Seguridad y Auditoría Informática

Auditoría de Bases de Datos

Ing. Alfredo Pardo

Año 2021

Tabla de Contenidos

Auditoría de Bases de Datos

Auditoría de Bases de Datos

La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utilizan esta tecnología.

Metodologías para la Auditoría de Bases de Datos

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.

Metodología de Evaluación de Riesgos

Esta metodología, conocida también como 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.

Una vez establecidos los objetivos de control, se especifican las técnicas específicas correspondientes a dichos objetivos. Un objetivo de control puede llevar asociadas varias técnicas que permiten cubrirlo en su totalidad. Estas técnicas pueden ser preventivas, detectivas y correctivas.

En caso de que los controles existan, se diseñan pruebas (denominadas pruebas de cumplimiento) que permiten verificar la consistencia de los mismos.

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 permiten dimensionar el impacto de estas deficiencias.

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.
Como resultado de la auditoría, se presentará un informe final en el que se exponen las conclusiones más importantes a las que se ha llegado, así como el alcance que ha tenido la auditoría.

Riesgos debidos a la utilización de Bases de Datos

- 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.)

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

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 costo-beneficio para cada una de las opciones. Se debe considerar entre estas alternativas la posibilidad de no llevar a cabo el proyecto así como la disyuntiva entre desarrollar y comprar.

Desafortunadamente, en bastantes empresas este estudio de viabilidad no se lleva a cabo con el rigor necesario, con lo que a medida que se va 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.

En COBIT se enfatiza la importancia de llevar a cabo una gestión de riesgos (valoración, identificación, medida, plan de acción y aceptación).

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 tenga aprobados la organización.

Otro aspecto muy importante de esta etapa es la aprobación de la estructura orgánica no sólo del proyecto en particular, sino también de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos.

Se pueden establecer acerca de este tema dos objetivos de control:

- Deben asegurarse responsabilidades para la planificación, organización, dotación de plantillas y control de los activos de datos de la organización. (Administrador de Datos).
- Debe asignarse la responsabilidad de la administración del entorno de la base de datos. (Administrador de Base de Datos).

Ambas funciones deben posicionarse en un nivel del organigrama lo suficientemente alto para asegurar su independencia.

Tareas del Administrador de Datos

- Realizar el diseño conceptual y lógico de la Base.
- Apoyar al personal de sistemas durante el desarrollo de aplicaciones.
- Formar al personal.
- Establecer estándares de diseño de BD, desarrollo y contenido del diccionario de datos.
- Diseñar la documentación incluida en el diccionario.
- 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 Base de Datos de la empresa.
- Identificar oportunidades de Compartición de Datos.
- Trabajar con los auditores en la auditoría de la Base.
- Proporcionar controles de Seguridad.

Tareas del Administrador de Base de Datos

- Realizar el diseño físico de la base de datos.
- Asesorar en la adquisición de hardware/software.
- 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 hardware.
- Asegurar la integridad de los datos, comprobando que se implementan los controles adecuados.
- Asegurar la confidencialidad.
- Proporcionar facilidades de prueba.
- Integrar paquetes, procedimientos, utilidades, etc. de soporte al SGBD.

- Desarrollar estándares, procedimientos y documentación.

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 uso.
- Uso y control de datos.
- Administración de Bases de Datos y desarrollo.

Debería existir también una separación de funciones entre el Administrador de Seguridad y el Administrador de la Base de Datos.

La situación que encuentra el auditor es que al no existir una descripción detallada de los puestos de trabajo, la separación de funciones es difícil de verificar.

Concepción de la Base de Datos y Selección del Equipo

En esta fase se empieza a diseñar la base de datos, por lo que deben utilizarse los modelos y las técnicas definidos en la metodología de desarrollo de sistemas de la empresa.

La metodología de diseño debería también emplearse para especificar los documentos fuentes, los mecanismos de control, las características de seguridad y las pistas de auditoría 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 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 actualidad contempla tres 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 importante aspecto a considerar es la definición de la arquitectura de la información, que contempla cuatro 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 un procedimiento riguroso; en el que se consideren, 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). En este

procedimiento se debe tener en cuenta el impacto que el nuevo software tiene en el sistema y en su seguridad.

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 los datos contempla además de su estructura, las asociaciones y restricciones oportunas, así como las especificaciones de almacenamiento de datos y 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 la alta dirección aprueben el diseño de los datos, al igual que el de las aplicaciones.

Una vez diseñada la BD, se procederá a su carga, ya sea migrando datos de un soporte magnético o introduciéndolos manualmente.

Las migraciones o conversiones de sistemas 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 deba a criterios establecidos por la dirección y que se haya aplicado un control estricto de la corrección de errores detectados en esta fase.

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

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; lo ideal es que los datos se validen y corrijan tan cerca del punto de origen como sea posible.

Uso 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 uso.

En esta fase, se debe comprobar que se establecen los procedimientos de uso 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.

Los objetivos de control para la gestión de datos especificados por COBIT son:

- Procedimientos de preparación de datos.
- Procedimientos de autorización de documentos fuente.
- Obtención de datos de documentos fuente.
- Manejo de errores de documentos fuente.
- Retención de documentos fuente.
- Procedimientos de autorización de datos.
- Verificación de exactitud, compleción y autorización.
- Manejo de errores de entrada de datos.
- Integridad del procesamiento de datos.
- Edición y validación del procesamiento de datos.
- Manejo de errores de procesamiento de datos.
- Retención y manejo de salidas.
- Distribución de salidas.
- Reconciliación y balanceo de salidas.
- Manejo de errores y revisión de salidas.
- Medidas de seguridad para informes de salidas.
- Protección de información sensible.
- Gestión de almacenamiento.
- Períodos de retención y términos de almacenamiento.
- Sistema de gestión de biblioteca de medios.
- Responsabilidades de gestión de la biblioteca de medios.
- Copias de respaldo y recuperación.
- Trabajos de copias de respaldo.
- Almacenamiento de respaldo.

El auditor debería llevar a cabo también una auditoría sobre el rendimiento de la BD, comprobando si se lleva a cabo un proceso de ajuste (tuning) y optimización adecuados.

Revisión Post-Implementación

Se debería establecer el desarrollo de un plan para efectuar una revisión post-implementación 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 los previstos.

Otros Procesos Auxiliares

A lo largo de todo el ciclo de vida de la base de datos se deberá controlar la formación que precisan tanto usuarios informáticos (administrador, analistas, programadores, etc.) como no informáticos, ya que la formación es una de las claves para minimizar el riesgo en la implementación de la base de datos.

Esta formación no se puede basar simplemente en cursos sobre el producto que se está instalando, sino que suele ser precisa una formación de base que resulta imprescindible cuando se pasa de trabajar de un entorno de archivos orientado al proceso a un entorno de bases de datos, por lo que supone de un "cambio filosófico"; lo mismo puede decirse si se cambia de tipo de SGBD (por ejemplo de relacional a documental).

Usuarios poco formados constituyen uno de los peligros más importantes de un sistema. Esta formación no debería limitarse al área de las 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 verificar si es suficiente y si se ajusta a los estándares establecidos por la metodología adoptada en la empresa.

Con este fin, resulta muy importante que se haya llevado a cabo un aseguramiento de calidad; lo ideal sería que en la propia empresa existiera un grupo de calidad que se encargara, entre otras cosas, de asegurar la calidad de los diseños de bases de datos.

Auditoría y Control Interno en un Entorno de bases de Datos

Cuando el auditor encuentra el sistema en uso, deberá estudiar el SGBD y su entorno. En el desarrollo y mantenimiento de sistemas informáticos en entornos de BD, deberían considerarse el control, la integridad y la seguridad de los datos compartidos por múltiples usuarios. Esto debe abarcar a todos los componentes del entorno de BD. El gran problema de las bases de datos es que su entorno es cada vez más complejo y no puede limitarse sólo al propio SGBD.

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. Hay también productos muy interesantes que permiten interrelacionar datos de diferentes entornos permitiendo realizar una verdadera "auditoría del dato".

Sistema de Monitorización y Ajuste (Tuning)

Este tipo de sistemas complementan las facilidades ofrecidas por el propio SGBD, ofreciendo mayor información para optimizar el sistema, llegando a ser en determinadas ocasiones verdaderos sistemas expertos que proporcionan 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 puesto que si actúa en un entorno concurrente puede degradarse fácilmente el nivel de servicio que haya podido establecerse con los usuarios.

Auditoría del Sistema Operativo (SO)

El SO es una pieza clave del entorno, puesto que el SGBD se apoyará en los servicios que ofrezca el SO en cuanto a control de memoria, gestión de áreas de almacenamiento intermedio (buffers), manejo de errores, control de confidencialidad, mecanismos de interbloqueo, etc.

Desafortunadamente, el auditor informático tiene serias dificultades para controlar de manera rigurosa la interfaz entre el SGBD y el SO, debido a que constituye información reservada de los fabricantes de los productos, además de requerir conocimientos específicos de las plataformas.

Protocolos y Sistemas Distribuidos

Cada vez más se está accediendo a las bases de datos a través de redes, con lo que el riesgo de violación de la confidencialidad e integridad se acentúa. También las bases de datos distribuidas pueden presentar graves riesgos de seguridad.

Se establecen cinco objetivos de control a la hora de revisar la distribución de datos:

1. El sistema de proceso distribuido debe tener una función de administración de datos centralizada que establezca estándares generales para la distribución de datos a través de las aplicaciones.
2. Deben establecerse funciones de administración de datos y de base de datos fuertes, para que puedan controlar la distribución de los datos.
3. Deben existir pistas de auditoría para todas las actividades realizadas por las aplicaciones contra sus propias bases de datos y otras compartidas.
4. Deben existir controles software para prevenir interferencias de actualización sobre las bases de datos en sistemas distribuidos.
5. Deben realizarse las consideraciones adecuadas de costos y beneficios en el diseño de entornos distribuidos.

Paquete de Seguridad

Existen en el mercado varios productos que permiten la implementación efectiva de una política de seguridad, puesto que centralizan el control de accesos, la definición de privilegios, perfiles de usuario, etc.

Un grave inconveniente de este tipo de software es que a veces no se encuentra bien integrado con el SGBD, pudiendo resultar poco útil su implementación si los usuarios pueden “saltarse” los controles a través del propio SGBD.

Técnicas para el Control de Bases de Datos en un Entorno Complejo

Existen muchos elementos del entorno del SGBD que influyen en la seguridad e integridad de los datos, en los que cada uno se apoya en la operación correcta y predecible de otros.

La dirección de la empresa tiene la responsabilidad fundamental por la coordinación de los distintos elementos y la aplicación consistente de los controles de seguridad. Para llevar a cabo esta labor se deben fijar claramente las responsabilidades sobre los diferentes componentes, utilizar informes de excepción efectivos que permitan monitorear los controles, establecer procedimientos adecuados, implementar una gestión rigurosa de la configuración del sistema, etc.

Cuando el auditor se enfrenta a un entorno de este tipo, puede emplear, entre otras, dos técnicas de control: Matrices de Control y Análisis de los Caminos de Acceso.

Matrices de Control

Estas matrices sirven para identificar los conjuntos de datos del SI junto con los controles de seguridad o integridad implementados sobre los mismos.

Los controles se clasifican en detectivos, preventivos y correctivos.

Análisis de los Caminos de Acceso

Con esta técnica se documentan el flujo, almacenamiento y procesamiento de los datos en todas las fases por las que pasan desde el mismo momento en el que se introducen, identificando los componentes del sistema que atraviesan (tanto hardware como software) y los controles asociados.

Con este marco, el auditor puede identificar las debilidades que exponen los datos a riesgos de integridad, confidencialidad, y disponibilidad, las distintas interfaces entre componentes y la compleción de los controles.