Metodología para Auditar Bases de Datos fundamentada en Estándares y Buenas Prácticas

Sandra Saucedo Mejía, Luis Alberto Gutiérrez Díaz de León, Alejandro Ayala López, Jorge Lozoya Arandia
Universidad de Guadalajara
Email {sandra.saucedo, luis.gutierrez, aayala, jorge.lozoya}@redudg.udg.mx

Resumen

La auditoría de base de datos permite identificar y corregir vulnerabilidades y problemas en una base de datos. Para llevar a cabo una correcta auditoría es necesario contar con políticas de seguridad efectivas, afinadas y adaptadas a las necesidades propias del ambiente de base de datos de la organización, el presente trabajo propone una metodología para auditoría de base de datos, misma que se fundamenta en estándares internacionales de seguridad y cuyo objetivo principal es aportar una forma de trabajar que permita entender las funciones del administrador de base de datos y concientizar a todos los involucrados en los procesos de trabajo de la organización en el uso responsable de la información, además de ser un referente para aquellas organizaciones que aún no tienen definidos sus procesos de auditoría de base de datos. La metodología consta de 5 etapas las cuales se desarrollaron con base en el modelo de madurez de COBIT, cada etapa contiene puntos de control que deben ser cubiertos y éstos están sustentados en los controles de seguridad del estándar de seguridad ISO/IEC.

Palabras clave

Auditoría de bases de datos, Seguridad en Tecnologías de Información, Estándares de Seguridad de Información.

1. Introducción

Una base de datos es un conjunto de datos almacenados y organizados que pueden ser utilizados con un fin específico, es un hecho que los datos son el activo más importante de una organización, por lo que la respuesta ante las amenazas de seguridad de los datos debe ser proporcionada de forma expedita y eficaz mediante una serie de procesos que permitan identificar y corregir las vulnerabilidades asegurando de esta manera la protección de la información, situación que en la actualidad es una de las más grandes preocupaciones de una organización [1].

El éxito de una organización depende en gran parte de la correcta gestión de la seguridad de su información, el objetivo de dicha gestión es proteger la información y garantizar su correcto uso, por supuesto, la seguridad de los sistemas informáticos y los procedimientos juegan un papel muy importante en la consecución de dicho objetivo [2].

La auditoría es un arma valiosa en la lucha contra las violaciones potenciales de los datos [3]. Aplicar auditorías de forma periódica en una base de datos es una práctica apropiada para identificar actividades sospechosas y supervisar los movimientos que se realizan en ésta por lo que dicha práctica se considera un elemento fundamental del sistema de control interno de una organización y como tal es un medio al servicio de la alta dirección destinado a salvaguardar los recursos, verificar la exactitud y veracidad de la información de las operaciones, estimular la observancia de las políticas previstas y lograr el cumplimiento de las metas y objetivos programados [4].

En la sociedad de hoy en día toda organización competitiva que actúa en un entorno de tecnologías de información (TI) debe establecer en sus procedimientos el uso de estándares de TI y buenas prácticas con el fin de adaptarse a los requisitos individuales de sus clientes potenciales. La creciente adopción de mejores prácticas de TI ha sido impulsada para el establecimiento y cumplimiento de ciertos requisitos en la industria de TI con la finalidad de mejorar la gestión de la calidad y la fiabilidad de la información [5]. La metodología que aquí se propone ambiciona que sea el personal interno a la organización

y específicamente el administrador de base de datos quien conozca y adecúe los procedimientos para abordar cada escenario de la auditoría con la finalidad de concretarla oportuna y exitosamente.

Esta metodología utiliza estándares enfocados a la seguridad ISO/IEC, COBIT e ITIL y basándose en el círculo de Deming permite aplicar a un proceso cualquiera una acción cíclica con el fin de asegurar la mejora continua de dichas actividades [9]. El uso de estándares permite cumplir con los requisitos, especificaciones técnicas y otros criterios precisos que garantizan que los productos y servicios se ajusten a su propósito, haciendo que la vida sea más simple y permitiendo un mayor grado de fiabilidad y efectividad de los bienes y servicios [6],[7],[8].

2. Estructura de la metodología

La metodología se fundamenta en un modelo de 5 etapas tomando como referencia el círculo de Deming y adaptado al prototipo de madurez de COBIT considerando 5 niveles y su correspondiente ponderación. Los objetivos de control de ISO/IEC 27001-27002 se alinean a COBIT e ITIL y se utilizan como referente para definir los procesos propios de la auditoría de base de datos.

3. Desarrollo de la metodología

En la *Figura 1* se muestra el modelo sobre el cual se fundamenta la metodología, en cada etapa se definen las tareas específicas de la auditoría de base de datos acorde a los objetivos de control de ISO/IEC 27001-27002 y COBIT, y al conjunto de directrices de "mejores prácticas" de ITIL.

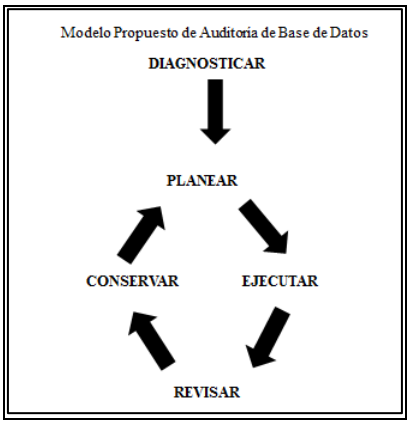

Figura 1. Modelo propuesto de auditoría de base de datos

3.1 Etapa 1 Diagnosticar

El objetivo general de esta etapa es obtener un panorama del estado actual de la organización y para ello se utiliza el modelo de madurez de COBIT mediante el cual una organización puede ubicarse en un determinado grado de madurez de acuerdo a la evaluación de un conjunto de objetivos de control. El modelo considera 5 niveles de madurez que tienen asignado un valor en un rango que oscila entre 0 y 1, esto significa que el nivel más bajo está asociado al valor 0 mientras que el nivel más alto se asocia al valor 1. Los objetivos de control que serán evaluados se dividen en 5 dominios o categorías los cuales se deben de cumplir en su totalidad para llegar al grado de madurez óptimo, en cada nivel se detallan los aspectos a evaluar. En la *Tabla 1* se muestra una descripción de los niveles de madurez y sus valores asignados.

NIVEL NO-EXISTENTE Valoración 0%
La organización opera de manera intuitiva, no cuenta con procesos definidos y documentados, no cumple con ninguna categoría.

NIVEL INICIAL Valoración 25%
Se identifican deficiencias en la operación de los procesos, los empleados no son conscientes de sus responsabilidades lo que conlleva a una desorganización de la entidad.

NIVEL DEFINIDO Valoración 50%
Se conocen las políticas de seguridad e información y los usuarios son conscientes de sus responsabilidades, pero, no existe documentación que avale estos puntos y se desconoce la legislación relativa al manejo de la información.

NIVEL ADMINISTRABLE Y MEDIBLE Valoración 75%
Existe una evaluación formal y documentada sobre la auditoría y riesgos asociados a ésta, pero no todos los problemas se identifican de forma rutinaria lo que significa que al ser medible no cumple en su totalidad con el 100%.

NIVEL OPTIMIZADO Valoración 100%
Este nivel cumple con todas las categorías mencionadas anteriormente, coexiste evaluaciones y monitoreo continuos.

Tabla 1. Modelo de madurez

3.1.1 Método de evaluación

Para generar la información que permita cuantificar el grado de madurez fundamentada en los objetivos de control se utiliza el método de la entrevista, ésta se llevará a cabo por el entrevistador y consiste en reunirse con cada individuo del área de base de datos para realizar una serie de preguntas que tienen como objetivo recabar información en un formulario previamente diseñado para posteriormente extraerla y concentrarla de tal manera que apoyado en la ponderación de las preguntas y las respuestas a éstas se obtenga el nivel de madurez que presenta la organización.

Para organizar las preguntas de la entrevista se definieron 5 categorías o dominios:

- Seguridad
- Responsabilidades
- Controles de la información
- Documentación de procedimientos
- Legislación en materia de uso de la información

Cada categoría contiene una serie de preguntas que van en función del número de objetivos de control referenciados en ISO/IEC 27001-27002. Se consideraron 58 objetivos de control que son los que se adaptan a las actividades específicas de la base de datos. En cada conjunto de preguntas se busca medir que tan de acuerdo o desacuerdo están los entrevistados con los planteamientos indicados y con base en ello se determinará el nivel de cumplimiento de cada categoría. Para cuantificar el nivel de conformidad o grado de acuerdo se utiliza la técnica de Likert [10].

3.1.2 Método de evaluación de preguntas

Para el cálculo del nivel de conformidad asociado a las respuestas de cada una de las preguntas de la entrevista se ha propuesto la ponderación que se muestra en la *Tabla 2*. Para facilitar el procesamiento ágil de las respuestas de la entrevista se determinaron valores de cumplimiento de 0 a 1 con una variación de 0.5 en cada nivel.

Ponderación de la respuesta para la entrevista	
Nivel de acuerdo	Valor de cumplimiento
Totalmente en desacuerdo	0
Parcialmente en desacuerdo	0.5
Totalmente de acuerdo	1

Tabla 2. Ponderación de los niveles de conformidad

3.1.3 Cálculo del grado de madurez por categoría

El procedimiento para el cálculo del grado de madurez se fundamenta en el método de evaluación de respuestas descrito anteriormente y se detalla a continuación haciendo referencia a la *Figura 2*.

Al recabar todas las respuestas de la entrevista se contabiliza el número de éstas obtenido para cada uno de los 3 niveles de conformidad y se anota el dato en la fila denominada "Número de Casillas" dentro del formato de planteamiento de preguntas, la cantidad obtenida se debe multiplicar por el valor de cumplimiento asociado a cada casilla con la finalidad de obtener un puntaje global por nivel de conformidad. Finalmente para alcanzar la evaluación general de la categoría se suman los puntajes globales de los 3 niveles de conformidad y se divide la sumatoria entre el número total de preguntas de la categoría, el resultado obtenido es el nivel de madurez de la categoría evaluada. Este procedimiento se realiza para cada una de las 5 categorías establecidas.

Control de la documentación					
Objetivo de Control	Preguntas	Evidencia	Resultado		
			Totalmente en desacuerdo	Parcialmente en desacuerdo	Totalmente de acuerdo
		Número de casillas			
		Valor asignado a cada casilla	0	0.5	1
		Puntos obtenidos por cada columna (no. Casillas x valor)			
Valor final de la categoría = suma de todas las columnas / número de preguntas que aplican					

Figura 2. Formato de planteamiento de preguntas

Toda vez que se tiene el grado de madurez por cada una de las 5 categorías y el valor asignado a éstas, se calcula el promedio general sumando dichos valores y dividiendo el total entre el número de categorías, el resultado obtenido es el grado de madurez general de la organización.

En la *Figura 3* se muestra el formato a llenar para la determinación del grado de madurez de la organización.

Realizado por:		Fecha:				
		Nivel de madurez				
		1	2	3	4	5
Categoría	Valor asignado	0	0.25	0.5	0.75	1
Seguridad						
Información						
Responsabilidad						
Controles						
Legislación de la información						
Puntos obtenios por cada columna						
Resusltado final = suma de todas las columnas / No. de categorías aplicables						

Figura 3. Formato para la determinación del grado de madurez

Ya determinado el grado de madurez de la organización se puede iniciar con las tareas de la etapa de *Planeación* que es la segunda fase del modelo. A partir de este momento el modelo consiste en una serie de iteraciones que van de la etapa 2 a la etapa 5 hasta que se alcance el grado de madurez óptimo de la organización.

3.2 Etapa 2 Planear

La planeación va en función del nivel de madurez adquirido, una vez que se obtiene el resultado de la ponderación se realiza la proyección considerando los puntos no alcanzados para obtener el grado de madurez óptimo. Para fines de la metodología se desarrollan las 5 categorías y en cada una de ellas se menciona de forma general lo más importante que se debe de cumplir de acuerdo al estándar ISO/IEC 27001-27002. A partir de los resultados obtenidos en la primera etapa del modelo ya se conoce el grado de madurez que tiene la organización en cada una de las 5 categorías establecidas, de manera que la etapa de planeación deberá abarcar solamente las tareas de aquellas categorías que aún no alcanzan el grado de madurez óptimo y están dirigidas a los objetivos de control que aún no se cumplen. De igual manera en cada nueva iteración a esta etapa de planeación el trabajo comprenderá las tareas que de acuerdo con las etapas de *Revisión* y *Conservación* correspondan a objetivos de control no satisfechos. Las tareas de planeación se definen de forma agrupada para cada una de las 5 categorías y se especifican a continuación.

3.2.1 Seguridad

La importancia que tiene la seguridad de la información y el poder que implica manejar información es un tema muy delicado que no está en el conocimiento de muchos, las organizaciones deben demostrar que realizan una gestión competente y efectiva de la seguridad de los recursos y datos que gestionan como es la implementación de políticas de seguridad, acuerdos de confidencialidad internos, acuerdos de confidencialidad con terceros, gestión de privilegios tanto a usuarios internos como externos, concientización del uso de la información y auditorías continuas.

3.2.2 Responsabilidades

Se deben identificar los procesos relacionados con las actividades que desarrollan los integrantes del área de bases de datos y de otras áreas que intervienen directa o indirectamente en el manejo de la información contenida en las bases de datos y los niveles de responsabilidad que conllevan dichas actividades, entre los mismos está la identificación de las áreas involucradas, así como la delimitación de la responsabilidad del personal tanto durante el periodo en el que se encuentra en funciones como al término de su contrato laboral.

3.2.3 Controles de la información

La organización debe definir un proceso para el control de los documentos y registros, la documentación definida debe ser adecuada a la actividad y tamaño del área, a la complejidad de los procesos y a la competencia del personal, el control de los documentos debe permitir una gestión eficaz y eficiente de los procesos. La organización debe contar con un repositorio de archivos en el cual se pueda disponer de los documentos y registros de forma rápida y contar con un sistema de seguridad que evite la posibilidad de fuga, plagio, apropiación del "saber hacer" en la documentación y/o registros del organismo. Se debe mantener esos documentos de forma legible, fácilmente identificables y recuperables.

3.2.4 Documentación de procedimientos

Uno de los principales inconvenientes en las organizaciones es que sus miembros hacen las cosas de diferentes maneras sin seguir una metodología única y uniforme. Cada uno apela a su propio criterio que no siempre es el mejor o a la memoria que no resulta infalible, por este motivo los resultados obtenidos suelen diferir entre pares o áreas similares, por

consiguiente para evitar estas diferencias la práctica más habitual y que mejores resultados ha dado globalmente es la documentación de procedimientos y procesos de cada sector para conformar un Manual de Procedimientos o Manual de Calidad.

3.2.5 Legislación en materia de uso de información

La organización tiene la libertad de calificar como confidencial, cualquier documento o información que a su juicio influya directa o indirectamente en la operación del área: métodos de negocio, documentos contractuales, propiedad intelectual, patentes, desarrollo de nuevos productos, entre otros. Respecto a la protección de la información confidencial dentro de la organización hay que considerar incluir en los contratos laborales de todos los trabajadores que por razón de su puesto y funciones acceden a información, acuerdos de confidencialidad que establezcan claramente las obligaciones de los trabajadores en este sentido.

3.3 Etapa 3 Ejecutar

A partir de los objetivos de control desarrollados en la etapa 2 del modelo, ya se conoce que se debe de cumplir y de esta manera la etapa de ejecución deberá abarcar las tareas de aquellas categorías que aún no alcanzan el grado de madurez óptimo y están dirigidas a los objetivos de control que aún no se cumplen.

3.4 Etapa 4 Revisar

Esta etapa se enfoca a comprobar que se cumplan cada uno de los objetivos de control especificados en la etapa de ejecución, se verifica a detalle que todo se efectué conforme al estándar, identificando de esta manera los puntos que se cumplen y los que no.

3.5 Etapa 5 Conservar

A partir de los objetivos de control que fueron identificados como cumplidos en la etapa 4 del modelo y que se encuentran asentados en la hoja de resultados de avance por etapas, se deben establecer tareas para garantizar que dichos controles se mantengan en el estado en el que se documenta y si éste no es el óptimo se deberá recurrir a las etapas anteriores para cumplir en su totalidad con los objetivos, de ninguna manera retroceder, siempre ver hacia adelante.

4. CONCLUSIONES

Toda organización es responsable de asegurar la protección de su información para garantizar el logro de sus objetivos. El área de administración de bases de datos tiene por objeto asegurar la integridad de la información y su correcta utilización, así como la documentación de los procesos propios del área utilizando lineamientos homogéneos que ayuden a mejorar el desempeño de los miembros de área.

La metodología propuesta para auditar bases de datos sirve como marco de referencia para mejorar las actividades que se desarrollan en el área de administración de base de datos de una organización al tiempo que permite conocer el estado actual de dicha área. Al estar fundamentada en estándares y buenas prácticas la metodología coadyuva a mitigar los riesgos asociados en el manejo de la información, apoya a la segregación de las funciones y asegura el correcto entendimiento de los procesos contribuyendo con ello a una mejor administración de la organización. Para asegurar el éxito en la implementación de la metodología para auditoría de base de datos en una organización no basta con imponerla, también es necesario crear conciencia en los miembros de la organización en lo referente al uso responsable de la información.

Es importante señalar que el objetivo de este trabajo se centró en la descripción de la metodología para auditar bases de datos, dejando para un siguiente trabajo la exposición de los resultados de la implementación de la metodología como parte de un caso de estudio.

5. BIBLIOGRAFIA

[1] S. Sumathi and S. Esakkirajan, "Database security and recovery," in Fundamentals of Relational Database Management SystemsAnonymous Springer Berlin / Heidelberg, 2007, pp. 353-379.

[2] N. Bhatnagar, "Security in Relational Databases," pp. 257-272, 2010.

[3] M. Caffrey, P. Finnigan, R. Geist, A. Gorbachev, T. Gorman, C. Green, C. Hooper, J. Lewis, N. Litchfield, K. Morton, R. Sands, J. Senegačnik, U. Shaft, R. Shamsudeen, J. Wilton, G. Wood and P. Finnigan, "User Security," pp. 467-505, 2010.

[4] WHITTINGTON, Ray O; PANY, Kurt, Principios de Auditoría, Mc. GrawHIll, Décimo Cuarta Edición, 2004.

[5] P. Năstase, F. Năstase and C. Ionescu, "Challenges Generated by the Implementation of the it Standards Cobit 4.1, Itil V3 and Iso/iec 27002 in Enterprises," Economic Computation & Economic Cybernetics Studies & Research, vol. 43, pp. 1-16, 07, 2009.

[6] R. Sheikhpour and N. Modiri, "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management," Indian Journal of Science & Technology, vol. 5, pp. 2170-2176, 02, 2012.

[7] M. Jelliti, M. Sibilla, Y. Jamoussi and H. B. Ghezala, "A Model Based Framework Supporting ITIL Service IT Management," vol. 50, pp. 208-219, 2010.

[8] P. Năstase, F. Năstase and C. Ionescu, "Challenges Generated by the Implementation of the it Standards Cobit 4.1, Itil V3 and Iso/iec 27002 in Enterprises," Economic Computation & Economic Cybernetics Studies & Research, vol. 43, pp. 1-16, 07, 2009.

[9] L. Milgram, A. Spector, and M. Treger, “Chapter 21 - Plan, Do, Check, Act: The Deming or Shewhart Cycle”, Managing Smart, Gulf Professional Publishing, Boston, 1999, pp. 25.

[10] 3 6 2011. [En línea]. Available: http://tesisdeinvestig.blogspot.mx/2011/06/escala-de-likert.html.