Auditoría de Bases de Datos

Auditoría de Bases de Datos

La gran difusión de los Sistemas de Gestión de Bases de Datos (SGBD) y la consagración de los datos como recursos fundamentales de las empresas, han hecho que el control interno y la auditoría de los mismos tomen cada día mayor interés.

Actualmente, el buen funcionamiento de los sistemas de información de las organizaciones depende principalmente de las bases de datos; y es por ello que, el control interno y la auditoría de las mismas resulta fundamental para el control y la auditoría de las aplicaciones que acceden a ellas, para proporcionar confianza en el sistema de información.

En el COBIT se destaca dos recursos principales que están relacionados con los sistemas de bases de datos:

- Define a la información como, *los datos en todas sus formatos, de entrada, procesados o de salida de los sistemas de información sea cuál sea la forma en que son usados por la organización*.
- La infraestructura, es decir, la tecnología e instalaciones, incluyendo el sistema de gestión de bases de datos.

Metodología para la auditoría de bases de datos

1-Se empieza fijando los **objetivos de control**, que minimizan los riesgos potenciales a los que está sometido el entorno de bases de datos.

2-Luego se especifican las técnicas específicas correspondientes a los objetivos. Un objetivo puede llevar asociadas varias técnicas que permiten cubrirlo en su totalidad. Las **técnicas de control** pueden ser:

- *Preventivas*
- *Correctivas*

3-Si existen controles se diseñan **pruebas de cumplimiento**, que permiten verificar la consistencia de los mismos.

4-Si las pruebas de cumplimiento detectan inconsistencias en los controles o si los controles no existen, se diseñan **pruebas sustantivas**, que permiten dimensionar el impacto de estas deficiencias.

5-Una vez valorados los resultados de las pruebas se obtienen conclusiones, que se comentan y discuten con los responsables de las áreas afectadas, con el fin de corroborar los resultados.

6-Por último, el auditor debe emitir una serie de *comentarios* que describan la situación, el riego existente, la deficiencia a solucionar y, sugerir la posible solución.

7-Como resultado de la auditoría se presenta un informe final en el que se exponen las conclusiones más importantes y el alcance que tuvo la auditoría.

Esta será la técnica a utilizar para auditar el entorno general de un sistema de base de datos, tanto para su desarrollo como durante la explotación.

Recomendaciones de los COBIT para auditoría de Bases de Datos

Los principales **objetivos de control** relacionados con las bases de datos son:

a. Definir la arquitectura de información
    i. Modelo corporativo de arquitectura de información
    ii. Diccionario de datos corporativo y reglas de sintaxis de datos
    iii. Esquema de clasificación de datos
b. Gestión de integridad
c. Gestionar datos
    i. Requisitos de negocio para la gestión de datos
    ii. Planes de almacenamiento y retención de datos
    iii. Sistema de gestión de bibliotecas de medios.
    iv. Eliminación de Datos
    v. Copia de respaldo y restauración
    vi. Requisitos de seguridad para gestión de datos

Se deben definir diferentes objetivos y métricas para cada objetivo de control, y para cada objetivo de control, se definen los **drivers de valor y riesgo**, y las **pruebas de diseño de control** correspondientes.

Objetivos de Control en el Ciclo de Vida de una Base de Datos

1-Estudio previo y plan de trabajo

Es importante elaborar un estudio tecnológico de viabilidad, en cual se contemplan distintas alternativas para alcanzar los objetivos del proyecto acompañados de un análisis de coste-beneficio para cada una.

Se debe considerar la posibilidad de no llevar a cabo el proyecto así como la disyuntiva entre desarrollar y comprar.

El auditor debe comprobar que la alta dirección revisa los informes de los estudios de viabilidad y si decide o no seguir adelante con el proyecto. Esto es importante, porque si no existe una decidida voluntad de la organización, aumentan el riesgo de fracasar en la implantación del sistema.

Es necesario, además, llevar a cabo una gestión de riegos.

En caso de que se decida llevar a cabo el proyecto, es fundamental establecer un plan director, debiendo el auditor verificar que dicho plan se emplee para el seguimiento y gestión del proyecto, y que cumple con los procedimientos generales de gestión de proyectos que tenga aprobados la organización.

Otro aspecto importante, es la aprobación de la estructura orgánica del proyecto y de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos para que en entorno de la base de datos funcione correctamente.

En la ITGI se contemplan diferentes roles relacionados con la Gestión de datos, y a la hora de detallar las responsabilidades hay que tener en cuenta la separación de funciones. Se recomienda una separación de funciones entre:

- El personal de desarrollo de sistemas y el de explotación
- Explotación y control de datos
- Administración de bases de datos y desarrollo.
- Administrador de la seguridad y el administrador de la base de datos.

Una separación de funciones no quiere decir que estas tareas deban ser desempeñadas por personas distintas, pero si que es un aspecto de control a tener en cuenta, para que en caso de no poder cumplirse, se establezcan controles compensatorios o alternativos.

2-Concepción de la base de datos y selección del equipo

En esta fase, se comienza a diseñar la base de datos, por lo que deben utilizarse modelos y técnicas definidas en la metodología de desarrollo, la cual también debe emplearse para especificar los documentos fuentes, slos mecanismos de control, las características de seguridad y las pistas de auditoría.

El auditor debe entonces analizar la metodología de diseño para determinar si es o no aceptable y luego comprobar su correcta utilización.

En cuanto a la selección del equipo, en caso de que la empresa no disponga de uno, deberá realizarse utilizando un procedimiento riguroso que considere las necesidades de la empresa y las prestaciones que ofrecen los distintos SGBD candidatos.

3-Diseño y carga

En esta fase se llevan a cabo los diseños lógico y físico de la base de datos, y es el auditor quien debe examinar si se han realizado correctamente, determinando además si la definición de los datos contempla la estructura, las asociaciones y restricciones oportunas, además de las especificaciones de almacenamiento de datos y la seguridad de los mismos.

El auditor toma muestras de ciertos elementos comprueba si la definición es completa y si ha sido aprobada por el usuario y el administrador de la base de datos.

Una vez diseñada, se procede a su carga, ya sea migrando o introduciendo datos manualmente.

Las migraciones o el paso de ficheros de una base de datos a otro representan un riesgo importante, por lo que deberán ser planificadas para evitar pérdida de información y la trasmisión de datos erróneos. También se deben realizar pruebas en paralelo, hasta verificar los criterios establecidos para detenerla, aplicando un control estricto de la corrección de errores.

En lo que respecto a la entrada manual de datos, hay que establecer un conjunto de controles que aseguren la integridad de los mismos.

Es aconsejable que los procedimientos y el diseño de los documentos fuentes minimicen los errores y las omisiones, además de establecer procedimientos de autorización de datos.

4-Explotación y mantenimiento

En esta fase se debe comprobar que se establezcan los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas sólo se modifica con autorización.

El auditor debería llevar a cabo una auditoría sobre el rendimiento del sistema BD, comprobando el proceso de ajuste y optimización adecuado.

5-Revisión post-implantación

No suele llevarse a cabo por falta de tiempo y recursos, pero debería establecer el desarrollo de un plan para efectuar una revisión post-implantación de todo sistema, con el fin de evaluar si:

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

6-Otros procesos auxiliares

A lo largo del ciclo de vida de la base de datos, debería controlase la formación que precisan los usuarios informáticos y no informáticos, ya que la formación en el área de bases de datos es un factor clave que minimiza el riesgo de implantación de la misma; además, dicha formación debería complementarse con conceptos de control y seguridad.

Otro aspecto importante a tener en cuenta por el auditor es la revisión de la documentación, que permita verificar si es suficiente y se ajusta a los estándares de calidad.

Auditoría y Control interno en un entorno de Bases de Datos

Cuando el auditor se encuentra el sistema en explotación debe estudiar el SGBD y su entorno.

1- 1- Sistema de gestión de base de datos

Entre los componentes podemos destacar el núcleo, el catálogo, las utilidades para el administrador, las que se encargan de la recuperación de la BD, rearranque, copias de respaldo, ficheros diarios, algunas funciones de auditoría y los lenguajes de cuarta generación.

La mayoría de los sistemas permite registrar operaciones realizadas sobre la base de datos en un fichero de pistas de auditoría.

El auditor deberá revisar la utilización de todas las herramientas que ofrece el propio de SGBD y las políticas y procedimientos que haya definido el administrador, para valorar si son suficientes o si deben ser mejorados.

2- 2- Software de auditoría

Son paquetes que pueden emplearse para facilitar la labor del auditor, en cuanto a la extracción de datos de la base, el seguimiento de las transacciones, datos de prueba, etc. Existen, además, algunos que permiten cuadrar datos de diferentes entornos.

3- 3-Sistema de monitorización y ajuste

Estos sistemas complementan las facilidades ofrecidas por el SGBD, ofreciendo mayor información para optimizar el sistema, proporcionando en ocasiones la estructura óptima de la base de datos y de ciertos parámetros del SGBD y del SO.

La optimización de la base de datos es fundamental sobre todo si actúa en un entorno concurrente que pueda degradar el nivel de servicio con los usuarios.

4- 4- Sistema operativo

El SO es una pieza clave del entorno, puesto que el SGBD se apoya en los servicios que este le ofrece en cuanto a control de memoria, gestión de las áreas de almacenamiento intermedio, manejo de errores, entre otros; lo que produce serias dificultades al auditor en lo que refiere al control de la interfaz, ya que dicha información es por lo general reservada por los fabricantes.

5- 5- Monitor de transacciones

Pueden considerarse un elemento más del entorno con responsabilidades de seguridad y rendimiento.

6- 6-Protocolos y sistemas distribuidos

Cada vez se accede más a las bases de datos a través de redes, implicando un mayor reisgo de violación de la confidencialidad e integridad.

7- 7-Paquetes de seguridad

Existen varios productos que permiten la implantación efectiva de una política de seguridad porque centralizan el control de accesos, la definición de privilegios, perfiles de usuario, etc.; pero presentan un grave inconveniente al integrar con el SGBD.

8- 8-Diccionario de datos

Se pueden auditar de manera análoga a las bases de datos. Un fallo en el diccionario de datos puede significar una pérdida de integridad de los procesos, siendo más peligroso que los fallos de las bases de datos, porque permiten introducir errores de forma repentina.

9- 9-Herramientas CASE

Estas herramientas suelen incorporar un diccionario de datos más amplio, en el que se almacena información sobre datos, programas, usuarios, además de diagramas, matrices y grafos de ayuda al diseño, constituyendo así una herramienta clave para el auditor, que le permite revisar el diseño de la base de datos, comprobar si se ha empleado correctamente la metodología y asegurar un nivel mínimo de calidad.

10- 10-Lenguajes de cuarta generación independientes

El auditor se puede encontrar con una amplia gama de generadores de aplicaciones, de formas, de informes, que actúen sobre la base de datos y que por lo tanto son un elemento a considerar en el entorno del SGBD.

Uno de los principales peligros que puede presentarse es aquel que surge de la inadecuada interfaz entre el L4G y el paquete de seguridad, y a la falta de código fuente, lo que dificulta el control de cambios en las aplicaciones.

El auditor debe estudiar los controles disponibles de los L4G, analizando si estos permiten construir procedimientos de control y auditoría; en caso de que no lo permitan no recomendar su utilización.

11- 11-Facilidad de usuario

Con la aparición de interfaces gráficas amistosas se ha desarrollado toda una serie de herramientas que permitan al usuarios acceder a los datos sin tener que conocer la sintaxis de los lenguajes del SGBD, por lo tanto el auditor, debe investigar las medidas de seguridad que ofrecen estas herramientas y las condiciones bajo las que fueron instaladas.

12- 12-Herramientas de "minería de datos”

Estas herramientas ofrecen soporte a la toma de decisiones, sobre datos de calidad integrados en el almacén de datos, debiéndose controlar las políticas de refresco y carga de los datos en el almacén a partir de las bases de datos operacionales existentes, así como la existencia de mecanismos de retroalimentación, que modifican las bases de datos operacionales a partir de los datos del almacén.

I3- 13- Aplicaciones

El auditor deberá controlar que las aplicaciones no atenten contra la integridad de la base de datos.

Conclusiones

Brathwaite (1985) "la tecnología de bases de datosssssssss ha afectado al papel del auditor interno más que a cualquier otro individuo". Esto se debe a la complejidad de la propia tecnología de bases de datos y al entorno del SGBD.

El gran número de componentes que forman dicho entorno y sus interfaces hacen necesario que el auditor deba examinar el entorno en el que el SGBD.

El auditor debe verificar que todos estos componentes trabajan conjunta y coordinadamente para asegurar que los sistemas de bases de datos continúan cumpliendo los objetivos de la empresa y que se encuentran controlados de manera efectiva.

Por lo que respecta al futuro de esta área, la aparición de nuevos tipos de bases de datos y la creciente distribución de los mismos, además de la creciente complejidad de sus entornos, se presentan como nuevos riegos para el auditor; convirtiendo a la auditoria y la toma de medidas de control en actividades indispensables para todas las organizaciones.