\AUDITORIA DE BASE DE DATOS

INDICE

01. INTRODUCCION

La gran difusión de los Sistemas de Gestión de Bases de Datos (SGBD), junto con la consagración de los datos como uno de los recursos fundamentales de las empresas, ha hecho que los temas relativos a su control interno y auditoria cobren, cada día, mayor interés.

Normalmente la auditoria informática se aplica de dos formas distintas; por un lado se auditan las principales áreas del departamento de informática: explotación, dirección, metodología de desarrollo, sistema operativo, telecomunicaciones, bases de datos, etc.; y, por otro, se auditan las aplicaciones desarrolladas internamente, (subcontratadas o adquiridas) que funcionan en la empresa. La importancia de la auditoria del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoria de las aplicaciones que utilizan esta tecnología.

02. METODOLOGÍAS PARA LA AUDITORÍA DE BASES DE DATOS.

Aunque existen distintas metodologías que se aplican en auditoría informática (prácticamente cada firma de auditores y cada empresa desarrolla la suya propia), se pueden agrupar en dos clases:

Metodología tradicional.- En este tipo de metodología el auditor revisa el entorno con la ayuda de una lista de control (checklist), que consta de una serie de cuestiones a verificar. Por ejemplo:

¿Existe una metodología de Diseño de Base de Datos? S N NA

(S es si, N no y NA no aplicable), debiendo registrar el auditor el resultado de su investigación.

Este tipo de técnica suele ser aplicada a la auditoría de productos de bases de datos, especificándose en la lista de control todos los aspectos a tener en cuenta.

Metodología de evaluación de riesgos: Este tipo de metodología, conocida también por *risk oriented approach,* es la que propone la ISACA, y empieza fijando los

objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno. A continuación, una lista de los riesgos más importantes según 2 autores:

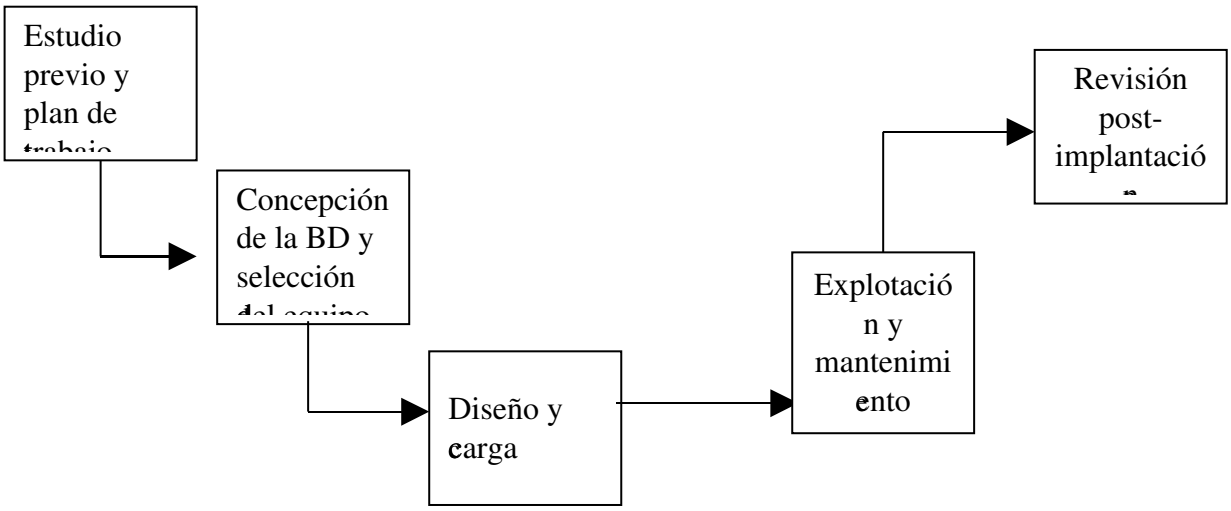
- Incremento de la "dependencia" del servicio informático debido a la concentración de datos
- Mayores posibilidades de acceso en la figura del administrador de la base de datos
- Incompatibilidad entre sistemas de seguridad de acceso propios del SGBD y el general de la instalación.
- Mayor impacto de los errores en datos o programas que en los sistemas tradicionales
- Ruptura de enlaces o cadenas por fallos del software o de los programas de aplicación
- Mayor impacto de accesos no autorizados al diccionario de la base de datos que a un fichero tradicional.
- Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas con el software de base de datos (administrador, programadores, etc.)

Como en la auditoría de desarrollo, se puede seguir la misma metodología, donde se establecen primeramente:

Objetivo de control (ejemplo: El SGBD deberá preservar la confidencialidad de la base de datos).
Técnicas de control. Una vez establecidos los objetivos de control, se especifican las técnicas específicas correspondientes a dichos objetivos (ejemplo: Se deberán establecer los tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a las bases de datos).
Un objetivo de control puede llevar asociadas varias técnicas que permiten cubrirlo en su totalidad. Estas técnicas pueden ser preventivas, detectivas (como monitorizar la BD) o correctivas (por ejemplo, una copia de respaldo o backup).
Pruebas de cumplimiento. En caso de que los controles existan, se diseñan unas pruebas (denominada *pruebas de cumplimiento)* que permiten verificar la consistencia de los mismos. Por ejemplo: Listar los privilegios y perfiles existentes en el SGBD.
Si estas pruebas detectan inconsistencias en los controles, o bien, si los controles no existen, se pasa a diseñar otro tipo de pruebas – denominadas *pruebas sustantivas* - que permitan dimensionar el impacto de estas deficiencias.
Prueba sustantiva. Comprobar si la información ha sido corrompida comparándola con otra fuente o revisando los documentos de entrada de datos y las transacciones que se han ejecutado.

Una vez valorados los resultados de las pruebas se obtienen conclusiones que serán comentadas y discutidas con los responsables directos de las áreas afectadas con el fin de corroborar los resultados. Por último, el auditor deberá emitir una serie de comentarios donde se describa la situación, el riesgo existente y la deficiencia a solucionar, y en su caso, sugerirá la posible solución.
Esta será la técnica a utilizar para auditor el entorno general de un sistema de bases de datos, tanto en su desarrollo como durante la explotación.

PRINCIPALES OBJETIVOS DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS



03. 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 de costo-beneficio para cada una de las opciones. Se debe considerar entre estas alternativas la posibilidad de no llevar a cabo el proyecto (no siempre está justificada la implantación de un sistema de base de datos) así como la disyuntiva entre desarrollar y comprar (en la práctica, a veces encontramos con que se ha desarrollado una aplicación que ya existía en mercados, cuya compra hubiese supuesto un riesgo menor, asegurándonos incluso una mayor cantidad a un precio inferior).
Lamentablemente, en bastantes empresas este estudio de viabilidad no se lleva a cabo con el rigor necesario, con lo que a medida que se van desarrollando, los sistemas demuestran ser poco rentables.
El auditor debe comprobar también que la alta dirección revisa los informes de los estudios de viabilidad y que es la que decide seguir adelante o no con el proyecto. Esto es fundamental porque los técnicos que han de tener en cuenta que si no existe una decidida voluntad de la organización en su conjunto, impulsada por los directivos, aumenta considerablemente el riesgo de fracasar en la implantación de sistema.
En caso de que se decida llevar a cabo el proyecto es fundamental que se establezca un plan director, debiendo el auditor verificar que efectivamente dicho plan se emplea para

el seguimiento y gestión del proyecto y que cumple con los procedimientos generales de gestión de proyectos que tengan aprobados la organización.
Otro aspecto importante en esta fase es la aprobación de la estructura orgánica del proyecto en particular, sino también de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos; recordemos que, para que un entorno de base de datos funcione debidamente, esta unidad es imprescindible.

Tareas del administrador de datos

- Realizar el diseño conceptual y lógico de la base de datos
- Apoyar al personal de sistemas durante el desarrollo de aplicaciones
- Formar al personal
- Establecer estándares de diseño de b.d. desarrollo y contenido del diccionario de datos
- Desarrollar políticas de gestión de datos
- Desarrollar planes estratégicos y tácticos para la manipulación de los datos
- Desarrollar los requisitos de los elementos del diccionario de datos
- Desarrollar normas para la denominación
- Controlar la integridad y seguridad de los datos
- Planificar la evolución de la bd de la empresa
- Identificar oportunidades de compartición de datos
- Trabajar con los auditores en la auditoría de la base de d.
- Proporcionar controles de seguridad
- Realizar el diseño físico de la b.d.
- Asesorar en la adquisición de hw y sw
- Soportar el SGBD
- Resolver problemas del SGBD y del software asociado
- Monitorizar el rendimiento del SGBD
- Ayudar en el desarrollo de planes que aseguren la capacidad hw.
- Asegurar la integridad de los datos, comprobando que se implantan los controles adecuados
- Asegurar la seguridad y confidencialidad
- Proporcionar facilidades de prueba
- Integrar paquetes, procedimientos, utilidades, etc. De soporte para al SGND
- Desarrollar estándares, procedimientos y documentarlos

A la hora de detallar las responsabilidades de estas funciones hay que tener en cuenta uno de los principios fundamentales del control interno: 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 base de datos y desarrollo

Debería existir también una separación de funciones entre el administrador de seguridad y el administrador de la base de datos. Esto no quiere decir que estas tareas tengan forzosamente que desempeñarlas personas distintas (lo que no sería viable en muchas y pequeñas y medianas empresas) pero sí que es un aspecto importante de control a considerar, por lo que en caso de que no pueda lograrse la separación de funciones, deberán establecerse controles compensatorios o alternativos: como, por ejemplo, una mayor atención de la dirección y la comprobación por parte de algún usuario del contenido y de las salidas más importantes producidas a partir de la BD.

La situación que el auditor encuentra normalmente en las empresas es que al no existir una descripción detallada de los puestos de trabajo (que incluyan responsabilidades, conocimientos, etc.), la separación de funciones es muy difícil de verificar.

04. CONCEPCIÓN DE LA BASE DE DATOS Y SELECCIÓN DEL EQUIPO.

En esta fase se empieza a diseñar la base de datos. La metodología de diseño debería también emplearse para especificar los documentos fuentes, los mecanismos de control, las características de seguridad y las pistas de auditoria a incluir en el sistema, estos últimos aspectos generalmente se descuidan, lo que produce mayores costos y problemas cuando se quieren incorporar una vez concluida la implementación de la base de datos y la programación de las aplicaciones.
El auditor debe por tanto, en primer lugar, analizar la metodología de diseño con el fin de determinar si es o no aceptable, y luego comprobar su correcta utilización. Como mínimo, una metodología de diseño de BD debería contemplar dos fases de diseño: lógico y físico, aunque la mayoría de las empleadas en la actualizad contempla 3 fases: además de las dos anteriores, una fase previa de diseño conceptual que sería abordada en este momento del ciclo de vida de la base de datos.

Un punto importante a considerar, objetivos de control relativos a:

- Modelo de arquitectura de información y su actualización, que es necesaria para mantener el modelo consistente con las necesidades de los usuarios y con el plan estratégico de tecnologías de la información
- Datos y diccionario de datos corporativo
- Esquema de clasificación de datos en cuanto a seguridad
- Niveles de seguridad para cada anterior clasificación de datos

En cuanto a la selección del equipo, en caso de que la empresa no disponga ya de uno, deberá realizarse utilizando procedimiento riguroso; en el que se considere por un lado, las necesidades de la empresa (debidamente ponderadas) y, por otro, las prestaciones que ofrecen los distintos SGBD candidatos (puntuados de manera oportuna).

05. DISEÑO Y CARGA

En esta fase se llevarán a cabo los diseños lógico y físico de la base de datos, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente: determinando si la definición de datos contemplan además de su estructura, las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad. El auditor tendrá que tomar una muestra de ciertos elementos (tablas, vistas, índices) y comprobar que su definición es completa, que ha sido aprobada por el usuario y que el administrador de la base de datos participó en su establecimiento.
Es importante que la dirección del departamento de informática, los usuarios e incluso, en algunas ocasiones, la alta dirección, aprueben el diseño de los datos, al igual que el de las aplicaciones.
Una vez diseñada una BD se procederá a su carga, ya sea migrando datos de un soporte magnético o introduciéndolos manualmente.

Las migraciones o conversiones de sistemas, con el paso de un sistema de ficheros a uno de base de datos, o de un tipo de SGBD (de jerárquico a racional), entrañan un riesgo muy importante, por lo que deberán estar claramente planificadas para evitar pérdida de información y la transmisión al nuevo sistema de datos erróneos. También se deberán realizar pruebas en paralelo, verificando que la decisión real de dar por terminada la prueba en paralelo, se atenía a los criterios establecidos por la dirección y que se haya aplicado un control estricto de la corrección de errores detectados en esta fase.
Por lo que respecta a la entrada manual de datos, hay que establecer un conjunto de controles que aseguren la integridad de los mismos. A este respecto, cabe destacar que las declaraciones escritas de procedimientos de la organización referentes a la entrega de datos a ser procesados deben asegurar que los datos se autorizan, recopilan, preparan, transmiten y se comprueba su integridad de forma apropiada.
También es aconsejable que los procedimientos y el diseño de los documentos fuentes minimicen los errores y las omisiones, así como el establecimiento de procedimientos de autorización de datos.
Un aspecto muy importante es el tratamiento de datos de entrada erróneos, para los que deben cuidarse con atención los procedimientos de reintroducción de forma que no disminuyan los controles; a este respecto lo ideal es que los datos se validen y corrijan tan cerca del punto de origen como sea posible.

06. EXPLOTACIÓN Y MANTENIMIENTO.

Una vez realizadas las pruebas de aceptación, con la participación de los usuarios, el sistema se pondrá (mediante las correspondientes autorizaciones y siguiendo los procedimientos establecidos para ello) en explotación.
En esta fase, se debe comprobar que se establecen 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 mediante la autorización adecuada.
Sería conveniente también que el auditor pudiera llevar a cabo una auditoría sobre el rendimiento del Sistema de BD, comprobando si se lleva a cabo un proceso de ajuste y optimización adecuados que no sólo consiste en el rediseño físico o lógico de la BD, sino que también abarca ciertos parámetros del SO e incluso la forma en que acceden las transacciones a la BD. Recordemos que la "función de administración de la base de datos debe ser la responsable de monitorizar el rendimiento y la integridad de los sistemas de BD".

07. REVISIÓN POST-IMPLANTACIÓN.

Aunque en bastantes organizaciones no se lleva a cabo, por falta de tiempo y recursos, se debería establecer el desarrollo de un plan para efectuar una revisión post-implantación de todo sistema nuevo o modificado con el fin de evaluar si:

- Se han conseguido los resultados esperados
- Se satisfacen las necesidades de los usuarios
- Los costos y beneficios coinciden con lo previsto