DESARROLLO DE UNA METODOLOGÍA PARA EL CONTROL DE RIESGOS PARA AUDITORIA DE BASE DE DATOS

JHON ALEXANDER LOPEZ
ANDRES FABIAN ZULUAGA TAMAYO

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA
2013

DESARROLLO DE UNA METODOLOGÍA PARA EL CONTROL DE RIESGOS PARA AUDITORIA DE BASE DE DATOS

JHON ALEXANDER LOPEZ
ANDRES FABIAN ZULUAGA TAMAYO

Metodología para el Control de Riesgos para la Auditoría de Bases de Datos

Director de Tesis
Omar Iván Trejos Buriticá, PhD.

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA
2013

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

_____

Ciudad y Fecha, (DD / MM / AAAA)

AGRADECIMIENTOS

Principalmente al amado de mi corazón JESUCRISTO MI SEÑOR Y DIOS por la vida que me ha regalado, sin tu ayuda no hubiera podido llegar hasta aquí ya que tú tienes el control de todo y toda sabiduría terrenal proviene de ti puesto que tú eres el sabio por excelencia.

A mi querida madre Martha Lucia López Castrillón porque aunque éramos una familia de escasos recursos siempre se esmeró por llevarme a la escuela y darme estudio inculcando en mí las ganas de salir adelante.

A mi hermosa esposa Alba Ruth Guevara Sabogal, vienes conmigo desde que saque mi grado de bachiller y ahora mi grado universitario. Han sido tiempos difíciles pero siempre has estado a mi lado y eso te será recompensado con creces.

A los motores que me impulsan a salir adelante mis dos preciosos hijos Valentina López Guevara y Juan Sebastián López Guevara. Gracias por apoyar a papa en este tan anhelado título universitario.

A mi compañero de proyecto de grado Andrés Fabián Zuluaga hicimos buen equipo de trabajo y esto se ve reflejado, un fraternal y caluroso abrazo.

Jhon Alexander López

Sin duda alguna te damos gracias a TI SEÑOR DIOS Y JESUS, por permitirnos disfrutar de cada instante, de cada logro, de cada dolor y de toda la felicidad que nos ofreces. Es una meta que me impulsaste a alcanzar, porque nunca me dejaste desistir.

A mi esposa Paula Andrea, por tener la paciencia y la compresión en aquellos instantes donde no podía estar y por brindarme ese apoyo incondicional en todo momento.

A mi hija Danna, porque eres la alegría de mi vida, la fuerza de mi existencia y la ganas de seguir luchando por lo que queremos.

A mi querida hermanita Sandra, porque sin su apoyo este camino hubiera sido muy difícil. Eres mi ejemplo y la inspiración de lograr siempre lo que nos proponemos.

A mis padres y mi hermana Diana, por el cariño y apoyo constante que me han brindado.

A la Universidad, a los compañeros que alcancé a conocer y me brindaron su amistad, al director de grado, un ser con gran conocimiento que nos guio hasta el final y al mi compañero de proyecto, Alexander López "El León", logramos culminar esta etapa con mucho esfuerzo.

Este será el inicio de una vida profesional llena de conocimiento.

.

Andrés Zuluaga

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

La importancia de la Auditoría de Bases de Datos radica especialmente en la necesidad de mitigar los riesgos asociados a la pérdida de datos y a la fuga de la información. Los riesgos hacen que las vulnerabilidades dentro de un sistema de información sean una puerta para que las amenazas sean una fuente de peligro. El presente trabajo de grado se fundamenta en la creación de una metodología diseñada para el control de estos riesgos y basada en las normas internacionales de auditoria y en las mejores prácticas para auditorias de sistemas de información.

Palabra clave: auditoria de sistemas, base de datos, riesgos de BD

ABSTRACT

The Importance of Database Auditing lies especially in the need to mitigate the risks associated with data loss and information leakage. The risks make vulnerabilities within an information system are a door that threats are a source of danger.

The present work is based on grade creating a methodology designed for controlling these risks and based on international auditing standards and best practices for information systems audits.

Keyword: audit of systems, database, BD risks

INTRODUCCION

La auditoría de las bases de datos dentro de un sistema de información es un proceso que permite medir diferentes riesgos y detectar vulnerabilidades y amenazas que pueden afectar los activos de una organización. Para poder determinar qué tan seguro están los datos, es necesario verificar que tan controlados tenemos los riesgos y que hacemos para evitar que se conviertan en amenazas.

Para lo anterior, se pretende desarrollar una metodología que sirva de soporte para que los auditores de sistemas de información especializados en auditorias de bases de datos, logren identificar, analizar y controlar los riesgos que pueden afectar la información de las centrales de datos.

CAPITULO 1

GENERALIDADES

1.2. NOMBRE DEL PROYECTO

Desarrollo de una metodología para el control de riesgos para auditoría de bases de datos.

1.3. OBJETIVOS DEL PROYECTO

1.3.1. Objetivo General

Desarrollar una metodología para control de riesgos para auditoria de bases de datos.

1.3.2. Objetivos Específicos

- Consultar fuentes bibliográficas referentes a la práctica de la Auditoría de los Sistemas de Información y del diseño y análisis de Metodologías para auditorias de sistemas basadas en riesgos.
- Conocer las normas nacionales e internacionales que dan soporte a las auditorías de Sistemas de Información.
- Conocer los riesgos y controles asociados a los diferentes tópicos de sistemas informáticos.
- Identificar algunas de las necesidades más recurrentes de los auditores de sistemas de diferentes organizaciones de la ciudad.

- Analizar e identificar los riesgos más comunes que afectan las bases de datos de los Sistemas de Información.
- Construir el modelo de diseño de la metodología propuesta basado en UML
- Desarrollar la metodología que soluciona el problema planteado

1.4. PLANTEAMIENTO DEL PROBLEMA

La información es uno de los activos más importantes de las organizaciones porque permite realizar las actividades de forma rápida y eficiente, y son fuente principal para que los gerentes y administrativos tomen decisiones correctas que dirijan a la empresa a tener un alto nivel de competitividad y posibilidades de desarrollo. Para muchas empresas, sus negocios se basan exclusivamente en los datos que puedan suministrar de forma veraz y rápida. Para que estos datos sean confiables en el momento de utilizarlos y se conviertan en información para toma de decisiones, se debe asegurar que su procesamiento sea eficiente porque se necesita información útil para que los resultados de las decisiones sean óptimas y eficaz porque se debe lograr que la información que se procese sea verdadera y necesaria para lo que se busca hacer con ella.

A pesar de que exista personal en las áreas de tecnología de las empresas capacitadas para cumplir sus funciones, no podemos obviar la necesidad de realizar controles y seguimientos que aseguren la integridad y seguridad de la información porque de ello depende la veracidad y completitud de los datos. Pero además de eso, se debe asegurar que dichos controles, evaluaciones, análisis y asesorías sean ejecutados de forma idónea y metódica con fin de obtener las conclusiones y recomendaciones más óptimas.

Los auditores de sistemas deben de tener una metodología complementaria a la norma que le sirva como soporte y guía para lograr los objetivos planteados y que le indique el procedimiento paso a paso para hallar y controlar los riesgos que un sistema de bases de datos pueda tener dentro o fuera de una organización.

El problema a resolver es la necesidad de diseñar una metodología de fácil acceso que facilite las labores administrativas del proceso de auditoría de base de datos y que permita analizar, gestionar y controlar los riesgos existentes para atajarlos a tiempo y evitar que aprovechen las vulnerabilidades de los sistemas de información.

1.5. JUSTIFICACIÓN

El desarrollo de una metodología para auditoría de bases de datos facilita que esta se convierta en una guía especializada o herramienta para quienes realizan procesos de auditoría, ya que se deben definir una serie de pasos metódicos que apunten a lo que se quiere concluir y que genere una lista de recomendaciones que mejoren las falencias encontradas.

Además, debe ser una fuente de información que analice las normas internacionales de auditoría presentes en el mercado y que las convierta en técnicas para auditoria de sistemas y gestión de riesgos.

Asociaciones como ISACA (Asociación de auditoría y Control de Sistemas de Información) apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información, lo

que puede generar una oportunidad de creación de empresa que fundamente su misión en el asesoramiento en auditorías de sistemas de bases de datos.

Este trabajo de grado se justifica porque puede convertirse en una fuente de documentación sobre el tema y en una herramienta para verificar la seguridad de la información y la detección de riesgos en la bases de datos de las organizaciones.

1.6. MARCO REFERENCIA

1.6.1. Marco Teórico

1.6.1.1. Tecnologías de bases de datos

Para comprender el proceso de una auditoría de bases de datos, se debe conocer su significado y su funcionamiento en los sistemas de información. Al obtener una visión y conocimiento del entorno informático, el auditor juzgará de manera eficiente, la naturaleza de la problemática y riesgos a los cuales se verá enfrentado al planificar y realizar la auditoría.

1.6.1.2. Definición de Base de Datos

Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular. El término de base de datos fue escuchado por primera vez en 1963 en un simposio celebrado en California, USA.

1.6.1.3. Características de las Bases de Datos

Entre las principales características de las bases de datos podemos mencionar:

- Independencia lógica y física de los datos
- Redundancia mínima
- Acceso concurrente por parte de muchos usuarios
- Integridad de los datos
- Consulta complejas optimizadas
- Seguridad de acceso y auditoría
- Respaldo y recuperación
- Acceso a través de lenguajes de programación estándar

1.6.1.4. Auditoría

La auditoría es el examen organizado de una situación relativa a un producto, proceso u organización, en materia de calidad, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado.

1.6.1.5. Clasificación de las Auditorias

Existen diversas formas de poder clasificar a la auditoría dependiendo del área de especialización. Sin embargo, y de acuerdo al estudio que se está realizando, solo se mencionarán dos tipos.

La primera de ellas es la auditoría de gestión, está orientada a la evaluación de aspectos relacionados con la eficiencia y productividad de los procesos de las

organizaciones. Este tipo de auditorías puede ser desempeñado por auditores internos como externos.

La segunda es la auditoría integral, realizada con el fin de evaluar en su totalidad los objetivos que existen en una organización y que deben de tener relación con el direccionamiento estratégico de esta.

Ambas auditorías deben integrar la auditoría en sistemas de información, ya que objetivo final es similar y los resultados los mismos.

1.6.1.6. Auditoria de Bases de datos

La Auditoría de Bases de Datos es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

- Quien accede a los datos
- Cuando se accedió a los datos
- Desde que tipo de dispositivo o aplicación.
- Desde que ubicación en la red
- Cual fue la sentencia SQL ejecutada
- Cuál fue el efecto del acceso a la base de datos.

1.6.1.7. Importancia de la Auditoria de Base de Datos

La importancia de la Auditoría de Bases de Datos radica especialmente en la necesidad de mitigar los riesgos asociados a la pérdida de datos y a la fuga de la información, pero también debemos considerar su importancia de acuerdo a los siguientes puntos:

- Toda información de la organización reside en bases de datos y deben existir controles relacionado con el acceso a la misma
- Se debe poder demostrar la integridad de la información almacenada en las bases de datos
- La información confidencial es responsabilidad de las organizaciones.

1.6.1.8 Análisis de Riesgos

El análisis de riesgos es la consideración del daño probable que puede causar en el negocio un fallo en la seguridad de la información, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información. A continuación se visualiza el proceso de evaluación de riesgo en una organización y la relación de las diferentes etapas que participan en el análisis.

Fuente: Análisis y gestión de riesgos base fundamental del SGSI.

VIII Jornada Nacional de Seguridad Informática ACIS

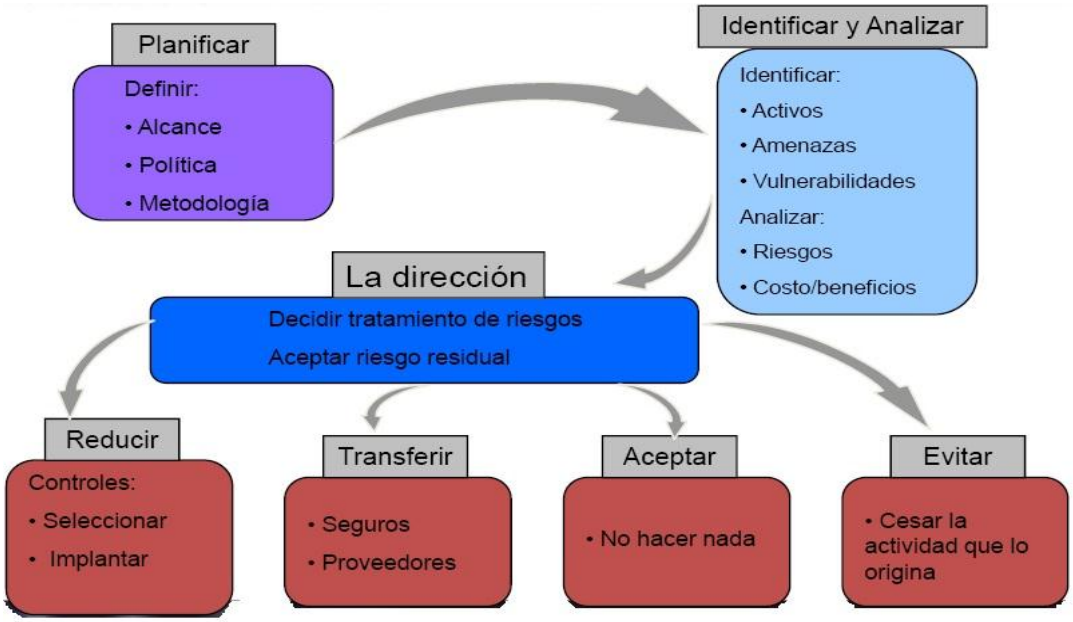
Autor: Juan Carlos Reyes Muñoz, director de Investigación y desarrollo para la firma Seltika, 2008.

Figura 1.Proceso de Evaluación del riesgo

La Figura 1 concluye que el control de riesgos como resultado del análisis de riesgos, es un proceso complejo que parte de la determinación de los activos y las amenazas. Las amenazas son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas de la información. La consecuencia de las amenazas si se materializa, es un incidente que modifica el estado de seguridad de los activos amenazados. Los controles de seguridad que se implementen se seleccionarán teniendo en cuenta las vulnerabilidad, no las amenazas, ya que las primeras son fallas o condiciones que permiten que las segundas afecten un activo de la organización. Al no gestionarse adecuadamente permitirá a las amenazas materializarse y causar daño.

1.6.2. MARCO CONCEPTUAL

- *Integridad de datos*: Estado de corrección y completitud de los datos ingresados en una base de datos.
- *Vulnerabilidad:* debilidad que comprometa la seguridad del sistema de información
- *Agujero de seguridad:* Es una vulnerabilidad de un sistema de información que permite mediante su explotación violar la seguridad del sistema.
- *Amenaza:* Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de un sistema.
- *Evaluación de riesgos:* Proceso en la que se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidad de ocurrencia y además se estima el impacto potencial de una falla de seguridad.



Fuente: Análisis y gestión de riesgos base fundamental del SGSI.

VIII Jornada Nacional de Seguridad Informática ACIS

Autor: Armando Carvajal, Msc en Seguridad Informática UnivOberta de Catalunya - España

Figura 2. Flujo para el análisis y gestión de riesgos.

1.6.3. MARCO LEGAL

1.6.3.1. Ley 1273 de 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

La ley 1273 de 2009 crea nuevos tipos penales relacionados con delitos informáticos y la protección de la información y los datos, con penas y multas significativas.

1.6.3.2. Ley 527 de 1999

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico, y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

1.7. DISEÑO METODOLÓGICO

El desarrollo de este trabajo está compuesto por tres (4) fases: levantamiento de la información, exploración, análisis de riesgos y diseño de la propuesta.

En la primera etapa de este trabajo, definida como fase de Levantamiento de la Información, se pretende realizar el proceso de búsqueda y consulta de toda la información relacionada con el tema propuesto.

Posteriormente, en la fase de exploración se realizarán las entrevistas a personas con experiencia en el tema. Estas entrevistas tienen como objetivo identificar algunas de las necesidades más recurrentes de los auditores de sistemas y dar una visión más clara de cómo funcionan las auditorías dentro de las organizaciones, especialmente aquellas relacionadas con las bases de datos.

Para la fase de Análisis de Riesgos, se crearán esquemas que faciliten la detección de riesgos, su análisis y control.

Por último se planteará una solución para el problema a resolver y se realizan los diferentes diseños que argumentarán dicha solución.

1.7.1. Hipótesis

¿Será posible plantear una metodología para el control de riesgos para bases de datos que facilite las labores administrativas de los auditores y que permita analizar, gestionar y controlar los riesgos existentes evitando vulnerabilidades y amenazas en los sistemas de información de las organizaciones?

1.7.2. Variables

- Identificador login del usuario que accede a la base de datos
- Fecha de acceso a la base de datos
- Identificador físico del equipo desde donde se accede a la base de datos
- Identificador de red desde donde se accede a la base de datos
- Instrucción SQL utilizada para consultar en la base de datos
- Proceso que desencadeno la Instrucción SQL

1.7.3. Instrumentos

El propósito del instrumento de entrevista para la etapa exploratoria descrita en el diseño metodológico, es determinar cómo es el proceso de auditoría de sistemas de información dentro de las organizaciones. Con esto, se obtiene una base del conocimiento que ayudara a fundamentar la solución de la metodología para el control de riesgos para auditoria de bases de datos propuesta en el presente proyecto.

El proceso de la entrevista se desarrollara en tres fases que permitirán conocer: 1. Información del entrevistado y su relación con la organización, 2. Información de

los procesos de auditoria en la organización y 3. Información de las conclusiones e informes presentados a la organización.

- Fase 1:
- ¿Qué cargo desempeña?
- ¿Cuál es el nivel de estudios que representa su cargo?
- ¿Cuál es el nombre del departamento, proceso o área al cual Ud. pertenece dentro de la organización?
- ¿Cuáles son las funciones principales de esta área y su papel dentro de la organización?

- Fase 2:
- Dentro de la organización, ¿A qué personas, procesos, sistemas críticos del negocio o información confidencial, está dirigida la auditoria de sistemas de información?
- ¿Cómo es el proceso de auditoría los sistemas de información que realizan dentro de la organización?
- ¿Qué debe de tener en cuenta para realizar el proceso de auditoria?
- Cuando finaliza el proceso de auditoría, ¿Qué se hace?
- ¿Se realizan auditorías externas para el sistema de información?
- ¿Qué tipo de informes se solicitan cuando se presenta una auditoria externa?
- ¿Cómo se elige quien o que procesos deben ser auditados?
- ¿Usan alguna herramienta que permita la planeación y revisión del proceso de auditoria?

- Fase 3:
- ¿Tiene indicadores que midan el proceso de la auditoria?
- ¿Qué herramientas o procedimientos permiten calcular o generar los indicadores de la auditoria?
- ¿Qué tipos de reportes son los más comunes dentro de la auditoria?
- ¿Considera necesario el conocimiento técnico de un auditor para realizar un proceso de auditora de sistemas de información?

CAPITULO II

ESTADO DEL ARTE

La auditoría de base de datos comprende la medición, seguridad, demostración, monitoreo y registro de los accesos a la información, incluyendo la capacidad de determinar quién, cuando, desde donde y desde que ubicación se accedió a los datos. Su importancia radica en que toda la información de la organización se encuentra almacenada en las bases de datos y deben de existir controles relacionados con el acceso a las mismas y con el hallazgo de riesgos que pueda afectarlos.

A continuación se revisan los resultados del rastreo del Estado de Arte para tener un panorama de los proyectos, artículos, tesis y libros que se encuentran en el mundo de las auditorias de los sistemas de información especialmente aquellas auditorias relacionadas con bases de datos.

2.1 PONENCIA ANALISIS Y GESTION DE RIESGOS, BASE FUNDAMENTAL DEL SGSI. METODOLOGIA MARGERIT

Autores e Institución. La ponencia *Análisis y gestión de riesgos, base fundamental del SGSI Caso Metodología Margerit* fue expuesta por el Msc en seguridad informática de la Universidad Oberta de Catalunya – España, especialista en construcción de software para redes de Uniandes – Colombia e Ingeniero de Sistemas de la Universidad Incca de Colombia, Armando Carvajal, en la VIII Jornada Nacional de Seguridad Informática ACIS realizado en Junio de 2008 en Colombia.

Resumen. En la documentación que argumenta la ponencia, se detalla una metodología exitosa muy probada creada por el Consejo Superior de Informática de España sobre el Análisis y Gestión de Riesgos de los Sistemas de Información denominada Margerit (Metodología de Análisis de Riesgos de los Sistemas de Información). El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos. Además, concientiza a los responsables de los sistemas de información de la existencia de los riesgos y de la necesidad de atajarlos a tiempo. “La medición es el primer paso para el control y la mejora. Si algo no se puede medir, no se puede entender. Si no se entiende, no se puede controlar. Si no se controla, no se puede mejorar” (H. James Harrington).

Contribución al proyecto. La metodología Margerit es una fuente importante para el proyecto en desarrollo debido a que presenta un método sistemático para analizar riesgos que pueden convertirse en base fundamental para apoyar la metodología propuesta pero enfocada a bases de datos. Además, permitirá descubrir y planificar las medidas oportunas para mantener los riesgos bajo control

2.2 PROYECTO DE GRADO *SISTEMAS DE AUDITORIAS PARA BASES DE DATOS DE ORACLE - SABDO*

Autores e Institución. El proyecto de grado *Sistema de Auditoria para Base de Datos – SABDO* fue elaborado por los estudiantes de la Facultad de Ingeniería en Ciencias Aplicadas Ondyna Lilian Fierro Montenegro y Juan Carlos García Pinchao para la obtención del título de Ingeniero en Sistemas Computacionales. La tesis se presentó en el año 2009 a la Escuela de Ingeniería en Sistemas Computacionales de Ibarra, Ecuador.

Resumen. Las nuevas tecnologías y sistemas cada vez más complejos requieren interfaces gráficas y amigables al usuario. Una base de datos maneja gran cantidad de datos desempeño y competitividad. La auditoría de la base de datos permite aumentar el nivel de seguridad, dando a conocer irregularidades en su manejo. El sistema de Auditoría de Base de Datos Oracle – SABDO, es una interfaz gráfica amigable, fácil de configurar para cubrir los requerimientos, de información de auditoría, del usuario. Permite realizar el rastreo de intrusos, cambios no autorizados en los datos y objetos de la base de datos, visualizando su ubicación, nombre de usuario, fecha, hora, etc. SABDO ha sido integrado al sistema académico de la Universidad Técnica del Norte con el objetivo de colaborar en la tarea de mantener la seguridad de la información contenida en su base de datos.

Contribución al proyecto. El funcionamiento de SABDO puede ser útil como herramienta dentro de la metodología que se utilizará para el control de riesgos para auditoria de bases de datos, ya que básicamente está registrando las mismas variables que se usarán y está apuntando al mismo propósito que es la seguridad de los datos. Sin embargo, la herramienta se enfoca en obtener resultados rápidos acerca de los accesos y modificaciones realizadas por los usuarios y olvida el análisis y control de riesgos de la bases de datos y de su relación con el sistema de información de la organización.

2.3 TRABAJO DE GRADO SISTEMA PARA LA GESTION DE AUDITORIAS EN BASES DE DATOS

Autores e Institución. El trabajo de grado *Sistema para la gestión de auditorías de bases de datos* fue elaborado por el estudiante del programa de Ingeniería Informática de la Escuela de Ingeniería de Antioquia, Lucas Vallejo Uribe para la obtención del título de Ingeniero Informático. El trabajo de grado se presentó en el año 2008en la ciudad de Envigado, Antioquia (Colombia).

Resumen. Para el proceso de auditorías de las T.I, se requieren conocimientos tanto técnicos como administrativos, donde los procesos técnicos requieren un alto conocimiento de las herramientas sobre los que son implementados.Este trabajo pretende resolver el caso particular de las herramientas del motor de base de datos Oracle 10g, donde a través de un sistema de información, se podrán implementar los diferentes métodos anteriormente mencionados, de manera que la ejecución de las auditorias de carácter técnico no sean una dificultad para los auditores que no conocen dichas herramientas.Basados en el análisis de varios expertos en el tema, las buenas prácticas de COBIT y el apoyo de la ingeniería de software, se presentan una serie de definiciones generales y los diferentes modelos que permiten la construcción de este sistema de información y adicionalmente se detallan las implementaciones utilizadas para las herramientas de Oracle Database 10g.

Contribución al proyecto. Este trabajo de grado se basa en una agrupación de buenas prácticas definidas sobre un conjunto de dominios y procesos enfocados directamente sobre el control de la organización a nivel de tecnologías de

información. Esto le permite al proyecto en desarrollo, crear pautas relevantes en el momento de realizar una auditoría de sistemas y resaltar el método más valioso para lograr los objetivos propuestos.

2.4 ARTICULO LAS DIEZ VULNERABILIDADES MÁS COMUNES DE LAS BASES DE DATOS

Autores e Institución. El artículo "*Las diez (10) vulnerabilidades más comunes de las bases de datos"*de la página web www.e-securing.com es escrito por Mauro Maulini R en el año 2011 e investigado por Alex Rothacker, gerente de AppSec'sTeam SHATTER

Resumen. Las organizaciones deben evaluar continuamente los paquetes de su software de base de datos para determinar si son realmente necesarios y desactivar los que no son necesarios para reducir las superficies de ataque. Tienen que ser cuidadosos en controlar los campos en las búsquedas para prevenir inyeccionesy tener conciencia de la debilidad en las credenciales de inicio de sesión. Y lo más importante, es necesario aplicar los parches de actualización de la casa matriz con regularidad. Alrededor de la mitad de las vulnerabilidades nombradas por Rothacker y su equipo están directa o indirectamente relacionadas con las prácticas flojas de gestión de parches en el entorno de base de datos.

Contribución al proyecto. Este articulo define un panorama claro de los riesgos que se deben tener en cuenta en el momento del desarrollo de la metodología planteada, y másaún, permite darle claridad al auditor de bases de datos que es

lo que se debe de tener en cuenta en el momento de hallar los riesgo y que se hace para su control y estabilización.

2.5 TRABAJO DE INVESTIGACION ENFOQUE METODOLOGICO DE LA AUDITORIA A LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

Autores e Institución. El trabajo de investigación *Enfoque metodológico de la auditoria a las tecnologías de información y comunicación* fue elaborado por los investigadores Carlos Yañez de la Melena y Sigfrid Enrique IbsenMuñozpara la participación al XIV Concurso Anual de Investigación “Auditoria de Gestión a las Tecnologías de Información y Comunicación” donde se participó con la Contraloría General de la República de Chile. El trabajo de investigación se presentó en Octubre de 2011.

Resumen. El proyecto “Enfoque metodológico de auditoría a las tecnologías de información y comunicación sobre la base del estándar COBIT 4.1 y la norma ISO/IEC 27002:2005”, tiene como objetivo entregar un marco referencial para desarrollar auditorías orientadas a los procesos del negocio, los sistemas de información y sus actividades de control. El Proyecto está estructurado en cinco capítulos: el 1re Capitulo presenta los antecedentes generales, los antecedentes de la organización y el objetivo general y específicos del proyecto, el 2do Capitulo se analizan los elementos de la auditoría a las tecnologías de información a través de sus aspectos generales y del análisis de las tecnologías de información y comunicaciones, el 3er Capitulo se presenta el estándar COBIT y la norma ISO/IEC 27002, el 4to Capitulo se aborda el enfoque metodológico

explicando los objetivos metodológicos, etapas, actividades y productos y Finalmente, en el 5to Capítulo se exponen las conclusiones del proyecto.

Contribución al proyecto. Se puede resaltar de este trabajo de investigación la propuesta que se hace para mejorar las auditorías a las tecnologías de información y las comunicaciones y la utilización de las normas ISO/IEC 27002:2005 y el estándar COBIT 4.1. El diseño de este contexto investigativo determina las pautas que se pueden utilizar para implementar parte de la metodología que se va a utilizar en la auditoria de bases de datos. Sin duda alguna, en este documento se observa la rigidez de la ejecución de auditorías en los sectores públicos y el compromiso de los mejores resultados al concluir el proceso.

2.6 PONENCIA ADMINISTRACION Y AUDITORIA DE LAS BASES DE DATOS

Autores e Instituciones. La ponencia *Administración y Auditorias para las Bases de Datos* fuepresentadapor el Ingeniero Héctor Pedro Libaratoriante las Jornadas Informáticas del Centro de Ingenieros Jujuy en Argentina en el año 2011.

Resumen. Las características de auditoría de la Base de Datos son muy poderosas y a menudo parecen muy complejas. Existe más de una opción disponible para auditar una base de datos. Es posible auditar casi todo con las características estándar, aunque no a nivel de fila. Si se necesita una auditoría de alto nivel, se utilizan los triggers de la base de datos y la auditoría de granularidad fina. Se debe tener presente que ambos métodos necesitan habilidades de programación para la puesta en ejecución y presentación de informes.

Contribución al proyecto. Esta ponencia proporcionara de forma muy específica los aspectos principales que se deben de tener en cuenta para la auditoria de bases de datos. Además, brinda información valiosa que se puede utilizar en el momento que se desarrolle la metodología propuesta, como lo son la *Auditoria de Privilegios* donde el objeto auditado es la realización de las acciones correspondientes a determinados privilegios del sistema, la *Auditoria de Objetos de Esquema* que es muy similar a la anterior, la *Auditoria de Granularidad Fina (FGA)* donde los mecanismos están más focalizados y precisos sobre los objetos a auditar y la *Auditoria con Triggers*donde se puede utilizarse para completar la integridad referencial, imponer reglas del negocio o para auditar cambios en los datos.

2.7 PONENCIA RETOS EN LA SEGURIDAD DE LAS BASES DE DATOS

Autores e Instituciones. La ponencia *Retos en la Seguridad de las Bases de Datos* fue presentada por Fred Pinto PhD, en la X Jornada de Seguridad Informática ACIS realizada en Junio de 2010 en Colombia

Resumen. La ponencia *Retos en la Seguridad de las Bases deDatos* enfatiza en los siguientes aspectos: trazabilidad en las acciones en Bases de Datos, blindaje de la Base de Datos, desarrollo y gestión de controles dentro del marco de alguna metodología, utilización de la auditoria como base para la implementación de controles, gestión de trazas de auditoría con herramientas que apoyen la implementación de controles.

Contribución al proyecto. La contribución más significativa de esta ponencia es la implementación de COSO (Committee of SponsoringOrganizations Of TheTreadwayCommission) como marco para la gestión de controles a las base de datos. Este tipo de orientación ofrece conceptos claves como procedimientos para control interno, cumplimiento de leyes y regulaciones y alineación de los controles con los objetivos estratégicos de la organización, que pueden complementar la metodología propuesta. Además, es importante incluir el contenido relacionado con los requerimientos de auditoría, lo que permite dar una orientación para especificar más profundamente la forma como se debe auditar las bases de datos.

2.8 TESIS AUDITORIA DE BASES DE DATOS

Autores e Institución. La Tesis de Licenciatura *Auditoria de Bases de Datos* fue elaborada por los estudiantes de la Facultad de Ingeniería de la Universidad Nacional de la Patagonia San Juan Bosco de Argentina, Hector Gabriel Ingravallo y Valeria Elizabeth Entraigas en el año 2007.

> Resumen. La Auditoria de Bases de Datos es una temática relativamente nueva si consideramos que las Bases de Datos y los motores que las manejan se han popularizado en estos últimos 15 años, no obstante la necesidad del control y registración del cambio de datos es un hecho que muchos profesionales siempre pensaron en poner en práctica. Este trabajo presenta una introducción teórica a la Auditoria Informática como marco general describiendo los diferentes conceptos de los objetos que la integran tanto como sus componentes y el marco legal argentino en el que se haya inmerso. Y como resultado práctico final se ofrece una herramienta que permite en forma sencilla, intuitiva y sobre todo centralizada mantener una registración sobre el cambio de los datos y su posterior análisis. Tal

herramienta tiene la capacidad de interactuar con cualquier DBMS y Base de Datos desarrollada siempre que esté previamente configurada.

Contribución al proyecto. La presente tesis hace un aporte significativo por la importancia de poder conocer el funcionamiento y desarrollo de una herramienta informática capaz de interactuar con diferentes gestores de bases de datos, y a la vez, permitir y definir qué datos se deben auditar, permitiendo explotar la información de trazas de actividad de manera fácil y segura. Además, esta herramienta muestra una opción en el momento de administrar datos ubicados en diferentes bases de datos que puede servir como una propuesta dentro de la metodología planteada en el presente proyecto. Esta opción consiste en el manejo de logs en el momento en que se registre actividad de los usuarios, modificaciones de los datos hechos por los usuarios y análisis centralizado y global de los cambios realizados por los usuarios a los datos. Se puede resaltar también como contribución al proyecto, el análisis y amplio estudio que se realiza del tema de la Auditoria como punto focal y función relevante en el desarrollo de las organizaciones, lo que permite tener un amplio margen y conocimiento para poder estructurar el planteamiento de la metodología para control de riesgos para auditorias de bases de datos.

2.9 TRABAJO DE INVESTIGACION “AUDITORIA DE GESTION A LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES”

Autores e Institución. El trabajo de investigación *Auditoria de Gestión a las Tecnologías de la Información y Comunicaciones* fue elaborado por Alberto Reyes Lazo y Francisco Antonio Villacorta Moran como participación de la Corte de

Cuentas de la Republica de El Salvador al XIV CONCURSO ANUAL DE INVESTIGACION DE LA OLACEFS en Octubre de 2011.

Resumen. Debido al acelerado incremento y desarrollo de las tecnologías de información y comunicaciones (TIC), se han experimentado cambios trascendentales en la evolución de la forma de vida de la sociedad actual, y por consiguiente en la forma en que los gobiernos administran las naciones, de esta manera las entidades gubernamentales hacen uso de las tecnologías de información y comunicaciones para el desarrollo de sus procesos y la prestación de servicios a la los ciudadanos. Así mismo, este crecimiento de las tecnologías no solo nos enfrenta a un mundo nuevo de procesos automatizados, y servicios más eficientes y efectivos basados en TIC, sino también a la aparición de nuevas formas de "Corrupción"; por lo tanto, se vuelve imprescindible controlar y fiscalizar de manera especializada la administración de los recursos tecnológicos, razón por la cual, las Entidades Fiscalizadoras Superiores (EFS) deben estar preparadas para los desafíos que implica fiscalizar dichas tecnologías.

Considerando el planteamiento anterior, se realizó esta investigación en cumplimiento con las especificaciones señaladas en las Bases del XIV Concurso Anual de Investigación promovido por la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores OLACEFS, estableciendo como tema "Auditoría de Gestión a Las Tecnologías de Información y Comunicaciones".

Por lo anterior se desarrolló una propuesta de solución para realizar la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, basada en estándares de aceptación mundial, y que sea adaptable a la realidad Tecnológica de cada país de Latinoamérica y del caribe, a través de las Entidades Fiscalizadoras Superiores (EFS), así mismo que se constituya en un instrumento para unificar criterios en materia de la

administración y fiscalización tecnológica de las entidades públicas, que permita identificar los riesgos en el proceso de la auditoria a la gestión TIC, para determinar constantemente el nuevo rumbo a seguir de las EFS, con el objetivo de que la capacidad de controlar y fiscalizar se mantenga al mismo ritmo en que avanzan las Tecnologías de información y comunicaciones. La propuesta de solución presentada en el Capítulo III de este documento, establece ocho componentes integrados, que dependen uno del otro para funcionar, los cuales interactúan entre sí con el objetivo de crear una estructura estandarizada, ordenada, sólida, dinámica y actualizable en el tiempo, la cual se llamará “Torre TIC de la Auditoria”. El primer componente “Unidad Especializada de Auditoria TIC“, se plantea la necesidad de crear un área/unidad especializada de auditoria TIC, como instancia para la planificación, desarrollo, monitoreo, coordinación, y en general la ejecución de la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones. El Segundo Componente “Base de Datos TIC de las entidades Fiscalizadas”, plantea el desarrollo de una base de datos con información de las plataformas tecnológicas de cada entidad sujeta a fiscalización, esto con el fin de que la EFS cuente con información que sirva para la toma de decisiones en la ejecución de la Auditoria a la Gestión TIC. El Tercer componente “Perfil del auditor TIC” define las capacidades, conocimientos y habilidades que un Auditor de TIC debe poseer, para el ejercicio de la Auditoria.El Cuarto componente “Desarrollo del conocimiento TIC” determina la necesidad de desarrollar el talento humano de nuestro equipo de auditoria, bajo un esquema de “capacitación continua”, basada en la especialización, con el fin de cubrir todas las áreas del conocimiento identificadas en el perfil del auditor TIC. El quinto componente “Estándares internacionales para la auditoría de gestión TIC” exhorta a utilizar las mejores prácticas relacionadas las TIC, específicamente COBIT, ITIL, ISO 27002, para posibilitar un gobierno eficaz de las actividades de control y ordenamiento de la gestión TIC. El Sexto

componente “Normativa TIC de las EFS” propone crear la normativa que establezca los criterios básicos de control que deben observarse en la gestión TIC, las cuales se han convertido en un instrumento esencial en la prestación de los servicios y representan rubros importantes en los presupuestos del Sector Público, estos basados en estándares de aceptación mundial en materia TIC y que sea tropicalizada a la realidad tecnológica de cada Nación. El Séptimo componente “Metodología de auditoría de gestión TIC”, plantea el proceso de la práctica de la auditoría de a la Gestión TIC. El octavo componte “Los N Vectores de la Auditoria de Gestión TIC”, determinan la dirección y sentido de la auditoria de gestión TIC, en la cual definimos los diferentes enfoques o áreas de importancia sobre las cuales se ejecutara la auditoria a las TIC. Al final del documento se presenta la bibliografía consultada y los anexos que se consideraron precisos para fortalecer el contenido de la investigación.

Contribución al proyecto. El presente trabajo investigativo relacionado con la *Auditoria de Gestión a las Tecnologías de la Información y Comunicaciones* es una contribución técnica al proyecto porque permite conocer las auditorías a Sistemas de Información basadas en estándares de aceptación mundial y adaptables a la realidad tecnológica de los países de Latinoamérica y del Caribe. Además, permite que se conozca el panorama de las auditorias de S.I en los países mencionados, lo que guía a la propuesta del presente proyecto a ser más aterrizada y enfática a las necesidades reales del mercado. Finalmente, este trabajo plantea una propuesta que denomina “Torre TIC de la Auditoria”, donde especifica 8 componentes que la integran. Dentro de estos componentes, existe uno específico que contiene un aporte significativo al proyecto, *Metodología de Auditoria de Gestión TIC*, donde se presentan una serie de etapas que pueden significar aportes o complementos a la propuesta planteada.

2.10 TRABAJO DE INVESTIGACION “MANUAL DE AUDITORIA DE GESTION A LAS TECNOLOGIAS DE INFORMACIONES”

Autores e Institución. El trabajo de investigación *Manual de Auditorias de Gestión a las Tecnologías de Información* fue elaborado por José Salvador Monterrosa y Carlos Eduardo Iglesias como participación de la Corte de Cuentas de la Republica de El Salvador al XIV CONCURSO ANUAL DE INVESTIGACION DE LA OLACEFS en Octubre de 2011.

Resumen. El presente manual de auditoría de gestión a las tecnologías de información y comunicaciones describe procedimientos que los auditores deben utilizar para verificar el uso de los recursos tecnológicos, confidencialidad, confiabilidad, integridad, disponibilidad de la información procesada por los sistemas de información automatizados y apoyo en la automatización de los procesos operativos y administrativos de la entidad para llegar a medir los indicadores de gestión de eficiencia, efectividad y economía de las tecnologías de información y comunicaciones implementadas por la institución y presentar conclusiones y recomendaciones oportunas y acertadas que sirvan de guía para corregir las deficiencias que pueden llegar a existir y lograr mejorarlas. El Capítulo I, describe las generalidades de lainvestigacion. En el Capítulo II Desarrollo de la investigación, se describen los objetivos del manual, el diseño, preparación y conservación de papeles de trabajo y la naturaleza de la documentación de auditoría en formato electrónico en cada ente fiscalizador, además de los procedimientos que deben desarrollar los auditores en la fase de planificación de auditoría y de los estándares internacionales que intervienen en el proceso de una auditoría de gestión a

las tecnologías de información y comunicaciones. El Capítulo III de la Planificación, describe el desarrollo de una auditoría de gestión a las TIC´s, en la fase de planificación, obteniéndose un entendimiento y comprensión de los aspectos siguientes: entorno de la entidad y del Área de Tecnología de Información, procesos sistematizados, administración de riesgos, evaluación de indicadores de gestión, control interno y organización del área de tecnología de información y comunicaciones, pues dicho conocimiento le brinda un marco conceptual, que le permite evaluar si la organización sigue un enfoque estructurado de gestión informática y si el mismo es adecuado, además el seguimiento a recomendaciones de auditorías anteriores, la elaboración de un plan de trabajo de auditoría y de la ejecución de guía de procedimientos de análisis previo y la elaboración del informe ejecutivo de análisis previo que contendrá los asuntos de importancia identificados y agrupados por proyectos de las áreas vulnerables o de impacto determinados. En el Capítulo IV de la Ejecución, se describen las pruebas asistidas por computadora que se pueden aplicar para investigación y la obtención de evidencia de las causas que originan una debilidad en gestión tecnológica, la evaluación y recolección de evidencia suficiente y apropiada que permitan emitir las conclusiones acerca de la operatividad de la gestión en tecnología de información y comunicaciones. El Capítulo V de Informe, describe la estructura que debe de contener un informe de resultados preliminares, la carta de gerencia, que dará a conocer a la administración todos aquellos asuntos de menor importancia, estos asuntos de menor importancia son riesgos que pueden ser administrados y que a juicio del auditor no son de impacto en la gestión de las tecnologías de la información y comunicaciones, al haber garantizado el derecho de defensa a la administración, analizado las respuestas y comentarios, se emite el informe de auditoría que sustenta las conclusiones del auditor sobre el uso de las tecnologías de información y

comunicaciones y medición de los indicadores de gestión de eficiencia, eficacia y economía de la entidad pública.

Contribución al proyecto. *El Manual de Auditoria de Gestión a las Tecnologías de Información* es un aporte importante al proyecto en desarrollo, ya que permite visualizar las diferentes etapas del proceso de auditoría en las tecnologías de información. Estos datos posibilitan que la metodología propuesta tenga bases sólidas y fundamentadas para poder aplicarse a la realidad. Además, es una guía que se debe de tener en cuenta en el momento de argumentar la propuesta y sin duda alguna, permitirá que los autores tengan conocimiento de los procedimientos empleados para realizar y ejecutar esta disciplina.

2.11 TESINA AUDITORIA A LA BASE DE DATOS SQL DEL SISTEMA "SEGURIDAD DE PRESAS" CONAGUA

Autores. La Tesina *Auditoria a la Base de Datos SQL del Sistema "Seguridad de Presas" CONAGUA* fue elaborada por los estudiantes EfrenRamirez Aguilar, Irais Elena Torres Flores, Judith Oralia Yañez Morales y Yazmin Mosqueda Jaramillo del Instituto Politécnico Nacional de México D.F en Agosto de 2010. Este trabajo se presentó como prueba escrita del Examen profesional para obtener el título de Licenciado en Ciencias de la Informática después de haber realizado el seminario "Auditoria de las Tecnologías de la Información y Comunicaciones".

Resumen. En la presente tesina se aplica la auditoria informática a la Base de Datos SQL del "Sistema de Seguridad de Presas" de la CONAGUA basado en la metodología COBIT, con el fin de dictaminar una

recomendación para que dicho sistema siga las mejores prácticas orientadas en la metodología antes mencionada.

Contribución al proyecto. Se puede decir que el aporte primordial de la presente Tesina es el planteamiento de una Metodología de Análisis de Riesgos que se enfoca en identificar las amenazas, vulnerabilidades, riesgos e impacto que se encuentran en los sistemas. Además, se explica detalladamente la metodología COBIT como procedimiento para Auditoria de Sistemas de Información, cuyo planteamiento se base es cuatro dominios específicos: planear y organizar, adquirir e implementar, entregar y dar soporte y monitorear y evaluar. Estas metodologías permiten que se forme un marco de trabajo para el desarrollo de la propuesta planteada en el presente proyecto.

2.12 TESIS UNA METODOLOGIA PARA AUDITAR TECNOLOGIAS DE INFORMACION

Autores. La Tesis *Una Metodología para Auditar Tecnologías de Información* fue elaborada por los estudiantes de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, David Plata Sánchez y Eduardo Hilario Ponce Casanova, como requisito para obtener en Título de Ingeniero en Computación. La Tesis se realizó bajo la dirección del Ing. Heriberto Olguín Romo en Septiembre de 2009.

Resumen. El objeto fundamental del presente trabajo de tesis es la elaboración de material de apoyo para auditar algunas Tecnologías de Información (TI), proporcionando al auditor herramientas para realizarlas,

mediante una serie de preguntas y actividades, con su correspondiente guía y/o sugerencias; así también, para cada una de ellas se sugieren una o varias recomendaciones, mismas que si se toman en cuenta mejorarán las políticas, normas y procedimientos de elaboración, implantación, operación y administración de los sistemas de información de empresas e instituciones, tanto públicas como privadas. La información mostrada es la recopilación de una serie de investigaciones a TI específicas, las cuales se obtuvieron de consultas principalmente a libros y páginas de Internet relacionadas con los temas. El trabajo realizado presenta para cada capítulo de Tecnología de Información, herramientas de apoyo para el auditor y recomendaciones. En forma general podemos decir que en el capítulo I se aborda la descripción de lo que es una Auditoría, así como una definición y objetivos de la realización de la misma. En el Capítulo II se describe brevemente que es una Tecnología de Información, tipos de Tecnologías de Información y como uno de los puntos centrales las Auditorías a Tecnologías de Información. En el Capítulo III se presenta la información acerca de un Programa Informático Colaborativo. En el Capítulo IV se ofrece la investigación realizada de un Sistemas Basados en el Conocimiento (KNOWLEDGE BASED SYSTEMS, KBS), en la cual la TI se utiliza para “generar” nuevo conocimiento a través de las herramientas que ésta conlleva, utilizando los diferentes métodos relacionados. El Capítulo V describe una de las tecnologías más utilizadas actualmente, Sistemas para el Soporte de Decisiones (DECISION SUPPORT SYSTEMS, DSS), es una Tecnología para empresas cuyo objetivo sea tener y mantener una ventaja competitiva. En el Capítulo VI se muestra la Tecnología de Información llamada Administración de la Cadena de Suministro (SUPPLY CHAIN MANAGEMENT, SCM), la cual administra procesos de intercambio, flujo de materiales y de información, que se establecen dentro de cada organización o empresa. En el Capítulo VII nos da un pequeño panorama acerca de la Planificación de Recursos

Empresariales (ENTERPRISE RESOURSE PLANNING, ERP), que son aplicaciones de gestiones de información, modulares y adaptables, que permiten integrar y automatizar las prácticas de negocio relacionadas con los aspectos operativos o productivos de una empresa. En el Capítulo VIII se otorga la descripción de la Administración de la Relación con los Clientes (CUSTOMER RELATIONSHIP MANAGEMENT, CRM), que es una estrategia que permite a las empresas identificar, atraer y retener a sus clientes. Por último en el Capítulo IX se presenta una descripción a los Sistemas de Flujo de Trabajo (WORKFLOW SYSTEMS, WS), en la que se lleva una secuencia lógica de actividades, que se ejecutan en forma síncrona o asíncrona. Actualmente existen muchas y variadas Tecnologías de Información, para las cuales se realizan auditorías, ya que contienen elementos de análisis, de verificación y de exposición de recomendaciones (debilidades y disfunciones), por lo cual se crea esta herramienta, que contiene los conceptos básicos sobre la tecnología por auditar, además de que el auditor puede disponer de material de apoyo para su proceso. El objetivo principal será entonces que este proyecto sea una referencia para el profesional de la auditoría a tecnologías de información, puesto que permitirá mayor eficiencia en su trabajo y contará con una base de conocimiento que pueda retroalimentar a los auditores y apoyar sus funciones; así como, mayor comunicación e integración en los equipos de trabajo.

Contribución al Proyecto. El aporte que realiza la tesis *Una Metodología para Auditar Tecnologías de Información* es el material de apoyo relacionado con las tecnologías de información y las metodologías y procedimientos de Auditoria que pueden convertirse en guía para el desarrollo de la propuesta planteada. Es importante resaltar que las experiencias de auditoria a tecnologías relacionadas en la tesis, son antecedentes importantes que se deben de estudiar más

detalladamente para poder extraer aportes que puedan ser importantes en la metodología a desarrollar.

CAPITULO III
TEORIA

3.1 METODOLOGIA DE CONTROL INTERNO

3.1.1 Introducción a las Metodologías

Según el *Diccionario de la Lengua de la Real Academia Española,* METODOes el "modo de decir o hacer con orden una cosa. Asimismo define el diccionario la palabra METODOLOGIA como "conjunto de métodos que se siguen en una investigación científica o una exposición de doctrina". Esto significa que cualquier proceso científico debe de estar sujeto a una disciplina de proceso definida con anterioridad que se llamara METODOLOGIA.

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la compone, desde su diseño de ingeniería hasta el desarrollo de software, al igual, que la auditoria de los sistemas de información.

Una metodología es necesaria para que un grupo de profesionales logren un resultado homogéneo como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras profesionales, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

La proliferación de metodologías en el mundo de la auditoria y el control informático se puede observar en los primeros años de la década de los ochenta, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas. Pero el uso de métodos de auditoria es casi paralelo al nacimiento de la informática.

Si definimos la “SEGURIDAD DE LOS SISTEMAS INFORMATICOS” como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoria es una de las figuras involucradas en este proceso de protección de la información y de sus medios de proceso. La informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de *contramedidas*, y la calidad y la eficacia de las mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos.

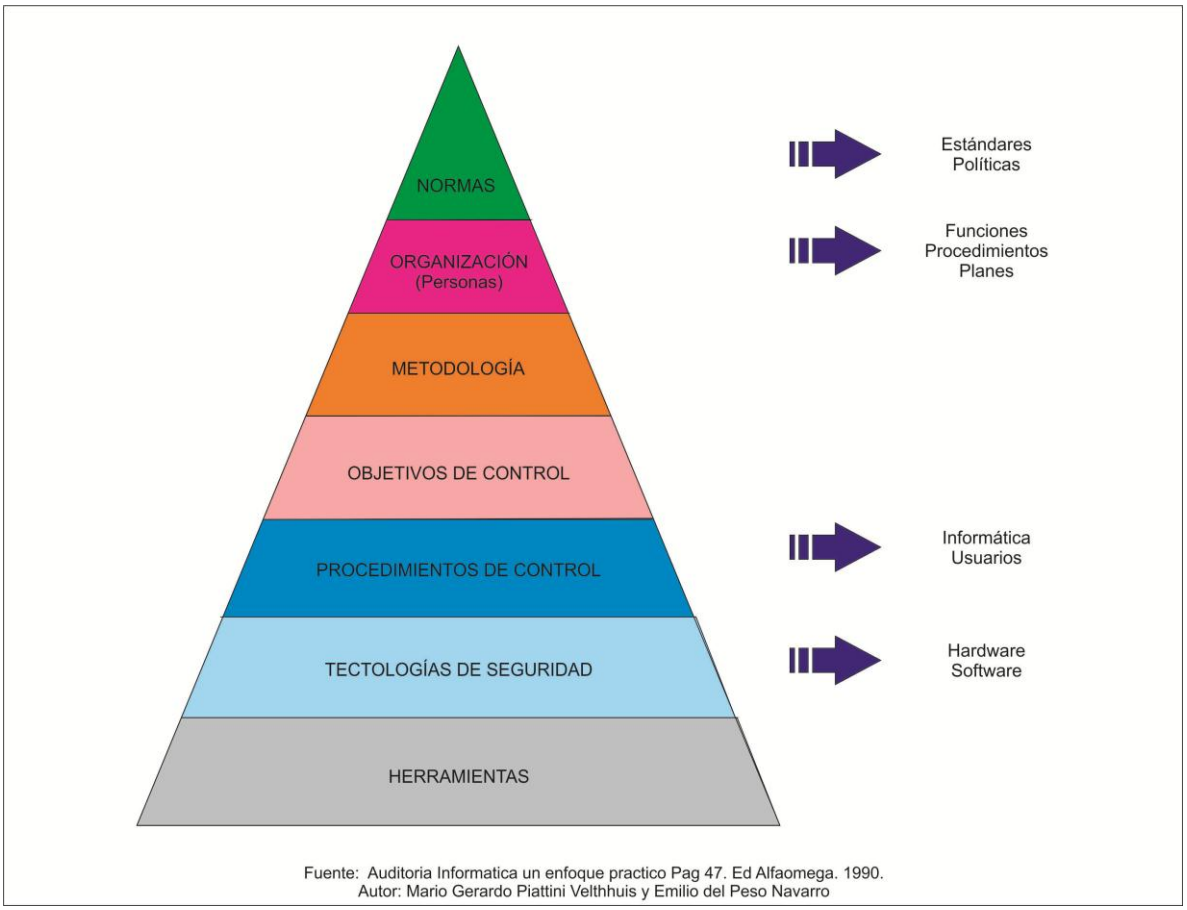


Figura 3. Factores que compone una contramedida

3.1.2 Los procesos y el auditor de Sistemas

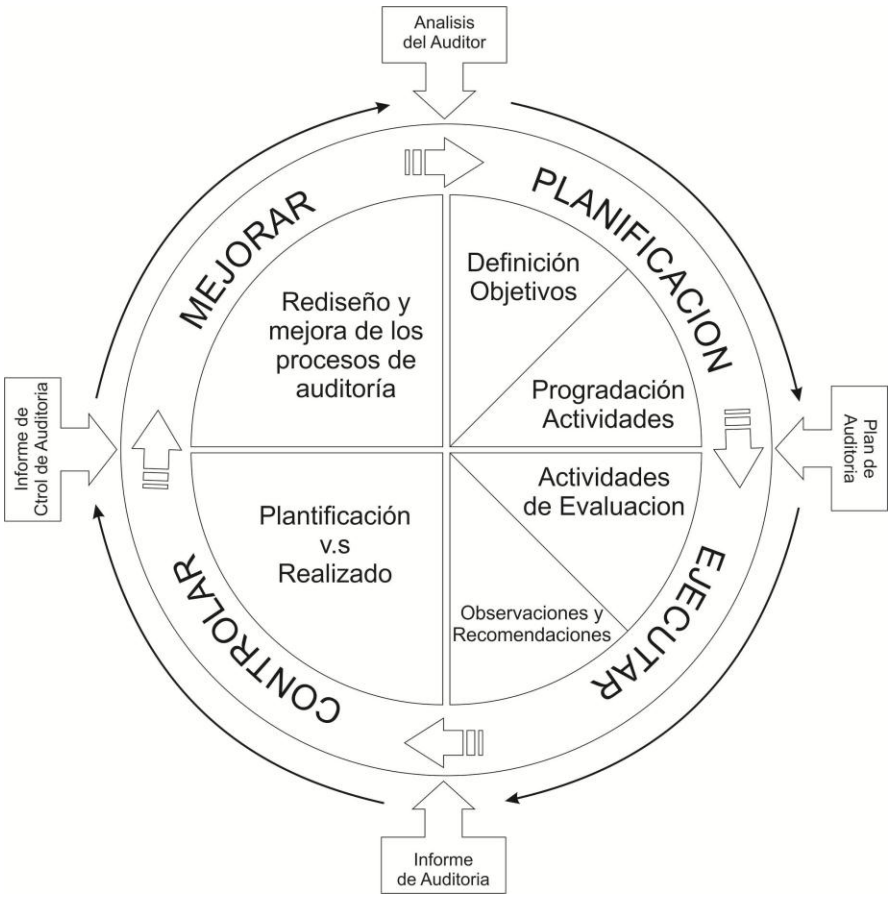
El ciclo de Edward Deming PDCA (Plan, Do, Check, Act), es un proceso que junto con el método clásico de resolución de problemas, permite la consecución de la mejora de la calidad en cualquier proceso de la organización. Supone una metodología para mejorar continuamente y su aplicación resulta muy útil en la gestión de los procesos. Este ciclo aplica en su totalidad para reflejar las actividades que realiza el auditor de sistemas. Es decir:

- *Planificación* de sus actividades basado en un enfoque de procesos con sus respectivos riesgos. El evento disparador será el acuerdo de realización de las actividades de auditoria de una fecha pautada para inicio de las actividades. La*Entrada*para este proceso es el análisis que el auditor realice de los procesos sustantivos y de apoyo y los riesgos estimados. En esta instancia se definen los objetivos y el alcance de la auditoria. El S*alida* es un documento donde se comunica las actividades a ejecutarse en un plazo determinado de tiempo. Se incluye el plan detallado de trabajo.

- *Ejecutar* las actividades focalizando los procesos más críticos para la organización. Algunos de los procedimientos tienen fines de control mientras que otros serán operativos. En esta instancia, se realizan las actividades de relevamiento y evaluación de cumplimiento de esos procedimientos de control. El propósito es emitir una opinión sobre que tanto mitigan los riesgos a los cuales está expuesto el proceso. La *Entrada* es el plan de auditoria y los recursos necesarios para cumplir con los objetivos de la auditoria. La *Salida* son el conjunto de elementos de prueba válidos y suficientes que permiten respaldar la opinión del auditor de sistemas y el informe de auditoría de sistemas (observaciones y recomendaciones) que constituye el producto final del proceso de auditoría.

- *Controlar* lo planificado contra lo realizado. La S*alida* del primero de los procesos y el detalle de las actividades realizadas con sus resultados generara la *Entrada* para este proceso. La S*alida* será un informe de control de auditoria con la explicación de los desvíos.

- *Mejora* continua de los propios procesos de auditoria y respectivas actividades (procedimientos). La *Entrada* de este proceso lo constituye todo el análisis realizado en el proceso anterior y la transformación consiste en el propio diseño de actividades que permitan incrementar la efectividad. La *Salida* lo constituye el rediseño de los propios procesos de auditoria.



Fuente: Los autores

Figura 4. Ciclo de Deming aplicado a la Auditoria de Sistemas

3.1.3 Tipos de metodologías

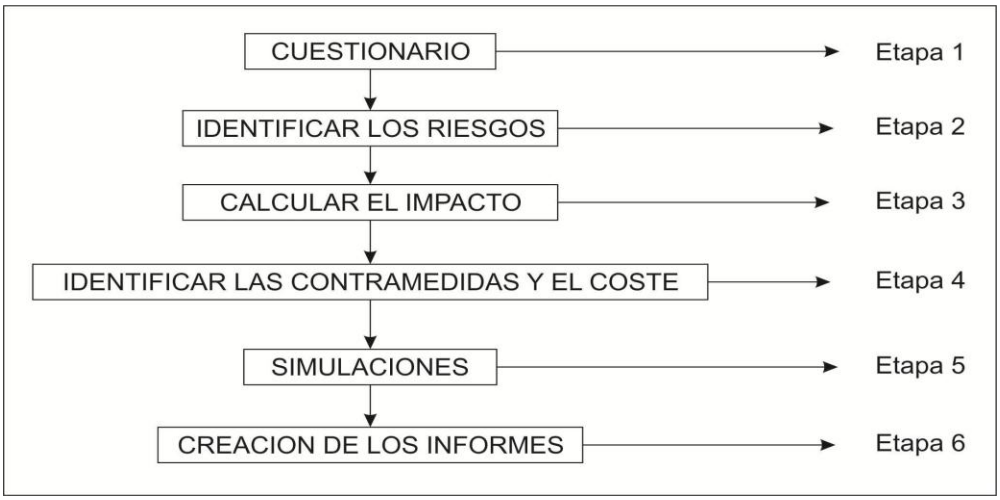
Todas las metodologías existentes desarrolladas y utilizadas en la auditoria de sistemas de información, se pueden agrupar en dos grande familias. Estas son:

- Cuantitativa: basada en un método matemático numérico que ayuda a la realización del trabajo.
- Cualitativa: basada en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

3.1.4 Metodologías más comunes

Las metodologías más comunes de evaluación de sistemas que podemos encontrar son de análisis de riesgos o de diagnóstico de seguridad, las del plan de contingencias, y las de auditoría de controles generales.

Metodologías de análisis de riesgo. Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas.



Fuente: Auditoria Informática un Enfoque práctico. Pág. 53 - Autores: Mario Piattini y Emilio del Peso

Figura 5. Esquema básico de una Metodología de análisis de riesgos

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir la posibilidad de que ocurra, acotar sus consecuencias, compartirlo con otra organización (contratando un seguro de cobertura), o en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Plan de contingencias. Es una estrategia planificada constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocios afectados por una paralización total o parcial de la capacidad operativa de la empresa.

Esta estrategia es el resultado de todo un proceso de análisis y definiciones que es lo que da lugar a las metodologías. Es muy importante tener en cuenta que el concepto a considerar es la continuidad en el negocio; estudiar todo lo que puede paralizar la actividad y producir perdidas.

- *Fase I. Análisis y Diseño.* Se estudia la problemática, las necesidades de los recursos, las alternativas del respaldo, y se analiza el coste/beneficio de las mismas.
- *Fase II. Desarrollo del Plan.* Se desarrolla la estrategia desarrollada, implantándose hasta el final todas las acciones previstas. Se define las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando así la documentación del plan.
- *Fase III. Pruebas y Mantenimiento.* En esta fase se definen las pruebas, sus características y ciclos, y se realiza la primera prueba como comprobación de todo el trabajo realizado, así como mentalizar al personal implicado.

3.2 SEGURIDAD EN BASES DE DATOS

Seguridad es la capacidad de un producto de software de proteger los datos y la información para que personas no autorizadas no puedan leerlos o modificarlos, y que el acceso no sea denegado a personal autorizado.

Gran parte de los errores en cuanto a la seguridad en bases de datos aun con el avance tecnológico suele producirse por la falta de preocupación de los procedimientos sencillos que a la larga se convierten en graves inconvenientes que afectan la seguridad.

Fuente: seguridad en el diseño de base de datos y sistemas de información.
Autor: Dr. Eduardo Fernández Medina, grupo de investigación Alarcos escuela superior de informática de ciudad real, universidad de castilla la mancha.

Figura 6. Esquema de seguridad en base de datos

3.2.1 Características importantes en la seguridad de bases de datos

Confidencialidad: prevenir / detectar / impedir el descubrimiento de información. En general la Confidencialidad se refiere a la protección de datos implicados en entornos altamente protegidos, como entornos militares, comerciales, etc. Privacidad se refiere a información sobre individuos. En la mayoría de los países la Privacidad está protegida por las leyes.

Integridad: prevenir / detectar / impedir la modificación inadecuada de información. La integridad de los datos es especialmente relevante, puesto que el éxito de una organización depende de lo correctas que son las operaciones que se llevan a cabo y la coherencia en los datos.

- *Integridad semántica:* Respeto en todo momento de las reglas de integridad definida en la base de datos.
- *Integridad Operacional:* Garantizar la consistencia de la base de datos con respecto al uso concurrente de la misma.

Disponibilidad: prevenir / detectar / impedir la denegación inadecuada del acceso a servicios ofrecidos por el sistema. Por ejemplo, en un entorno militar, cuando el mando correspondiente da la orden de lanzar el misil, el misil es disparado. En entornos comerciales, las órdenes de pago deben ser hechas en el momento. También relacionada con los mecanismos de recuperación de la base de datos ante caídas del sistema.

3.2.2 Medida de Seguridad

Físicas. Comprenden el control de quienes acceden al equipo.

Personal. Determinación del personal que tiene acceso autorizado.

Sistema Operativo. Técnicas que se establecen para proteger la seguridad del Sistema Operativo.

SGBD. Utilización de las herramientas que facilita el SGBD.

3.2.3 Tipos de Seguridad de bases de datos

En la actualidad se acostumbra hablar de dos tipos de mecanismos de seguridad de base de datos:

Los *Mecanismos de seguridad discrecionales*se usan para otorgar privilegios a los usuarios, incluida la capacidad de tener acceso a archivos, registros o campos de datos específicos en un determinado modo.

Los *Mecanismos de seguridad obligatorios* sirven para imponer igualdad de múltiples niveles clasificando los datos y los usuarios en varias clases (o niveles) de seguridad e implementando después la política de seguridad apropiada de la organización.

El *cifrado de datos* es una técnica que sirve para proteger datos confidenciales que se transmiten por satélite o por algún otro tipo de red de comunicaciones. El cifrado puede proveer protección adicional a secciones confidenciales de una base de datos. Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado que tenga acceso a los datos codificados tendrá problemas para descifrarlos, pero un usuario autorizado contara con algoritmos de codificación para descifrarlos.

Un problema de seguridad común a todos los sistemas de cómputo es el de evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información o para efectuar cambios malintencionados en una porción de la base de datos. El mecanismo de seguridad de un SGBD debe incluir formas de restringir el acceso al sistema como un todo. Esta función se denomina *control de acceso* y se pone en prácticas creando cuentas de usuario y contraseñas para que el SGBD controle el proceso de entrada al sistema.

3.2.4 La seguridad de la Base de Datos y el DBA

El administrador de la base de datos (DBA) es la autoridad central que controla un sistema de este tipo. Entre las obligaciones del DBA están otorgar privilegios a los usuarios que necesitan usar el sistema y clasificar los usuarios y los datos de acuerdo con la política de la organización. El DBA tiene una *cuenta privilegiada* en el SGBD, que confiere capacidades extraordinarias no disponibles para las cuentas y usuarios ordinarios de la base de datos. Las ordenes privilegiadas del DBA incluye órdenes para otorgar o revocar privilegios a cuentas individuales, usuarios o grupos de usuarios, y para efectuar los siguientes tipos de acciones.

- Creación de cuentas
- Concesión de privilegios
- Revocación de privilegios
- Asignación de niveles de seguridad

El DBA es responsable de la seguridad global del sistema de base de datos. La acción 1 controla el acceso a la base de datos, las acciones 2 y 3 se usan para controlar las autorizaciones discrecionales, y con la acción 4 se controla la autorización obligatoria.

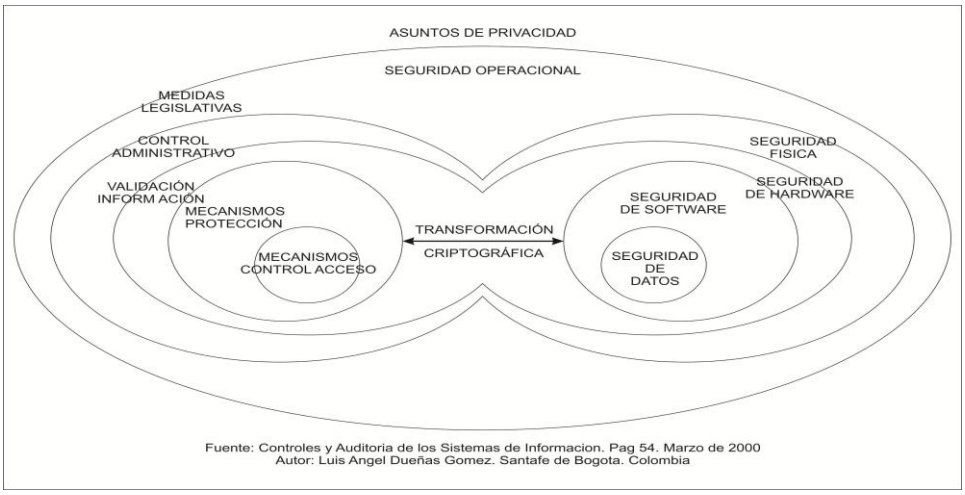


Figura 7. La seguridad en un sistema de computación

3.3 AUDITORIA EN SISTEMAS DE INFORMACION

La auditoría de sistemas es una disciplina encargada de aplicar un conjunto de técnicas y procedimientos con el fin de evaluar la seguridad, confiabilidad y eficiencia de los sistemas de información. Adicionalmente se encarga de evaluar la seguridad en los departamentos de sistemas, la eficiencia de los procesos administrativos y la privacidad de la información.

3.3.1 Clases de Auditoria de Sistemas

La auditoría de cumplimiento en sistemas, tiene como fin principal establecer si se están cumpliendo los controles establecidos e identificar y verificar la existencia y funcionalidad de los controles sobre una función específica del procesamiento de datos.

Lo que se persigue en una auditoria, es verificar si existen controles y probar su eficiencia, para ello es necesario aplicar diferentes técnicas de auditoria. Lo importante es que arroje información confiable y segura.

3.3.1.1 Auditoria alrededor del computador

También conocida como auditoria sin la utilización del computador, en ella se hace uso de listados de computador, para verificar la veracidad de la información. La información se evalúa tomando los resultados arrojados por el computador, construyendo las cifras finales a partir de los saldos iniciales, aplicándole los documentos fuente.

Esta técnica es aconsejable aplicarla en los sistemas de procesamiento de datos que tengan rastros de auditoria bien detallados de donde se pueda obtener datos suficientes para hacer el trabajo de campo.

3.3.1.2 Auditoria a través del computador

A diferencia del anterior, aquí se utiliza el computador como herramienta para comprobar los registros existentes, con él se obtiene información sobre la operación de los programas de computador y los controles que tiene incorporados. Adicionalmente se utilizan otras técnicas para comprobar los controles organizacionales y de procedimientos y obtener evidencia de que están funcionando adecuadamente.

Lo más frecuentes es que los auditores confeccionen datos de prueba con el fin de someterlos al procesamiento de los programas que tiene el cliente. También se utiliza algún software de auditoria que complementa las pruebas, como sacar muestras de los archivos, buscar registros que cumplan condiciones especiales, hacer estadísticas sobre el comportamiento de los archivos o de variables de un archivo, etc.

En estas auditorías se utilizan recursos existentes para corroborar los datos existentes en el sistema, pero no se desarrollan programas para hacerlo, ni se cuestionan los utilitarios o los sistemas operaciones sobre su configuración, seguridad, eficiencia, conveniencia para la instalación, o si la forma como están concebidos los sistemas, se ajusta a las necesidades de la empresa.

3.3.1.3 Auditoria con el Computador

Cuando se utiliza el computador como medio para llevar a cabo el trabajo, se impone al personal de auditoria la necesidad de conocer con cierto grado de profundidad los elementos básicos de un computador a nivel de software y hardware. Por un lado requiere saber las técnicas de diseño de sistemas de información para poder evaluarlos, la forma como se definen y hacen los

programas porque es necesario usar el computador para comprobar la información existente en los archivos maestros, la confiabilidad de la información generada y validez de los datos de entrada.

3.3.2 Etapas de una Auditoria de Sistemas

Para que los resultados del trabajo a desarrollar satisfagan las necesidades planteadas, es necesario tener en cuenta algunas etapas durante el desarrollo del mismo.

Definición de los objetivos. Se establece que se va a hacer y que se persigue, para confrontar los resultados finales con los propuestos.

Recopilación de la información básica. Consiste en conocer de manera general la empresa, el flujo de las transacciones, funciones, atribuciones, actividades desarrolladas, controles, etc. Esta información es necesaria para cualquier tipo de trabajo a desarrollar y será materia de consulta para todo el personal.

Diseño de técnicas para evaluar el control interno. Lo primero que se busca es tener una idea general de la existencia de controles al interior del departamento, en las aplicaciones y en general en las áreas motivo de estudio. Luego se necesita conocer si esos controles son suficientes y de una manera general se obtiene una idea de lo confiable que puede ser. Dependiendo de la planeación de la auditoria, se procede a escoger las técnicas que se van a emplear para lograr la información requerida.

Evaluación del sistema de control interno. Se toma la información recopilada, se analiza y se hace una idea de los controles existentes. Dependiendo del concepto que se forme en esta etapa, depende el tamaño de las muestras empleadas para evaluar los controles individuales y la cantidad de pruebas a aplicar.

Diseño de pruebas de auditoria. Con el fin de verificar los controles y medir las deficiencias existentes, se debe diseñar procedimientos de auditoria. Para ello se emplean las técnicas de auditoria que son herramientas empleadas para evaluar los controles.

Aplicación de la pruebas. Después de diseñar las pruebas, se procede a aplicarlas con el fin de recoger la información necesaria para el análisis. Se utilizan pruebas de cumplimiento para verificar si se están cumpliendo los procedimientos establecidos en la empresa, y pruebas sustantivas para corroborar la exactitud de la información.

Evaluación de resultados. Los hechos controlados se someten a estudio, esta es la parte concluyente del trabajo. Los datos recopilados se someten a un riguroso análisis, de tal manera que se pueda concluir si hay controles, si son suficientes y eficientes y si cumplen con los objetivos para los cuales fueron diseñados.

Elaboración del Informe. Después de hacer los análisis de rigor, se procede a emitir un concepto sobre la confiabilidad del área motivo de estudio. El dictamen puede ser favorable, en el sentido que el auditor considera que en su opinión el sistema es confiable, porque tiene los mecanismos de seguridad necesarios, o por el contrario considere que no es seguro ni confiable y que amerita una revisión e implantación de controles.

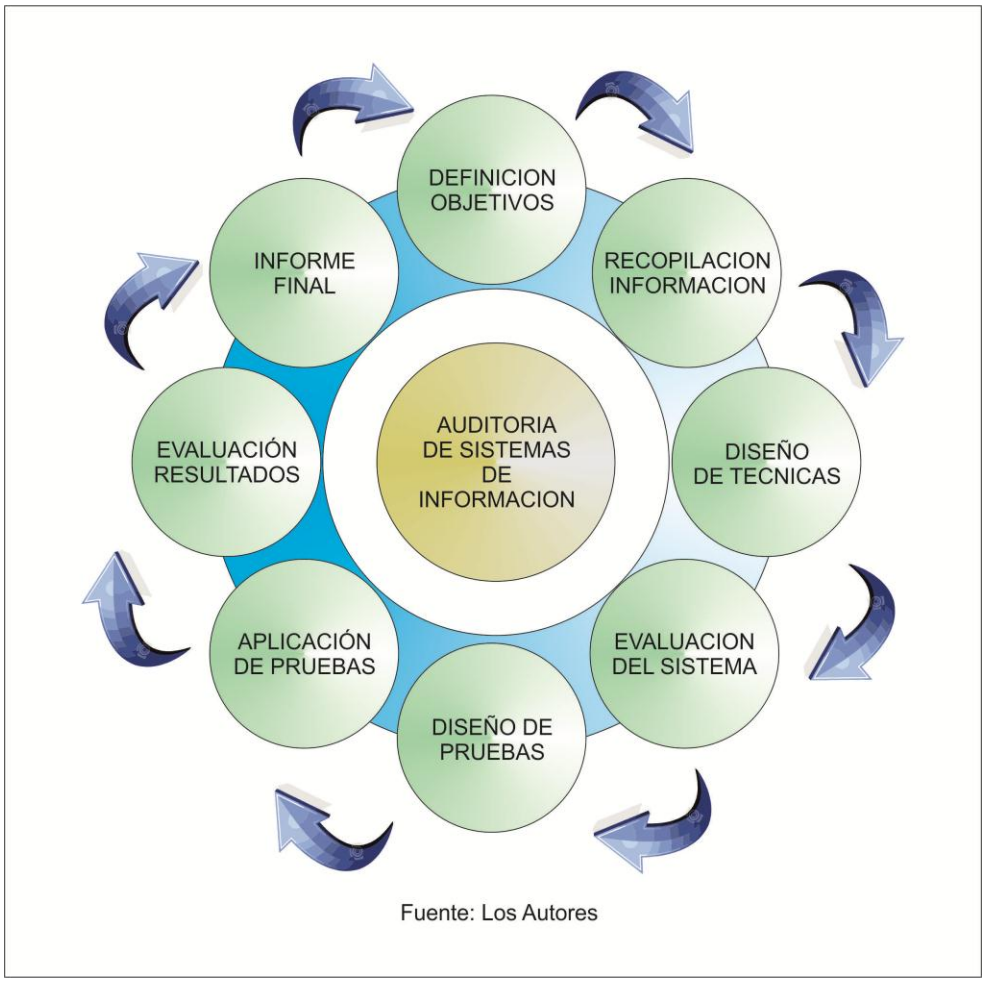


Figura 8. Etapas de la Auditoria de Sistemas de Información

3.4 BASES DE DATOS

3.4.1 Definición base de datos

Es una colección de archivos interrelacionados que son creados con un Sistema Manejador de Bases de Datos (DBMS). El contenido de una base de datos engloba a la información concerniente de una organización, de tal manera que los datos estén disponibles para los usuarios, una finalidad de la base de datos es eliminar la redundancia o al menos minimizarla.

Los tres componentes principales de un sistema de base de datos son el hardware, el software DBMS y los datos a manejar, así como el personal encargado del manejo del sistema.

3.4.2 Modelo de datos entidad-relación (E-R)

El modelo entidad-relación es el modelo conceptual más utilizado para el diseño conceptual de bases de datos. Fue introducido por Peter Chen en 1976. El modelo entidad-relación está formado por un conjunto de conceptos que permiten describir la realidad mediante un conjunto de representaciones gráficas y lingüísticas.

Entidad. Cualquier tipo de objeto o concepto sobre el que se recoge información: cosa, persona, concepto abstracto o suceso. Las entidades se representan gráficamente mediante rectángulos y su nombre aparece en el interior. Un nombre de entidad sólo puede aparecer una vez en el esquema conceptual.

Relación (interrelación). Es una correspondencia o asociación entre dos o más entidades. Cada relación tiene un nombre que describe su función. Las relaciones se representan gráficamente mediante rombos y su nombre aparece en el interior.

Cardinalidad. La cardinalidad con la que una entidad participa en una relación especifica el número mínimo y el número máximo de correspondencias en las que puede tomar parte cada ocurrencia de dicha entidad. La participación de una entidad en una relación es obligatoria si la existencia de cada una de sus ocurrencias requiere la existencia de, al menos, una ocurrencia de la otra entidad participante. Si no, la participación es opcional. Una de las trampas que pueden encontrarse ocurre cuando el esquema representa una relación entre entidades, pero el camino entre algunas de sus ocurrencias es ambiguo. El modo de

resolverla es reestructurando el esquema para representar la asociación entre las entidades correctamente.

Atributo. Es una característica de interés o un hecho sobre una entidad o sobre una relación. Los atributos representan las propiedades básicas de las entidades y de las relaciones. Toda la información extensiva es portada por los atributos. Gráficamente, se representan mediante bolitas que cuelgan de las entidades o relaciones a las que pertenecen.

Identificador. Un identificador de una entidad es un atributo o conjunto de atributos que determina de modo único cada ocurrencia de esa entidad. Toda entidad tiene al menos un identificador y puede tener varios identificadores alternativos. Las relaciones no tienen identificadores.

3.4.3 Sistema de Gestión de Bases de Datos (DBMS databasemanagementsystem)

Un sistema de gestión de bases de datos (DBMS) consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a ellos, es básicamente un sistema computarizado para llevar registros, es decir, un sistema cuya finalidad general es almacenar información y permitir a los usuarios realizar una variedad de operaciones sobre dichos registros, por ejemplo: insertar, borrar, modificar, agregar, consultar. La colección de datos se denomina base de datos (BD).El objetivo primordial de un DBMS es proporcionar que a su vez sea conveniente y eficiente para ser utilizado al extraer o almacenar información en la BD. Los sistemas de bases de datos están diseñados para gestionar grandes bloques de información, que implica tanto la definición de estructuras para el almacenamiento como de mecanismos para la gestión de la información. Además los DBMS deben mantener la seguridad de la información almacenada pese a la

caída del sistema o accesos no autorizados. Los objetivos principales de un sistema de base de datos es disminuir los siguientes aspectos:

Redundancia e inconsistencia de datos. Puesto que los archivos que mantienen almacenada la información son creados por diferentes tipos de programas de aplicación existe la posibilidad de que si no se controla detalladamente el almacenamiento, se pueda originar un duplicado de información, es decir que la misma información sea más de una vez en un dispositivo de almacenamiento.

*Dificultad para tener acceso a los datos.*Un sistema de base de datos debe contemplar un entorno de datos que le facilite al usuario el manejo de los mismos. El sistema debe de prever estas situaciones desde que se realiza el diseño para evitar una deficiencia.

Aislamiento de los datos. Puesto que los datos están repartidos en varios archivos, y estos no pueden tener diferentes formatos, es difícil escribir nuevos programas de aplicación para obtener los datos apropiados.

Anomalías del acceso concurrente. Para mejorar el funcionamiento global del sistema y obtener un tiempo de respuesta más rápido, muchos sistemas permiten que múltiples usuarios actualicen los datos simultáneamente. En un entorno así la interacción de actualizaciones concurrentes puede dar por resultado datos inconsistentes. Para prevenir esta posibilidad debe mantenerse alguna forma de supervisión en el sistema.

Problemas de seguridad. La información de toda empresa es importante, aunque unos datos lo son más que otros, por tal motivo se debe considerar el control de

acceso a los mismos, no todos los usuarios pueden visualizar alguna información, por tal motivo para que un sistema de base de datos sea confiable debe mantener un grado de seguridad que garantice la autentificación y protección de los datos.

*Problemas de integridad.*Los valores de datos almacenados en la base de datos deben satisfacer cierto tipo de restricciones de consistencia. Estas restricciones se hacen cumplir en el sistema añadiendo códigos apropiados en los diversos programas de aplicación.

3.4.4 Tipos de bases de datos.

Las bases de datos pueden ser diseñadas de distintas formas, dependiendo de los requerimientos organizacionales y la complejidad de la información, por esta razón se mencionan varios tipos de bases de datos.

Bases de datos jerárquicas. Son bases de datos que, como su nombre indica, almacenan su información en una estructura jerárquica. En este modelo los datos se organizan en una forma similar a un árbol (visto al revés), en donde un nodo padre de información puede tener varios hijos. El nodo que no tiene padres se le conoce como raíz, y a los nodos que no tienen hijos se les conoce como hojas.

Bases de datos simples o planas. Las bases de datos simples son aquellas que están formadas por una sola tabla de datos. Este tipo de bases de datos son muy fáciles de crear y utilizar; cubren la mayoría de necesidades de los particulares.

Bases de datos en red. Se puede considerar al modelo de bases de datos en red como de una potencia intermedia entre el jerárquico y el relacional. Su estructura es parecida a la Jerárquica aunque bastante más compleja, con lo que se consiguen evitar, al menos en parte, los problemas del modelo jerárquico

Bases de datos relacionales. Este modelo intenta representar la base de datos como un conjunto de tablas aunque las tablas son un concepto simple e intuitivo, existe una correspondencia directa entre el concepto informático de una tabla, y el concepto matemático de una relación, lo cual es una gran ventaja, pues permite efectuar formalizaciones de una manera estricta mediante las herramientas matemáticas asociadas, como puede ser el álgebra relacional en el ámbito de las consultas.

3.5 LEYES Y NORMAS

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

A continuación se nombran los artículos más representativos que se utilizaran como soporte para el presente proyecto.

Capítulo I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Art 269A: Acceso abusivo a un sistema informático
- Art 269B: Obstaculización ilegitima de sistemas informáticos o red de telecomunicaciones.
- Art 269C: Interceptación de datos informáticos.
- Art 269D: Daño informático.
- Art 269E: Uso de software malicioso
- Art 269F: Violación de datos personales

Capitulo II. De los atentados informáticos y otras infracciones.

- Art 269I: Hurto por medios informáticos y semejantes.
- Art 269J: Transferencia no consentida de activos

La ley 1273 de 2009 crea nuevos tipos penales relacionados con delitos informáticos y la protección de la información y los datos, con penas y multas significativas.

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico, y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Norma Internacional de auditoria 530. Muestreo de la auditoria y otros medios de prueba. El propósito de esta Norma Internacional de Auditoría (NIA) es establecernormas y proporcionar lineamientos, sobre el uso de procedimientos demuestreo en la auditoría y otros medios de selección de partidas para reunirevidencia en la auditoría.

Al diseñar los procedimientos de auditoría, el auditor deberá determinar losmedios apropiados para seleccionar las partidas sujetas a prueba a fin de reunirsuficiente evidencia apropiada de auditoría para cumplir los objetivos de losprocedimientos de auditoría.

Norma ISO/IEC 27001:2005. La norma ISO/IEC 27001 que en siglas significa Technology Security Techniques viene a ser la evolución de buenas prácticas ISO creado en 1995, para lo cual su creación conlleva un progreso certificable llamado estándar 27001. Este tipo de certificación facilitara a la Seguridad Informática al momento de establecer, implantar, operar, supervisar, mantener, mejorar un SGSI.

El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información.

En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios.

• La política de seguridad

• Organización para la seguridad de la información

• Gestión de activos de información

• Seguridad del personal

• Seguridad física y ambiental

• Gestión de comunicaciones y operaciones

• Control de acceso

• Adquisición, desarrollo y mantenimiento de sistemas

• Gestión de incidentes de la seguridad de la información

• Gestión de la continuidad del negocio

• Cumplimiento

Los principios rectores en la norma ISO/IEC 27002 son los puntos de partida para la implementación de seguridad de la información. Se basan en los requisitos legales o en las mejores prácticas generalmente aceptadas.

COBIT 4.1. COBIT es un acrónimo formado por las siglas derivadas del Control Objetives forInformation and RelatedTechnology (Objetivos de Control para la Información y Tecnologías Relacionadas). Este conjunto de objetivos representa el producto de un proyecto de investigación desarrollado por la InformationSystemAudit and Control Fundation (ISACF) que fue publicado inicialmente en el año 1996.

COBIT es un conjunto de objetivos de control aplicables a un ambiente de tecnologías de información que lograron definirse gracias a un trabajo de investigación y búsqueda de consenso entre la normatividad de distintos cuerpos colegiados, estándares técnicos, códigos de conducta, prácticas y requerimientos de la industria y requerimientos emergentes para industrias específicas.

El propósito de COBIT es proporcionar una guía estándar que tenga una aceptación internacional sobre los objetivos de control que deben de existir en un ambiente de tecnología de información para asegurar que las organizaciones logren los objetivos de negocio que dependen de un adecuado empleo de dicha tecnología.

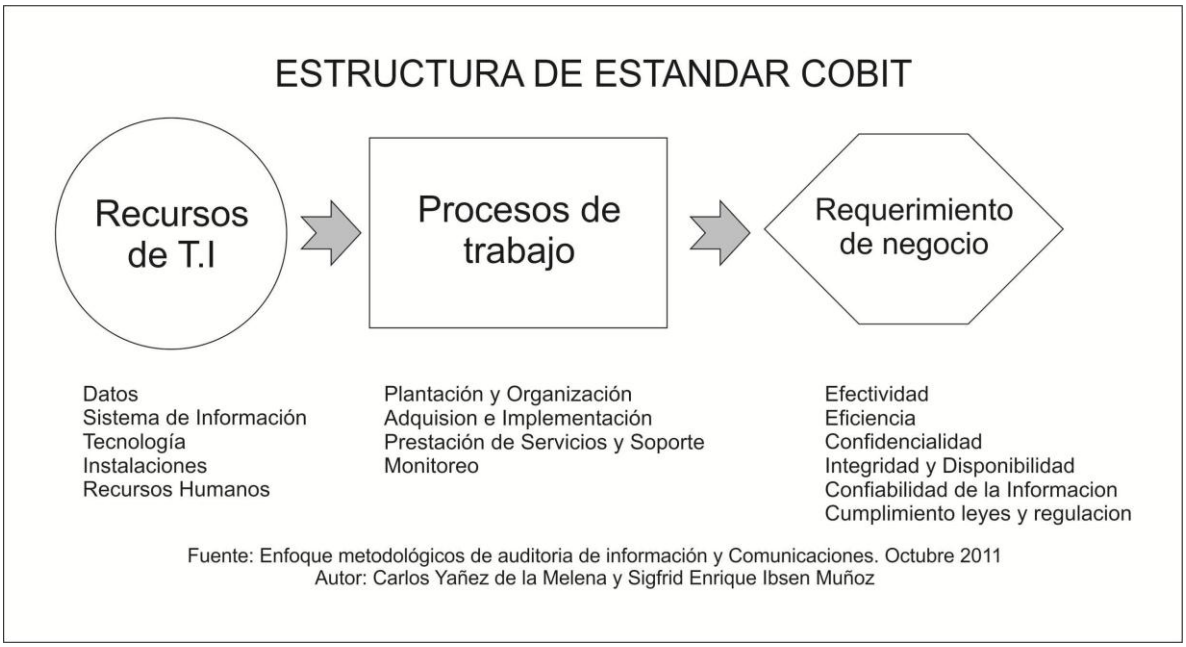


Figura 9. Estructura del Estándar COBIT

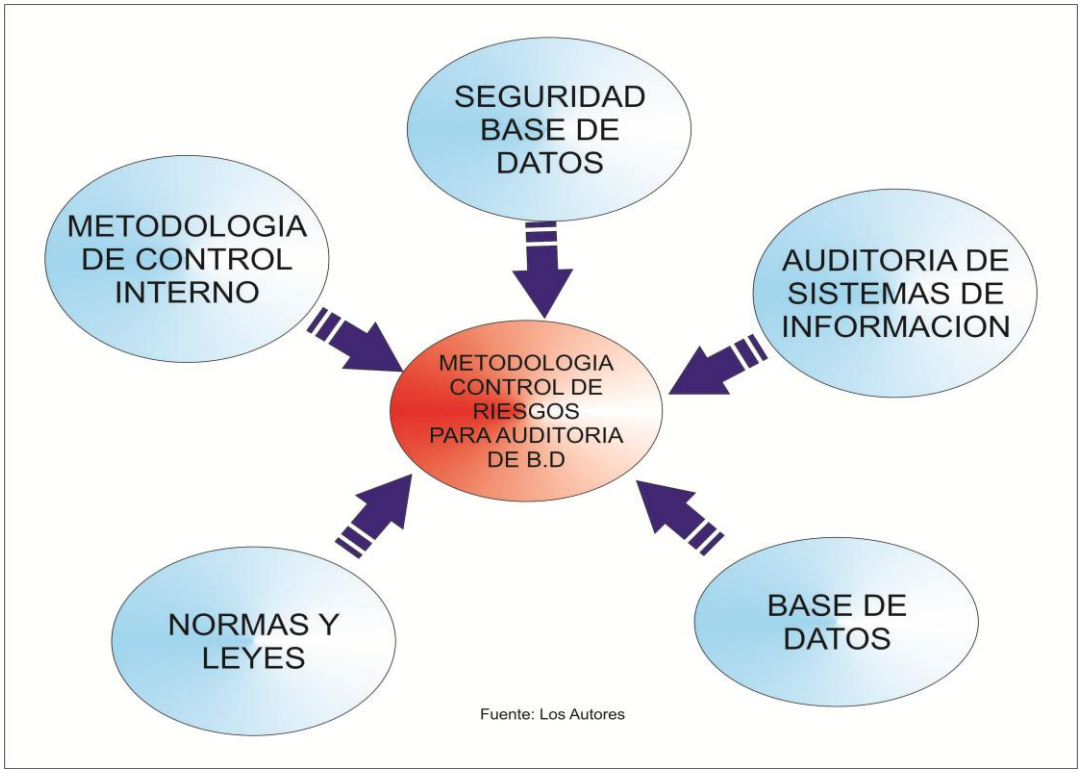


Figura 10. Contorno de metodología propuesta

CAPITULO IV

DESARROLLO DEL PROYECTO

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

Normalmente la auditoria en sistemas de información se aplica de dos formas diferentes; por un lado, se auditan las principales áreas del departamento de informática: dirección, metodología de desarrollo, sistema operativo, telecomunicaciones, base de datos, etc.; y por el otro lado, se auditan las aplicaciones que funcionan en la empresa. La importancia de la auditoria de Bases de Datos radica en que es el punto de partida para poder realizar la auditoria de las aplicaciones que utilizan esta tecnología.

El propósito de una auditoria de sistemas de información es evaluar la seguridad, confiabilidad y eficiencia de los sistemas de información a través de un conjunto de técnicas y procedimientos aplicados. Ahora bien, la metodología planteada en este proyecto le permitirá a los auditores informáticos poder controlar los riesgos a los que esta expuestos las tecnologías de bases de datos y evitar de esta forma la vulnerabilidad en la seguridad y confiabilidad de la información.

4.1 PLANTEAMIENTO DE LA METODOLOGIA

La metodología propuesta es una herramienta de apoyo que permite incorporar el uso del estándar COBIT, la norma técnica ISO/IEC 27002 y el Método MAGERIT para gestión de riesgos en los Sistemas de Información. A continuación se presenta las etapas que componen la metodología:

A. ETAPA I: Planificación de la Auditoria de Base de Datos

1. Plan de auditoria preliminar.
2. Recopilación de la información de la organización.
3. Definición de objetivos y alcance de la auditoria.

B. ETAPA II: Ejecución de la auditoria de base de datos

4. Evaluación del sistema de control interno.
5. Análisis de riesgos en las bases de datos.
6. Diseño de pruebas de auditoria.
7. Ejecución de las pruebas de auditoria.
8. Evaluación de los resultados de las pruebas de auditoria.

C. ETAPA III: Resultado de la Auditoria

10. Elaboración del informe con los resultados de la auditoria
11. Seguimiento a las observaciones de la auditoria

4.1.1 Síntesis de actividades por etapas

En el siguiente diagrama, se presenta un resumen de las diferentes actividades que componen las etapas para realizar la Metodología para Control de Riesgos para Auditoria de Base de Datos – MCRABD.

ACTIVIDADES DE LA METODOLOGIA		**ACTIVIDADES A EJECUTARSE**	**RESULTADOS DE LA ACTIVIDAD**
1	Plan de Auditoria Preliminar	• Conformar el grupo de trabajo que realizara la Auditoria de Base de Datos • Estimar el tiempo necesario para realizar la auditoria.	• Definición del perfil del personal requerido. • Cronograma de actividades por etapas con horas estimadas para realizar la Auditoria.
2	Levantamiento de la información de la Organización	• Levantamiento de la información sobre el estado actual y características de la organización, infraestructura, recursos humanos y técnicos, procesos de negocios y sistemas de información que lo	• Documentos de trabajo de la Auditoria • Documento con definición de los procesos de negocio y diagramas descriptivos • Ficha técnica de los sistemas de información que soportan los procesos de

		soportan. • Diseño de flujograma de los procesos de negocio. • Realizar Ficha Técnica de los sistemas de información que soporta los negocios.	negocios. • Documentos con información de las áreas de la organización y su relación con los sistemas de información. • Perfiles del personal de sistemas que tienen relación con los sistemas de información y con la Base de Datos • Perfiles de los usuarios estrellas de las diferentes áreas, claves el en proceso de auditoría.
3	Definición de objetivos y alcance de la Auditoria de B.D	• Seleccionar los objetivos principales de la auditoria. • Elaborar el programa de auditoria detallado. • Definir el alcance de la auditoria de Base de Datos.	• Lista de los objetivos que debe ser alcanzados por el proceso de auditoría. • Programa de auditoria de Base de Datos detallado. • Alcance de la auditoria definido.

4	Evaluación de Sistemas de Control Interno	• Analizar la información encontrada y definir los controles existentes en el sistema de información y en la base de datos.	• Tamaño de la muestra empleada para evaluar los controles en las base de datos.
5	Análisis de riesgos en las Base de Datos	• Determinar que amenazas se encuentra expuesta la Base de Datos • Determinar que salvaguardas hay disponibles y que tan eficaces son frente al riesgo. • Estimar el impacto de un riesgo	• Lista de amenazas identificadas • Lista de salvaguardas eficaces frente a los riesgos • Lista de impacto por riesgo detectado.
6	Diseño de pruebas de Auditoria de B.D	• Elaboración de procedimientos de auditoria de B.D para cada control a evaluar	• Lista de controles evaluados y su resultado
7	Ejecución de las pruebas de auditoria	• Ejecutar pruebas de cumplimiento utilizando técnicas de ejecución	• Lista de controles verificados por el auditor. • Soporte de las

		manuales o asistidas por computador	pruebas de auditoria realizadas.
8	Evaluación de los resultados de las pruebas de Auditoria de B.D	• Evaluar los resultados de las pruebas efectuadas. • Desarrollar el análisis de las observaciones de auditoría y puntos mejorables para los controles y datos deficientes. • Identificar las causas, el impacto y las implicaciones de la observaciones para la organización y verificar los estándares y mejores prácticas que no se cumplen. • Diseñar los resultados de la auditoria para los resultados no satisfactorios.	• Listado con análisis de observaciones de auditoría para pruebas de cumplimiento. • Conclusiones de los resultados obtenidos.

9	Elaboración del Informe con los resultados de la Auditoria	• Elaborar resumen de observaciones. • Desarrollar y aprobar informe preliminar. • Emitir informe preliminar • Diseñar conclusiones generales y específicas de la auditoria. • Elaborar y aprobar informe final de auditoría. • Emitir informe final de auditoría.	• Resumen de observaciones obtenidas. • Informe final de auditoria • Expediente de auditoría con observaciones referenciadas
10	Seguimiento a las Observaciones de Auditoria de B.D	• Planificar seguimiento a las observaciones de auditoría. • Analizar y evaluar resultados del seguimiento. • Elaborar informe de seguimiento	• Programa de seguimiento • Listado con el resultado del cumplimiento de observaciones • Informe de seguimiento

Tabla 1. Síntesis de actividades por etapa

4.2 ETAPA 1. PLANIFICACION DE LA AUDITORIA DE BASE DE DATOS

La primera fase de la auditoría comprende la realización de un plan de auditoría preliminar con el propósito de definir los objetivos de la auditoría, asignar los recursos y estimar el tiempo necesario para efectuar la revisión.

4.2.1 Plan de auditoria preliminar

En esta etapa se diseña la planeación a seguir para la realización de la auditoria, de igual manera se definen los servicios con prioridad de auditoría para cada sector de la base de datos y se estima el tiempo de las actividades a realizar para ejecutar el proceso de Auditoria.

Para hacer una adecuada planeación de la auditoria, se debe seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo; con ello podemos determinar el número y características del personal de auditoria, las herramientas necesarias, el tiempo y el costo, así como definir los alcances de la auditoria. Se debe de tener en cuenta que la inadecuada planeación repercutirá en una serie de problemas, que pueden provocar que no se cumplan con la auditoria o bien que no se efectúe con el profesionalismo que debe de tener el desarrollo de cualquier auditoria.

Para lograr una adecuada planeación, lo primero que se requiere es obtener información general sobre la organización y sobre el funcionamiento de la Base de Datos que administra la información de la empresa. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, y con base a esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

4.2.1.1 Programa de trabajo para el desarrollo de la Auditoria

Este documento consta de tres secciones:

- *Objetivos de la auditoría:* En esta sección se incluyen los objetivos de control generales que se buscan con la realización de la auditoría en Base de Datos.
- *Alcance de la auditoría:* En esta sección se definen los procesos de negocio y sistemas de información que serán revisados.
- *Programación de actividades:* Incluye la secuencia de pasos que deberán ejecutarse para desarrollar las etapas de la auditoría.

4.2.1.2 Asignación de recursos y estimación del tiempo requerido para realizar la auditoria

Con base en la complejidad técnica de los procesos de negocio y sistema de información sujetos a auditoría y en el volumen de trabajo estimado para satisfacer los objetivos propuestos, es necesario definir las competencias necesarias del equipo de auditoría y estimar las necesidades de tiempo que se requerirán. Suponga que se presupuestan 480 horas para todo el trabajo, las que podrían ser asignadas así: 15% para labores de supervisión, 20% para el auditor a cargo y el restante 65% para los auditores en terreno.

No	**Nivel de Responsabilidad**	**Horas Asignadas**
1	Supervisor	72
2	Auditor a cargo	96
3	Auditor en terreno	312

Tabla 2. Asignación de Horas de Auditoria

Por cada una de las etapas de la metodología, un modelo de distribución de tiempo podría ser el siguiente:

No	Nivel de Responsabilidad	Horas Asignadas
1	Plan de Auditoria preliminar	40
2	Levantamiento de la Información de la Organización	40
3	Definición de objetivos y alcance de la Auditoria de B.D	40
4	Evaluación de Sistemas de Control Interno	120
5	Análisis de riesgos en la Base de Datos	30
6	Diseño de pruebas de auditoria de B.D	80
7	Ejecución de las pruebas de Auditoria.	40
8	Evaluación de los resultados de la pruebas de Auditoria de B.D	40
9	Elaboración de informe con los resultados de la auditoria	40
10	Seguimiento a las observaciones de auditoria de B.D	40

Tabla 3. Estimación de horas por Etapas

4.2.2 Levantamiento de la información de la organización

Esta etapa tiene como objetivos conocer y comprender el ambiente de organización, tecnológico y operativo de los procesos de negocio y los sistemas de información que los soportan. Implica para el auditor, realizar un levantamiento de la información detallada a través de entrevistas con las personas apropiadas,

de observación de la forma como se ejecutan las operaciones y de la comprensión de la lógica del negocio, los flujos de información, el rol de las personas y dependencias que intervienen en el manejo de las operaciones y otros aspectos que el auditor considere importantes.

El objetivo de este primer contacto es percibir rápidamente la estructura fundamental y diferencias principales entre la organización a auditar y otras organizaciones que se hayan investigado.

Cuando se realiza por primera vez la auditoría en un servicio, la información relevante obtenida en esta etapa se organiza en un documento conocido como archivo permanente o expediente continuo de auditoría. Si el archivo ya existe, es necesario su revisión y actualización con los cambios efectuados desde la última auditoría. Si no existe, es necesario crearlo e identificarlo correctamente.

Este documento contiene información sobre los objetivos y procesos que soportan los sistemas de información y sobre los recursos de tecnología utilizados (instalaciones de procesamiento, infraestructura, personal, contratos, etc.) y la importancia relativa de las cifras que se procesan y otros datos de interés.

4.2.2.1 Proceso de levantamiento de la información

El levantamiento de información que se realiza en esta etapa, tiene como finalidad asegurar que el auditor comprenda la filosofía y las características de funcionamiento de los procesos de negocio y sistemas de información en estudio. Esto es imperativo dentro del proceso de la auditoría, puesto que toda la pericia y el conocimiento técnico del auditor serían inaplicables si antes no obtiene la comprensión de aspectos claves del universo que será auditado.

Como resultado de esta actividad, el auditor obtiene la siguiente información:

a. De los procesos del negocio
    - Estructura organizacional
    - Estructura de las áreas propietarias de la información de los procesos de negocio
    - Clientes interno y externos
    - Dependencias de la organización
    - Tareas o actividades que realiza cada dependencia
    - Terceros que intervienen en el manejo de la información almacenada en las bases de datos
    - Políticas y procedimientos establecidos en la organización para confidencialidad de la información
    - Normas legales e institucionales que rigen el funcionamiento del servicio
    - Información sobre fraudes y otros antecedentes en las operaciones del servicio

b. De las tecnologías de información que soportan el negocio
    - Funciones y operaciones del negocio que ejecutan el sistema
    - Modelo entidad/relación de las bases de datos de los sistemas
    - Diccionario de datos de los modelos entidad/relación
    - Inventario de documentos fuentes y otros medios de entrada de datos
    - Personas claves que dan soporte técnico a la operación y mantención de las bases de datos
    - Terceros que prestan servicios de tecnologías de información para los procesos de negocio.
    - Inventario de informes que producen los sistemas y destinatarios de los mismos
    - Manuales existentes con la documentación técnica y del usuario

- Plataforma en la que funcionan los sistemas de información (sistema operativo, software de desarrollo y motor de base de datos utilizados)
- Si el sistema de información fue adquirido; datos del proveedor, año de adquisición, versión en producción, cantidad de usuarios con licencia, poseen programas fuentes y contrato de mantención)
- Si el sistema de información fue desarrollado internamente (tipo de lenguaje utilizado, archivos fuentes y ejecutables, fecha de ingreso a producción, versión actual en producción).

4.2.3 Definición de los objetivos y del alcance de la Auditoria de Base de Datos

El objetivo de esta etapa es identificar, analizar y seleccionar los objetivos de control aplicables a los procesos de negocio y sistemas de información sujetos a auditoría. Estos objetivos de control serán incorporados al programa de auditoría detallado.

4.2.3.1 Selección de los objetivos

En este paso de la metodología se deben seleccionar los objetivos de control que sean aplicables a la auditoría de los procesos de negocio y sistemas de información en revisión. Se debe de tener en cuenta que los objetivos de la auditoria deben estar relacionado con lo que se quiere encontrar o controlar y en los que busca la gerencia de la organización para reducir los riesgos de las amenazas en los datos de la empresa. Estos objetivos deben de estar encaminados a la minimización de los riesgos potenciales a los que está sometido el entorno.

4.3 ETAPA II: EJECUCION DE LA AUDITORIA

Esta etapa de la auditoría comprende un análisis del sistema de control interno de la organización con el objetivo de planificar y realizar las pruebas de cumplimiento y sustantivas que evaluarán si los controles operan de forma adecuada y cumplen con resguardar el cumplimiento de los objetivos y requisitos del negocio.

4.3.1 Evaluación del sistema de control interno

En esta etapa los auditores deben evaluar el sistema de control interno existente en los procesos de negocio y sistemas de información objeto de la auditoría, como base para determinar la naturaleza y extensión de las pruebas de auditoría que se requieran.

Evaluar el sistema de control interno significa: “determinar si los controles establecidos en los procesos de negocio y los sistemas de información, ofrecen la protección apropiada para reducir los riesgos a niveles aceptables para la organización”.

El propósito de la evaluación de control interno, es determinar si es suficiente y efectiva para proteger a la organización, contra los riesgos que podrían afectarla en los procesos de negocio y sistemas de información que se están auditando. Esto es, evaluar la confiabilidad de los controles utilizados para prevenir o detectar y corregir las causas de los riesgos y minimizar el impacto que estos tendrían en caso de llegar a materializarse.

La evaluación del sistema de control interno produce resultados intermedios, de valor importante para las etapas restantes del proceso de auditoría, estos son:

1) El auditor fundamenta su opinión sobre la confiabilidad que ofrecen los controles utilizados, para reducir la probabilidad de ocurrencia o el impacto de los riesgos. Los resultados de esta evaluación sirven al auditor como base para determinar la naturaleza y extensión de las pruebas de auditoría que se consideren necesarias y apropiadas a las circunstancias.

2) El auditor identifica y soporta debilidades y oportunidades de mejoramiento (observaciones de auditoría) en la estructura de los controles. Estas observaciones son insumos para el informe de auditoría.

3) El auditor identifica los controles que deberán verificarse en la etapa de ejecución de pruebas de auditoría, para determinar que realmente existen, están operando y son entendidos por las personas encargadas de ejecutarlos (pruebas de cumplimiento).

4) El auditor identifica los datos críticos y actividades sobre las cuales es necesario aplicar pruebas para verificar la exactitud y confiabilidad de los cálculos y de la información que producen los sistemas de información para apoyar el desarrollo de las operaciones del negocio (pruebas sustantivas).

5) El auditor documenta las observaciones de auditoría para los procesos de negocio y los sistemas de información que los soportan. Esta presenta las debilidades y deficiencias de control interno y seguridad identificadas en la evaluación de controles.

4.3.2 Análisis de riesgos en las Bases de Datos

Cuando en el momento de crear datos en las bases de datos, no se tiene en cuenta la existencia previa de otros considerados como padres o sea que los originen, las bases de datos se van llenando de basura o datos que no pertenecen a nadie. Para evitar la presencia de estos errores, es necesario validar la integridad referencial, asegurando que existan primero los datos básicos, así aseguramos que un movimiento pertenezca a alguien.

En la medida que se van realizando operaciones con las bases de datos, se va presentando un reacomodamiento de los registros, dejando espacios en blanco, registros marcados como borrados que requieren ser retirados e índices que necesitan ser actualizados. Estas circunstancias ocasionan degradación en el funcionamiento de la base de datos que hacen necesario hacer mantenimiento permanente con el fin de hacer más ágil su funcionamiento.

Las bases de datos son una buena solución para satisfacer algunas necesidades de información. Pero un error en el diseño puede resultar fatal para su funcionamiento. Las bases de datos están compuestas por varias tablas que agrupan información de acuerdo con criterios determinados. Esta filosofía nos puede llevar a que si no tenemos cuidado con los usuarios pueden acceder información no autorizada.

El acceso concurrente de varios usuarios sobre un mismo registro constituye un riesgo, porque si no se controla, el sistema se puede bloquear al no poder atender el requerimiento simultáneamente.

Un erro frecuente en el diseño de bases de datos es definir tablas con muchos campos lo cual las hace demasiado grandes, violando los principios básicos del diseño. Tablas demasiado grandes hacen que al leer los datos se ocupen muchos campos de memoria principal que podrían emplearse en otros procesos.

También podríamos estar frente de bases de datos con muchas tablas lo cual dificulta el tiempo de proceso, porque para consultar cierta cantidad de datos tiene que hacer varias lecturas.

El no tener metodología para el diseño de las bases de datos nos puede llevar a tener un diseño que no consulta las técnicas para un buen modelo, reflejándose en una degradación del tiempo de respuesta.

La falta de documentación dificulta el mantenimiento, entendimiento y administración de la base de datos.

4.3.3 Diseño de las pruebas de auditoría

El objetivo de esta etapa es definir y diseñar los procedimientos de auditoría de base de datos para obtener evidencia válida y suficiente de la operación de los controles existentes (pruebas de cumplimiento) y de la integridad de la información (pruebas sustantivas). Las pruebas pueden ser realizadas con procedimientos manuales o asistidas por computadora.

Estas pruebas se aplican sólo a los controles que en la evaluación de control interno presentaron un nivel de protección apropiado. El auditor debe verificar que:

- Los controles identificados y evaluados en la etapa anterior están operando como se previó. Estas se denominan pruebas de cumplimiento.
- La información manejada, procesada o producida por el proceso de negocio o sistema de información, es exacta y confiable, es decir, refleja la realidad. Estas son las pruebas sustantivas.

De la ejecución de esta etapa se obtienen los siguientes productos:

- *Para pruebas de cumplimiento:* Por cada técnica de comprobación a emplear, un documento con las especificaciones de diseño de cada prueba, indicando los controles a probar, el procedimiento y los recursos requeridos para ejecutar la prueba.
- *Para pruebas sustantivas:* Por cada técnica de comprobación a utilizar, un documento con las especificaciones de diseño de cada prueba, indicando los datos a verificar, el procedimiento y los recursos requeridos para ejecutar la prueba.

4.3.3.1 Identificación de controles claves que serán verificados

Las pruebas de cumplimiento y sustantivas no se aplican para todos los controles existentes, identificados y evaluados satisfactoriamente en la etapa anterior. Por razones de efectividad y eficiencia, es suficiente con probar solamente una muestra de controles seleccionados cuidadosamente, aplicando criterios que consulten su importancia para asegurar calidad, seguridad, cumplimiento con aspectos legales y confiabilidad de los procesos de negocio y sistemas de información sujetos a auditoría. Tales controles se denominarán claves.

Un control clave se define como el control que es vital o de la mayor importancia para asegurar el correcto funcionamiento de los procesos, sistemas y las actividades del negocio sujetas a auditoría.

Los controles claves son aquellos que, a juicio del auditor, son indispensables para evitar o detectar y corregir el efecto o la probabilidad de ocurrencia de las causas de riesgo que generan riesgo alto. También, pueden considerarse claves aquellos controles que con mayor frecuencia actúan sobre varias causas de

riesgo, es decir, tienen efecto múltiple. Se asume que entre mayor frecuencia tenga un control, mayor será su importancia y por consiguiente podrá ser considerado clave.

Otro criterio que podría emplear el auditor para seleccionar los controles clave es la clase de control. Por ejemplo, podría decidir seleccionar una muestra de controles automatizados y otra muestra de controles manuales.

4.3.4 Ejecución de las pruebas de auditoría

La siguiente etapa del proceso de auditoría consiste en ejecutar el plan de pruebas de auditoría especificado en la etapa anterior. Estas pruebas pueden ser asistidas por computador o completamente manuales. Por cada prueba que se ejecute deben adjuntarse los soportes correspondientes. Estos consisten en documentos, archivos, programas de computador y cualquier otra evidencia que compruebe la ejecución de la prueba y muestre los resultados obtenidos.

Como resultado de las pruebas de auditoría ejecutadas, se obtienen entre otros los siguientes soportes:

- Lista de comprobación de controles revisados por el auditor
- Documentación sobre los procedimientos y controles establecidos en los procesos de negocio o sistemas de información sujetos a auditoría
- Muestras de documentos, listados y cualquier otro material de evidencia relacionado con deficiencias, debilidades o irregularidades identificadas por la auditoría
- Archivos de datos utilizados por el auditor en las pruebas de auditoría asistidas por computador

- Documentos con la preparación de las entrevistas y con las notas tomadas por el auditor durante su realización

- Documentación de los programas o scripts desarrollados por el auditor para realizar las pruebas asistidas por computador.

4.3.4.1 Herramientas de auditoría de Bases de datos

Los auditores pueden utilizar diferentes métodos para revisar los controles de las bases de datos en funcionamiento y las operaciones en el centro de servicios informáticos. Como se señala en Menkus (1991), “en el desarrollo y mantenimiento de sistemas informáticos en entornos de bases de datos, 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 Base de Datos”. El gran problema de las bases de datos es que su entorno cada vez es más complejo y no puede limitarse solo al propio SGBD.

A continuación se describe en qué consiste cada técnica o herramienta.

- *Sistema de Gestión de Bases de Datos (SGBD).* En cuanto a las funciones de auditoria que ofrece el propio sistema, todos los productos del mercado permiten registrar ciertas operaciones realizadas sobre la base de datos en un fichero de pistas de auditoria (*audit trail*). El auditor deberá revisar la utilización de todas las herramientas que ofrece el propio SGBD y las políticas y procedimientos que sobre su utilización haya definido el administrador.

- *Software de auditoria.* 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.

- *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 optima de la base de datos y de ciertos parámetros del SGBD y del SO.

- *Sistema Operativo.* El SO es una pieza clave del entorno, puesto que el SGBD se apoyara, en mayor o menor medida en los servicios que le ofrezca el SO en cuanto al control de memoria, gestión de áreas de almacenamiento interno (buffers), manejo de errores, control de confidencialidad, mecanismos de interbloqueo, etc. El auditor debe control de manera rigurosa la interfaz entre el SGBDS y el SO, debido a que en parte, constituye información reservada de los fabricantes de los productos.

- *Monitor de transacciones.* Algunos autores lo incluyen dentro del propio SGBD, pero actualmente, puede considerarse un elemento más del entorno con responsabilidades de confidencialidad y rendimiento.

- *Protocolos y Sistemas Distribuidos.* Cada vez más se está accediendo a las bases de datos a través de redes, con el riesgo de la violación de la confidencialidad e integridad. También las bases de datos distribuidas puede presentar graves riesgos de seguridad.

- *Paquetes 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

usuarios, 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.

- *Diccionarios de Datos.* Los propios diccionarios de datos se pueden auditar de manera análoga a la base de datos, las diferencias entre uno y el otro, residen principalmente en que un fallo en una base de datos puede atentar contra la integridad de los datos y producir un mayor riesgo financiero, mientras que un fallo en un diccionario de datos, pude llevar a una perdida de integridad de los procesos.

- *Herramientas CASE (Computer Aided System / Software Engineering) e IPSE(Integrated Project Support Environments).* Llevan incorporado un diccionarios de datos mucho mas amplio donde se almacenan además de información sobre datos, programas, usuarios, etc, los diagramas, matrices y grafos de ayuda del diseño.

- *Lenguaje de Cuarta Generación (L4G) independientes.* Además de las herramientas que ofrezca el propio SGBD, el auditor se puede encontrar con una amplia gama de generadores de aplicaciones, de formas, de informes, etc. Que actúan sobre la base de datos y que por tanto, también son un elemento importante a considerar en el entorno de SGBD. El auditor deberá estudiar los controles disponibles en los L4G utilizados en la empresa, analizando con atención si permiten construir procedimientos de control y auditoria dentro de las aplicaciones y, en caso negativo, recomendar su construcción utilizando lenguajes de tercera generación.

- *Facilidades de usuarios.* Con la aparición de interfaces graficas fácil de utilizar se han desarrollado toda una serie de herramientas que permiten al usuario final acceder a los datos sin tener que conocer la sintaxis de los

lenguajes de SGBD. También se puede incluir las diferentes facilidades que ofrecen algunos SGBD que permiten la conexión con paquetes ofimáticos, pudiendo acceder a la base de datos. El auditor debe tener atención en los procedimientos de carga y descarga de datos.

- *Herramienta de Minería de Datos.* Estas herramientas ofrecen soporte a la toma de decisiones sobre datos de calidad integrados en el almacén de datos.

4.3.4.2 Técnicas para probar los controles en los sistemas

Se utilizan para probar cálculos, programas o aplicaciones completas con el propósito de evaluar los controles, verificar la exactitud del procesamiento y el cumplimiento con los procedimientos de procesamiento establecidos.

Tales técnicas son usadas para dos propósitos: evaluar los sistemas de aplicación y probar el cumplimiento.

Método de datos de prueba. Este procedimiento ejecuta programas de aplicación de computador utilizando archivos de datos de prueba y verifica la exactitud del procesamiento comparando los resultados del procesamiento de los datos de prueba con los resultados predeterminados para la prueba. Los auditores usan esta técnica para probar la lógica del procesamiento seleccionado, las rutinas de cálculos y las características de control dentro de los sistemas de información. Los datos de prueba son transacciones simuladas que incluyen idealmente todo tipo de condiciones posibles, incluyendo aquellas que el sistema es incapaz de manejar, debido a la carencia de controles apropiados. Quiere decir esto, que la lista de transacciones simuladas debería probar condiciones tanto válidas como

inválidas. Los datos de prueba deben ser procesados con los programas regulares del sistema.

Propósito de los datos de prueba. El auditor no puede ver físicamente las operaciones y los controles dentro de la caja negra (sistema de información) pero puede ver un listado de los resultados de la prueba donde por ejemplo, algunas transacciones que deberían ser rechazadas no lo fueron o donde condiciones de desbordamiento causaron errores o transacciones fuera de límite fueron procesadas como si fueran correctas (ejemplo transacciones de clientes que exceden el límite de crédito). El auditor también puede determinar si la caja negra está procesando apropiadamente las transacciones válidas. El uso de los datos de prueba abre ventanas en la caja negra, porque las transacciones simuladas se procesan en el sistema de computador y generan resultados que son comparados por el auditor con resultados esperados, preparados manualmente con anterioridad. Es decir, antes de ejecutar los datos de prueba, el auditor calcula los resultados que debería obtener y luego los compara con los obtenidos en la prueba.

¿Cómo preparar los datos de prueba? Generalmente, los datos de prueba se aplican de la siguiente manera:

- Se debe revisar todo el sistema de controles.

- Sobre la base de esta revisión se diseñan las transacciones para probar aspectos seleccionados del sistema o el sistema completo.

- Los datos de prueba se transcriben a los formatos de entrada al sistema.

- Los datos se convierten (graban) a medios utilizables por el computador. El auditor debe verificar la conversión mediante rutinas de balanceo o en los listados de validación que se produzcan. Además, debe guardar el medio magnético que contiene la información hasta cuando realice la prueba.

Ventajas y desventajas de los datos de prueba

- Ventajas:
  - Su uso puede limitarse a funciones específicas del programa, minimizando el alcance de la prueba y su complejidad
  - Es una buena herramienta de aprendizaje para los auditores porque su uso requiere mínimos conocimientos de informática
  - No se requiere que el auditor tenga grandes conocimientos técnicos
  - Tiene buena aplicación donde son pocas las variaciones y combinaciones de transacciones
  - Da una evaluación y verificación objetiva de los controles de programa y de otras operaciones que serían impracticables por otros medios
  - Los datos de prueba se podrían correr sorpresivamente para descubrir la posible modificación de programas sin autorización e incrementar la efectividad de otras pruebas realizadas

- Desventajas:

    - Se requiere bastante cantidad de tiempo y esfuerzo para preparar y mantener un lote de datos de prueba representativo. Cualquier cambio en programas, diseño de registros y sistema implican cambiar los datos de prueba.

    - En algunos casos el auditor puede no probar el sistema que realmente está en producción

    - En un sistema complejo con gran variedad de transacciones es difícil anticipar todas las condiciones significativas y las variables que deberían probarse.

    - El auditor debe estar bastante relacionado con la lógica de programación que está probando

    - La prueba en si misma no detecta todos los errores. Cuando los programas son muy complejos, pueden existir infinidad de rutas y es muy difícil seguirlas todas

    - Hay una probabilidad muy alta que los datos de prueba no detecten manipulaciones inadecuadas de una cuenta o cantidad específica

4.3.5 Análisis del resultado de las pruebas de auditoría

El objetivo de esta etapa es analizar y evaluar los resultados de las pruebas de cumplimiento y sustantivas, efectuadas en la etapa anterior, con el propósito de

obtener conclusiones de la auditoría sobre el funcionamiento de los procesos de negocio y sistemas de información objeto de la auditoría.

En esta etapa, se analizan los resultados de las pruebas de auditoría que fueron ejecutadas por medios manuales o asistidas por computador y se generan indicadores de la protección existente para cada control clave asociado con los procesos de negocio y sistemas sujetos a auditoría. Los resultados pueden ser satisfactorios o insatisfactorios y de ellos se generan observaciones que son analizadas para determinar su impacto en el negocio.

Las observaciones se refieren a desviaciones que se detectan en las pruebas de auditoría, respecto a los estándares, de la tecnología de información, a la normativa legal y las políticas y procedimientos establecidos en la organización.

Como resultado del análisis y evaluación de los resultados de las pruebas de auditoría ejecutadas, se obtienen los siguientes productos:

- Lista de controles clave comprobados por el auditor en terreno.

- Documentación de las observaciones de auditoría obtenidas como resultado de las pruebas de cumplimiento y sustantivas, el análisis de las deficiencias identificadas y/o oportunidades de mejoramiento.

Evaluación del resultado de las pruebas de cumplimiento. El análisis de los resultados de las pruebas de cumplimiento se realiza utilizando la agrupación de controles por técnica de comprobación.

Por cada técnica de comprobación utilizada, para todo el proceso de negocio o el sistema de información, el auditor procede a analizar los resultados obtenidos como se indica a continuación:

- Por el grupo de controles verificados con una misma técnica de comprobación, establecer globalmente si los resultados de la prueba son satisfactorios o no satisfactorios y generar una conclusión de la auditoría.

- Desarrollar las observaciones de auditoría. Por cada técnica de comprobación utilizada se pueden generar una o más observaciones.

- Consolidar los resultados de las pruebas de auditoría.

El análisis del grado de satisfacción de los objetivos de control para las pruebas de cumplimiento se realiza utilizando la agrupación de controles por objetivo de control.

Las respuestas obtenidas para cada uno de los objetivos de control sustanciados por el auditor, se procesan siguiendo los pasos que se indican a continuación:

1. Por cada objetivo de control seleccionado, calificar el grado de satisfacción según los resultados de las pruebas efectuadas

Para evaluar el grado de protección de los controles agrupados por objetivo de control, es necesario registrar al menos una observación por cada control verificado con resultado insatisfactorio.

Un control verificado con resultado insatisfactorio puede estar asociado a varios objetivos de control. Por consiguiente, una observación puede impactar a varios objetivos de control.

2. Para cada control verificado con resultado insatisfactorio, desarrollar una observación de auditoría

A cada objetivo de control pueden corresponder varias observaciones, al menos uno por cada control que presenta resultado insatisfactorio.

Si un control que presenta resultado insatisfactorio está asociado con varios objetivos de control, es suficiente con desarrollar una sola vez la observación, analizando su impacto en todos los objetivos relacionados con el control.

Esta última etapa permite consolidar las calificaciones del grado de satisfacción de los objetivos de control para cada proceso de negocio y sistema de información.

Evaluación de los resultados de las pruebas sustantivas. Para analizar los resultados de las pruebas sustantivas, el auditor procede como se indica a continuación:

1. Establecer si los resultados de la prueba sustantivas son satisfactorios o no

Para los datos claves verificados por cada proceso de negocio o sistema de información, se debe concluir si los resultados de las pruebas son satisfactorios o no y generar una observación de auditoría por cada prueba con resultado negativo.

2. Desarrollar las observaciones de auditoría

Por cada dato verificado se pueden generar una o varias observaciones.

4.4 FASE III: COMUNICACIÓN DE LOS RESULTADOS

Esta es la última fase de la auditoría, en ella se resumen los resultados más significativos obtenidos en las etapas anteriores.

Estos son los insumos para elaborar el informe de auditoría con el cual se comunicará a la alta dirección y a los demás interesados, las observaciones y conclusiones sobre las características de seguridad, calidad y confiabilidad de la información y de los recursos tecnológicos y humanos que intervienen en las actividades de control de los procesos de negocio y sistemas de información.

4.4.1 Elaboración de los informes con los resultados de la auditoría

Los informes tienen como objetivo comunicar al servicio sobre el resultado de la auditoría, que éste conteste cada una de las observaciones con los antecedentes pertinentes y posteriormente se elabore y envíe el informe final con las conclusiones de la auditoría.

4.4.2 Estructura y contenido de los informes

El objetivo del informe preliminar es comunicar al servicio las observaciones encontradas, suscitar la respuesta con las acciones de mejoramiento para solucionar los problemas detectados.

El propósito del informe final es atender las respuestas del servicio a las observaciones y desarrollar las conclusiones de auditoría.

El informe preliminar consta de las siguientes tres secciones:

a) Objetivos y alcance de la auditoría

Breve descripción de los objetivos que se propuso la auditoría, de los aspectos de seguridad examinados, los objetivos de controles y las dependencias en las que se efectuó la revisión. También, se mencionan el período de tiempo que cubrió la revisión y el rango de las fechas durante las cuales se efectuó la auditoría.

Se describen los objetivos específicos fijados en el programa de auditoría. Para definir el alcance, se detallan los aspectos de control generales revisados (objetivos de control básicos) por la auditoría. Este párrafo es importante como punto de referencia para que el destinatario evalúe la importancia de las observaciones detectadas por la auditoría.

b) Antecedentes generales

Este capítulo contiene una breve descripción de las características y atributos del área auditada. El objetivo es ubicar al destinatario del informe dentro de un marco de referencia que le ayude a comprender el informe y la importancia de las observaciones de la auditoría.

c) Observaciones de la auditoría

Esta parte del informe presenta, para cada proceso y sistema evaluado, las observaciones y debilidades de control identificados por la auditoría que debe contestar la administración.

Para elaborar el informe final de auditoría, se realiza lo siguiente:

Luego de recibir la respuesta al informe preliminar, el auditor analiza los descargos y antecedentes enviados por el servicio y desarrolla las conclusiones para cada observación y la conclusión general de la auditoría.

4.4.3 Aseguramiento de la calidad de los informes de auditoría

Verificar que la forma y el contenido del informe con los resultados de la auditoría cumplan con el mínimo exigidos por los estándares y las mejores prácticas recomendados por los expertos. Si alguna de las respuestas a las preguntas que se incluyen a continuación es negativa, significa que el informe necesita más trabajo de revisión.

Lista de comprobación de calidad de los informes de auditoría.

1. ¿Todos los puntos del informe atañen al destinatario del mismo?

2. ¿Todas las observaciones incluidas en el informe fueron respondidas por el auditado para determinar su exactitud?

3. ¿Todas las observaciones y conclusiones incluidas en el informe son suficientemente explícitas, para que las áreas entiendan su significado e importancia y se motiven a tomar acciones correctivas?

4. ¿Todas las observaciones incluidas en el informe son lo suficientemente importantes como para justificar el tiempo que el auditado dedique a su lectura?

5. ¿En los papeles de trabajo existe suficiente evidencia para soportar las observaciones y conclusiones de la auditoría?

6. ¿Todas las conclusiones incluidas en el informe fueron evaluadas con suficiente detalle para determinar su costo/beneficio?

7. ¿Si las conclusiones incluidas no son viables por costo/beneficio, otras circunstancias justifican su inclusión en el informe?

8. ¿En el informe se incluyen únicamente puntos que tienen alto potencial de pérdidas y bajo costo correctivo?

9. ¿Tienen sentido los títulos utilizados para encabezar las observaciones?

10. ¿El informe cumple con las expectativas de la jefatura?

11. ¿Existe claridad en los beneficios para los auditados que justifican la incorporación de las observaciones de control interno especificadas en el informe final?

12. ¿El informe se emite oportunamente de modo que el máximo beneficio pueda obtenerse de él?

Las observaciones y puntos mejorables deberán incluir exclusivamente aspectos que sean importantes, de beneficio para el servicio y factibles de implantar sin causar costos significativos. Cada punto tendrá asignado un número de secuencia y un título que exprese de manera resumida lo que se detectó, utilizando un lenguaje positivo y constructivo.

A continuación, se deben presentar los beneficios que obtendrá el servicio auditado al solucionar la deficiencia o problema observado. Es aquí donde el auditor debe mostrar que su trabajo contribuye al mejoramiento de los procesos y sistemas de la organización.

Para cada observación de la auditoría siempre se deberán expresar los beneficios para la organización. Como por ejemplo, para incrementar la eficiencia, prestar un

mejor servicio a los usuarios, ahorrar costos, evitar que los errores pasen inadvertidos, mejorar la información que recibe la alta dirección, etc.

- El beneficio debe enfocarse para el usuario, no para el auditor
- No decir que el beneficio es mejorar el control interno. Tampoco que es para mejorar los procedimientos
- Evitar decir: “Es necesario que se establezcan controles de acceso”, es decir “es necesario establecer controles de acceso”
- Deberá expresarse con palabras que describan la realidad de la manera más exacta posible y con un lenguaje simple
- Se escribe en infinitivo
- Evitar el uso de superlativos

La conclusión de la auditoría debe expresar su concepto sobre la protección que ofrecen los controles y procedimientos utilizados por la organización para asegurar la confiabilidad de los procesos y sistemas auditados.

4.4.4 Seguimiento a las observaciones de la auditoría

El objetivo de esta etapa es establecer las fechas de compromiso para verificar que los responsables de las observaciones detectadas, inicien e implementen las acciones correctivas.

En esta etapa se acuerda con los auditados, las fechas de compromiso para atender las observaciones de la auditoría. También, se definen los responsables de atender estos compromisos y se registran los datos de planeación del seguimiento, además de las fechas específicas para verificar dicho seguimiento, junto con los cargos de los responsables de verificar el seguimiento y los

resultados del mismo. Con las actividades de esta etapa se termina el trabajo de auditoría.

Los productos de esta etapa son los siguientes:

- Programa de seguimiento del informe final
- Listado con verificación de cada observación pendiente
- Emisión del informe con los resultados del seguimiento

4.4.5 Planificar el seguimiento a las observaciones de la auditoría

Elaborar tabla con los siguientes encabezados:

- Observación
- Cargo responsable de tomar la acción
- Fecha de compromiso para implantar la acción de mejoramiento
- Fecha de seguimiento prevista

Establecer fechas de compromiso de común acuerdo con el encargado de cada observación:

- Fijar una fecha de compromiso
- Fijar una fecha de seguimiento
- Fijar una alerta de compromiso y seguimiento

Ejecutar el seguimiento a las observaciones de la auditoría. El objetivo es verificar que se hayan implantado las acciones correctivas requeridas para atender las observaciones informadas por la auditoría. Con el fin de establecer políticas,

normas y procedimientos acordes a mejorar las deficiencias encontradas en los procesos de negocio y sistemas de información.

Establecer una descripción detallada de la acción implantada y la opinión del auditor al respecto, así como los comentarios del auditado y sus respectivas conclusiones con respecto a la acción implantada.

Informe de seguimiento de la auditoría. Al finalizar el seguimiento se elabora el informe con la información definida en la planificación del seguimiento.

- Observaciones corregidas, pendientes de implementar y no implementadas.
- Porcentajes total de observaciones implementadas.
- Conclusión del proceso de seguimiento.

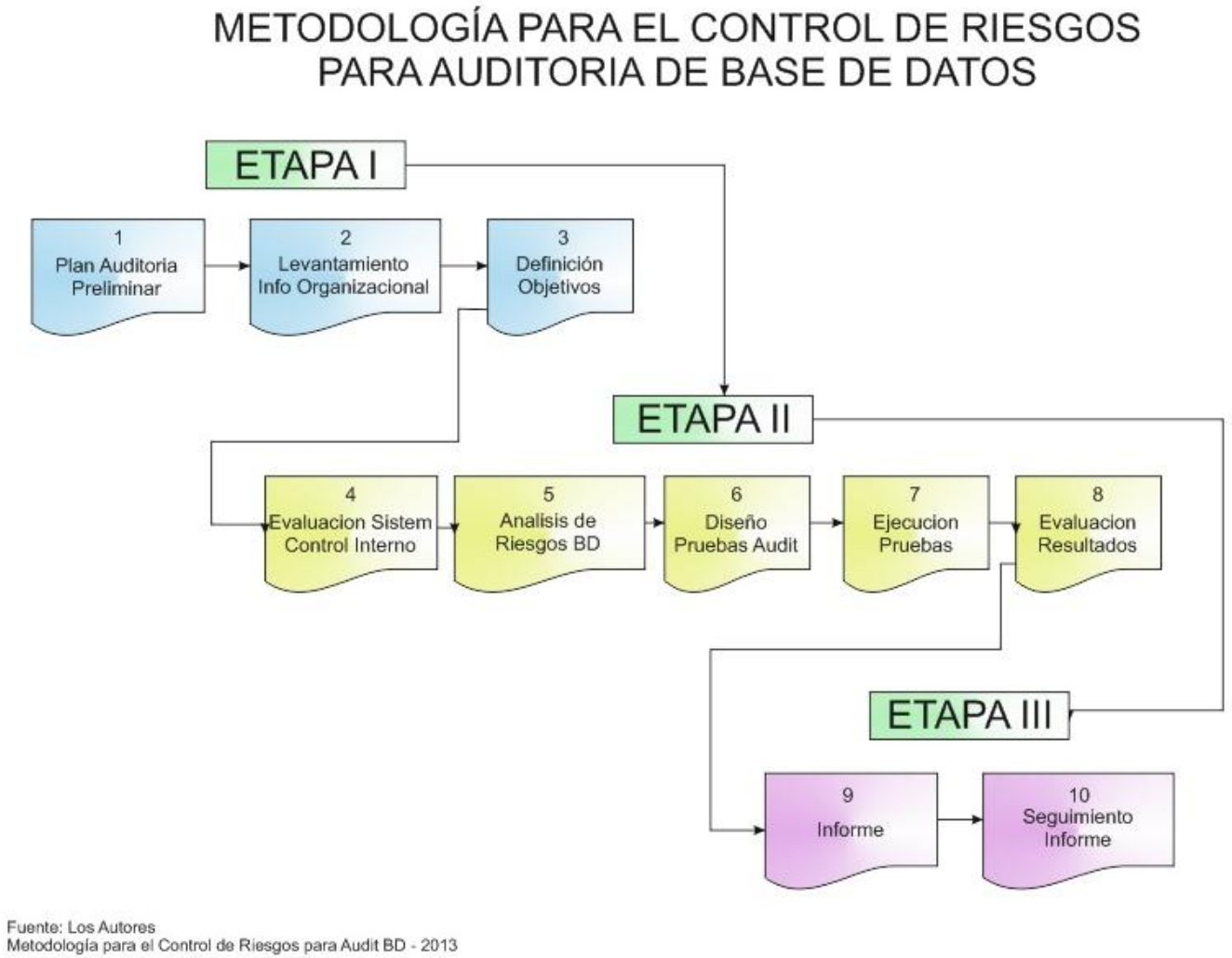


Figura 10. Metodología para el Control de Riesgos para Auditoria de B.D

CAPITULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La complejidad de la tecnología de bases de datos y su entorno crecen aceleradamente, por tanto su auditoría y control requieren de personal capacitado y con los conocimientos claros de la función que realizan. La presente metodología fue realizada con el propósito de ser fuente de información para auditores que desean incrementar su experiencia en la auditoria de bases de datos y el conocimiento de sus riesgos y vulnerabilidades.

La metodología para control de riesgos para auditoria de bases de datos, permite que el auditor y su equipo utilizar un criterio uniforme para seleccionar los objetivos de control y herramientas de auditoría que los conducirá a la obtención de un informe fundamentado en estándares conocidos a nivel internacional.

La incorporación del estándar COBIT 4.0 y la norma técnica ISO/IEC 27002 a la metodología propuesta, es una fortaleza que ayuda a los auditores a orientarse de mejor forma respecto a los requisitos del negocio que tienen relación con el uso de la tecnología. Cada día surgen nuevas tendencias y productos que aparentemente ayudan a cumplir de forma más eficiente y eficaz los objetivos planteados por la organización pero que, por otro lado, aumentan la complejidad con la cual deben lidiar los directores y ejecutivos a cargo de la administración.

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones especialmente a las bases de datos, debe ser ejecutada bajo una estrategia como la metodología propuesta, que permita a las Entidades Fiscalizadoras mantener una superioridad tecnológica sobre las entidades sujetas a fiscalización, para vigilar, controlar, regular, monitorear y actuar ante los avances de las TIC.

La especialización en áreas TIC dentro del desarrollo continuo del talento humano de los auditores es de vital importancia para que los auditores estén actualizados y sean competentes en la ejecución de la auditoria a la gestión de las Tics.

La metodología propuesta permite la revisión y la evaluación de los controles, riesgos, vulnerabilidades y amenazas a las bases de datos de las organizaciones, a fin de que por medio del señalamiento se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Durante el desarrollo de este proyecto se pudo observar la creciente dependencia de toda organización en su activo informático más importante “la información”, ésta debe ser correctamente gestionada, controlada, auditada y asegurada por medio de controles que prevengan la ocurrencia de situaciones de riesgo para la organización y que a su vez asegure su integridad, disponibilidad y confidencialidad tanto de los datos como de los procesos.

5.2 RECOMENDACIONES

La metodología para control de riesgos para auditoria de bases de datos se convertirá en una fuente de información para los auditores de sistemas de información que dentro de sus funciones, auditen y controles los riesgos que a diario está expuesta las centrales de información.

El trabajo propuesto podrá ser utilizado como material bibliográfico para la academia, lo que permitirá sintetizar en un solo documento las normas internaciones de auditoria y los métodos de buenas prácticas para auditoria de sistemas de información.

Convertir la metodología propuesta a una serie de buenas prácticas para auditoria de bases de datos, promulgara la confiabilidad y el buen uso de su contenido.

La metodología propuesta puede ser complemento para procesos de auditoria que se realicen en las organizaciones, logrando incrementar su uso y mejorando sus buenas practicas.

GLOSARIO

- ANALISIS DE RIESGO: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.

- AMENAZA: persona o cosa vista como posible fuente de peligro o catástrofe. Ejemplos: inundación, incendio, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.

- DML: (data manipulation language) dentro del lenguaje SQL, son las sentencias cuya ejecución modifica la información al interior de la base de datos. Estas sentencias son insert, update, delete, etc.

- DDL: (data definition language) dentro del lenguaje SQL, son las sentencias cuya ejecución devuelve información almacenada dependiendo de los criterios usados. Create y alter son sentencias DDL.

- EXPOSICION O IMPACTO: la evaluación del efecto del riesgo. Ejemplos: vidas humanas, imagen de la empresa, honor, defensa nacional, etc.

- OBJETO DE BASE DE DATOS: son las estructuras usadas dentro de un gestor de bases de datos para almacenar y controlar la información. Dentro de estas encontramos: tablas, vistas, procedimientos almacenados, triggers, índices, secuencias.

- RIESGO: la probabilidad de que una amenaza llegue a acaerce por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes.

- TRIGGER: es una serie de instrucciones que se ejecutan cuando se produce algún evento dentro de la base de datos.

- VULNERABILIDAD: la situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaerce y así afectar el entorno informático. Ejemplos: falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de soportes magnéticos, falta de cifrado en las telecomunicaciones, etc.

REFERENCIAS BIBLIOGRAFICAS

CARVAJAL, Armando. Análisis y gestión de riesgos, base fundamental del SGSI. Caso: Metodología Magerit. VIII Jornada Nacional de Seguridad Informática ACIS. Junio 2008

FIERRO MONTENEGRO, Ondyna Lilian. GARCIA PINCHAO, Juan Carlos. SABDO: Sistema de auditoria para bases de datos de Oracle. Proyecto previo aprobación para la obtención del título de Ingeniero en Sistemas Computacionales. Escuela de Ingenierías en Sistemas Computacionales Ibarra (Ecuador). Abril 2009

INGRAVALLO, Hector Gabriel. ENTRAIGAS, Valeria Elizabeth. Auditoria de Bases de Datos. Tesis de Grado. Universidad Nacional de la Patagonia San Juan Bosco. Argentina. 2007

LIBARATORI, Héctor Pedro. Administración y auditorias para las Bases de Datos. Ponencia presentada en las Jornadas Informáticas del Centro de Ingenieros de Jujuy. Argentina. 2011

MAULINI R., Mauro. Las diez (10) vulnerabilidades más comunes de las bases de datos. Artículo de la página web www.e-securing.com. 2011

PINTO, Fred. Retos en la seguridad de las Bases de Datos. Ponencia presentada en la X Jornada de Seguridad informática ACIS. Colombia. Junio de 2010

PLATA SANCHEZ, David. PONCE CASANOVA, Eduardo Hilario. Metodología para auditar tecnologías de información. Universidad Nacional Autónoma de México. 2009

RAMIREZ AGUILAR, Efrén. TORRES FLORES, Irais Elena. YAÑEZ MORALES, Judith Oralia. MOSQUERA JARAMILLO, Yazmín. Auditoria a la Base de Datos SQL del Sistema “Seguridad de Presas” Conagua. Tesina. Instituto Politécnico Nacional de México D.F. Agosto de 2010

REYES LAZO, Alberto. VILLACORTA MORAN, Antonio. Auditoria de gestión a las tecnologías de la información y comunicaciones. Trabajo de Investigación. XIV Concurso anual de investigación de la OLACEFS. Corte de Cuentas de la Republica de El Salvador. Octubre de 2011.

SALVADOR MONTERROSA, José. IGLESIAS, Carlos Eduardo. Manual de auditoria de gestión a las tecnologías de información. Trabajo de Investigación. XIV Concurso anual de investigación de la OLACEFS. Corte de Cuentas de la Republica de El Salvador. Octubre 2011

VALLEJO URIBE, Lucas. Sistema para la gestión de auditorías en base de datos. Trabajo de grado para optar al título de ingeniero informático. Escuela de Ingeniería de Antioquia (Colombia). 2008

YAÑEZ DE LA MELENA, Carlos. IBSEN MUÑOZ, Sigfrid Enrique. Enfoque metodológico de la auditoría a las tecnologías de información y comunicaciones. Trabajo de investigación para la participación al XIV Concurso Anual de Investigación Investigación “Auditoria de Gestión a las Tecnologías de Información y Comunicación”. Contraloría General de la República de Chile. Octubre de 2011.

BIBLIOGRAFIA GENERAL

CAMISON, Cesar. La gestión de la calidad por procesos. Técnicas y herramientas de calidad. Cap. 6: Métodos para la mejora y el desarrollo de procesos. 2009 http://www.mailxmail.com/curso-gestion-calidad-procesos-tecnicas-herramientas-calidad

CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. Ley de la protección y de los datos.2009. www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

CONGRESO DE LA REPUBLICA. Ley 527 de 1999. Ley que reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. 1999

CONGRESO NACIONAL DE PROFESIONALES DE CIENCIAS ECONOMICAS. Auditoria de Sistemas con Enfoque en procesos. Riesgos y Controles. Ciudad Autónoma de Buenos Aires. Junio 2010

DUEÑAS GOMEZ, Luis Ángel. Controles y Auditorias de los Sistemas de Información. 1ra Ed. Orión Editores Ltda. Santafé de Bogotá, D.C. Colombia. Marzo de 2000

ECHENIQUE GARCIA, José Antonio. Auditoria en Informática. McGRAW-HILL Interamericana de México SA de CV. México, 1990

ELMASRI, Ramez. NAVATHE, Shamkant B. Sistemas de Bases de Datos Conceptos Fundamentales. 2da Ed. Versión en Español de Roberto Escalona García, México. DF. 2000

FRANKLIN F., Enrique Benjamín. Auditoria Administrativa. 1ra Ed. Editorial McGraw-Hill Interamericana Editores. México 2001

GOMEZ ALZATE, Jorge Eduardo. Introducción al Control de Procesos. Universidad Tecnológica de Pereira. 1990

HERNANDEZ ALVAREZ, Giovanni. Legislación Colombiana e Internacional en computación, auditoria de sistemas y microfilmación. Ediciones Jurídicas Gustavo Ibañez. Colombia. 1993

MAGERIT- Versión 3.0. Metodología de Análisis y Gestión de riesgos de los sistemas de Información. Dirección General de Modernización Administrativa. Ministerio de Hacienda y Administraciones Públicas. Gobierno de España. Madrid. Octubre de 2012

PIATTINI VELTHUIS, Mario Gerardo. NAVARRO, Emilio del Peso. Auditoria Informática Un enfoque Práctico. Alfaomega Grupo Editor SA de CV. Santafé de Bogotá, Colombia. 1998

VIII Jornada Nacional de la Seguridad Informática ACIS. Junio 2008
http://www.acis.org.co/

W. LOTT, Richard. Auditing the Data Processing Function.Editorial AMACOM.New York 1981.