Seguridad y Auditoría Informática

Auditoría de Bases de Datos

Metodologías para la Auditoría de Bases de Datos

Metodología Tradicional

Metodología de Evaluación de Riesgos

Objetivos de Control -> Técnicas
(Preventivas, Detectivas, Correctivas)

- Pruebas de Conformidad
- Pruebas Sustantivas (Impacto)

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

- Estudio Previo y Plan de Trabajo
- Concepción de la Base de Datos y Selección del Motor
- Diseño y Carga
- Uso y Mantenimiento
- Revisión Post-Implementación
- Otros Procesos Auxiliares

Estudio Previo y Plan de Trabajo

- Análisis de Viabilidad sobre alternativas para alcanzar objetivos. Análisis costo-beneficio. Decisiones desde no realizar el proyecto, hasta desarrollar vs comprar.

- La decisión seguir adelante o no con el proyecto recae en la dirección. El auditor debe comprobar que los informes de viabilidad se revisan previamente.

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

- De llevarse a cabo el proyecto, debe establecerse un Plan Director alineado a los procedimientos de la organización.

Estudio Previo y Plan de Trabajo (cont.)

- Aprobación de estructura del proyecto y responsables de gestión y control de la base de datos.

- Objetivos de Control:

  - Responsabilidades para la planificación, organización, plantillas y control de los activos de datos de la organización -> **Administrador de Datos**

  - Responsabilidad de la administración del entorno de la base de datos -> **Administrador de Base de Datos**

  - Posicionamiento en el organigrama lo suficientemente alto para asegurar su independencia

Concepción de la Base de Datos y Selección del Motor

- Se diseña la base de datos con los modelos y las técnicas definidos en la metodología de desarrollo de sistemas de la empresa.

- Esta metodología debería también emplearse para especificar el código fuente, los mecanismos de control, las características de seguridad y las pistas de auditoría a incluir en el sistema.

- 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 fases de diseño lógico y diseño físico.

Concepción de la Base de Datos y Selección del Motor (cont.)

- La definición de la arquitectura de la información, contempla cuatro objetivos de control relativos a:
  - Modelo de arquitectura de información y su actualización
  - Datos y diccionario de datos corporativo
  - Esquema de clasificación de datos en cuanto a seguridad
  - Niveles de seguridad para cada anterior clasificación de datos

- La selección del motor deberá realizarse utilizando un procedimiento riguroso en el que se consideren:
  - Las necesidades de la empresa (debidamente ponderadas).
  - Las prestaciones que ofrecen los distintos SGBD candidatos (puntuados de manera oportuna).

Diseño y Carga

- Se llevarán a cabo los diseños lógico y físico de la base de datos, por lo que el auditor determinará 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.

- Este diseño debe estar aprobado por la dirección del departamento de informática, los usuarios e incluso la alta dirección.

- Una vez diseñada la BD, se procederá a su carga.

- Las migraciones o conversiones de sistemas 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.

Diseño y Carga (cont.)

- 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.

- Para el tratamiento de datos de entrada erróneos, 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

- El sistema se pondrá en marcha, mediante las correspondientes autorizaciones y siguiendo los procedimientos establecidos.

- Se debe comprobar que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas sólo se modifica mediante la autorización adecuada.

- COBIT especifica objetivos de control para la gestión de datos.

- 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 deberá efectuar una revisión post-implementación 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

- Se deberá controlar la formación que precisan tanto usuarios informáticos como no informáticos, ya que la formación es una de las claves para minimizar el riesgo en la implementación de la base de datos.

- 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.

Otros Procesos Auxiliares (cont.)

- 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.

- 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

SGBD y su entorno

- Software de Auditoría
- Sistema de Monitorización y Ajuste (Tuning)
- Auditoría del Sistema Operativo (SO)
- Protocolos y Sistemas Distribuidos
- Paquete de Seguridad

Técnicas para Control de Bases de Datos en Entornos Complejos

- Existen muchos elementos del entorno del SGBD que influyen en la confidencialidad e integridad de los datos, algunos de ellos interdependientes.

- En cuanto a Seguridad, 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.

- El auditor puede emplear dos técnicas de control:
  - Matrices de Control
  - Análisis de los Caminos de Acceso

Matrices de Control

- Sirven para identificar los conjuntos de datos del SI junto con los controles de confidencialidad 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, identificando los componentes del sistema que atraviesan y los controles asociados.

- 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.

Consejos para Auditoría y Evaluación de Bases de Datos

Consejos para Auditoría y Evaluación de Bases de Datos

No Alejarse del Objetivo

Planificar en Consecuencia

Automatizar lo que se pueda

Ir más allá de la Auditoría Tradicional

Informar Métricas Significativas

No Alejarse del Objetivo

- ✓ Hacer que la base de datos sea un componente crítico de cualquier auditoría IT
- ✓ Incluir las bases de datos como parte de auditorías frecuentes de aplicaciones
- ✓ No dejar que la falta de conocimiento de bases de datos sea un problema
- ✓ No dejar que el DBA sea una piedra en el camino

Consejos para Auditoría y Evaluación de Bases de Datos

No Alejarse del Objetivo

Planificar en Consecuencia

Automatizar lo que se pueda

Ir más allá de la Auditoría Tradicional

Informar Métricas Significativas

Planificar en Consecuencia

- ✓ Entender el Alcance
  - ¿Qué tipos de bases de datos, versiones y sistemas operativos?
  - ¿Qué aplicaciones soporta?
  - ¿Cómo fluyen los datos desde y hacia la base de datos?
- ✓ Asociarse con el DBA
  - Hacer que se sientan cómodos con el proceso
  - Asegurarles que los procesos no van a interferir con el rendimiento de la base de datos
- ✓ Asignar los recursos apropiados
  - Controles a auditar - ¿Cuál es nuestra línea de base?
    - CIS Benchmark, Programas de ISACA, ITIL, ¿otros?
  - ¿Lo podemos hacer con personal interno de la empresa?
    - ¿Experto interno?
    - ¿Contratamos a otro experto?
    - ¿Podemos usar una herramienta?

Consejos para Auditoría y Evaluación de Bases de Datos

No Alejarse del Objetivo

Planificar en Consecuencia

Automatizar lo que se pueda

Ir más allá de la Auditoría Tradicional

Informar Métricas Significativas

Automatizar lo que se pueda

- ✓ ¿Solamente entrevistas?
  - Entrevistas basadas en procesos no producirán resultados significativos
- ✓ ¿Corremos Scripts?
  - ¿Tenemos la habilidad de proveer scripts independientes al DBA para que nos de la información correcta para revisar?
  - ¿Tenemos la habilidad de revisar los datos en bruto arrojados por esas consultas?
- ✓ Herramienta
  - Automatizada y la mejor posible

Consejos para Auditoría y Evaluación de Bases de Datos

No Alejarse del Objetivo

Planificar en Consecuencia

Automatizar lo que se pueda

Ir más allá de la Auditoría Tradicional

Informar Métricas Significativas

Ir más allá de la Auditoría Tradicional

- ✓ Generalidades de la Auditoría Tradicional
  - Puede perderse algo crítico
  - Las bases de datos tienen configuraciones complejas y pueden variar

Auditoría	Evaluación de Seguridad
✓ Dirigida por control de procesos ✓ Más general ✓ Conjunto de controles más pequeño a revisar ✓ Se hacen movimientos sólo para cumplir	✓ Más específica a la tecnología ✓ Necesita responder: ¿Estamos seguros? y ¿Cuál es el riesgo? ✓ ¿Cómo afecta esto la Confidencialidad, Integridad y Disponibilidad?

Ir más allá de la Auditoría Tradicional

Auditoría	Evaluación de Seguridad
✓ Necesito examinar si la longitud de la contraseña está establecida en 8 caracteres	✓ Necesito examinar si los intentos de inicio de sesión fallidos son controlados y cada cuantos se bloquea la cuenta ✓ Necesito examinar si la complejidad de contraseña está habilitada ✓ Necesito examinar si la longitud de la contraseña está establecida en 8 caracteres

Consejos para Auditoría y Evaluación de Bases de Datos

No Alejarse del Objetivo

Planificar en Consecuencia

Automatizar lo que se pueda

Ir más allá de la Auditoría Tradicional

Informar Métricas Significativas

Informar Métricas Significativas

- ✓ Resumen Ejecutivo
- ✓ Observaciones
- ✓ Detalles Interesantes

#	Severidad	Área de Prueba (Interna, Externa)	Breve Descripción	Sistemas y Aplicaciones Afectados	Riesgo Técnico	Pasos para Resolver la Vulnerabilidad	Nivel Estimado de Esfuerzo para Resolver la Vulnerabilidad (Alto/Medio/Bajo)
...	...	...	...	...	...	...	...

¿Preguntas?

¡Muchas Gracias!