Certificación y controles de seguridad en Bases de Datos: Auditoría de SGBDs

Miguel Expósito Martín

Universidad de Cantabria

miguel.exposito@unican.es

26/11/2018

Visión general

Introducción

Introducción

La gran difusión de los SGBDs, junto con la consagración de los datos como uno de los recursos fundamentales de las empresas, han hecho que los temas relativos a su control interno y auditoría cobren mayor interés. Las bases de datos se han convertido en el corazón de los sistemas de información de las organizaciones, que cada día dependen más del buen funcionamiento de estas para su supervivencia.

Control interno

El control interno informático vela diariamente porque todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, leyes, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática. Su misión es asegurarse de que las medidas obtenidas de los mecanismos implantados por cada responsable sean correctas y válidas.

Introducción

El control interno y la auditoría de bases de datos resultan fundamentales para el control y la auditoría de las aplicaciones que acceden a las mismas y para proporcionar confianza sobre todo el sistema de información.

Auditoría

La auditoría informática es un proceso puntual que recoge, agrupa y evalúa evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

El ITGI (Information Technology Governance Institute) destaca en COBIT:

- Se define la información como *los datos en todos sus formatos, de entrada, procesados o de salida de los sistemas de información sea cual sea la forma en que son usados por la organización.*
- La infraestructura, es decir, la tecnología e instalaciones, incluyendo el SGBD.

Metodología para la auditoría de SGBDs

Metodología

Según ISACA[1], se empezaría fijando objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno de bases de datos. Por ejemplo:

- Objetivo de conrol: preservar la confidencialidad.
- Técnica de control: establecer tipos de usuarios, perfiles y privilegios.
- Prueba de cumplimiento: listar los privilegios y perfiles existentes en el SGBD.
- Prueba sustantiva: comprobar si la información ha sido corrompida comparándola con otra fuente o revisando documentos de entrada de datos y transacciones que se han ejecutado.

Una vez evaluados los resultados, se obtienen unas conclusiones que serán comentadas y discutidas con los responsables directos de las áreas afectadas. Como resultado de la auditoría, se presentará un informe final en el que se expondrán las conclusiones más importantes a las que se ha llegado, así como el alcance de la misma.

[1] https://www.isaca.org/

Recomendaciones de COBIT

Metodología

En COBIT, los principales objetivos de control relacionados con SGBDs son los siguientes:

- Definir la arquitetura de información.
  - Modelo Corporativo de Arquitectura de Información.
  - Diccionario de Datos Corporativo y Reglas de Sintaxis de Datos.
- Esquema de Clasificación de Datos.
- Gestión de Integridad.
- Gestionar Datos.
  - Requisitos de negocio para la gestión de datos.
  - Planes de almacenamiento y retención de datos.
  - Sistema de gestión de bibliotecas de medios.
  - Eliminación de datos.
  - Copia de respaldo y restauración.
  - Requisitos de seguridad para gestión de datos.

Objetivos de control en el ciclo de vida de una base de datos

Objetivos de control: estudio previo y plan de trabajo

En esta primera fase, es muy importante elaborar un **estudio tecnológico de viabilidad** en el cual se contemplen distintas alternativas para alcanzar los objetivos del proyecto acompañados de un análisis coste-beneficio de cada una de las opciones. Entre las alternativas a considerar estará la posibilidad de no llevar a cabo el proyecto (no siempre se necesita un SGBD), así como la disyuntiva entre desarrollo y compra.

La Dirección deberá revisar los estudios de viabilidad, ya que si no existe una decidida voluntad de la organización en su conjunto, impulsada por los directivos, el riesgo de fracaso aumenta considerablemente.

También será necesario llevar a cabo una **gestión de riesgos** y el establecimiento de un **plan director** en caso de que se decida llevar a cabo el proyecto.

Objetivos de control: estudio previo y plan de trabajo

Un aspecto muy importante en esta fase es la aprobación de la estructura orgánica de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos, separando funciones:

- Desarrollo de sistemas y explotación.
- Explotación y control de datos.
- Administración de bases de datos y desarrollo.

Para facilitar la asignación de funciones y roles se puede utilizar una matriz RACI (*Responsible, Accountable, Consulted, Informed*)

Objetivos de control: concepción y selección de equipo

En esta fase se comienza a diseñar la base de datos siguiendo modelos y técnicas definidos por la metodología de desarrollo de la Organización. El auditor debe, en primer lugar, analizar la metodología de diseño; y en segundo lugar, comprobar su correcta utilización. Como mínimo, esta metodología deberá contemplar aspectos físicos y lógicos.

Advertencia

¡¡Hay auditores que piensan que ciertas metodologías no existen o no son metodologías!! Ej: Extreme programming.

Objetivos de control: diseño y carga

En esta fase se llevan a cabo los diseños físico y lógico de la BD, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente, determinando si la definición de los datos contempla, además de su estructura, las asociaciones y restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a seguridad.

Una vez realizado el diseño, se procederá a la carga o alimentación de la BD, planificando y probando convenientemente dichas tareas. Es aconsejable establecer controles que aseguren la integridad de los datos.

Objetivos de control: explotación y mantenimiento

Terminada la fase anterior, el sistema se pondrá, mediante las correspondientes autorizaciones y siguiendo los procedimientos establecidos para ello, en explotación. Se deberá comprobar que se establecen los procedimientos de explotación y mantenimiento que aseguran que los datos se traten de forma congruente y exacta.

También sería conveniente que el auditor pudiera llevar a cabo una auditoría sobre el rendimiento del sistema de BD, comprobando si se han llevado a cabo los procesos de ajuste fino y optimización adecuados.

Objetivos de control: revisión posterior y procesos auxiliares

La revisión post-implantación debe evaluar si:

- Se han conseguido los resultados esperados.
- Se satisfacen las necesidades de los usuarios.
- Los costes y beneficios coinciden con los previstos.

A lo largo de todo el ciclo de vida de la BD se deberá controla la formación que precisan tanto los usuarios informáticos como no informáticos, dado que **la formación es clave para minimizar el riesgo en una implantación de base de datos**. Esta formación no debería limitarse al área de bases de datos, sino que tendría que ser complementada con formación relativa a los conceptos de control y seguridad.

Además, el auditor tendrá que revisar la documentación que se produce a lo largo de todo el proceso para comprobar que es suficiente y si se ajusta a los estándares establecidos por la metodología adoptada. A este respecto, resulta importante llevar a cabo un **aseguramiento de la calidad**.

Auditoría y control interno en un entorno SGBD

Auditoría y control interno en un entorno SGBD

- SGBD: núcleo (kernel), catálogo, utilidades del administrador.
- Monitorización y ajuste: información para optimizar el SGBD.
- Sistema operativo: las interfaces entre SGBD y SO suelen ser cerradas por los fabricantes.
- Paquetes de seguridad: permiten implantar una política de seguridad. A veces no se encuentra bien integrado con un SGBD.
- Diccionarios de datos: se pueden auditar, puesto que son bases de metadatos. Un fallo en un diccionario de datos suele llevar consigo una pérdida de integridad de los procesos.
- Herramientas CASE: soporte al diseño y concepción de SGBDs. Permiten al auditor revisar el diseño de la BD.
- 4GLs: uno de los peligros más graves de los 4GL es que no se apliquen controles con el mismo rigor que a programas desarrollados en lenguajes de tercera generación.
- Facilidades de usuario: determinadas hojas de cálculo permiten establecer conexiones a las bases de datos. El auditor deberá prestar especial atención a los procedimientos de carga y descarga de datos desde la BD usando paquetes ofimáticos.

Ejercicio 4.1

Uno de los objetivos de control de COBIT relacionados con bases de datos es el del establecimiento de una política de copias de seguridad.

1. Realice un volcado de la tabla actor de la BD sakila. Restáurela en otra base de datos creada al efecto.
2. Proponga una política de copias de seguridad para una base de datos MariaDB.

Ejercicio 4.2

Defina un procedimiento para la selección de SGBDs.

Referencias

Mario Piattini Velthuis et al. (2008)

Auditoría de Tecnologías y Sistemas de Información.