	014	Tlalpan
09	015	Venustiano Carranza
09	016	Xochimilco
10	000	DESCONOCIDO
10	001	Canatlán
10	002	Canelas

Tipos de integridad

Tipo de integridad	Tipo de restricción
Dominio	♦ Verificación de valor nulo ♦ Valor por omisión (default) ♦ Verificación de valor (check)
Entidad	♦ Llave primaria (primary key) ♦ Valor único (unique)
Referencial	♦ Llave foránea (foreign key)

[Integridad de datos]Forzando la integridad

- Integridad declarativa
  - Los criterios de integridad se declaran en las definiciones de los objetos.
  - Se implementa mediante el uso de restricciones declarativas que se definen directamente en tablas y columnas:
    - Restricciones de llave
    - Valores por omisión
    - Valores de verificación

[Integridad de datos]Forzando la integridad

- Integridad procedimental
  - Criterios definidos en *scripts*.
  - Se implementa mediante el uso de procedimientos almacenados y triggers.
  - Se puede implementar en el cliente o en el servidor.

Contenido

[Control de Acceso] DAC

- Control de acceso discrecional (DAC)
  - Medio por el que se restringe el acceso a los objetos a usuarios específicos o grupos de usuarios.
  - El propietario de un objeto puede otorgar privilegios de acceso a otros usuarios sobre el mismo objeto, directamente o indirectamente.

[Control de Acceso] DAC

- Privilegios
  - Medio por el que SQL implementa el DAC.
  - Se conceden privilegios por medio de una instrucción GRANT y se usan para especificar una acción permitida sobre un objeto específico

Vistas

- Los usuarios tienen acceso a la vista, pero no a la tabla base.
- Apropiadas para restricciones de columna
- Soportan herramientas de acceso y consultas ad-hoc
- Están especificadas en SQL - Son independientes del DBMS
- Se soporta la actualización

Contenido

Contenido

1. **Introducción**
2. **Problemas de seguridad en bases de datos**
3. **Integridad de datos**
4. **Control de acceso**
5. **Arquitecturas de seguridad**
6. **Mejores prácticas**

[Mejores prácticas] Recomendaciones

- Usar un sistema de detección de intrusos, especialmente en servidores de bases de datos en línea y de alto riesgo.
- Cambiar las contraseñas de las cuentas creadas por omisión durante la instalación. Asignar contraseñas fuertes a las mismas.
- Deshabilitar las cuentas de invitado y las cuentas de demostración o ejemplo definidas durante la instalación. Eliminar estas cuentas en las bases de datos de producción.

[Mejores prácticas] Recomendaciones

- Mantener actualizado el DBMS con las versiones más recientes del software y de los parches de seguridad liberados por el fabricante del software.
- No permitir que las aplicaciones consulten o manipulen directamente la base de datos mediante instrucciones SELECT, INSERT, UPDATE o DELETE. Usar procedimientos almacenados en su lugar.

[Mejores prácticas] Recomendaciones

- En las aplicaciones, restringir la ejecución de instrucciones de SQL dinámico.
- Impedir que las aplicaciones acepten instrucciones de SQL de los usuarios y las ejecuten sobre la base de datos.
- Hacer que los usuarios consulten los datos mediante vistas en lugar de otorgarles acceso a las tablas base.

[Mejores prácticas] Recomendaciones

- Habilitar la auditoría de acceso al sistema operativo y al servidor de base de datos. Revisar el registro de auditoría buscando los eventos fallidos de acceso y buscar tendencias con la finalidad de detectar posibles intrusos.
- Monitorear cuidadosamente los registros (logs) de error y de eventos y disparar automáticamente alertas relacionadas con la seguridad y con errores. Proteger los archivos de registro (log) mediante permisos apropiados de sistema operativo.

[Mejores prácticas] Recomendaciones

- En ambiente de bases de datos distribuidas, eliminar el acceso a los servidores que no se utilicen. Utilizar cuentas de acceso con mínimos privilegios para los servidores relacionados.
- Almacenar los archivos utilizados para carga masiva de datos o por lotes (batch) en un directorio con los permisos apropiados. Eliminar los archivos una vez que hayan sido utilizados.

- Para asegurar la replicación de datos sobre internet o sobre una red de área amplia (WAN), implementar una red privada virtual (VPN).
- Definir y aplicar una política de respaldo periódico. Almacenar los medios de respaldo en un lugar seguro. Realizar regularmente restauraciones de la base de datos a partir de los respaldos.