UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS

CARRERA DE CONTADURIA PÚBLICA

MÉTODO DE GESTIÓN DE RIESGOS PARA LA AUDITORÍA DE BASE DE DATOS RELACIONAL

Proyecto de Grado para la obtención de Titulo de Licenciatura

Postulante: Nitza Sauter Estevez

Tutor: M.Sc. Miguel Cotaña Mier

La Paz – Bolivia

2016

DEDICATORIA

A mi madre Lizett, quien con su ejemplo de amor, respeto y sacrificio me demostró que la brecha de lo imposible y posible lo determina la voluntad.

A mi abuela Hilda, quien con su fortaleza y determinación me enseño que la edad no es un obstáculo para conseguir lo que uno quiere.

A mis hermanos Edson y Raydel, quienes con amor y paciencia me alentaron para lograr terminar este proyecto.

AGRADECIMIENTO

A mi tutor M. Sc. Miguel Cotaña Mier por su valiosa colaboración en el desarrollo del proyecto.

A Grover Choque, quien en la meta establecida fue base fundamental con su apoyo incondicional y paciencia.

A Daniela Arredondo, por su apoyo en el trayecto de la vida universitaria.

INDICE

RESUMEN EJECUTIVO

El crecimiento en el uso de los Sistemas de Información y la prestación de servicios basados en ambientes tecnológicos, accesos remotos y de almacenamiento de información en medios electrónicos incrementa la problemática actual de seguridad. Este es un aspecto de vital importancia, dado el incremento de las amenazas y nivel de vulnerabilidades que el uso de las TI representa para la Empresa, En este sentido, la gestión de riesgos debe formar parte de la cultura organizacional, quienes gestionan el riesgo de forma eficaz y eficiente, tienen más probabilidad de alcanzar sus objetivos y hacerlo a menor costo.

El desarrollo de un método de Gestión de Riesgos para la Auditoría de Base 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 actividades, acciones y tareas metódicos que apunten a lo que se quiere concluir y que genere una lista de recomendaciones que mejoren las falencias encontradas.

La gestión de riesgos en ambientes tecnológicos, bajo estándares internacionales, es relativamente nueva por lo que la aplicación del modelo, puede definirse como un proceso sistemático, por el cual el auditor de Base de Datos Relacional obtiene y evalúa objetivamente evidencias respecto a afirmaciones sobre el objeto que es sometido a análisis con el fin de formarse una opinión sobre ello y reportar sobre el grado en que dicha afirmación se ajusta a un conjunto de estándares. Para la ejecución de cada etapa del modelo, se considera los elementos de entrada, procesamiento de esos elementos de entrada y generar elementos de salida.

Al utilizar el método, podrán evaluar el contenido de las diferentes actividades y aplicar los controles que considere necesario en forma sistemática y disciplinada con el objetivo de minimizar los riesgos y lograr los objetivos.

CAPITULO 1

Marco Introductorio

1. Introducción

Desde los comienzos de la computación, los recursos informáticos (incluyendo la información), han estado expuestos a una serie de peligros o riesgos que han aumentado y evolucionado conforme se globalizan las comunicaciones; de otro lado, el acceso a las Tecnologías de Información y Comunicaciones (TICs), ha generado un incremento en las oportunidades para obtener información, el cual a su vez es directamente proporcional al número de eventuales y posibles amenazas que de ello se desprenden.

Estas amenazas exponen a las organizaciones a riesgos que pueden impactar la seguridad de los sistemas, la continuidad de las operaciones, la materialización de los fraudes (Internos o externos), producir daños en la infraestructura y la consecuente pérdida o alteración de información sensible, así como multas, sanciones, daños a la infraestructura, entre otros aspectos.

Las Bases de Datos (BD) no protegidas son el sueño de cualquier ciberdelincuente. Contienen los datos más valiosos de la empresa, blanco fácil de un ataque. No es de extrañar que las bases de datos sean el objetivo principal de los ciberataques más sofisticado de los hackers y, cada vez más, de usuarios que trabajan en la empresa y que cuentan con determinados privilegios.

Las bases de datos son el centro de atención para cualquier institución y/o empresa de hoy en día, ya que constituyen uno de los soportes fundamentales para el proceso de toma de decisiones gerenciales; de ahí la importancia de que los datos guardados en ellas sean confiables y de calidad. Uno de los procesos en la construcción de estas y que contribuye a lograr este objetivo, es la limpieza de los datos.

Las empresas están tomando consciencia de la importancia de la calidad de sus datos para ahorrar costes y hacer rentables las inversiones realizadas en los complejos sistemas de CRM[(1)]. Empiezan a darse cuenta de que la calidad de los datos no es solo responsabilidad del área de Tecnología, sino de toda la empresa, puesto que es un asunto para situar en el mismo nivel que cualquier otro servicio crítico de la empresa.

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

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

El término Auditoria según donde se esté aplicando puede tener diferentes connotaciones. Una de ellas es "Proceso analítico que consiste en el examen de los libros, cuentas, comprobantes y registros de una empresa con el objeto de precisar si son correctos los estados financieros, de acuerdo con principios de contabilidad generalmente aceptados".

---

(1). CRM (Customer RelationShip Management). Gestión de las Relaciones con los Clientes.

También podemos encontrar otras definiciones posibles como: un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso.

La auditoría consiste en la emisión de una opinión profesional sobre un determinado objeto. El objeto, ahora es Tecnología de la Información (TI). Es de este aspecto que se deriva puntualmente la Auditoria de los Sistemas de Información o también llamadas Auditorias Informáticas.

Los términos anteriores involucran a sistemas automáticos de procesamiento, procesamiento no automático y sus correspondiente interfaces. Los sistemas automáticos de procesamiento son uno de los elementos que intervienen en la auditoria y tienen dos grandes componentes que son el hardware y el software.

La Auditoria de Bases de Datos es una temática relativamente nueva si consideramos que las Bases de Datos y los Sistemas Gestores de Bases de Datos (SGBD) que las manejan se han popularizado en estos últimos, no obstante la necesidad del control y registro del cambio de datos es un hecho que muchos profesionales siempre pensaron en poner en práctica.

El presente proyecto de grado, hace un aporte significativo al proporcionar un método y/o metodología para auditar procesos en la Base de Datos Relacional, basada en la gestión de riesgos.

2. Antecedentes

Todo tipo de empresa pequeña, mediana o grande, requieren que se analicen constante y regularmente todos los datos almacenados en la Base de Datos, con el fin de verificar su calidad y suficiencia en cuanto a los requerimientos de negocio para la información: control, integridad y confidencialidad.

Existen esfuerzos muy aislados en nuestro Estado Plurinacional para implementar auditorías a las Bases de Datos.

A nivel mundial, la revolución tecnológica aplicada a la Auditoría de Base de Datos, ha crecido a pasos agigantados.

La extracción de conocimiento a partir de los datos almacenados en una Base de Datos, implica ejecutar controles adecuados.

De la investigación efectuada, se ha podido consultar los siguientes trabajos existentes en la biblioteca de la Carrera de Contaduría Pública:

- ✓ Evaluación de los Sistemas de Información y su tecnología como base para determinar el grado de confianza en el procesamiento de la Información Financiera. Trabajo Dirigido, defendido el 2005 por: José Antonio Celis Rioja. El objetivo fue proporcionar a la auditoría financiera una metodología que contenga procedimientos y técnicas para evaluar los Sistemas de Información y su tecnología, y determinar el grado de confianza en el procesamiento de la información financiera.
- ✓ Un enfoque metodológico para auditoría de Tecnologías de la Información y Comunicaciones. Caso: Registro único para la administración tributaria municipal. Tesis de Grado, defendido el 2012 por: Janhett Ramos Maldonado. El

objetivo fue la elaboración y sistematización de un enfoque metodológico para la ejecución de auditorías de Tecnologías de la Información y Comunicación en el marco de las Normas de Auditoria Gubernamental de Tecnologías de la Información y Comunicación en los procesos tecnológicos de la administración pública.

3. Planteamiento del problema

Aún cuando el concepto de Tecnología Informática (TI) es aparentemente entendido y las necesidades y expectativas en el uso de ella pueden resultar claras para la gran mayoría de las personas, es común seguir observando la exposición de los riesgos en las TI, las cuales se encuentran relacionadas con elementos tales como:

- ✓ la seguridad,
- ✓ la continuidad del negocio,
- ✓ los fraudes (Internos o externos),
- ✓ daños en la infraestructura tecnológica,
- ✓ la pérdida, destrucción o modificación de información sensible,
- ✓ las multas o sanciones,

Por ello es necesario realizar análisis y diseñar instrumentos que mantengan controlados estos riesgos. En este caso, los controles son un instrumento que facilitan la actividad y minimizan los impactos negativos, manteniendo el riesgo en niveles adecuados. Para nuestro objeto de estudio, la Empresa Curtiembre "CUEROBOL requiere controles que mitiguen los riesgos producidos en el ámbito de sus activos informáticos.

Cuando no se tiene una capacidad de reacción ante las amenazas de seguridad antes de que afecten el negocio, se expone el patrimonio, la credibilidad y finalmente el futuro

de la organización, por lo tanto la administración de la seguridad de sus infraestructuras y el valor del negocio que ofrecen, se debe convertir en una preocupación primordial para cualquier empresa.

El crecimiento en el uso de los Sistemas de Información (SI) y la prestación de servicios basados en ambientes tecnológicos, accesos remotos y de almacenamiento de información en medios electrónicos incrementa la problemática actual de seguridad, tal como lo plantea la metodología ITIL en su versión 3. este es un aspecto de vital importancia que debe ser asumido a la brevedad, dado el incremento de las amenazas y nivel de vulnerabilidades que el uso de las TI representa para la Empresa, unido al escaso personal especializado y actualizado con la consecuente dificultad para establecer los impactos económicos en el nivel de riesgo.

En este sentido, la gestión de riesgos debe formar parte de la cultura organizacional, quienes gestionan el riesgo de forma eficaz y eficiente, tienen más probabilidad de alcanzar sus objetivos y hacerlo a menor costo.

Al evaluar el estado en los niveles de riesgos en TI (Tecnología Informática) a los cuales se encuentra expuesta la Empresa Curtiembre “CUEROBOL” y proponer unos controles que los mitiguen se busca dar respuesta a las expectativas a sus necesidades, encaminando los esfuerzos a optimizar las condiciones de seguridad y, lo que es esencial, a crear una cultura de seguridad y trabajo en equipo.

Los datos almacenados en una Base de Datos, adecuadamente interrelacionados, generan información. La información es el activo más importante con que cuenta cualquier organización y a través de ella la alta gerencia pueda tomar las mejores decisiones para generar ingresos y beneficios. Los procesos de negocio de la organización se basan exclusivamente en los datos que puedan suministrar de forma

íntegra y rápida. Para que esos 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 eficaces 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 la Información (TI) posiblemente capacitadas para cumplir sus funciones, no se puede 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 de Información (ASI) deben contar con un método y/o 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 un método y/o metodología que facilite las actividades en el proceso de auditoría de Base de Datos y que permita analizar, gestionar y controlar los riesgos existentes para detectar a tiempo y evitar que aprovechen las vulnerabilidades de los Sistemas de Información.

4. Formulación del problema

¿Será posible plantear un método para el control de riesgos para Bases de Datos, bajo el enfoque del modelo relacional, que facilite las actividades de los auditores y que permita analizar, gestionar y controlar los riesgos existentes evitando vulnerabilidades y amenazas en el registro y control de la Empresa Curtiembre "CUEROBOL"?

5. Objetivos

5.1. Objetivo General

Desarrollar un método de gestión de riesgos para la Auditoria de Bases de Datos, bajo el modelo relacional.

5.2. Objetivos Específicos

- ✓ Conocer el medio en el cual se desenvuelve la Empresa Curtiembre "CUEROBOL" para determinar el marco contextual y conceptual de la situación en estudio;
- ✓ Determinar las debilidades o vulnerabilidades del Sistemas de información empleado por la Empresa Curtiembre "CUEROBOL" y proponer algunos controles que puedan mitigar la materialización de los riesgos en TI.
- ✓ Investigar fuentes bibliográficas referentes a la práctica de la Auditoría de Sistemas y del diseño y análisis de métodos y/o metodologías para auditorias de sistemas basadas en riesgos;
- ✓ Fortalecer la metodología de administración de riesgos de la Empresa "CUEROBOL";
- ✓ Establecer mecanismos de control sobre los datos de la institución que permita prevenir los riesgos de administración de los mismos;

- ✓ Analizar e identificar los riesgos más comunes que afectan las bases de datos;
- ✓ Desarrollar el método.

6. Importancia y Justificación del Estudio

El desarrollo de un método y/o 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 actividades, acciones y tareas metódicos que apunten a lo que se quiere concluir y que genere una lista de recomendaciones que mejoren las falencias encontradas.

El adecuado aseguramiento de los recursos con que cuenta una organización es uno de los objetivos de la gestión de riesgos, entendido éste como la posibilidad de que cualquier amenaza explote una vulnerabilidad específica para causar daño a un activo, lo que genera en la organización una incertidumbre sobre los objetivos , sin que sea posible determinar el momento en que dicho evento adverso pueda presentarse, por lo que se hace necesario implementar instrumentos y herramientas que permitan tomar medidas para disminuir la probabilidad de que ésta se materialice y el consecuente impacto que pueda tener.

El riesgo está presente en la ejecución de cualquier actividad, por lo que las instituciones se ven en la necesidad de instrumentar metodologías y herramientas para la protección de sus activos, con la intención de gestionarlo y almacenarlo, de allí que sea indispensable reconocer los riesgos a los cuales se encuentra expuesta para adoptar controles que le permitan minimizar los efectos adversos que generan los procesos apoyados por las TI, que a su vez son originados en amenazas provenientes tanto del interior como del exterior de la Empresa.

Todo lo anterior se encuentra inmerso en un entorno en el cual los responsables de gestionar las herramientas tecnológicas deben contar con los controles necesarios que le permitan mitigar los riesgos a los cuales se ven expuestos en la gestión de sus procesos, pues en la actualidad no solamente ha cambiado el volumen del uso de la tecnología, hoy el acceso a los sistemas de información empleando las TI no es exclusivo de los profesionales en informática, a ellos pueden ingresar la casi totalidad de la población (Zamora, 2008); del mismo modo, el acceso a las TICs no sólo es posible con los recursos propios, también se extiende a otros organismos, pues no existen fronteras físicas debido posibilidad de conectividad a Internet y a la apertura de las redes corporativas. A su vez, el grado de complejidad de la tecnología utilizada ha aumentado considerablemente, tornándola cada vez más difícil de administrar, lo cual ha obligado a la elaboración de controles que puedan mitigar los riesgos inherentes a las TI, sus impactos y prevenir las amenazas que contribuyan a su materialización.

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 institucional.

6.1. Justificación económica

El uso de un método y/o metodología para la auditoría de Base de Datos Relacional agrega valor a la institución, porque minimiza costos teniendo a disposición una referencia metodológica.

6.2. Justificación social

Una nueva cultura de control, da paso de una sociedad industrial a una sociedad de sobreabundancia de información y comunicación; pasar de la simple idea de mitigar

riesgos y amenazas a la capacidad de brindar garantía razonable de integridad, confiabilidad, disponibilidad y auditabilidad de los datos contenidos en una Base de Datos.

6.3. Viabilidad

El alcance del objetivo de este trabajo será viable solo si los integrantes de la organización cambien de actitud. Y acepten que no podemos quedar aislados del resto del mundo en cuanto al control de la Base de Datos.

7. Alcances y aportes

7.1 Alcances

Es interés de este trabajo plasmar un documento que sin ser exhaustivo sea una guía para la introducción al estudio del tema de auditoria, en particular al de auditoria informática y más puntualmente al estudio de auditoria en Bases de Datos en lo referente a trazas de actividad generadas en el uso de datos sobre cualquier DBMS relacional.

El estudio de los tipos de Bases de Datos es extenso, por lo que limitaremos nuestro alcance a Bases de Datos Relacional.

Nos apoyaremos en conceptos de gestión de riesgos, bajo el modelo ISO y las Normas de Auditoria Gubernamental, son de aplicación obligatoria en nuestro Estado Plurinacional, para entidades públicas, bajo los siguientes enfoques:

- ✓ Enfoque a las seguridades;
- ✓ Enfoque a la información;

- ✓ Enfoque a la infraestructura tecnológica;
- ✓ Enfoque al software de aplicación;
- ✓ Enfoque a las comunicaciones y redes.

7.2 Aportes

El presente trabajo permite a quien lo aborde utilizar su ingenio y pericia para crear mecanismos que realicen auditoria sobre los datos; de allí que los destinatarios más beneficiados serán profesionales en sistemas y auditoria que requieran una referencia metodológica específica y sencilla que les brinde la capacidad de realizar controles efectivos.

Por lo que se propone y diseñar un método y/o metodología de gestión de riesgos para la ejecución de auditorías de Bases de Datos Relacional.

CAPITULO II

Marco Institucional

2. MARCO INSTITUCIONAL

2.1. Introducción

La empresa de cueros "CUERBOL" funciona desde hace aproximadamente 19 años en Viacha, periodo en el cual ha incrementado su desarrollo industrial, productivo y tecnológico, teniendo preferencia en exportación a Perú y licitaciones en territorio Boliviano.

Especializados en la obtención de cueros de vaca para calzados y chamarras cuenta con un personal altamente capacitado que le permite a la empresa tener un alto prestigio.

2.2. Conformación Jurídica y Administrativa

2.2.1. Identificación de la Empresa

La empresa se identifica con los siguientes datos:

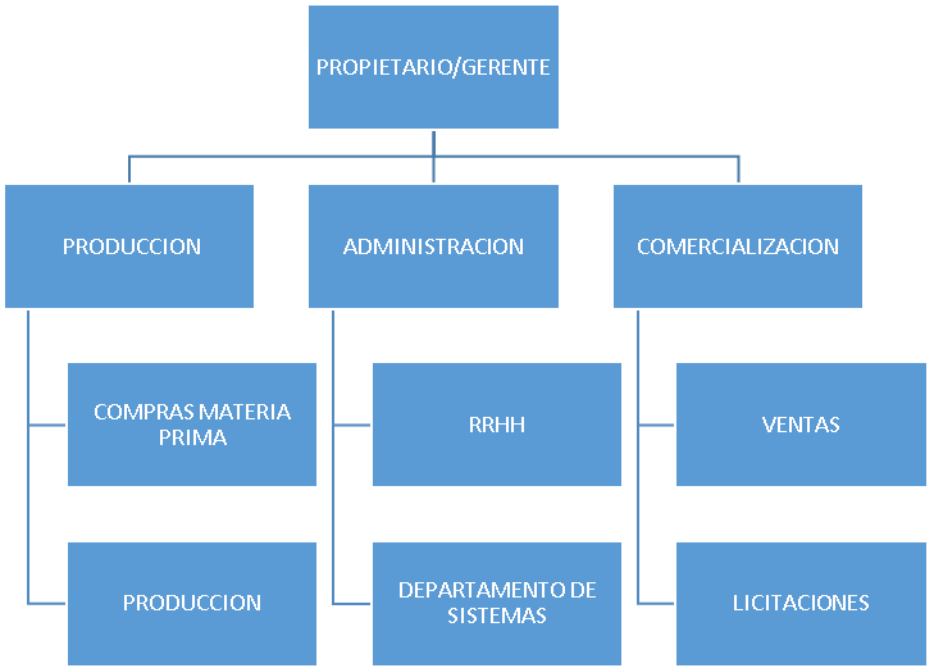
Razón social	:	EMPRESA CURTIEMBRE "CUEROBOL"
Rama-actividad	:	Producción y comercialización de cuero de vaca
Subsector	:	Industrial
Tipo de empresa	:	Mediana
Conformación jurídica	:	SRL
Composición del capital	:	100% nacional

2.2.2. Ubicación Geográfica

La empresa se encuentra ubicada en Viacha a 5 kilómetros de la plaza principal en la zona Bolívar calle Irpachico.

2.2.3. Estructura Administrativa

La empresa es supervisada en su proceso de producción, administración y comercialización por miembros de la familia a la que pertenece. La estructura se detalla a continuación:



2.3. Misión y Visión De La Empresa

2.3.1. Misión

Producir con calidad, directamente al consumidor final con precios competitivos de sus artículos de cuero en general impulsando el desarrollo económico basándose en una administración con capacidad de cambio y personal capacitado

2.3.2. Visión

Llegar a ser líder en su rama a nivel local, nacional e internacional, brindando productos de calidad con compromiso de trabajo en beneficio de sus clientes y promoviendo el desarrollo del país.

2.4. Proceso del Curtido

2.4.1. Saladeros

El saladero es el local o galpón donde se almacenarán las pieles saladas (barraca).Este lugar debe ser aireado, fresco y sin sol directo. En la medida de lo posible las pieles deben ser saladas (iniciar su conservación) en un plazo máximo de 4 horas después del desuello.

2.4.2. Remojo

Como explicamos anteriormente las pieles saladas o secas, que llegan, o que están estibadas en las curtiembres tienen un grado de deshidratación muy poco favorable a la reacción con productos curtientes. Antes de la curtición, debe llevarse la piel al estado de hidratación o hinchamiento que tiene en el animal vivo, y veremos que con ello recupera su original flexibilidad, morbidez y plenitud, cambiando

adecuadamente la estructura fibrosa, como para facilitar la penetración y absorción de los productos curtientes

2.4.3. Pelambre

Luego de la operación de remojo, las pieles suficientemente hidratadas, limpias, con algunas proteínas eliminadas de su estructura, pasan a las operaciones de pelado, donde fundamentalmente se pretende, por un lado eliminar el pelo o la lana, y por otro aflojar las fibras de colágeno con el fin de prepararlas apropiadamente para los procesos de curtido

2.4.4. Dividido

Esta operación es una operación absolutamente mecánica. La acción de la máquina de dividir se basa en seccionar la piel, apoyada entre dos cilindros, mediante una cuchilla en forma de cinta sin-fin.

2.4.5. Desencalado

El Desencalado sirve para eliminación de la cal contenida en el baño de pelambre y para el deshinchamiento de las pieles (la cal que se ha agregado al proceso durante la operación de pelambre).

2.4.6. Piquelado

La finalidad de éste proceso es acidular hasta un determinado pH, las pieles en tripa antes de la curtición al cromo, al aluminio o cualquier otro elemento curtiente. Con ello se logra bajar los niveles de astringencia de los diversos agentes curtientes.

2.4.7. Rebajado

En esta operación se ajusta el espesor del cuero a lo deseado. El objetivo principal es conseguir cueros de espesura uniforme, tanto en un cuero específico como en un lote de cueros.

2.4.8. Neutralizado

Antes de comenzar la recurtición con curtientes orgánicos naturales o sintéticos hay que neutralizar el cuero curtido al cromo para posibilitar a los recurtientes y colorantes una penetración regular en el cuero. Si se seca el cuero al cromo sin haberlo previamente neutralizado conduce a defectos en el cuero terminado o también en los productos de elaboración

2.4.9. Teñido

El teñido consiste en un conjunto de operaciones cuya finalidad es conferirle al cuero determinada coloración, ya sea superficialmente, en parte del espesor o en todo el espesor para mejorar su apariencia, adaptarlo a la moda e incrementar su valor. De acuerdo a las necesidades se realizará:

2.4.10. Engrase y secado

En general, el engrase es el último proceso en fase acuosa en la fabricación del cuero y precede al secado. Junto a los trabajos de curtición es el proceso que sigue en importancia, influenciando las propiedades mecánicas y físicas del cuero. El secado es la fase final en donde se obtiene el cuero seco y listo para su comercialización.

2.5. Tipos de Acabado

En el proceso de curtir el cuero se pueden obtener distintos acabados que son destinados a diferentes mercados y usos, la curtiembre CUEROBOL manea 3 tipos d acabado en cueros: napa, gamuzón y costra.

2.5.1. Napa

Cuero napa es el término común para referirse al cuero liso curtido a cromo, especialmente suave.

2.5.2. Gamuzón

La segunda capa de cuero que queda después de la napa es el gamuzón, es de textura más áspera que la napa y un poco más gruesa, también su costo es menor que el cuero napa, se pueden obtener de varios colores y en el proceso de lijar se podría afinar el cuero.

Existen dos calidades en el cuero gamuzón:

- De Primera.- es el cuero que no tiene ninguna deformidad ni falla, se encuentra en cueros que fueron debidamente procesados y que lograron llegar a esta última etapa sin sufrir ningún problema.
- De Segunda.- se refiere a los cueros que sufrieron algún tipo de desperfecto en el proceso y por lo cual existen partes que no tienen la misma calidad y por lo tanto su precio es más bajo.

2.5.3. Costra

Es la segunda capa del cuero que mediante la utilización de algunos químicos adquiere una dureza y grosor distintos al de cuero napa y gamuzón, es utilizado en la

realización de zapatos por su resistencia y dureza, su costo es menor que el de cuero napa pero mayor que del gamuzón.

2.6. Comercialización

2.6.1. Exportación

La exportación se realiza mayormente a Perú y tiene como fin la zapatería y confección de chamarras y carteras que posteriormente regresan al país para su venta.

2.6.2. Licitaciones en Bolivia

A pesar de contar con un mercado amplio la empresa CUEROBOL se encamino en el mercado de la zapatería y confección de chamarras cono sus clientes principales ya que la calidad y tipo de cuero está diseñado para ese fin.

2.7. Programa utilizado para el Control de Ventas

La empresa CUEROBOL utiliza el programa "StockBase" para realizar el control de sus ventas y clientes, a pesar que generalmente realiza licitaciones con otras empresas, la empresa tiene una base de datos de todos sus clientes a partir del año 2009 y sus ventas realizadas semanalmente.

CAPITULO III

Marco Teórico

3. Marco Teórico

La Seguridad de los SI es un tema que cada vez adquiere mayor complejidad al interior de las Empresas. La Arquitectura de Seguridad requiere una serie de controles para lograr niveles de impacto aceptables de los riesgos inherentes, y es el marco teórico primordial con el que cuenta una empresa a efecto de que todo el personal contribuya a la seguridad de los activos de información.

La Seguridad debe incluir políticas, normas y procedimientos, los cuales a su vez son parte de la cultura organizacional. Para su implantación se requiere de un proceso de internalización en el personal, lo cual indudablemente lleva tiempo. Así mismo, la Arquitectura de Seguridad contempla lo relacionado con las tecnologías de seguridad, las cuales deben responder a estándares tecnológicos o lo que se manifiesta en la literatura científica como "*Mejores Prácticas"* (IT Governance Institute & Office of Goverment Commerce, 2008), las cuales podemos encontrar en COBIT, modelo empleado como una herramienta de control para la auditoria y gestión de riesgos de las tecnologías Informáticas ITIL, empleado para establecer el ciclo de mejoramiento de las TI.

El uso de las Tecnologías de la Información y Comunicación (TIC´s) adquiere cada vez mayor participación en los procesos de las organizaciones. En este sentido, la información cobra importancia para sobrevivir frente a la competencia y permanecer en el mercado. Factores como el uso de Internet y demás herramientas que faciliten la comunicación traen consigo innumerables ventajas, pero igualmente enfrentan a las organizaciones a amenazas más complejas; la probable materialización de ellas pueden exponer a la pérdida o modificación de la información, y por ende se crea la necesidad de diseñar e implementar estrategias que permitan gestionar y controlar los nuevos riesgos, relacionados todos ellos con TI.

Este trabajo sirve de apoyo para establecer riesgos y reconocer controles en ambientes computarizados, identificar las posibles amenazas o causas de los riesgos, los

controles utilizados para minimizar las amenazas a riesgos, entre otros aspectos necesarios en los modelos de gestión de riesgos, de manera que pueda ser herramienta en la gestión de procesos para las Empresas del sector Social y Solidario.

El presente capítulo, pretende mostrar la referencia teórica relacionada a seguridad, Bases de Datos, tipos, modelo relacional; para luego, proporcionar un modelo para auditar procesos en la Base de Datos Relacional, basada en la gestión de riesgos y reconocer controles en ambientes computarizados.

3.1 Gestión de riesgos

Hoy en día las organizaciones tratan de gestionar el riesgo a diferentes niveles. Lamentablemente, no aplican normas generalmente aceptadas que establezcan un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz.

Se debe tratar de obtener los elementos necesarios para conocer las amenazas que puedan afectar los procesos apoyados por las TI, así como los eventos de pérdida potencial ocurridos y para cada uno de los factores de riesgo (agentes generadores), las causas o vulnerabilidades que al ser explotadas por los agentes generadores materializan el riesgo, los efectos o impactos en los objetivos y metas de la organización y las actividades del proceso en las que se puede presentar o se presentó la amenaza de riesgo.

La administración de riesgos emplea una vasta terminología que debe ser claramente entendida por los interesados en control de riesgos. Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales. Aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades.

Beneficios para la organización

- ✓ Facilita el logro de los objetivos de la organización;

- ✓ Hace a la organización más segura y consciente de sus riesgos;
- ✓ Mejoramiento continuo del Sistema de Control Interno;
- ✓ Optimiza la asignación de recursos;
- ✓ Aprovechamiento de oportunidades de negocio;
- ✓ Fortalece la cultura de autocontrol;
- ✓ Mayor estabilidad ante cambios del entorno.

Beneficios para el Departamento de Auditoría

- ✓ Soporta el logro de los objetivos de la auditoría;
- ✓ Estandarización en el método de trabajo;
- ✓ Integración del concepto de control en las políticas organizacionales;
- ✓ Mayor efectividad en la planeación general de Auditoría;
- ✓ Evaluaciones enfocadas en riesgos;
- ✓ Mayor cobertura de la administración de riesgos;
- ✓ Auditorías más efectivas y con mayor valor agregado.

3.1.1 Proceso de Gestión de Riesgos

I. Establecer Contexto

I.1. Establecer el Contexto Estratégico

Definir la relación entre la organización y el ambiente en el que opera.

I.2. Establecer el Contexto Organizacional

Entender la organización, sus capacidades y habilidades

Conocer sus objetivos y estrategias.

I.3. Identificar Objetos Críticos

Entendiendo por objeto, el área, proceso o actividad o cualquier otro elemento en que se pueda subdividir la organización y sobre el cual se pueda efectuar administración de riesgos.

Definir los criterios bajo los cuales se pueda establecer la criticidad de un objeto respecto de otro

II. Identificar Riesgos

II.1. Establecer un marco específico de administración de riesgos

Entender la actividad o parte de la organización para la cual se aplicará el proceso de administración de riesgos.

II.2. Desarrollar criterios de evaluación de riesgos

Definir e identificar los criterios de análisis y el nivel de aceptación de los riesgos

II.3. Identificar la estructura

Separar la actividad o proyecto en un conjunto de elementos que facilite su comprensión y análisis.

II.4. Identificar riesgos

Responder ¿qué puede ocurrir? Identificar los eventos que puedan afectar los elementos de la estructura identificada en el numeral 2.3.

II.5. Identificar causas

¿Cómo y por qué pueden ocurrir los eventos identificados como riesgos? Identificar lo que motiva, dispara o genera los eventos y los escenarios más significativos.

III. Análisis de Riesgos

III.1. Valorar el riesgo inherente

Asignar valor al evento de materialización del riesgo propio del objeto de análisis.

III.2. Determinar Controles Existentes

Identificar las actividades o mecanismos de control implementados para mitigar los riesgos inherentes.

III.3. Identificar Nivel de Exposición

Resultante de aplicar la fórmula:

Nivel de Exposición = Riesgo inherente - Controles

IV. Evaluar y priorizar

IV.1. Comparar contra Criterios y Definir prioridades de riesgo

Comparar el resultado del análisis de riesgo realizado contra los criterios establecidos en el numeral 1. Marco general de referencia.

Las comparaciones de análisis de riesgo realizadas sobre diferentes áreas de la organización o sobre los diferentes procesos le permitirán priorizar los riesgos sobre los cuales ha de centrar la atención para definir una opción de tratamiento.

V. Tratamiento del Riesgo

V.1. Identificar opciones de tratamiento

Para la actividad o componente al cual aplicó el proceso de administración de riesgos, determine las posibles formas de reducir o mitigar el riesgo.

V.2. Evaluar opciones de tratamiento

Bajo las consideraciones del marco de referencia definido, establecer cuáles de las opciones de tratamiento identificadas se ajustan a la organización y reducen el riesgo a un nivel de exposición aceptable.

V.3. Preparar planes de tratamiento

Elaborar los planes que le permitan poner en práctica las opciones de tratamiento del riesgo seleccionadas.

V.4. Implementar Plan de tratamiento

Poner en marcha el plan definido.

Es recomendable que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión

del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización.

3.1.2 Elementos del riesgo

El riesgo es "el efecto de la incertidumbre en la consecución de los objetivos" ISO 31000:2009

- ✓ *Incertidumbre* (puede que nunca ocurra).
- ✓ El riesgo importa y debe gestionarse porque tiene un *efecto (positivo y negativo)*.
- ✓ Ese efecto es sobre los *objetivos* fijados.

Los elementos del riesgo son:

- ✓ Activos;
- ✓ Amenazas;
- ✓ Vulnerabilidad;
- ✓ Exposición;
- ✓ Riesgo;
- ✓ Salvaguarda.

Tienen interrelación unos elementos con otros. Las amenazas explotan las vulnerabilidades, las cuales resultan en exposiciones. La exposición es un riesgo y el riesgo es mitigado por salvaguardas. Las salvaguardas protegen los activos que son puestos en peligro por las amenazas.

El punto de partida de la identificación del riesgo es el conocimiento de los elementos del riesgo que se describen a continuación:

3.1.3. Activo

Es cualquier cosa dentro de una ambiente que deberá ser protegido. Este puede ser un archivo de computador, un servicio de red, un recurso del sistema, un proceso, un programa, un producto, la infraestructura de Tecnología de Información, una base de datos, un dispositivo de hardware, software, instalaciones físicas y otros. Si una organización coloca algún valor a un ítem bajo su control y estima que ese ítem es bastante importante para proteger, este se marca como un activo para propósitos de gestión y análisis de riesgos. La pérdida o divulgación de un activo puede resultar en detrimento general de la seguridad, pérdida de productividad, reducción de utilidades, gastos o costos adicionales, discontinuidad de la organización y numerosas consecuencias intangibles.

3.1.4. Valuación de un activo

Es un valor monetario asignado a un activo basado en el costo actual y gastos no monetarios. Este incluye costos de desarrollo, mantenimiento, administración, publicidad, soporte, reparación y remplazo. Estos también incluyen valores difíciles de determinar tales como credibilidad pública, soporte de la industria, mejoramiento de la productividad, tener y beneficios de socio.

3.1.5. Probabilidad

Mide la longitud y fuerza con la que se obtiene un resultado (o conjunto de resultados) luego de llevar a cabo un experimento aleatorio, del que se conocen todos los resultados posibles, bajo condiciones suficientemente estables (Miller & Freund, 2004). La probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción de control o de disminución, o sea, debe considerarse en cada caso

qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

3.1.6. Amenaza

Cualquier potencial ocurrencia que puede causar un efecto indeseable o no esperado para una organización o para un activo específico. Las amenazas son cualquier acción o inacción que puede causar daño, destrucción, alteración, pérdida o divulgación de activos o que podrían bloquear el acceso o impedir el mantenimiento de los activos.

Las amenazas pueden ser grandes o pequeñas y de la misma manera pueden ser sus consecuencias. Pueden ser accidentales o intencionales. Pueden ser generadas por las personas, las organizaciones, el hardware, las redes, estructuras o la naturaleza (British Standards Institution, 2002).

3.1.7. Agentes de amenazas

Son los que intencionalmente explotan las vulnerabilidades. Usualmente son personas, pero también pueden ser programas, hardware o sistemas.

3.1.8. Eventos de amenazas

Son la explotación accidental de las vulnerabilidades. Incluyen incendio, terremoto, inundación, fallas del sistema, errores humanos (originados por falta de entrenamiento o por ignorancia) y caídas de energía eléctrica.

3.1.9. Impactos

Las consecuencias de la ocurrencia de las distintas amenazas generalmente se consideran de forma negativa y son ellos los que se establecen al momento de determinar cuánto puede perder la Empresa en caso de que el atacante logre tener éxito.

Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo. Se puede establecer que las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio. Otras no tan comunes, felizmente, son la pérdida de vidas humanas, afectación del medio ambiente, etc

3.1.10. Vulnerabilidad

Es la ausencia o la debilidad de una salvaguarda o contramedida, es decir, un defecto, errores y ambigüedades en las leyes y normas, omisión o descuido, error, limitación, fragilidad o susceptibilidad en la infraestructura o cualquier otro aspecto de la organización. Si es explotada, pueden ocurrir pérdidas o daños a los activos. Son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto. Una vulnerabilidad común es contar con antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.

3.1.11. Exposición al riesgo

Susceptibilidad a perder activos debido a una amenaza. Existe la posibilidad de que una vulnerabilidad pueda ser explotada por un agente de amenaza o un evento de amenaza. No significa que esté ocurriendo un evento que resulta en pérdidas; significa que hay una vulnerabilidad y una amenaza que pueden ser explotadas y que hay la posibilidad que un evento de amenaza ocurra.

3.1.12. Riesgo

Es la posibilidad de que cualquier amenaza específica explote una vulnerabilidad específica para causar daño a un activo. Este es una estimación de probabilidad, posibilidad u oportunidad. A mayor probabilidad de ocurrencia de un evento de amenaza, mayor es el riesgo.

Cada acción de exposición es un riesgo. Cuando lo escribimos como una fórmula, el riesgo puede ser definido como:

Riesgo = Amenaza + vulnerabilidad

Entonces la reducción del agente de amenaza o de la vulnerabilidad, directamente conducen a la reducción del riesgo. Cuando un riesgo se materializa, un agente de amenaza o un evento de amenaza toman ventaja de una vulnerabilidad y causan daño o divulgación de uno o más activos. El propósito amplio de la seguridad es prevenir la materialización de los riesgos, mediante la remoción de las vulnerabilidades y el bloqueo de los agentes de amenaza y los eventos de amenaza que pueden exponer los activos. Como una herramienta de gestión de riesgos, la seguridad es la implementación de protecciones o salvaguardas. El riesgo es el efecto de una amenaza expresado en términos monetarios, multiplicado por la frecuencia de ocurrencia en un periodo de tiempo.

Para estimar el riesgo que genera una amenaza es necesario considerar dos variables:

(1) I: El valor de las pérdidas que genera la amenaza de riesgo cada vez que se presente y,

(2) F: La cantidad estimada de veces que se presente la amenaza de riesgo en un periodo de tiempo (frecuencia probable de ocurrencia de la amenaza).

El Riesgo es el resultado de multiplicar estas dos variables;

R = I * F

3.1.13. Pérdida anual estimada (PAE)

En la estimación del riesgo, la variable "Costo de la Amenaza" determina que tan crítica puede ser la causa del riesgo. La criticidad puede estimarse para un periodo de tiempo dado, como por ejemplo un año; en este caso es el valor de la Pérdida Anual Estimada (PAE).

PAE = Pérdidas que genera cada ocurrencia por las veces que ocurra en un año. $300.000 = $100.000 x 3 veces al año.

3.1.14. Salvaguarda o Contramedida

Es cualquier cosa que remueve una vulnerabilidad o protege contra una o más amenazas específicas. Es cualquier acción o producto que reduce el riesgo a través de la eliminación o reducción de una amenaza o una vulnerabilidad en cualquier sitio dentro de la organización. Son la única manera de mitigar o remover el riesgo. Un salvaguarda puede ser la instalación de un parche de software, hacer un cambio en la configuración, contratar guardias de seguridad, electrificar un perímetro de defensa e instalar luces (International Information Systems Security Certification Consortium, 2012)..

3.1.15. Ataque

Un ataque es la explotación de una vulnerabilidad por un agente de amenaza. En otras palabras, es cualquier intento de explotar una vulnerabilidad de la infraestructura de seguridad de una organización para causar daño, pérdida o divulgación de activos. También puede verse como cualquier violación o falla en la adhesión a la política de seguridad de la organización.

3.1.16. Rompimiento o Infracción de Seguridad

Es la ocurrencia de la omisión o impedimento de un mecanismo de seguridad por parte de una agente de amenaza. Cuando una infracción se combina con un ataque, el resultado es una penetración o intrusión.

3.1.17. Penetración

Es la condición en la cual un agente de amenaza obtiene el acceso a la infraestructura de una organización a través de la burla o engaño de los controles de seguridad y está habilitado para directamente poner en peligro los activos.

3.2. Tecnologías de Bases de Datos

La cantidad de información disponible crece, literalmente, de manera explosiva, y el valor de los datos como activo de las organizaciones está ampliamente reconocido.

Para que los usuarios obtengan el máximo rendimiento de su enormes y complejos conjuntos de datos son necesarias herramientas que simplifiquen las tareas de administrar los datos y de extraer información útil en el momento preciso. En caso contrario, los datos pueden convertirse en una carga cuyo coste de adquisición y de gestión supere ampliamente el valor obtenido de ellos.

Los datos almacenados en un Sistema de Información son el activo más importante en la toma de decisiones para la consecución de los objetivos institucionales.

En el mundo actual existe una cada vez mayor demanda de datos. Esta demanda siempre ha sido patente en empresas y sociedades, pero en estos años la demanda se ha disparado más debido al acceso multitudinario a las redes integradas en Internet y a la aparición de pequeños dispositivos (móviles y PDA) que también requieren esa

información. En informática se conoce como dato a cualquier elemento informativo que tenga relevancia para un usuario. Desde su nacimiento, la informática se ha encargado de proporcionar herramientas que faciliten la gestión de los datos. Antes de la aparición de las aplicaciones informáticas, las empresas tenían como únicas herramientas de gestión de datos a los cajones, carpetas y fichas en las que se almacenaban los datos. En este proceso manual, el tipo requerido para manipular estos datos era enorme. Sin embargo el proceso de aprendizaje era relativamente sencillo ya que se usaban elementos que el usuario reconocía perfectamente.

Las operaciones que permiten su administración son las que determinan su fiabilidad. El hecho de que esos datos y sus operaciones sean manipulados por seres humanos les agrega una componente de error, voluntario o no, que implica un riesgo para la organización. Se desprende de aquí la necesidad de realizar Auditorías Informáticas y como parte de ellas la de poder analizar trazas de actividad de los usuarios sobre los datos de las aplicaciones. Tanto desde el punto de vista legal como desde el punto de vista de auditoria es requerido que los sistemas de bases de datos puedan registrar la actividad sobre datos claves, para posteriormente poder rastrear el momento y el usuario que ha realizado una determinada modificación, incorporación o eliminación de datos. Por tanto, prevenir, evitar y/o restringir tales riesgos se convierte en una tarea y un reto difícil de relegar para aquellos que trabajan cotidianamente con Bases de Datos y les interesa garantizar su integridad, confidencialidad y fiabilidad en el mayor grado posible.

Las Bases de Datos, es un activo intangible, definido a través de la NIC 38: "*Un activo intangible, es un activo identificable, sin apariencia física y de carácter no monetario".*

Sabemos que los datos son administrados de alguna manera, estos pueden estar almacenados en diferentes lugares e implementados sobre diferentes gestores de datos, lo que implica una dificultad a la hora de establecer controles sobre los mismos.

Si bien, varios de los diferentes motores de bases de datos ofrecen como parte de su funcionalidad una herramienta capaz de establecer trazas de auditoria para el seguimiento de los cambios sobre un conjunto de datos previamente seleccionados mientras que otros no las poseen, esto no alcanza para establecer un control total sobre los mismos.

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.

3.2.1. Definición de Base de Datos

Las bases de datos existen desde que el ser humano empezó a almacenar datos en algún soporte. Si por datos entendemos dibujos, que lo son, entonces las primeras bases de datos fueron las paredes de las cuevas donde nuestros ancestros dibujaron las pinturas rupestres.

Una base de datos es un conjunto de datos, que generalmente describe las actividades de una o varias organizaciones relacionadas. Por datos, queremos decir hechos conocidos que pueden registrarse y que tienen un significado implícito.

En otras palabras, una base de datos tiene alguna fuente de la cual provienen los datos, algún grado de interacción con los sucesos del mundo real, y una audiencia que está activamente interesada en el contenido de la base de datos.

Una definición general, podemos expresarla de la siguiente manera: Una Base de Datos (BD) es una colección de datos operacionales almacenados sin redundancias perjudiciales y utilizadas para una o más aplicaciones, de una empresa en particular.

Una base de datos puede tener cualquier tamaño y complejidad, y puede crearse y mantenerse manualmente o puede ser informatizada mediante un conjunto de programas de aplicación diseñados específicamente para dicha tarea o bien mediante un sistema de gestión de bases de datos.

3.2.2. Sistema y Arquitectura de un Sistema de Base de Datos (SBD)

Un SBD es un sistema cuyo propósito general es el de almacenar y recuperar información inherente a la organización donde opera.

La arquitectura de un SBD contempla:

- ✓ NIVEL EXTERNO: Describe solo parte de la BD(mundo real)
- ✓ NIVEL CONCEPTUAL: Describe que datos son almacenados en la BD y las relaciones que existen entre los datos. (mundo de ideas)
- ✓ NIVEL INTERNO: Describe el almacenamiento físico de los datos(mundo de datos)

Este tipo de arquitectura a 3 niveles (ANSI/SPARC), es muy utilizada en el diseño de bases de datos relacionales. Ver figura 2.1

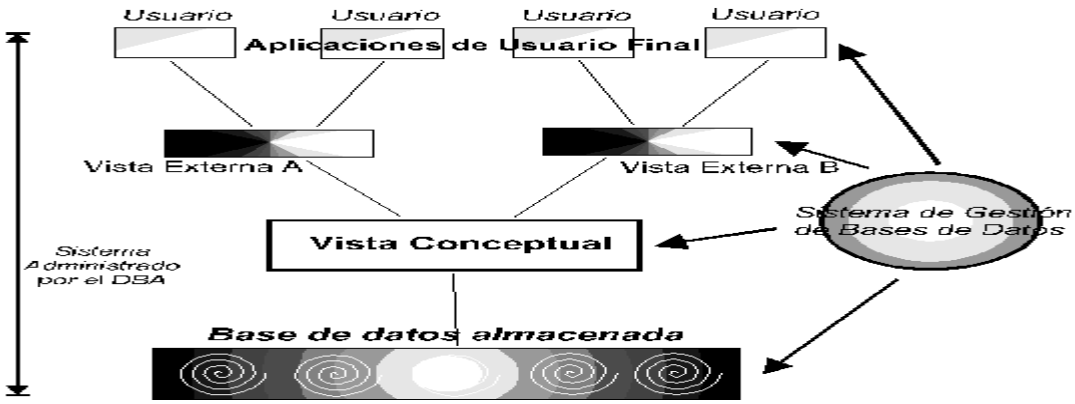


Fig. 2.1 Arquitectura según ANSI/SPARC

La arquitectura de un Sistema de Base de Datos considera tanto los datos internos como los datos externos de la organización, que son almacenados en un repositorio de datos o en un almacén de datos, para luego generar información para una adecuada toma de decisiones.

3.2.3 Elementos y Características de los SBD

Los elementos de un sistema de base de datos son los mismos que los de un sistema de información:

- ✓ **Hardware.** Máquinas en las que se almacenan las bases de datos. Incorporan unidades de almacenamiento masivo para este fin;
- ✓ **Software.** Es el sistema gestor de bases de datos. La aplicación que permite el manejo de la base de datos.
- ✓ **Datos.** Incluyen los datos que se necesitan almacenar y los metadatos que son datos que sirven para describir lo que se almacena en la base de datos.
- ✓ **Usuarios.** Personas que manipulan los datos del sistema. Podemos mencionar tres categorías:
  1. **Usuarios finales**. Aquellos que utilizan datos de la base de datos para su trabajo cotidiano que no tiene por qué tener que ver con la informática.

Normalmente no utilizan la base de datos directamente, sino que utilizan aplicaciones creadas para ellos a fin de facilitar la manipulación de los datos. Estos usuarios sólo acceden a ciertos datos.

2. **Desarrolladores**. Analistas y programadores encargados de generar aplicaciones para los usuarios finales.
3. **Administradores.** También llamados DBA (Data Base Administrator), se encargan de gestionar las bases de datos. Hay que tener en cuenta que las necesidades de los usuarios son muy diferentes en función del tipo de usuario que sean: a los finales les interesa la facilidad de uso, a los desarrolladores la potencia y flexibilidad de los lenguajes incorporados del sistema de bases de datos, a los administradores herramientas de gestión avanzada para la base de datos.

Entre las características, podemos mencionar:

- ✓ Control de la redundancia;
- ✓ Evitar la inconsistencia;
- ✓ Compartimiento de los datos;
- ✓ Integridad y seguridad de los datos;
- ✓ Estandarizar la información en el sistema;
- ✓ Independencia de datos.

3.2.4 Tipos de Bases de Datos

- ✓ Base de Datos Jerárquica;
- ✓ Base de Datos Relacional;
- ✓ Base de Datos de Red;
- ✓ Base de Datos Orientada a Objetos;
- ✓ Base de Datos Distribuidas;
- ✓ Base de Datos Objeto Relacional;
- ✓ Base de Datos Multidimensionales;

- ✓ Base de Datos Transaccionales;
- ✓ Base de Datos Documentales;
- ✓ Base de Datos Declarativas (deductivas y funcionales).

3.2.5 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 Sistemas Gestores de Bases de Datos.

3.2.6 Bases de Datos Relacional

El modelo de datos relacional organiza y representa los datos en forma de tablas o relaciones:

REPRESENTACIÓN LÓGICA	REPRESENTACIÓN FÍSICA	MODELO RELACIONAL
Tabla	Archivo secuencia	Relación
Fila	Registro	Tupla
Columna	Campo	Atributo

- ✓ **Atributo (Ai)**: Elemento susceptible de tomar valores (cada una de las columnas de la tabla);

- ✓ **Dominio (Di):** Conjunto de valores que puede tomar un atributo (se considera finito);
- ✓ **Tupla:** Cada uno de los elementos que contiene una instancia de la relación (filas).

Relación R(Ai..An)

Subconjunto del producto cartesiano D1×……×Dn (esto es, una tabla)

En una relación hay que distinguir dos aspectos:

Esquema de la relación: Los atributos A1..An

Por ejemplo: Empleados (id_empleado, pat, mat, nom, tarifa_hr, tipo_de_oficio, id_supv)

Instancia de la relación: El conjunto de tuplas

{(x1,x2,..,xn)} ⊆ D1×D2×……...×Dn que la componen en cada momento.

Consecuencias de la definición de relación como conjunto de tuplas:

- ✓ No existen tuplas duplicadas (concepto de clave primaria);
- ✓ No existe orden en las tuplas (ni en los atributos).

Esquema de la base de datos

Una base de datos relacional es un conjunto finito de relaciones junto con una serie de restricciones o reglas de integridad:

- ✓ **Restricción de integridad**: Condición necesaria para preservar la corrección semántica de la base de datos;
- ✓ **Esquema de la base de datos:** Colección de esquemas de relaciones junto con las restricciones de integridad que se definen sobre las relaciones.

Instancia de la base de datos

- ✓ **Instancia (o estado) de la base de datos:** Colección de instancias de relaciones que verifican las restricciones de integridad;
- ✓ **Base de datos relacional:** Instancia de la base de datos junto con su esquema.

Restricciones de integridad:

Asociadas a las tuplas de una relación

Por ejemplo: $0 \leq \text{edad} \leq 80$;

$\text{impuestos} \leq \text{sueldo}$

En ocasiones, no se conoce el valor de un atributo para una determinada tupla. En esos casos, a ese atributo de esa tupla se le asigna un **valor nulo (null)**, que indica que el valor de ese atributo es desconocido o, simplemente, que ese atributo no es aplicable a esa tupla.

Asociadas a las relaciones de la base de datos

- ✓ **Clave primaria:** Conjunto de atributos seleccionados para identificar unívocamente a las tuplas de una relación;
- ✓ **Integridad de entidad:** Los atributos de la clave primaria no pueden tomar valores nulos, ya que la clave primaria debe permitirnos identificar unívocamente cada tupla de la relación.

Asociadas a las relaciones de la base de datos

- ✓ **Clave externa:** Conjunto de atributos de una relación cuyos valores en las tuplas deben coincidir con valores de la clave primaria de las tuplas de otra relación;

- ✓ **Integridad referencial:** Todos los valores no nulos de una clave externa referencian valores reales de la clave referenciada.

Asociadas a las relaciones de la base de datos

La integridad referencial mantiene las conexiones en las bases de datos relacionales:

$$\text{imparte.MATERIA} \in \text{profesor.MATERIA}$$

El profesor que imparte una asignatura debe existir en la tabla de profesores.

$$\text{cuenta.sucursal} \in \text{sucursal.numero}$$

Una cuenta tiene que pertenecer a una sucursal existente.

El proceso de diseño de bases de datos

Problema:

Diseñar la estructura lógica y física de una o mas bases de datos para atender a las necesidades de información de los usuarios en una organización para un conjunto definido de aplicaciones.

Actividades paralelas:

- ✓ Diseño del contenido y estructura de la base de datos;
- ✓ Diseño de las aplicaciones de la base de datos.

El proceso de diseño de bases de datos

Fase 1:

Análisis de requisitos

Recabar información sobre el uso que se piensa dar a la base de datos (elicitacion de requisitos del sistema).

Fase 2:

Diseño conceptual (modelo E/R)

Creación de un esquema conceptual de la base de datos independiente del SGDB que se vaya a utilizar.

Fase 3:

Elección del sistema gestor de bases de datos

Elección del modelo de datos (tipo de SGDB) y del SGDB concreto (p.ej. relacional, multidimensional…).

Fase 4:

Diseño lógico

Creación del esquema conceptual para el modelo de datos del SGDB elegido (p.ej. paso del modelo E/R a un conjunto de tablas).

Fase 5:

Diseño físico

Creacion de la base de datos utilizando el DDL (lenguaje de definición de datos del SGDB).

Fase 6:

Uso y mantenimiento

Gestión de los datos utilizando el DML (lenguaje de manipulación de datos del SGDB).

Del modelo E/R al modelo relacional:

Diseño lógico de bases de datos relacionales

Transformación de un diagrama E/R en un esquema relacional (esto es, en un conjunto de tablas):

1. Se transforman en tablas todas los tipos de entidades y relaciones que aparecen en el diagrama E/R;

2. Se seleccionan las claves primarias para cada una de las tablas de nuestro esquema lógico;
3. Se fusionan aquellas tablas que compartan su clave primaria.

Entidades

Cada tipo de entidad da lugar a una tabla en la base de datos.

- ✓ **Atributos:** Los atributos del tipo de entidad.
- ✓ **Clave primaria:** Una de las claves candidatas del conjunto de entidades.

Entidades débiles

- ✓ **Atributos:** Además de los atributos propios de la entidad débil, los atributos pertenecientes a la clave primaria de la entidad fuerte de la que depende existencialmente la entidad débil;
- ✓ **Clave primaria:** La clave primaria de la entidad fuerte más un conjunto de atributos propio de la entidad débil (discriminante).

Relaciones

Cada tipo de relación da lugar a una tabla en la base de datos.

- ✓ **Atributos:** Los atributos de las claves primarias de las entidades que intervienen en la relación mas los atributos propios de la relación.

Clave primaria:

Si la relación no tiene atributos propios:

- ✓ **Relación muchos a muchos**: La unión de las claves de los conjuntos de entidades que intervienen;
- ✓ **Relación uno a muchos**: La clave correspondiente al conjunto de entidades que participa en la relación con cardinalidad “muchos”;
- ✓ **Relación uno a uno**: Una de las claves de las entidades intervinientes en la relación (cualquiera).

Si hay atributos propios de la relación:

- ✓ Los atributos correspondientes al tipo de relación, a los que tal vez añadiremos algunos atributos propios dependiendo de la semántica del problema.

Claves externas:

- ✓ Una por cada una de las claves primarias de las entidades que intervienen en la relación.

NOTA

Las relaciones entre entidades débiles y fuertes no hay que pasarlas a tablas porque la relación se recoge como parte de la clave primaria de la entidad débil (la parte correspondiente a la clave primaria de la entidad fuerte es una clave externa que apunta a la tabla derivada de la entidad fuerte).

El modelo relacional, es el modelo más utilizado para modelar problemas reales y administrar datos dinamicamente. Su idea fundamental es el uso de "relaciones". Durante su diseño, una BD relacional pasa por el proceso de normalización.

3.2.6.1 Formas normales

Las formas normales definidas en la Teoría de Base de Datos Relacionales representan una guía y una orientación para el diseño de registros. Las reglas de normalización están destinadas a prevenir anomalías en las actualizaciones e inconsistencia en los datos.

Las directrices que se ofrecerán parten del supuesto de que aquellos campos que no constituyen una clave serán actualizados frecuentemente. El propósito de la normalización es mejorar la integridad de los datos a través de la minimización de la redundancia y la inconsistencia, pero con algún posible costo en ciertas aplicaciones.

El término **normalización** se usa algunas veces en relación a una forma normal particular. Esto es, un conjunto de registros puede ser normalizado con respecto a la segunda forma normal pero no con respecto a la tercera.

Cuando se diseña una Base Datos mediante el modelo relacional, al igual que ocurre con otros modelos, obtenemos diferentes esquemas relacionales y no todos ellos son equivalentes, ya que unos van a representar la realidad mejor que otros.

Con la teoria de la normalizacion, se consigue una formalización en el diseño lógico de la Base de Datos Relacional (BDR).

Considerando las siguientes dependencias:

- ✓ Dependencia funcional;
- ✓ Dependencia funcional completa;
- ✓ Dependencia funcional trivial;
- ✓ Dependencia funcional elemental;
- ✓ Dependencia funcional transitiva;
- ✓ Dependencia multivaluada:
- ✓ Dependencia de combinación.

Primera Forma Normal

Para que una tabla pueda ser considerada una relación no debe admitir grupos repetitivos, esto es, debe estar en primera forma normal.

Se dice que una relacion esta en 1FN cuando cada atributo solo toma un valor del dominio simple subyacente.

Segunda Forma Normal

Esta basada en el concepto de dependencia plena y en las interrelaciones existentes entre los atributos principales de una relación.

Se dice que una relación esta en 2FN sí y solo si: Está en 1FN y cada atributo no principal tiene Dependencia Funcional Completa respecto de cada una de las claves.

Tercera Forma Normal

Esta basada en el concepto de Dependencia Funcional Transitiva.

Un esquema de relación R está en 3FN Sii. Esta en 2FN y no existe ningún atributo no principal que dependa transitivamente de alguna clave R

Forma Normal Boyce-Cood

Para ciertos problemas fueron insuficientes las tres primeras formas normales, en relaciones que presentaban varias claves candidatas compuestas que se solapaban.

Se dice que una relación se encuentra en FNBC sí, y solo sí, todo determinante es una clave candidata.

SQL (Structured Query Languaje)

- ✓ La mayoria de los SGBD relacionales proveen un lenguaje de alto nivel, en el que el usuario solo especifica lo que desea como resultado, dejando las decisiones de como ejecutar la consulta para el sistema.
- ✓ El SQL es lenguaje standard de BD.
- ✓ Incorpora el *algebra relacional* y *el calculo relacional*

3.2.7 Bases de Datos móviles

En el comienzo de los dispositivos móviles (Palm, IPAQ, PDA'S) sus aplicaciones inalámbricas eran totalmente desconectadas de las empresas o sistemas de computación. En otras palabras no requerían el intercambio de información con otros sistemas o con uno centralizado. Así que para aquel entonces no se hablaba de tiempo real en gestión de datos a nivel móvil. Las aplicaciones más reconocidas se limitaban a libreta de direcciones, horarios, organizadores, juegos, agendas y las más sofisticadas contaban con un pequeño paquete de oficina.

Algunas de esas aplicaciones contaban con pequeñas bases de datos y otras almacenaban la información en archivos de texto; para aquel momento funcionaban correctamente, pero a medida que avanza la tecnología, las personas necesitan más. Por eso los fabricantes de SGBD se vieron en la necesidad de crear SGBD móviles que permitan la construcción de bases de datos relacionales para los dispositivos móviles que tal cual se denominan Bases de Datos Móviles.

El dispositivo móvil Se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales. De acuerdo con esta definición existen multitud de dispositivos móviles, desde los reproductores de audio portátiles hasta los navegadores GPS, pasando por los teléfonos móviles, los PDA's o los Tablet PC's. Se caracterizan por ser aparatos pequeños, con algunas capacidades de procesamiento, móviles o no, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, sin embargo pueden realizar otras más generales.

Normalmente se asocian al uso de una persona, La mayoría de estos aparatos pueden ser transportados en el bolsillo del propietario y otros están integrados dentro de otros mayores, controlando su funcionalidad Ej. Un IPOD conectado a su docking, minicomputadoras de equipos de sonido, lavadoras, hornos, vehículos. Sin importar el dispositivo hoy en día todos cuentan con una o más bases de datos embebidas que dan apoyo a las aplicaciones y servicios que funcionan en ellos.

No obstante, el mayor problema que limita estos desarrollos tecnológicos, es que los sistemas de información se ven afectados por problemas de vulnerabilidad en la seguridad de sus datos, así como su costo y la disponibilidad en cualquier momento de esta información hacia el usuario. Ante tal situación, las bases de datos móviles pueden ofrecer soluciones a algunos de los aspectos mencionados con anterioridad. Una base de datos móvil es aquella que es portable y posee una independencia del servidor corporativo de bases de datos, pero puede comunicarse con este servidor desde cualquier punto remoto para compartir datos corporativos. La arquitectura básica de una base de datos móvil, ver Figura 2.2:

Fig. 2.2 FUENTE: SQL Anywhere. Arquitectura BD móvil

En el mundo actual existe cada vez mayor demanda de datos. Esta demanda siempre ha sido patente en empresas y sociedades, pero en estos años la demanda se ha disparado más debido al acceso multitudinario a las redes integradas en Internet y a la aparición de pequeños dispositivos (móviles y PDA) que también requieren esa información. En informática se conoce como dato a cualquier elemento informativo que tenga relevancia para un usuario. Desde su nacimiento, la informática se ha encargado de proporcionar herramientas que faciliten la gestión de los datos. Antes de la aparición de las aplicaciones informáticas, las empresas tenían como únicas herramientas de gestión de datos a los cajones, carpetas y fichas en las que se almacenaban los datos. En este proceso manual, el tipo requerido para manipular estos datos era enorme. Sin embargo el proceso de aprendizaje era relativamente sencillo ya que se usaban elementos que el usuario reconocía perfectamente.

3.2.7.1 Sistemas Gestores de Bases de Datos móviles

Muchos fabricantes ofrecen SGBD móviles capaces de comunicarse con los principales SGBD relacionales. Estos SGBD móviles están adaptados a los recursos limitados de las unidades móviles y proporcionan una serie de funcionalidades adicionales:

- ✓ Comunicación con el servidor centralizado de base de datos mediante técnicas de comunicación inalámbrica;
- ✓ Replicación de datos en el servidor centralizado de base de datos y en el dispositivo móvil;
- ✓ Sincronización de datos entre el servidor centralizado de base de datos y el dispositivo móvil;
- ✓ Gestión de datos en el dispositivo móvil;
- ✓ Análisis de los datos almacenados en el dispositivo móvil.

Algunos ejemplos de Sistemas Gestores de bases de datos móviles son: **Anywhere Solutions**, empresa filial de Sybase, lidera el ranking del mercado de bases de datos móviles gracias a SQL Anywhere. Este paquete proporciona bases de datos que pueden utilizarse tanto a nivel de servidor (soporta máquinas de hasta 64bits) como a nivel de dispositivo móvil. SQL Anywhere se compone de las siguientes tecnologías:

- ✓ *SQL Anywhere Server*: sistema gestor de bases de datos relacionales para los sistemas de bases de datos móviles;
- ✓ *Ultralite*: sistema gestor de bases de datos que puede embeberse en dispositivos móviles;
- ✓ *Mobilink*: tecnología de sincronización para el intercambio de datos entre bases de datos relacionales y bases de datos no relacionales;
- ✓ *QAnywhere*: facilita el desarrollo de aplicaciones móviles robustas y seguras;
- ✓ *SQL Remote*: permite a los usuarios de dispositivos móviles sincronizar sus datos con otras bases de datos SQL Anywhere.

DB2 Everyplace de IBM es una base de datos relacional y un servidor de sincronización que permite extender las aplicaciones y los datos empresariales a dispositivos móviles. Gracias a un consumo de recursos reducido, esta base de datos puede integrarse en dispositivos como PDAs y teléfonos móviles. Microsoft también ofrece una base de datos para dispositivos móviles. Se trata de Microsoft SQL Server Compact 3.5, un motor de bases de datos que permite desarrollar aplicaciones en cualquier plataforma Windows incluyendo Tablet PCs, Pocket PCs, Smart Phones y equipos de escritorio. **Oracle Database Lite 10g** es la solución de Oracle para desarrollar aplicaciones en entornos móviles. Proporciona un cliente que permite la realización de consultas SQL para acceder a los datos locales del dispositivo y un servidor para gestionar los datos de forma centralizada. Otros productos menos utilizados son Borland's JDataStore, una base de datos Java para dispositivos móviles y aplicaciones Web, o MobiSnap, un proyecto de investigación cuyo objetivo es soportar el desarrollo de aplicaciones con bases de datos relacionales en entornos móviles.

3.2.7.2 Aplicaciones móviles y tipos de datos

Las aplicaciones móviles se clasifican en las dos siguientes categorías:

- ✓ aplicaciones verticales y
- ✓ aplicaciones horizontales.

En las aplicaciones verticales, los usuarios acceden a los datos en una celda específica; fuera de la celda los datos no están disponibles. En las aplicaciones horizontales, los datos están distribuidos por todo el sistema, y los usuarios pueden acceder a ellos desde cualquier celda.

La aplicación horizontal más común es el acceso al correo electrónico.

Los datos se clasifican en tres categorías:

Datos privados: pertenecen a un usuario y sólo él puede acceder a ellos y manejarlos. Por ejemplo, los datos del perfil de un usuario de cualquier aplicación que gestione datos personales.

- ✓ **Datos públicos**: pueden ser consultados por cualquier usuario, pero sólo pueden ser modificados por una única fuente. Por ejemplo, los datos de las cotizaciones de la bolsa.
- ✓ **Datos compartidos**: pueden ser accedidos por un grupo determinado de usuarios, quienes tienen permisos para leerlos y para escribirlos. Por ejemplo, los datos de seguros de una compañía aseguradora que vende productos utilizando agentes comerciales.

Tipos

Actualmente estamos comprobando como los diferentes tipos de bases de datos móviles tienen un gran auge. Debido principalmente al desarrollo de las comunicaciones

inalámbricas y a los ordenadores portátiles o laptop, PDAs (del inglés Personal Digital Asistan), teléfonos móviles o celulares, y cualquier otro aparato de similares características.

Este enorme desarrollo de los tipos de bases de datos móviles es debido al auge que tienen actualmente las redes inalámbricas y las comunicaciones vía satélite, lo que permite el poder acceder a datos desde prácticamente cualquier sitio. Los usuarios se pueden acceder a este tipo de bases de datos móviles desde cualquier punto fuera de la empresa, por ejemplo si están visitando a un cliente y necesitan un listado de precios poder acceder al último y más actual de todos.

Una base de datos es el conjunto de datos o información de contenido similar almacenados de forma ordenada para su posterior uso. Y una base de datos móviles sería una base de datos portable y físicamente independiente del servidor corporativo que nos la suministra, y que nos permite comunicarnos con ella desde cualquier lugar remoto compartiendo su información.

Los tipos de bases de datos móviles son a grandes rasgos:

- ✓ Las bases de datos móviles de las diferentes empresas o bases de datos corporativas móviles;
- ✓ Las bases de datos móviles que se crean a través de los teléfonos móviles;
- ✓ Las bases de datos móviles que son consecuencia de las comunicaciones inalámbrica generadas por los ordenadores portátiles, PDAs u otro aparato que tenga acceso a Internet.

3.2.7.3 Factores en el diseño de Base de Datos

Se considera que el almacenaje y la disponibilidad de los datos en cualquier momento, la seguridad de la información, procesamiento de consultas, manejo de transacciones, tiempo de respuesta, control de concurrencias y adaptabilidad al entorno como los factores más claves para diseñar una base de datos. Es así que se ha logrado caracterizar grandes grupos o áreas en las cuales se debe basar un diseño de bases de datos móviles:

Sensibilidad: las aplicaciones de los dispositivos móviles deben poder ofrecer la información de interés del usuario en cualquier lugar y hora del día. Por tal razón, la base de datos del dispositivo móvil solo hará uso de las tablas de la base de datos central que le sean útiles al usuario, debido a los recursos físicos que limitan al dispositivo como tal. Inclusive, en ocasiones de algunas tablas solo toma las columnas y/o filas que le son de interés, por lo que se deben crear nuevos esquemas de la base de datos central para llevar a cabo esto. Otro de los factores importantes que se deben manejar en estas bases de datos es el tiempo que se demora en realizar una consulta. Para tal efecto se suelen usar dos técnicas, la primera consiste en reunir todos los datos de interés en un solo sitio y agruparlos en un modelo transaccional de clúster. El segundo método consiste en almacenar en la memoria cache del dispositivo los datos que son consultados con más frecuencia. Finalmente, se debe tener en cuenta el tipo de datos que se quieren manejar y la cantidad de información que se va guardar para tener en cuenta que no entre en conflicto con la memoria que posee el dispositivo móvil. Se recomienda también realizar una rápida normalización para evitar usar consultas en las cuales se deban hacer Join sobre las tablas existentes. No sobra decir que aunque el número de usuarios que realicen las consultas sobre la base de datos sea grande, el desempeño del sistema no se debe afectar.

Consistencia de Datos y Concurrencia: debido a la alta concurrencia de los datos por parte de muchos usuarios y a las actualizaciones que la base de datos móvil realiza, en

ocasiones se presentan inconsistencias en los datos. Por tal razón, la base debe ser capaz de trabajar tanto en forma online como offline, y debe estar bien sincronizada con los servidores de bases de datos centralizadas para que los datos que se obtengan en cualquier forma sean consistentes.

Sincronización y Resolución de Conflictos: la capa de sincronización de estos sistemas es importante ya que debe mantener la base de datos actualizada debido a los Insert y Delete que se realizan sobre la misma. El problema radica en que muchos acceden a la base de datos al mismo tiempo y la sincronización para cada usuario del sistema puede ser demasiado compleja. Para dar solución a esto, se puede hacer uso de la fragmentación y replicación de la información, así cada usuario posee la información que necesita y es más fácil de actualizar. Sin embargo, si no se puede realizar fragmentación a la base de datos, otra de las opciones que se puede manejar es el uso de prioridades de acuerdo al rol del usuario que esté usando el sistema.

Seguridad: las bases de datos que se manejan, deben estar protegidas de código malicioso e incluso que no puedan ser vistos por terceros. Esto es realmente importante para mantener confidencialidad de los usuarios de un sistema, así como de los recursos que manejan como por ejemplo en un banco. Para tal fin, las aplicaciones que usan estas bases de datos deben hacer uso de sistemas de encriptación y de autenticación de los usuarios.

3.3 El modelo CobiT (Control Objectives for Information and Related Technologies)

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y

administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte a COSO (Committee Of Sponsoring Organisations Of The Treadway Commission) Marco de Referencia Integrado – Control Interno, el marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como a marcos compatibles similares.

3.3.1 Marco de Trabajo de COBIT

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo.

COBIT da soporte al gobierno de TI (Figura 2.3) al brindar un marco de trabajo que garantiza que:

- ✓ TI está alineada con el negocio
- ✓ TI habilita al negocio y maximiza los beneficios
- ✓ Los recursos de TI se usan de manera responsable
- ✓ Los riesgos de TI se administran apropiadamente

Figura 2.3 Fuente: COBIT

COBIT es una herramienta gerencial que le permite a las organizaciones grandes o pequeñas administrar la información de manera efectiva, eficiente, integra y confiable, bajo el estudio de los procesos y actividades, utilizando los recursos de las tecnología de información como los datos, las aplicaciones, tecnología y el recurso humano, con la finalidad de satisfacer los objetivos del negocio, en donde la información necesita cumplir con ciertos criterios, a los cuales COBIT le llama requerimientos de negocio para la información.

El desarrollo de COBIT ha resultado en la publicación de:

- un **Resumen Ejecutivo** el cual, consiste en un Síntesis Ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT) y el Marco Referencial (el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de IT);

- el **Marco Referencial** que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de IT que son impactados en forma primaria por cada objetivo de control;
- **Objetivos de Control**, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de IT;
- **Guías de Auditoría,** las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de IT de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de IT con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o recomendaciones de mejoramiento;
- Un **Conjunto de Herramientas de Implementación**, el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

Propuesta por la **ISACF** (Information Systems Audit and Control Foundation). Es la principal propuesta metodológica realizada a nivel internacional para abordar la Auditoria de Sistemas de Información. Supone un paso muy importante al considerar que, a efectos de auditoria, el sistema de información de una organización es único, aunque ciertos procesos se realicen de forma manual y otros mediante el uso de la informática.

La filosofía de CobiT asimila los principios de reingeniería de empresas (BPR) y divide las funciones que ha de realizar un sistema de información en procesos que, a su vez, están subdivididos en actividades y tareas más simples.

Los sistemas de información están orientados a los procesos y por tanto su auditoria se debe adaptar a estos conceptos.

COBIT reúne principios que permiten a la empresa construir una gobernabilidad efectiva (ver evolución en figura 2.4) y un marco de gestión basado en un conjunto holístico de facilitadores que optimiza la información y la inversión en tecnología y el uso para el beneficio de las partes interesadas.

Figura 2.4. Fuente: COBIT® 5 Introduction Presentation © 2012 ISACA

COBIT ayuda a las empresas a crear valor óptimo de TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de los recursos.

COBIT permite que la información y la tecnología relacionada para ser gobernado y administrado de manera integral para el conjunto de la empresa, teniendo en el pleno de extremo a extremo del negocio y áreas funcionales de responsabilidad, teniendo en cuenta los intereses relacionados con la TI de grupos de interés internos y externos.

Los **principios** (ver figura 2.5) y los **facilitadores** de COBIT son de carácter genérico y útil para las empresas de todos los tamaños, ya sea comercial, sin fines de lucro o en el sector público.

Figura 2.5 Fuente: COBIT® 5 Introduction Presentation © 2012 ISACA

3.3.2 **El modelo** CobiT **– Audiencia**

CobiT esta diseñado para ser utilizado por tres audiencias distintas:

- ✓ Gestores, para ayudarlos a lograr a las autoridades de la educación superior un balance entre los riesgos y las inversiones en control en un ambiente de Tecnologías de la Información (TI) frecuentemente impredecible.
- ✓ Usuarios, para obtener una garantía (autoridades, docentes, estudiantes y administrativos) en cuanto a la seguridad y control de los servicios de TI proporcionados internamente o por terceras partes.
- ✓ Auditores de Sistemas de Información: para dar soporte a las opiniones mostradas a los Gestores sobre los controles internos. También puede ser utilizado dentro de la educación superior por el responsable de un proceso de en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de las TI en entes educativos

3.3.3 **El modelo** CobiT **– Fundamentos**

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de la organización y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI. Para alcanzar los requerimientos educativos, la información necesita satisfacer ciertos criterios:

- ✓ Requerimientos de Calidad:
  - Calidad
  - Coste
  - Entrega (servicio)
- ✓ Requerimientos Fiduciarios:
  - Efectividad y eficiencia de las operaciones
  - Fiabilidad de la información
  - Cumplimiento de leyes y normas
- ✓ Requerimientos de Seguridad:
  - Confidencialidad
  - Integridad
  - Disponibilidad

En CobiT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos educativos:

- ✓ Datos, los objetos de datos en el sentido más amplio, externo e interno, estructurado y no estructurado, gráficos, sonidos, etc.
- ✓ Aplicaciones, suma de procedimientos manuales y automatizados.
- ✓ Tecnología, hardware, sistemas operativos, SGBD's, redes, multimedia, etc.
- ✓ Infraestructura, recursos para instalar y soportar los sistemas de información.

✓ Personas, habilidades, conocimientos y productividad para planificar, organizar, adquirir, entregar, soportar y supervisar sistemas y servicios de información.

3.3.4 El modelo CobiT – Estructura

La estructura de CobiT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".

Se definen 34 objetivos de control generales (OCGs), uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios (ver figura 2.6):

Figura 2.6. Fuente: COBIT

Los 34 OCGs (ver figura 2.7) propuestos se concretan en 302 objetivos de control detallados (OCDs).

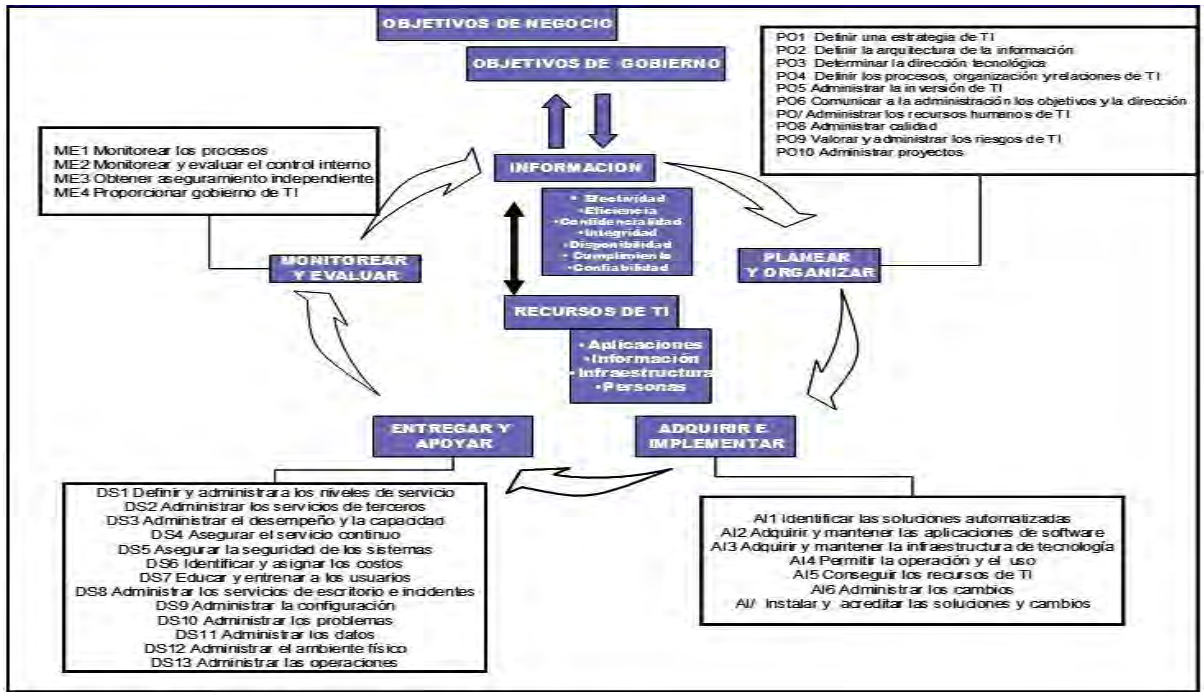


Figura 2.7 Fuente: COBIT

Un control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos de la educación superior se alcanzarán y que los eventos no deseados se preverán o se detectarán, y corregirán".

Un objetivo de control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de las TI".

En suma, la estructura conceptual (ver figura 2.8) se puede enfocar desde tres puntos de vista:

- Los *recursos* de las TI,
- Los *criterios empresariales* que debe satisfacer la *información*, y
- Los *procesos* de las TI.

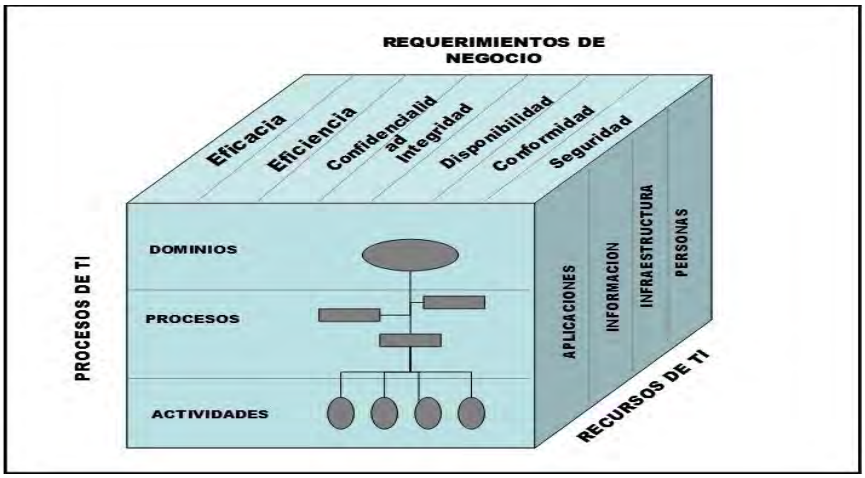


Figura 2.8 Fuente: COBIT

3.3.5 Objetivos de Control Generales

- ✓ **Planear y Organizar**
  - PO 1 Definir un Plan Estratégico de TI
  - PO 2 Definir la Arquitectura de la Información
  - PO 3 Determinar la Dirección Tecnológica
  - PO 4 Definir la Organización e Interrelaciones en TI
  - PO 5 Gestionar la Inversión en TI
  - PO 6 Comunicar Objetivos y Dirección a la Gerencia
  - PO 7 Gestionar los Recursos Humanos
  - PO 8 Asegurar Cumplimiento de los Requerimientos Externos
  - PO 9 Evaluar Riesgos
  - PO 10 Gestionar los Proyectos
  - PO 11 Gestión de la Calidad
- ✓ **Adquirir e Implementar**
  - AI 1 Identificación de Soluciones
  - AI 2 Adquisición y Mantenimiento de Aplicaciones Software

- AI 3 Adquirir y Mantener la Infraestructura Tecnológica
- AI 4 Desarrollar y Mantener los Procedimientos de TI
- AI 5 Instalación y Acreditación de Sistemas
- AI 6 Gestión de Cambios

✓ **Monitorear y Evaluar**

- M 1 Supervisar los Procesos
- M 2 Evaluar la Idoneidad del Control Interno
- M 3 Obtener Estimaciones Independientes
- M 4 Mantener una Auditoría Independiente

✓ **Entregar y dar Soporte**

- DS 1 Definir Niveles de Servicio
- DS 2 Gestionar los Servicios a Terceros
- DS 3 Gestionar el Rendimiento y la Capacidad
- DS 4 Asegurar un Servicio Continuo
- DS 5 Garantizar la Seguridad de los Sistemas
- DS 6 Identificar y Asignar Costes
- DS 7 Formar y Entrenar a los Usuarios
- DS 8 Asistir y Aconsejar a los Clientes de TI
- DS 9 Gestión de la Configuración
- DS 10 Gestionar Problemas e Incidentes
- DS 11 Gestionar los Datos
- DS 12 Gestionar las Infraestructuras
- DS 13 Gestionar las Operaciones

3.4. Auditoria

Conceptualmente la auditoria, toda y cualquier auditoria [Hernández 2000], “es la actividad consistente en la emisión de una opinión profesional sobre si el objeto

sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas".

El objeto hoy en día es Tecnología de la Información (TI), algunas áreas principales son:

- ✓ Bases de Datos;
- ✓ Software;
- ✓ Hardware;
- ✓ Redes de ordenadores;
- ✓ Sistemas Expertos;
- ✓ Agentes inteligentes;
- ✓ Redes neuronales;
- ✓ Ofimática;
- ✓ Inteligencia Artificial;
- ✓ Domótica.

La auditoría es la acumulación y evaluación objetiva de evidencia para establecer e informar sobre el grado de correspondencia entre la información examinada y criterios establecidos.

Sus principales características son:

- ✓ **Contenido,** una opinión.
- ✓ **Condición,** profesional.
- ✓ **Justificación,** sustentada en determinados procedimientos (la opinión profesional se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma).
- ✓ **Objeto,** una determinada información obtenida en un cierto soporte.
- ✓ **Finalidad,** determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

Es un proceso que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión. Por lo que urge, participar desde la concepción misma del proyecto de desarrollo de sistemas.

3.4.1. **Clases de** Auditoria

Las principales Clases de Auditoria [Sanchez 2000] son:

- ✓ Por el sujeto que la efectúa:
  - **Interna**, auditores que forman parte en la educación superior;
  - **Externa**, auditores ajenos a la organización;

- ✓ Por su contenido y fines:
  - **De Gestión,** afecta a la situación global de la comunidad educativa;
  - **Organizativa,** analiza la adecuación de la estructura organizativa;
  - **Operacional,** hasta qué punto se están cumpliendo los objetivos establecidos e identificación de los puntos que necesitan mejorar;
  - **Financiera,** examen y verificación del estado financiero, acompañado de una opinión sobre su fiabilidad;
  - **Contable,** adecuación de los criterios empleados para recoger los hechos mediante apuntes contables en los estados financieros;
  - **Informática,** examen y verificación del correcto funcionamiento y control del sistema informático en la educación superior;
  - **Económico-Social,** diagnóstico sobre el proceso económico y los resultados sociales obtenidos.

- ✓ Por su amplitud:
  - **Total,** afecta a toda la comunidad de la educación superior;
  - **Parcial,** se concentra en determinados elementos;
  - Por su frecuencia:
  - Permanente;

- Ocasional.

En forma específica, podemos señalar:

- ✓ **Auditoría financiera (contable):** La actividad del auditor consiste en revisar la correcta aplicación de los registros contables y operaciones financieras de las empresas;
- ✓ **Auditoría administrativa:** Es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones;
- ✓ **Auditoría operacional:** Es la revisión sistemática y exhaustiva, sistemática y especifica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones;
- ✓ **Auditoría integral:** Es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluarla de manera integral, todas sus áreas administrativas;
- ✓ **Auditoría gubernamental:** Es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental.
- ✓ **Auditoría informática:** Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos, y demás componentes;
- ✓ **Auditoría fiscal:** Es realiza a los registros y operaciones contables de una empresa;
- ✓ **Auditoría laboral:** Es realizada a las actividades, funciones y operaciones relacionadas con el factor humano de una empresa;

- ✓ **Auditoría de proyecto de inversión:** Es la revisión y evaluación que se realizan a los planes, programas y ejecución de las inversiones de los recursos económicos de una institución pública o privada;
- ✓ **Auditoría a la caja chica o caja mayor (arqueos):** Es la revisión periódica del manejo del efectivo que se asigna a una persona o área de una empresa, de los comprobantes de ingresos y egresos generados por sus operaciones cotidianas;
- ✓ **Auditoría al manejo de mercancías (inventarios):** Es la revisión física que se realiza a través del conteo de los bienes, productos y materias primas, intermedias o de consumo final de una empresa;
- ✓ **Auditoría ambiental:** Es la evaluación que se hace de la calidad del aire, la atmósfera, el ambiente, las aguas, ríos, lagos y océanos, así como la conservación de la flora y la fauna.

3.4.2. Definición de auditoría

La Auditoría representa el examen de los Estados Financieros de una entidad, con el objeto de que el Contador Público independiente emita opinión profesional respecto a si dichos estados presentan la situación financiera, los resultados de las operaciones, las variaciones en el capital contable y los flujos de efectivo de una empresa, de acuerdo a normativa vigente.

La auditoría tiene implicaciones relacionadas a la responsabilidad que el profesional asume, la cual toca los ámbitos ético, legal y moral.

3.4.3. Importancia de la auditoría

Los auditores en los negocios son muy importantes, por cuanto la gerencia sin la práctica de una auditoría no tiene plena seguridad de que los datos económicos registrados realmente son verdaderos y confiables. Es la Auditoría la que permite conocer con bastante razonabilidad la situación real de una empresa.

3.4.4 Razonabilidad de la información financiera

Los estados financieros de las empresas deben prepararse y presentarse de acuerdo a la política contable establecida, para que puedan tener razonabilidad en la presentación de la situación financiera, los resultados de las operaciones y los flujos de efectivo de la empresa.

Razonabilidad, es sinónimo de justicia, conforme a las políticas contables y criterios profesionales. La razonabilidad se concreta con la aplicación de los principios contables.

3.4.5 Control: base para el desarrollo de la auditoria

El control es una de las fases del proceso administrativo, le corresponde:

- Comparar los resultados obtenidos contra los resultados determinados en el proceso de planeación de la estrategia organizacional y de sus actividades tácticas y operativas con el fin de:
  - ✓ Determinar el nivel de cumplimiento y;
  - ✓ Ajustar los diferentes parámetros y características de los procesos mediante los cuales se busca el cumplimiento de los objetivos organizacionales.

Cualquier forma de control está basada en el uso de un lazo de retroalimentación (feedback) mediante el cual se compara la salida (output) del proceso o sistema controlado contra valores de referencia, de modo que al presentarse desviaciones, por exceso o por defecto, se produce una señal de "corrección" que debe ser alimentada al proceso para corregir las desviaciones observadas en la salida.

Control Interno

Han sido desarrollados para proveer una garantía razonable de que los objetivos del negocio serán alcanzados y que se previenen o detectarán y corregirán los casos de riesgo no deseados.

Los controles internos tales como las políticas, procedimientos, prácticas y estructuras organizativas son desarrollados y/o diseñados.

El control interno es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una seguridad razonable en cuanto a la consecución de objetivos:

- ✓ Eficacia y eficiencia de las operaciones;
- ✓ Confiabilidad de la información financiera;
- ✓ Cumplimiento de leyes y normas aplicables.

Componentes Control Interno

La entidad se esfuerza por alcanzar los objetivos para lo cual necesita de los siguientes componentes:

- ✓ **Ambiente de control**, propicio para el ejercicio de las actividades.
- ✓ **Evaluación de riesgos**, que atentan el logro de los objetivos de la entidad.
- ✓ **Actividades de control**, que permita minimizar los riesgos identificados.
- ✓ **Supervisión**, para evaluar el diseño y funcionamiento del control interno.

En resumen, el "ambiente de control": Es la base de los otros componentes, ya que en el ambiente de control se evalúan los riesgos y se definen las actividades de control y simultáneamente se capta información y se comunica bajo un proceso supervisado y corregido oportunamente.

Objetivos del Control Interno

Los objetivos del control interno son declaraciones del resultado deseado o del propósito a ser alcanzado implementando procedimientos de control. En otras palabras, control es el medio por el cual se alcanzan los objetivos de control.

Esquemas metodológicos tradicionales

- ✓ Auditoria de cumplimiento – un enfoque reactivo
- ✓ auditoria del Cumplimiento de un estándar
- ✓ Auditoría de Cumplimiento de una "mejor práctica"
- ✓ Auditoria del Cumplimiento de la *opinión del auditor*
- ✓ Auditoria del desarrollo de sistemas – un enfoque proactivo
- ✓ Aseguramiento interno – un enfoque coactivo

3.4.6 Control Interno – Marco Integrado

3.4.6.1 ¿Qué es COSO? (ver figura 2.9)

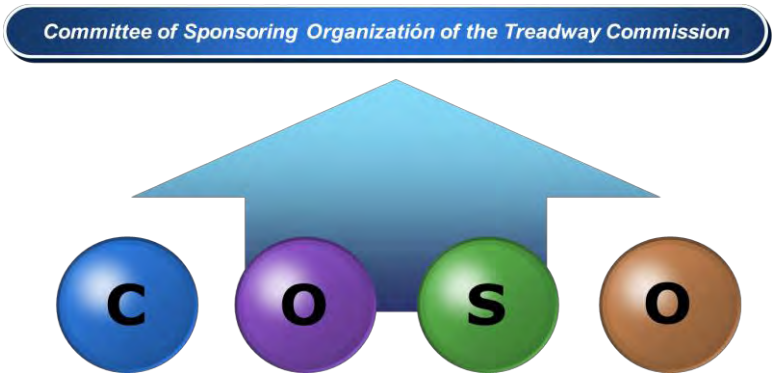


Figura 2.8 Fuente: COSO

Organización voluntaria del sector privado, establecida en los EEUU, dedicada a proporcionar orientación a la gestión ejecutiva y las entidades de gobierno sobre los aspectos fundamentales de organización de este, la ética empresarial, control interno, gestión del riesgo empresarial, el fraude, y la presentación de informes financieros.

COSO ha establecido un modelo común de control interno contra el cual las empresas y organizaciones pueden evaluar sus sistemas de control.

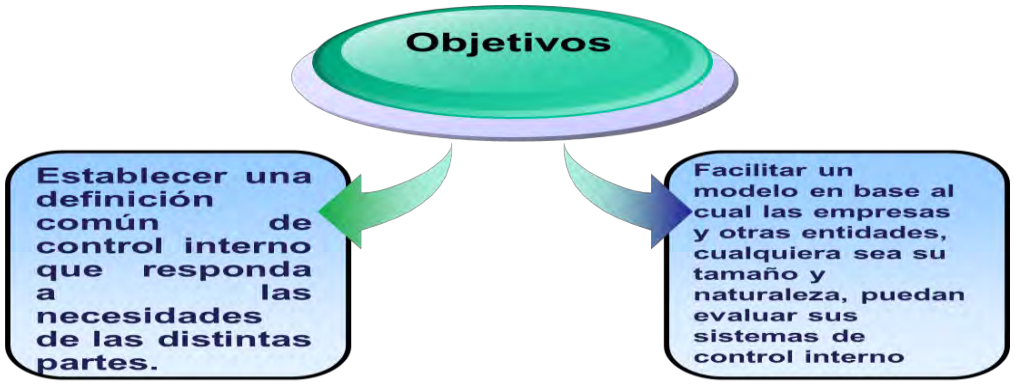
3.4.6.2 Informe COSO

Hacia fines de Septiembre de 2004, como respuesta a una serie de escándalos, e irregularidades que provocaron pérdidas importante a inversionistas, empleados y otros grupos de interés, nuevamente el Committee of Sponsoring Organizations of the Treadway Commission, publicó el Enterprise Risk Management - Integrated Framework (COSO II) y sus Aplicaciones técnicas asociadas, el cual amplía el concepto de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral de riesgo.

A nivel organizacional, este documento destaca la necesidad de que la alta dirección y el resto de la organización comprendan cabalmente la trascendencia del control interno, la incidencia del mismo sobre los resultados de la gestión, el papel estratégico a conceder a la auditoría y esencialmente la consideración del control como un proceso integrado a los procesos operativos de la empresa y no como un conjunto pesado, compuesto por mecanismos burocráticos.

A nivel regulatorio o normativo, el Informe COSO ha pretendido que cuando se plantee cualquier discusión o problema de control interno, tanto a nivel práctico de las empresas, como a nivel de auditoría interna o externa, o en los ámbitos académicos o legislativos, los interlocutores tengan una referencia conceptual común, lo cual hasta ahora resultaba complejo, dada la multiplicidad de definiciones y conceptos divergentes que han existido sobre control interno.

3.4.6.3 Objetivos de COSO



COSO I y COSO II ERM

COSO: Marco conceptual integrado, 1992

COSO ERM: Marco de Gestión Integral de Riesgo, 2004

3.4.6.4 Componentes COSO:

Ambiente de Control:

Sirve como la base fundamental para los otros componentes del ERM, dándole disciplina y estructura.

Dentro de la empresa sirve para que los empleados creen conciencia de los riesgos que se pueden presentar en la empresa;

Evaluación del Riesgos:

Identificación y análisis de los riesgos relevantes para la consecución de los objetivos, constituyendo una base para determinar cómo se deben administrar los riesgos. Las respuestas: evitarlo, reducirlo, compartirlo, aceptarlo;

Actividades de Control:

Son las políticas y procedimientos para asegurar que las respuesta al riesgo se lleve de manera adecuada y oportuna. Tipos: Preventiva, detectivas, manuales, computarizadas o controles gerenciales;

Establecimiento de objetivos.

Es importante para que la empresa prevenga los riesgo, tenga una identificación de los eventos, una evaluación del riesgo y una clara respuesta a los riesgos en la empresa.

La empresa debe tener una meta clara que se alineen y sustenten con su visión y misión, pero siempre teniendo en cuenta que cada decision con lleva un riesgo que debe ser previsto por la empresa;

Identificación de eventos:

Se debe identificar los eventos que afectan los objetivos de la organización aunque estos sean positivos, negativos o ambos, para que la empresa los pueda enfrentar y proveer de la mejor forma posible.

La empresa debe identificar los eventos y debe diagnosticarlos como oportunidades o riesgos. Para que pueda hacer frente a los riesgos y aprovechar las oportunidades;

Información y Comunicación:

La información es necesaria en todos los niveles de la organización para hacer frente a los riesgos identificando, evaluando y dando respuesta a los riesgos.

La comunicación se debe realizar en sentido amplio y fluir por toda la organización en todo los sentidos.

Debe existir una buena comunicación con los clientes, proveedores, reguladores y accionistas;

Monitoreo:

Sirve para monitorear que el proceso de administración de los riesgos sea efectivo a lo largo del tiempo y que todos los componentes del marco ERM funcionen adecuadamente.

El monitoreo se puede medir a través de: Actividades de monitoreo continuo y evaluaciones puntuales.

3.4.6.5 Control Interno versus Auditoria Interna

- ✓ **Control Interno:** es un sistema que interrelaciona controles financieros, administrativos, contables, etc. ideados y puestos en práctica por los directivos de la organización con el objetivo de que su gestión sea ordenada, sus activos sean preservados y sus registros sean correctos. Su desventaja es que no garantiza una administración eficiente ni evita el fraude dado por la complicidad entre los directivos con cargos de confianza.
- ✓ **Auditoria Interna:** es la actividad dedicada a realizar una revisión de operaciones contables, financieras, operativas, etc., aplicadas por la gerencia de la empresa con el objetivo de evaluar la eficacia del control interno. Es desempeñada por un departamento dependiente directamente de la gerencia de la empresa, con un staff ubicado en la estructura jerárquica del organigrama.

3.4.6.6 Control Interno Informático

El control interno y la auditoria son facetas que nos son conocidas en general en otros ambientes, tales como en el ámbito contable y/o en el financiero pero no lo son tanto en el informático. Y mucho menos lo son teniendo en cuenta que algunos componentes tecnológicos actuales que permiten el almacenamiento, procesamiento y

administración de los datos se han desarrollado hace no muchos años atrás y solo han alcanzado su masificación en estos últimos años, con lo que han permitido una evolución del software gradual pero acelerada. Esa misma evolución es la que ha proporcionado distintos mecanismos para agrupar, compartir y asegurar la consistencia y baja redundancia de los datos de una organización.

Es a partir de conseguir estos objetivos que anteriormente eran críticos para esa misma organización es que comenzó a surgir la necesidad de verificar y controlar la validez, integridad y seguridad de los datos acumulados como así también de las operaciones que los manipulan.

Componentes auditables

- ✓ Auditoria Física;
- ✓ Auditoria Ofimática;
- ✓ Auditoria de la Dirección;
- ✓ Auditoria de la Explotación;
- ✓ Auditoria del Desarrollo;
- ✓ Auditoria del Mantenimiento;
- ✓ Auditoria de Bases de datos;
- ✓ Auditoria de técnicas de Sistemas;
- ✓ Auditoria de Calidad;
- ✓ auditorias de la Seguridad;
- ✓ Auditoria de Redes;
- ✓ Auditoria de Aplicaciones.

Posibles problemas

Es bien conocido o debería serlo por parte de los profesionales en Sistemas el aspecto relevante del control interno en todas las áreas relacionadas a la informática y en

particular a los sistemas de información y al ciclo de vida de los mismos. Además de ello hay que tener en cuenta que este se encuentra inmerso dentro de una organización en la cual tiene sentido, ya que su objetivo es aportar al desarrollo de la misma, permitiéndole alcanzar su finalidad empresarial a través del crecimiento administrativo, financiero y de gestión.

En particular los datos manejados por un sistema de información de la organización son el activo más importante en la toma de decisión para la consecución de los objetivos.

Ahora bien, el hecho de que esos datos y sus operaciones sean manipulados por seres humanos les agrega una componente de error, voluntario o no, que implica un riesgo para la organización.

Se desprende de aquí la necesidad de realizar Auditorías Informáticas y como parte de ellas la de poder analizar trazas de actividad de los usuarios sobre los datos de las aplicaciones.

3.4.6.7 El Auditor Informático

Existen aspectos contrapuestos entre los auditores actuales que quieren desempeñarse dentro de la auditoria informática ya que los auditores dedicados a la auditoría financiera y/o contable que poseen amplia experiencia en esas áreas no la poseen en tecnologías de información, debido a que estas no se hallaban presentes en su formación básica mientras que los profesionales informáticos adolecen de materias cuyos contenidos contengan temas sobre organización, planificación y administración de recursos como tampoco de técnicas de auditoria de administración de datos.

Además estos últimos tampoco podrían auditar cualquier tipo de sistema de información dado que su variedad junto a las diferentes tecnologías que los pueden integrar hacen difícil que un mismo profesional pueda especializarse en todas ellas.

3.5 Auditoría 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.

3.5.1 Sistemas de Bases de Datos auditables

El control interno como la auditoria empezó a prosperar en la informática concentrándose en el objeto que se controla o audita, el Sistema de Información y sus componentes. En nuestro caso las Bases de Datos y los DBMS utilizados.

Eso hace que los auditores deban seleccionar diferentes soluciones dependiendo de la infraestructura de datos del modelo auditado. Tanto desde el punto de vista legal como desde el punto de vista de auditoria es requerido que los sistemas de bases de datos puedan registrar la actividad sobre datos claves, para posteriormente poder rastrear el momento y el usuario que ha realizado una determinada modificación, incorporación o eliminación de datos.

Por lo que, prevenir, evitar y/o restringir tales riesgos se convierte en una tarea y un reto profesional difícil de relegar para aquellos que trabajan cotidianamente con Bases de Datos y les interese garantizar su integridad, confidencialidad y fiabilidad en el mayor grado posible.

3.5.2 Capas auditables

- ✓ DBMS, componentes auditables
  - Políticas de administración de datos;
  - Políticas de actualización del software;
  - Políticas de tuning.
- ✓ Bases de Datos, componentes auditables:
  - Esquema conceptual;
  - Diseño de Base de Datos;
  - Tablas;
  - Restricciones.

Estos últimos componentes son objeto del estudio y desarrollo del presente proyecto.

3.5.3 Metodologías para la auditoria de Bases de Datos

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

3.5.4 Metodología tradicional

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

DESCRIPCIÓN	S	N	NA
¿Existe una metodología de diseño de BD?			

El auditor deberá registrar el resultado de su investigación: S, si la respuesta es afirmativa, caso contrario con N, NA (no aplicable).

Este tipo de técnica suele ser aplicada a la auditoría de bases de datos, especificándose en la lista de control todos los aspectos a tener en cuenta. Así, por ejemplo, si el auditor se enfrenta a un entorno Oracle 8, en la lista de control se recogerán los parámetros de instalación que más riesgos comportan, señalando cuales su rango adecuado. De esta manera si el auditor no cuenta con la asistencia de un experto en el producto, puede comprobar por lo menos los aspectos más importantes de su instalación.

3.5.5 Metodología de evaluación de riesgos

Este tipo de metodología, conocida también por risk oriented approach, es la que propone la ISACA y empieza fijando los objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno. Los riesgos más importantes que lleva consigo la utilización de una base de datos. Considerando estos riesgos, se podrían definir por ejemplo el siguiente:

Objetivo de control:

El SGBD deberá preservar la confiabilidad de la base de datos.

Una vez establecidos los objetivos de control, se especifican las técnicas específicas correspondientes a dichos objetivos.

Técnicas de control:

Se establecen los tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a la base de datos.

- ✓ Incremento de dependencia del servicio informático debido a la concentración de datos;
- ✓ Mayores posibilidades de acceso en la figura del administrador de la Base de Datos;
- ✓ Incompatibilidades entre sistemas de seguridad de acceso propios del SGBD y el general de la instalación:
- ✓ Mayor impacto de los errores de datos o programas que en los sistemas tradicionales;
- ✓ Ruptura de enlaces o cadenas por fallos del software o de los programas de aplicación;
- ✓ Mayor impacto de accesos no autorizados al diccionario de la Base de Datos que a un fichero tradicional;
- ✓ Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas con el software de Bases de Datos.

Un objetivo de control puede llevar asociadas varias técnicas que permiten cubrirlo en su totalidad. Estas técnicas pueden ser:

- ✓ Preventivas (como las mencionadas líneas arriba);
- ✓ Detectivas (como monitorizar los accesos a la BD);
- ✓ Correctivas (por ejemplo, una copia de respaldo).

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

Prueba de cumplimiento:

Listar los privilegios y perfiles existentes en el SGBD.

Si estas pruebas detectan inconsistencias en los controles, o bien, si los controles no existen, se pasa a detectar otro tipo de pruebas (denominadas pruebas sustantivas) que permitan dimensionar el impacto de estas deficiencias.

Prueba sustantiva:

Comprobar si la información ha sido corrompida comparándola con otra fuente, o revisando, los documentos de entrada de datos y las transacciones que se han ejecutado.

Una vez valorados los resultados de las pruebas se obtienen unas conclusiones que serán comentadas y discutidas con los responsables directos de las áreas afectadas con el fin de corroborar los resultados. Por último, el auditor deberá emitir una serie de comentarios donde se describa la situación, el riesgo existente y la deficiencia a solucionar que ha tenido la auditoria.

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

Esta será la técnica a utilizar para auditar el entorno general de un sistema de Bases de Datos, tanto en su desarrollo como durante su explotación.

3.6 El proceso de la auditoría informática

El proceso de la auditoría informática (Echenique, 1990) es similar al que se lleva a cabo a los de estados financieros, en el cual, los objetivos principales son:

salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias.

Para que una auditoría sea exitosa, debe tomar en cuenta básicamente 3 etapas:

a) Planificación de la auditoría Informática;

b) Ejecución de la auditoría Informática;

c) Finalización de la auditoría Informática.

3.6.1 Planificación de la auditoría Informática

En esta fase se establecen las relaciones entre auditores y colaboradores de la organización, para determinar el alcance y objetivos. Se hace un bosquejo de la situación de la entidad, acerca de su organización, sistema contable, controles internos, estrategias y demás elementos que le permitan al auditor elaborar el programa de auditoría que se llevará a efecto.

Elementos Principales de esta Fase:

1. Conocimiento y Comprensión de la Entidad;
2. Objetivos y Alcance de la auditoría;
3. Análisis Preliminar del Control Interno;
4. Análisis de los Riesgos;
5. Planeación Específica de la auditoría;
6. Elaboración de programas de Auditoría.

3.6.1.1 Objetivos de control en el ciclo de vida de una Base de Datos

Consideraremos algunos objetivos y técnicas de control a tener en cuenta a lo largo del ciclo de vida de una base de datos, quea barca desde el estudio previo hasta su explotación.

Estudio previo y plan de trabajo

Es esta primera fase, es muy importante elaborar un estudio tecnológico de viabilidad en el cual se contemplen distintas alternativas para alcanzar los objetivos del proyecto acompañados de un análisis coste-beneficio para cada una de las opciones. Se debe considerar entre estas alternativas la posibilidad de no llevar a cabo el proyecto (no siempre está justificada la implantación de un sistema de bases de datos) así como la disyuntiva entre desarrollar y comprar (en la práctica, a veces nos encontramos con que se ha desarrollado una aplicación que ya existía en el mercado, cuya compra hubiese supuesto un riesgo menor, asegurándonos incluso una mayor calidad a un precio inferior).

Desafortunadamente, en muchas empresas este estudio de viabilidad no se lleva a cabo con el rigor necesario, con lo que a medida que se van desarrollando, los sistemas demuestran, a veces, ser poco rentables.

3.6.2 Ejecución de la auditoría Informática

La ejecución de la auditoría informática, constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI. Para la recolección de información, se pueden aplicar las siguientes técnicas:

- ✓ Entrevistas;
- ✓ Simulación;
- ✓ Cuestionarios;
- ✓ Análisis de la información documental entregada por el auditado;
- ✓ Revisión y Análisis de Estándares;

- ✓ Revisión y Análisis de la información de auditorías anteriores.

La evidencia se clasifica de la siguiente manera:

a) Evidencia documental.

b) Evidencia física.

c) Evidencia analítica.

d) Evidencia testimonial.

Una vez que tenemos información real y confiable, procedemos a evaluar y probar la manera en la que han sido diseñados los controles en la organización, para el mejoramiento continuo de la misma, para esto el equipo de Auditoría utilizara medios informáticos y electrónicos que permitan obtener resultados reales.

El equipo de auditores, para poder dar una opinión sobre un sistema o proceso informático, debe comprobar el funcionamiento de los sistemas de aplicación y efectuar una revisión completa de los equipos de cómputo

3.6.3 Finalización de la auditoría Informática

Para finalizar un proceso de Auditoría Informática, se debe presentar un informe que contenga conclusiones y recomendaciones, necesarias para que una empresa este en mejoramiento continuo, esta documentación debe ser redactada por el equipo de Auditoría y entregarse a la Alta Dirección de la empresa para su evaluación y análisis.

CAPITULO IV

Desarrollo

4.1. Fundamentos del método

Se hace imperiosa la necesidad, a raíz de lo enunciado en capítulos anteriores, que efectúen auditorías a las Bases de Datos Relacionales, basadas en la gestión de riesgos, los mismos que estén acordes con estándares y normas internacionales para la auditoria.

El método de Gestión de Riesgos para la Auditoria de Base de Datos Relacional, se basa en conceptos como la Auditoria Financiera, Bases de Datos, modelo COSO, y la metodología COBIT.

4.1.1. Características del método

El método que se propone a ser implementada tiene las siguientes 3 características:

- ✓ **Está enfocada a diferentes áreas funcionales,** la auditoria basada en la gestión de riesgos es aplicable a todo tipo de áreas y/o departamentos del negocio, específicamente en la empresa "CUEROSBOL", por lo cual los estándares, normas y prácticas de auditoria son amplios.
- ✓ **Es genérica,** en la actualidad, existen organizaciones que cuentan con diversos sistemas para diferentes niveles que coadyuvan a la labor de las personas que cumplen también roles determinados. Por lo que la metodología será genérica para poder ser aplicable a cada una de estas unidades, conservando la independencia con respecto a las plataformas tecnológicas.
- ✓ **Esta adecuada a la realidad de nuestro país,** la brecha cultural entre los países desarrollados y los países subdesarrollados como la nuestra, de alguna manera incidirán en el alcance del modelo que se plantea.

4.1.2. Objetivos generales del modelo

Para aplicar el modelo se requiere la participación efectiva de los actores de la organización, como los accionistas, unidades de auditoria interna, unidades de sistemas como principales entes primarios. El método trata de satisfacer los siguientes objetivos:

- ✓ **Objetivos para la alta gerencia,** los diferentes niveles de autoridad en la organización: directores, unidades de auditoría interna, gerentes administrativos, trabajadores del conocimiento, gerentes operativos, luego de brindar apoyo técnico y económico para la implantación del modelo, podrán contar con información oportuna y fiable para una adecuada toma de decisiones.
- ✓ **Objetivos para unidades de auditoria interna,** incentivar a que las unidades de auditoria interna, no solo se dediquen al control interno financiero, mas al contrario realicen esfuerzos para que efectúen una adecuada evaluación técnica y administrativa de los recursos tecnológicos, con el fin de minimizar los riesgos.

4.2. Desarrollo del método

La auditoria y control interno o externo implica la aplicación de métodos rigurosos en conformidad con los estándares y las directrices de auditoria de Bases de Datos generalmente aceptados para proveer una garantía razonable de que la tecnología de información (TI) y los sistemas de información en la organización sean controlados, supervisados y determinados de una manera adecuada.

La aplicación del modelo, puede definirse como un proceso sistemático, por el cual el auditor de Base de Datos Relacional (BDR) obtiene y evalúa objetivamente evidencias respecto a afirmaciones sobre el objeto que es sometido a análisis con el fin de formarse una opinión sobre ello y reportar sobre el grado en que dicha afirmación se ajusta a un conjunto de estándares.

El modelo se dividirá en tres etapas ver Fig. 4.1:

La función de Gestión de Riegos para la Auditoría de Base de Datos Relacional se basa en un cuestionario de diagnóstico (ver Tabla 4.1) preliminar, luego debe estar contemplada en el POA (Programación Operativa Anual) que establezca con claridad los cursos de acción que justifiquen el desarrollo de la función de auditoria en la

organización para la aplicación del modelo y para delegar autoridad a la función de auditoria.

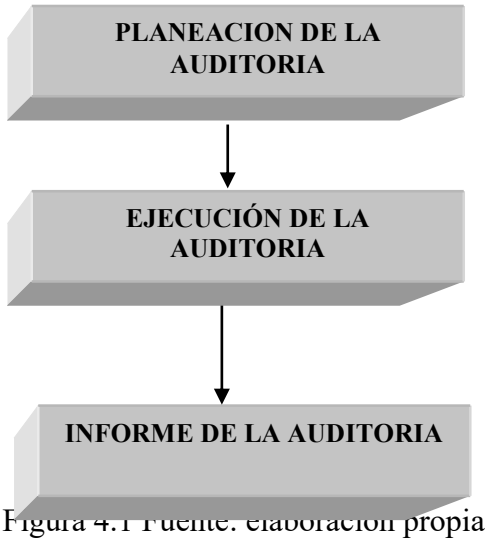


Figura 4.1 Fuente: elaboración propia

El análisis preliminar de control interno reviste de vital importancia, porque del resultado se comprenderá la naturaleza y extensión del plan de auditoria y la valoración y oportunidad de los procedimientos a utilizarse durante el examen.

El análisis, incluye a la dirección y las áreas usuarias. De la dirección, se intenta poder saber el grado de satisfacción y confianza que tiene en los productos, servicios y recursos informáticos. Este primer paso, también sirve para detectar las fortalezas, aciertos y apoyos que brinda la función de informática y las oportunidades de negocio que ésta puede ofrecer para hacerle más competitivo.

El documento o memorando debe ser emitida por la alta gerencia describiendo la autoridad general, el alcance y las responsabilidades de la función de auditoria. Al fin y al cabo, la alta gerencia serán los responsables de desarrollar e implementar planes a largo y corto plazo que satisfagan los objetivos institucionales.

Este es un primer paso fundamental para llevar adelante auditorías a unidades de la organización, antes de aplicar las tres etapas que se propone en el presente trabajo. Para la ejecución de cada etapa del modelo, se considera los elementos de entrada, procesamiento de esos elementos de entrada y generar elementos de salida.

CONCEPTO	DESCRIPCION	OBSERVACIONES
Plan estratégico de la organización (solicitar organigrama)		
Áreas funcionales de la organización * *		
Políticas, estándares referente a la gestión de riesgos *		
Manual de funciones, planes de contingencia, seguridad, informes *		

¿Existe una gestión de riesgos en el Área de Sistemas **1 = Excelente, 2 = Buena**

Soluciones de consultoría - Asesoría y soporte en la definición, evaluación y selección de estrategias para minimizar riesgos.	( ) ( ) ( ) ( )
Soluciones de configuración - Se realizan escaneos periódicos de seguridad para detectar posibles infecciones al software, Se realizan evaluaciones de la configuración?	( ) ( ) ( ) ( )
Soluciones de diseño de Base de Datos - El modelo conceptual de la Base de Datos, es el adecuado?	( ) ( ) ( ) ( )
Servicios operativos - Instalación de Software, equipos y redes - Capacitación al personal en el uso de herramientas de BD - Soporte a fallas de software - Soporte a fallas de hardware y comunicaciones	( ) ( ) ( ) ( )

Tabla 4.1 Cuestionario de diagnóstico preliminar

4.2.1 Etapa de planeación de la auditoria

La Fig. 4.2 muestra un plan de ejecución de la etapa de planeación.

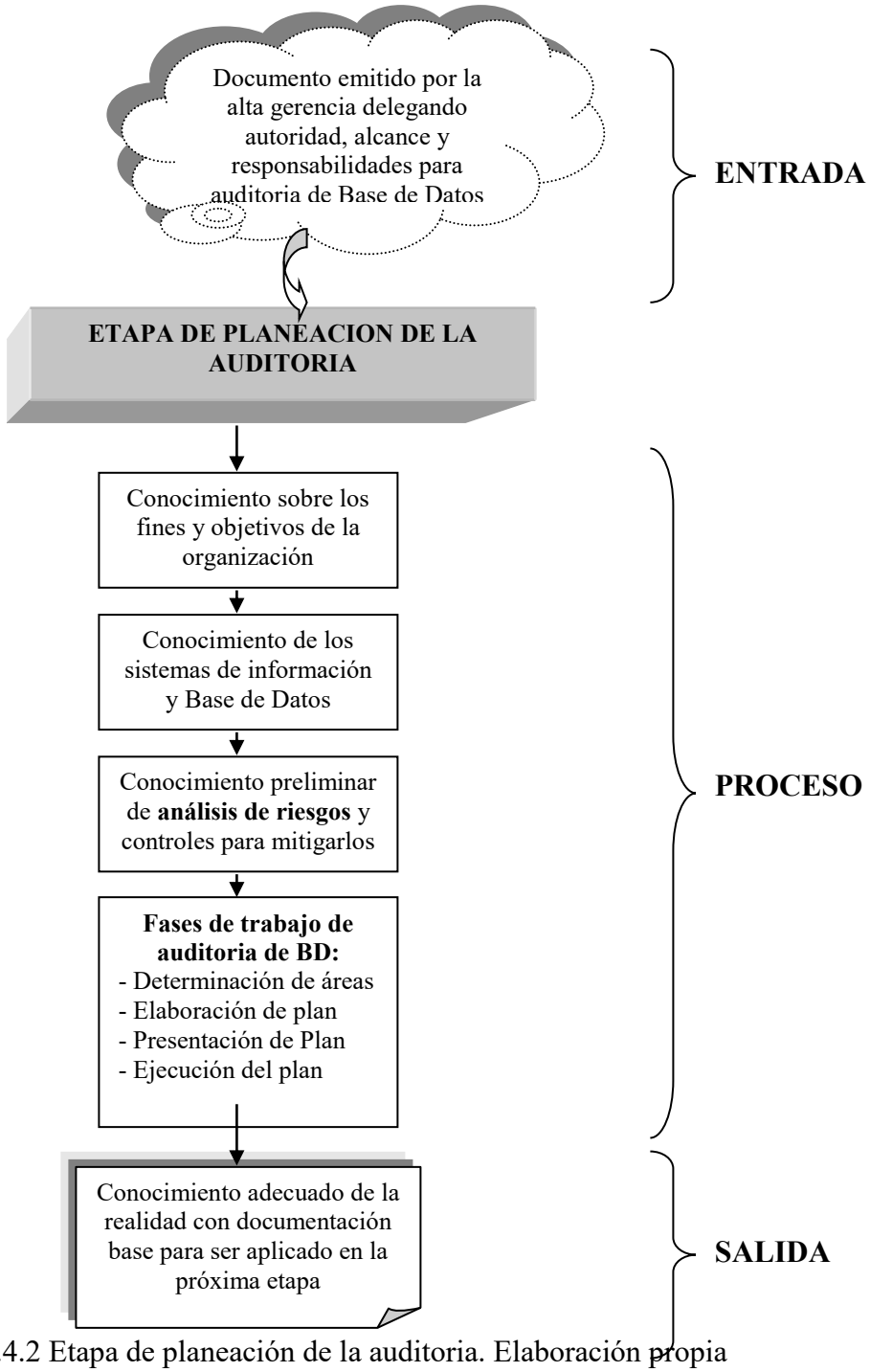


Figura.4.2 Etapa de planeación de la auditoria. Elaboración propia

Elementos de entrada para la planeación

Los elementos de entrada para la etapa de planeación, están constituidos por la aprobación documentada de la realización de la auditoria a una determinada unidad de la organización por parte de la alta gerencia, adjuntado documentación para delegar autoridad y alcance a la función de auditoria de Base de Datos Relacional.

Proceso de la planeación

Antes de iniciar una auditoria de Base de Datos, es imprescindible realizar una planificación adecuada. La planeación consiste tanto a corto plazo que toma en cuenta los problemas de auditoria que serán cubiertos durante el año, como a largo plazo que se refiere a los planes de auditoria que tomaran en cuenta los cambios en la dirección estratégica de la tecnología de la información y comunicación de los entes superiores y los cambios que ocurrirán en el ambiente de TIC.

Entre las actividades a ejecutar en la etapa de planificación, podemos señalar los siguientes:

Conocimiento sobre los objetivos estratégicos de negocio y los objetivos de los procesos de negocio

Proveen una línea de acción dentro del dominio organizacional, La documentación clave a recopilar y evaluar será:

- Plan estratégico de la organización y del centro de procesamiento de la información;
- Planes a corto, mediano y largo plazo del área de TI;
- Políticas, estándares y procedimientos para el área de SI;
- Estructura organizacional;
- Manual de funciones y responsabilidades del personal del área de sistemas;
- Planes de contingencia y seguridad;
- Informes de auditorías efectuadas en anteriores gestiones.

4.2.1.2.2 Conocimiento de los Sistemas de Información en la organización

A través de este procedimiento se documentara todos los sistemas de información y la tecnología que la soporta, diseño de la Base de Datos y requerimientos de la entidad que cumplan sus objetivos trazados. El ASI, en base a este conocimiento, podrá detectar debilidades y fortalezas a procesos operativos, diseño y de la calidad, oportunidad y eficiencia de la información producida y administrada por el sistema Informatico. La información relevante a reunir será:

- ✓ Tecnología de soporte,
- ✓ Software de gestor de Base de Datos,
- ✓ Tipos de reportes,
- ✓ Portabilidad e interfases con otros sistemas,
- ✓ Procedimientos y controles escritos sobre las aplicaciones en explotación
- ✓ Contratos de adquisición de sistemas y soporte.

El sistema en explotación (ver figura 4.3) de la Empresa de cueros "CUEROBOL", muestra la pantalla principal:

Figura.4.3 Sistema StockBase

El menú principal (ver figura 4.4), contiene módulos como:

- ✓ Productos,
- ✓ clientes,
- ✓ proveedores,
- ✓ vendedores,
- ✓ caja,

- ✓ ventas, compras

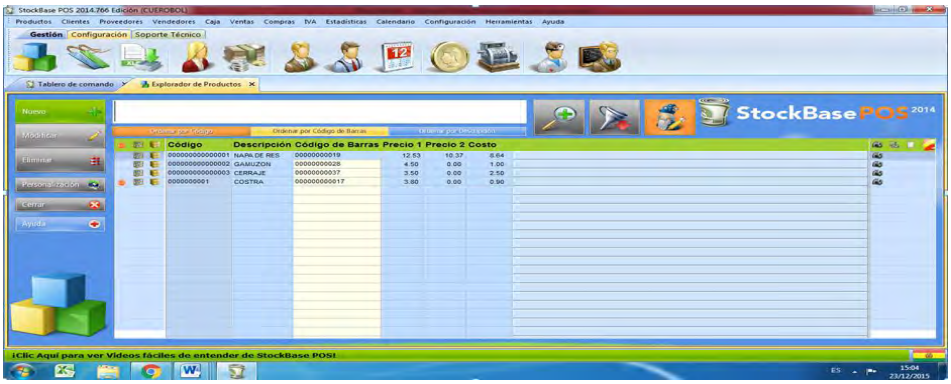


Figura.4.4 Menú del sistema

4.2.1.2.3 Conocimiento preliminar del análisis de riesgos

En base a la documentación reunida. El análisis del riesgo permite identificar los riesgos y vulnerabilidades para determinar los controles que se necesitan para mitigar esos riesgos (directrices para la Gerencia de Seguridad de TI publicados por la ISO)[1]. Es importante poder identificar y diferenciar los tipos de riesgo y los controles usados para mitigarlos. Los riesgos tienen los elementos siguientes:

- ✓ Amenazas a los procesos
- ✓ Amenazas a los activos,
- ✓ Impacto sobre los activos basados en amenazas y vulnerabilidades,
- ✓ Probabilidades de amenazas.

Los riesgos en la organización son las amenazas que pueden tener un impacto sobre los activos o sobre los procesos u objetivos. Se debe enfocar en una clase particular de riesgos asociados con la información y con los Sistemas de Información y procesos subyacentes de información que generan, almacenan y manipulan la información. Esta clase de riesgos posibilita la perdida de confidencialidad, disponibilidad o integridad de la información.

[1] "El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y ocasiones perdida o daño a los activos. El impacto o severidad relativos del riesgo es proporcional al valor de la perdida/daño y a la frecuencia estimada de la amenaza para el negocio"

Por lo tanto, se debe administrar el riesgo, identificando las debilidades y amenazas y decidir que contramedidas llevar adelante, para reducir el nivel de riesgo hasta un nivel aceptable. En general, el riesgo puede ser transferido, rechazado, reducido o aceptado.

Las amenazas ocurren a causa de las vulnerabilidades (conocimientos limitados del personal, planes de contingencia inadecuados, modelo conceptual deficiente, herramienta inadecuada, tecnología de soporte no probada, redes de ordenadores no protegidas).

4.2.1.1.4. **Fases de trabajo,** en base a la documentación reunida y determinado el riesgo tecnológico, se deben definir las fases de auditoria, que consiste en procedimientos totalmente documentados para alcanzar los objetivos de la auditoria a sistemas de información planificada.

El proceso de planeación de la auditoria de Base de Datos, comprenderá el desarrollo de cuatro fases ver Figura. 4.5:

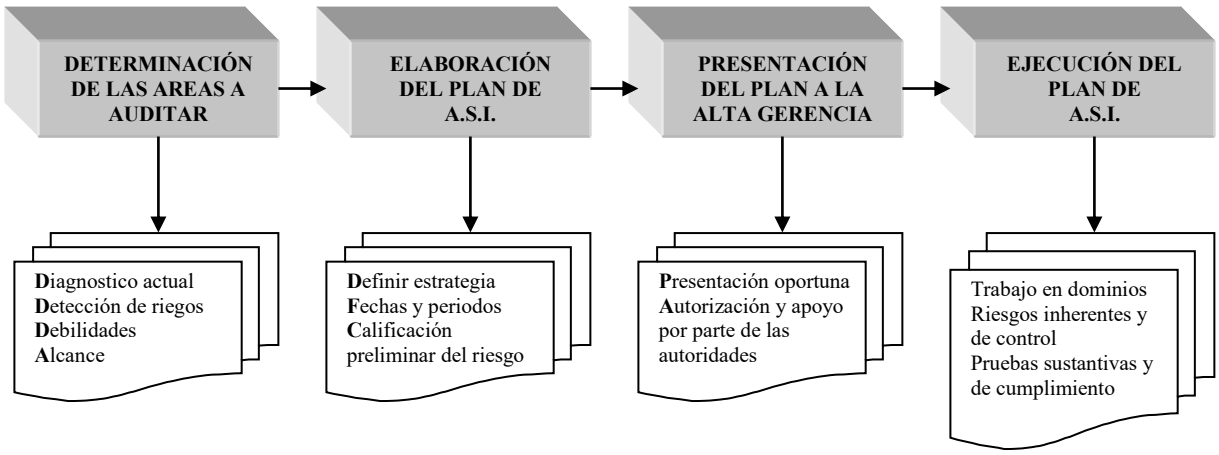


Figura.4.5 Fases para la planeación

- Determinación de las áreas a auditar:
  - Tener una comprensión adecuada de las áreas funcionales (ventas y marketing, manufactura y producción, finanzas y contabilidad, recursos humanos) en la organización,
  - Entender el accionar, objetivos trazados, proceso y tecnología con que cuenta la organización,
  - Conocer los requerimientos, naturaleza y condiciones de sus sistemas actuales
  - Efectuar una revisión del control interno,
  - Establecer el alcance en base a procedimientos.

    La amplitud y profundidad de los procedimientos que se apliquen definen su alcance,
  - Lograr una valoración preliminar del riesgo tecnológico de las áreas funcionales, debilidades y fortalezas, a través de la matriz de riesgos (ver tabla 4.2) cuyo objetivo principal es detectar riesgos (ver Tabla 4.3) de mayor peligro y que requieren una revisión formal y oportuna, utilizando parámetros de medición y evaluación posibles sin caer en un análisis detallado, ya que solo se trata de detectar la problemática principal de cada área.

    Si al evaluar se advierte anomalías de considerable importancia, se deben tomar acciones inmediatas con el fin de eliminarlas o al menos minimizarlas.

    Los parámetros para medir el nivel de riesgo se pueden basar en la experiencia y conocimiento sobre el control de riesgos o el grado de profundidad que se desee dar a la auditoria

ÁREA FUNCIONAL: **JEFE AUDITORIA INTERNA:** **FECHA ELABORACIÓN**

4. AREAS SUCEPTIBLE A AUDITAR	ASPECTOS O ELEMENTOS A EVALUAR	RIESGO POR ELEMENTO	CLASIFICACION DEL RIESGO	AREA POR AUDITAR SEGÚN CLASIFICACION
Departamento de informática	- Misión y objetivos - Organización - Servicios - Parámetro de medición			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Usuarios de informática	- Comunicación - Administración de recursos - Grado de satisfacción			Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
Control interno	- Políticas y procedimientos			Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
Ciclo de diseño e implementación de Bases de Datos	- Métodos - Técnicas - Herramientas - Capacitación			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Mantenimiento	- Hardware - Software - Sistemas de información - Telecomunicaciones			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Redes LAN	- Administración - Instalación - Operación / seguridad			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Telecomunicaciones	- Administración - Instalación - Operación / seguridad			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Hardware	- Administración - Instalación - Operación / seguridad			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Software	- Administración - Instalación - Operación / seguridad			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Seguridad	- Hardware - Software - Plan de contingencia			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
herramientas	- Métodos - Técnicas - Herramientas - Capacitación			Pasos para auditar cada componente y área según el nivel de riesgo estimado.
Datos	- Métodos - Técnicas - Herramientas - Capacitación			Pasos para auditar cada componente y área según el nivel de riesgo estimado.

Tabla 4.2 Matriz de riesgos

ACTIVIDAD	RIESGOS
Software sin licencia	- Problemas legales - Mala imagen como ente superior - Amenazas de virus - Dificultad de actualizar a niveles de usuarios.
Inexistencia de métodos y procedimientos para un control efectivo	- Trabajo desarrollado según el criterio de cada individuo, - Sistemas individualistas - No existe seguimiento al desarrollo de sistemas de información, - No se utiliza un método formal, - Dependencia hacia el personal que desarrollo el sistema.
Comunicación casi nula entre desarrolladores y las autoridades de la organización	- Desconocimiento de objetivos de la institución - Desviación en cumplimiento a de requerimientos de la comunidad, - Prioridades no atendidas, - Recursos tecnológicos desperdiciados - Falta de compromiso con la institución,

Tabla 4.3 Detección de riesgos

Para comprender o conocer las áreas funcionales, el auditor de sistemas de información (ASI) debe seguir los siguientes pasos:

- Recorrer las instalaciones clave de las áreas funcionales (centros de cómputo, jefatura de sistemas, área de desarrollo de sistemas, área de análisis y diseño de sistemas, área de diseño de bases de datos, área de control de calidad),
- Obtener conocimiento de la actividad organizacional (ventas, compras, registro contable, clientes, proveedores, productos),
- Entrevistas a personas clave de las áreas funcionales,
- Revisar reportes anteriores.

➢ Elaboración del plan (ver Tabla 4.4):

- Área a auditar, matriz de riesgos, prioridades de las autoridades,
- El plan elaborado en esta es general, ya que solo busca plantear los datos básicos para que las autoridades respectivas analice y apruebe,

- Estimar el tiempo necesario para auditar cada área determinada en la matriz de riesgos,
- Definir fechas estimadas de inicio y terminación por área de revisión,
- Plan de entrevistas a personas involucradas en unidades a auditar,
- Establecer fechas de revisión formales e informales,
- Definir recursos tecnológicos, equipo de evaluación por áreas,
- Definir herramientas y métodos de auditoria y control para evaluar procesos, efectuar pruebas sustantivas y respaldar los objetivos de control que no se cumplen.

UNIDAD FUNCIONAL: **JEFE AUDITORIA INTERNA:**

FECHA ELABORACIÓN

AREA POR auditar	**ELEMENTOS DEL AREA A AUDITAR**	**PRIORIDAD ASIGNADA**	**CLASIFICACION DEL RIESGO**	**FECHA INICIO/TERMINACION**
Área seleccionada	Elementos seleccionados	Número		dd/mm/aa dd/mm/aa
Área seleccionada	Elementos seleccionados	Número		dd/mm/aa dd/mm/aa
Área seleccionada	Elementos seleccionados	Número		dd/mm/aa dd/mm/aa

Tabla 4.4 Plan general de auditoria de sistemas

- Presentación del plan a la alta gerencia:
  - Presentación oportuna y detallada del plan, para obtener el visto bueno (aprobación) inicial de la alta gerencia (firma), recursos humanos clave, para continuar con el trabajo de auditoria,
  - Presentación del plan conteniendo: resumen del diagnostico actual, áreas a auditar, matriz de riesgos, prioridades en la auditoria.
- Ejecución del plan de auditoria de sistemas
  - En base al cubo (ver Figura 4.6) de Cobit, aplicar los dominios: Planeación organización, adquisición e implementación, entrega y soporte, monitoreo,

- Pruebas de cumplimiento y pruebas sustantivas

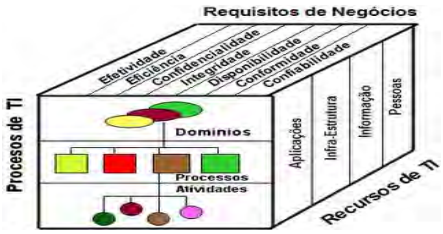


Fig.4.6 Cubo de Cobit

La finalidad de cualquier auditoria de SI es identificar los objetivos de control y los controles relacionados que se ocupan del objetivo. Por lo tanto, se debe identificar los controles clave, luego comprobar estos controles a través de métodos de verificación como:

Pruebas de cumplimiento, determina si los controles están siendo aplicados en una forma que cumple con las políticas y los procedimientos establecidos en la organización. La identificación de puntos clave de control permitirá al ASI desarrollar un entendimiento preliminar a través de pruebas de cumplimiento de esos controles para verificar si están funcionando como se esperaba.

Pruebas sustantivas, fundamenta la integridad de un procesamiento real. Existe una interrelación entre el nivel de los controles internos y la cantidad de pruebas sustantivas que se requieren. Si los resultados de los controles de comprobación revelaran la presencia de controles internos adecuados, entonces se tiene la justificación para minimizar los procedimientos sustantivos. Lo contrario, si la prueba de control revelara que existen puntos débiles en los controles que podrían generar dudas sobre la integridad, exactitud o validez de la información, seria conveniente aplicar una prueba sustantiva para aliviar dudas.

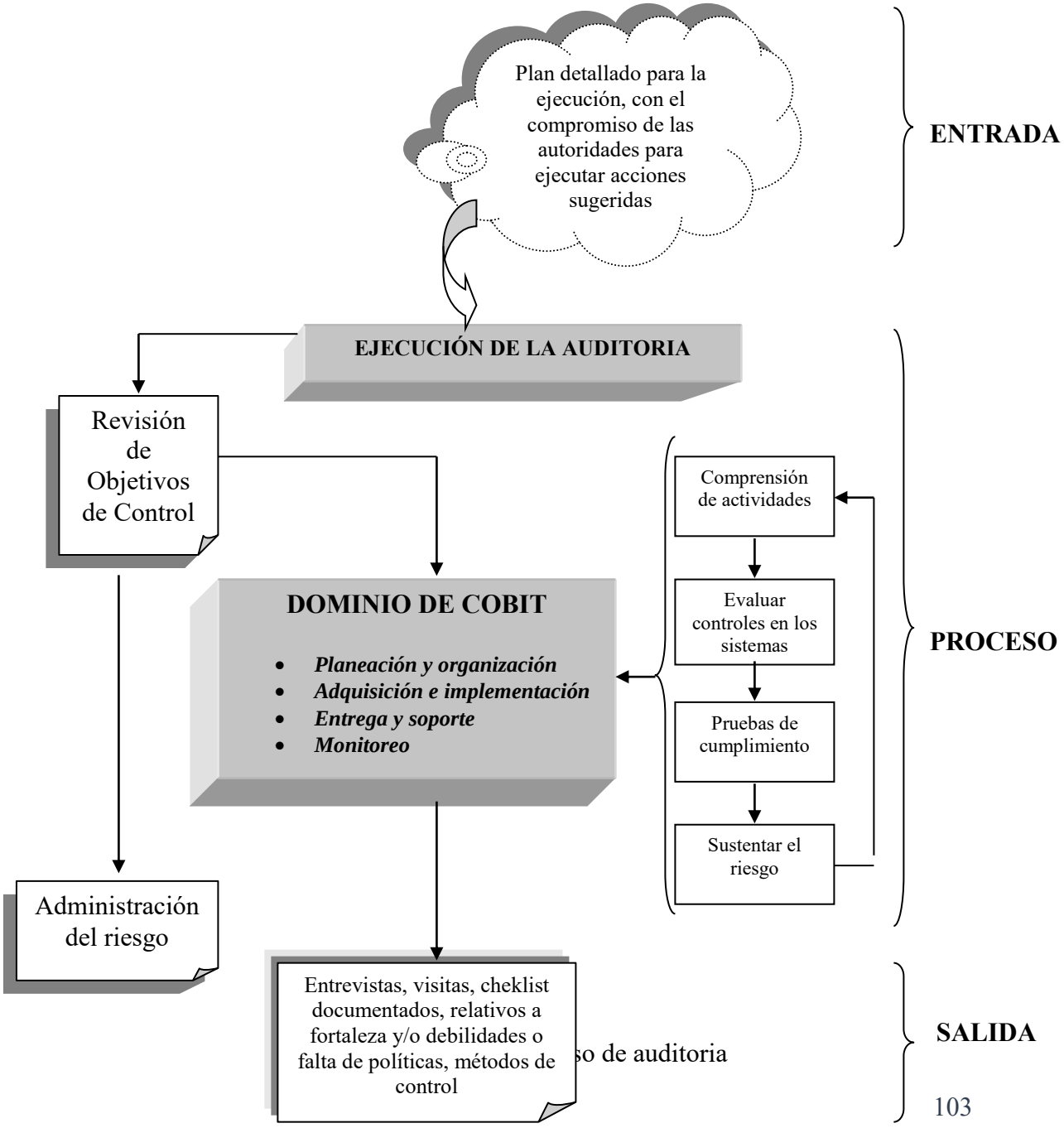
4.2.1.3 Elementos de salida para la planeación

Los elementos de salida de la etapa de planeación consisten en un plan de trabajo de auditoria de Base de Datos basado en la gestión de riesgos debidamente aprobado por

la alta gerencia y autorizados para la ejecución delegando autoridad y dando un soporte económico y técnico mediante un instructivo por escrito a las áreas a ser evaluadas.

4.2.2. Etapa de Ejecución de la auditoria

La Figura 4.7 muestra el proceso de auditoria



so de auditoria

4.2.2.1 Elementos de entrada para la etapa de ejecución

El plan detallado (ver Tabla 4.5), será la guía del proyecto de auditoria de sistemas a las áreas funcionales del negocio, desde el punto de vista de la comunidad, ya que describen tareas, productos concluidos, responsables, involucrados, fechas de revisión. Es el detalle final del plan. La alta gerencia hará un seguimiento en base al plan aprobado. Con el plan terminado y aprobado en la etapa de planeación, puede ejecutarse la auditoria de Base de Datos en las unidades de la organización.

TAREA	ACTIVIDADES	PRODUCTOS	RESPONSABLE	ACTORES	FECHA I / F
Verifica datos	1.Revisar datos de la unidad 2.Documentar	Prioridades y matriz de riesgos aprobados	Supervisor / auditor de sistemas	Alta gerencia /empleados /gerentes	dd/mm/aa
Evaluación de unidades por auditar	1.Concertar citas 2.Realizar entrevistas 3.Realizar visitas 4.Aplicar cheklist 5.analizar información 6.Informe preliminar 7.Ordenar informe preliminar 8.Revisar informe preliminar	- Comprometer - Documentos de respaldo - - Datos - Obs. Conclusión, recom - Fortalezas, debilidades, - Documentos - Datos - Informe preliminar actualizado, aprobado	ASI ASI ASI ASI ASI SUPERVISOR/ASI ASI ASI	COMUNIDAD/RH COMUNIDAD/RH RESPONSABLES COMUNIDAD/RH COMUNIDAD/RH COMUNIDAD/RH COMUNIDAD/RH COMUNIDAD/RH	
Documentar el informe final	1.Elaborar informe de autoridades 2.Informe detallado	- Informe de alto nivel - Informe detallado para usuarios	SUPERVIDOR ASI	 COMUNIDAD/RH	
Revisión del informe	1.Presentar informes 2.Aprobación informe 3.Compromiso autoridades	- Informes revisados - Informes aprobados - Ejecutar acciones sugeridas	RESPONSABLE ASI	RECTOR USUARIOS SUPERVIDOR	

Tabla 4.5 Plan detallado de la auditoria de sistemas

4.2.2.2Procedimiento de los procesos

Para desarrollar procesos efectivos de auditoria, se debe lograr una comprensión clara del sistema de aplicación que sé esta revisando, luego evaluar y verificar dichos sistemas y procesos, con el fin de asegurar que los riesgos se manejen en conformidad con los objetivos de la organización. Esta etapa comprende el análisis detallado de los sistemas de información y la ejecución de pruebas ya sean de cumplimiento o sustantivas de los objetivos de control, que en base a estos resultados se valorara el estado de los sistemas de información y se podrán determinar el nivel de riesgo tecnológico en la organización.

Luego de un trabajo detallado en la etapa de planificación, suelen identificarse ciertos riesgos como resultado por ejemplo: de un inadecuado proceso de registro de mercadería y/o productos en devolución. En base a estos y otros riesgos detectados en la etapa de planeación, se deben realizar otros análisis para evaluar y verificar la existencia de deficiencias de control e identificar los efectos de estas deficiencias.

La metodología Cobit, permite evaluar, verificar y documentar el cumplimiento de objetivos de control. Un objetivo de control es una declaración del resultado deseado o propósito a lograr al implementar procedimientos específicos de control dentro de la organización. Por esta razón podemos estructurar en los siguientes pasos:

4.2.2.2.1 Administración de riesgos

El proceso de administración de riesgos sigue los siguientes pasos: el primer paso es la identificación y clasificación de los recursos de información (información y datos, hardware, software, servicios, documentos, recursos humanos), el segundo paso, es estudiar las amenazas y vulnerabilidades (errores, daño intencional, fraude, robo, falla de sistema/equipo).

Debemos tener una participación relevante en la elaboración del análisis de riesgos para establecer el plan de auditoria o bien hacer por separado pero alineado su propio análisis de riesgos y el plan de auditoria de TI. La evaluación de riesgos, debe seguir el ciclo (ver figura 4.8) de administración de riesgos:

Fig.4.8 Fuente: elaboración propia

4.2.2.2.1.1 Conjunto de expectativas

Se debe alcanzar los objetivos generales y estratégicos de empresa Curtiembre "CUEROBOL", en base a la información obtenida para tomar las mejores decisiones.

Uno de los elementos más importantes que fortalecen el análisis del riesgo es la definición de los factores que inciden de manera general en cada uno de los procesos TI. Los factores más comunes son:

- ✓ Recursos humanos;
- ✓ Herramientas para el manejo de los procesos de TI;
- ✓ Complejidad de los procesos de TI y de las aplicaciones;
- ✓ Documentación de los procesos de TI y de las aplicaciones;
- ✓ Nivel de supervisión y monitoreo de los procesos y prácticas de TI;
- ✓ Ambiente de control y controles sobre los procesos de TI y de las aplicaciones
- ✓ Efecto en clientes y usuarios de T.I.

4.2.2.2.1.2 Identificación del riesgo:

Se deben identificar riesgos en el diseño de la Base de Datos Relacional (BDR), relaciones de las entidades en base a los atributos clave, cardinalidad, diccionario de datos.

Asimismo, se deben identificar los procesos críticos. ¿Qué puede funcionar mal?. ¿Qué oportunidades se pueden perder?

1. Metodología para realizar el inventario de riesgos:

- ✓ Analizar el plan estratégico de TI con el fin de listar los riesgos identificados por la Gerencia de TI;
- ✓ Consulta a la Auditoría Interna sobre los riesgos identificados como parte del proceso de desarrollo del plan anual;
- ✓ Indagación con los miembros del Comité de TI sobre riesgos de TI percibidos por ellos;
- ✓ Entrevistas con jefes funcionales o dueños de procesos de TI;
- ✓ Entrevista con el responsable de riesgos de la Entidad;
- ✓ Recopilación de riesgos de TI según bases de datos de las mejores prácticas.

2. Definición del universo de procesos.

Medición del riesgo

Se realiza la evaluación de probabilidades e impacto. Se realiza la revisión de controles existentes.

1. Análisis de Riesgos:

- ✓ **Inventario de riesgos de TI**: detalle pormenorizado de riesgos identificados con base en las indagaciones y entrevistas;
- ✓ **Universo de procesos**: detalle de procesos del área de TI;
- ✓ **Mapa de riesgos por procesos del área de TI**: comprende una gráfica de los principales procesos del Área de TI, priorizados de acuerdo al nivel de exposición;
- ✓ **Matriz de riesgos por procesos**: documento que describe cada uno de los riesgos identificados y que objetivo de TI están amenazando directamente;

- ✓ **Mapeo de estructura organizativa**: corresponde a la relación de riesgos y los puestos que se ejecutan dentro del área de TI.

2. Plan Inicial de Auditoria Interna de TI: documento que especifica los objetivos, alcance, programa de ejecución y recursos requeridos y asignados.

Estar consciente en el impacto de un mal diseño de la Base de Datos al no cumplir con la Integridad Referencial de una BDR y las Formas Normales.

4.2.2.2.1.4 Valoración de los controles

Se deben ejecutar controles internos, tomando como base las mejores prácticas de la industria del diseño de Base de Datos Relacional. En esta fase es importante el análisis, diseño e implementación de los Controles Generales de TI.

Determinar la integridad referencial a través de controles preventivos, detectivos y correctivos en el diseño de BDR.

4.2.2.2.1.5 Mitigación y control de riesgos

Los controles generales de TI auxilian a mitigar riesgos tales como los de continuidad del negocio, daño a la imagen y los de fraude.

- ✓ Arquitectura
- ✓ Continuidad del Negocio
- ✓ Contratación & Externalización
- ✓ Recursos Humanos TI
- ✓ Seguridad de la Información
- ✓ Privacidad & Protección de Datos
- ✓ Gestión de Proyectos
- ✓ Gestión de registros
- ✓ Gestión de Activos
- ✓ Gestión del Cambio

- ✓ Gestión del Riesgo TI
- ✓ Operaciones
- ✓ Seguridad Física & Ambiental
- ✓ Gestión de Problemas
- ✓ Licenciamiento de Tecnología
- ✓ Gobernabilidad de TI

Una clara identificación de claves primarias y alternas, junto con atributos que no son claves pero, que son propias de la entidad ayuda a mitigar riesgos en el diseño final del modelo conceptual.

4.2.2.2.1.6 Monitoreo y control del riesgo

Los riesgos para cada área funcional se representan en el modelo de Impacto / vulnerabilidad. Este modelo (ver figura 4.9) se utiliza para ayudar a la auditoría y gestión interna en la determinación de la respuesta global del riesgo.

Áreas Funcionales

1) Arquitectura;
2) Continuidad del Negocio;
3) Contratación & Externalización;
4) Recursos Humanos TI;
5) Seguridad de la Información;
6) Privacidad & Protección de Datos;
7) Gestión de Proyectos;
8) Gestión de registros;
9) Gestión de Activos;
10) Gestión del Cambio;
11) Gestión del Riesgo TI;
12) Operaciones;
13) Seguridad Física & Ambiental;

14) Gestión de Problemas;

15) Licenciamiento de Tecnología;

16) Gobernabilidad de TI.

Fig.4.9 Fuente: elaboración propia

Realizar seguimiento desde la asignación de nombres de las entidades, sus relaciones y el Gestor de Base de Datos que es la herramienta para implementar la BDR.

Valoración del desempeño: Una BDR, debe ser confidencial, íntegra y confiable.

4.2.2.2.2 Comprensión de actividades

Permitirá documentar las diferentes actividades de las áreas funcionales con referencia a los objetivos de control, como también internalizar conocimiento del estado de los controles y medidas existentes:

Entrevistas a la alta gerencia, gerentes administrativos, trabajadores del conocimiento, gerentes operativos y al personal encargado del área a auditar, para poder tener un conocimiento sobre:

- Requerimientos de la organización y sus riesgos colaterales,
- Estructura orgánica de la organización,
- Roles y responsabilidades de unidades y de recursos humanos,
- Políticas y procedimientos,
- Legislación jurídica,
- Métodos de auditoria y control implementadas,
- Informes anteriores.

Documentar los recursos de TI existentes

- Hardware,
- Software,
- Bases de Datos,
- Servicios,
- Recursos humanos calificados.

Entendimiento de la auditoria de sistemas y sus tendencias

Alcanzar una comprensión adecuada del sistema de información a evaluar revisando la documentación disponible.

4.2.2.2.3 Evaluar controles en los sistemas

En esta fase se debe evaluar la metodología y los procesos por medio de los cuales se abordan el desarrollo, la adquisición, la implementación y el mantenimiento de los sistemas de información de la organización, para asegurar que los mismos satisfagan los objetivos de la institución. Se puede mencionar tres tareas:

- ✓ Evaluar los procesos por medio de los cuales se desarrollan e implementan los sistemas de información para asegurar que los mismos contribuyan al logro de los objetivos de la organización,
- ✓ Evaluar los procesos por medio de los cuales se adquieren e implementan los sistemas de información para asegurar que los mismos contribuyan al logro de los objetivos de la organización,
- ✓ Evaluar los procesos por medio de los cuales se realiza el mantenimiento a los sistemas de información para asegurar el soporte continuo de los objetivos de la organización.

Los controles de la aplicación son controles sobre las funciones de entrada, proceso y salida de información. Los controles de los sistemas de información incluyen métodos para asegurar:

- ✓ Que solo se introducen y actualizan información completa, exactos y validos,
- ✓ Que el procesamiento realice la tarea en forma correcta,
- ✓ Que la información histórica se mantenga invariable a través del tiempo.

Estos controles pueden estar constituidos por pruebas de edición, autenticación de niveles de acceso, reportes de datos incorrectos, faltantes o de excepción. Los controles automatizados deben estar acoplados con procedimientos manuales para asegurar la debida investigación de las excepciones.

En los sistemas de información es crítico que se mantengan la integridad y la disponibilidad de las bases de datos. A continuación se detalla algunos controles para asegurar la integridad de la base de datos:

- ➢ Establecer normas de definición y monitorear de cerca su cumplimiento,
- ➢ Establecer diferentes niveles de controles de acceso para los datos, atributos, entidades y archivos para impedir el acceso no autorizado,
- ➢ Realizar una reorganización de la base de datos para reducir el espacio en disco no usado y verificar las relaciones definidas de los datos.
- ➢ Documentar los procedimientos de reestructuración de la base de datos cuando se realicen cambios lógicos, físicos o de procedimiento,
- ➢ Usar herramientas analizadores de bases de datos, para mantener y monitorear la eficiencia de la base de datos.

La administración efectiva de los datos almacenados en la base de datos, permite asegurar que los datos permanezcan completos, precisos y validos durante su entrada, actualización y almacenamiento por intermedio de controles generales efectivos, tomando en consideración:

- ➢ **Diseño,** verificar la existencia de un modelo de bases de datos, que las entidades definidas tengan un nombre significativo, los nombres de atributo sean adecuados (claves primarias y secundarias), el tipo de datos a almacenar sea el

adecuado, la longitud definida para los atributos sea lo estrictamente necesario y la documentación de los nombres de atributo sean entendibles,

- **Controles sobre documentos fuente,** recabar documentos que contengan requerimientos del usuario, diseño conceptual de la base de datos (relaciones con cardinalidad especifica), diseño lógico, diseño físico y software de aplicación requerida.
- Controles, sobre entrada, procesamiento y salida,
- **Recuperación y almacenamiento de datos,** establecer copias de respaldo de los datos y procedimientos de recuperación para asegurar la disponibilidad de los datos,
- **Autenticación e integridad de los datos,** previa verificación del nivel acceso del usuario, se podrá manipular los datos de la base de datos.
- **Modelo de datos y estándares de representación de datos,** Identificar el modelo de datos implementado como ser: modelo entidad-relación, modelo objeto relacional, modelo orientado a objetos, etc., y procedimientos para almacenar información.
- **Integración y consistencia en todas las plataformas,** que garantice la seguridad y confidencialidad de los datos, se deben verificar los procedimientos de importación y exportación con otros sistemas.
- **Legislación jurídica**, legislación boliviana en cuanto al manipuleo de información de las bases de datos.

4.2.2.2.4. Pruebas de cumplimiento

Las pruebas se realizan en cada una de las fases del ciclo de vida del sistema de información, para asegurar que las medidas de control, funcionan como fueron prescritas, de forma consiste y continúa y para concluir si el ambiente de control es apropiado. Los elementos básicos son:

- ✓ **Plan de pruebas,** desarrollados en las primeras fases del ciclo de vida y retroalimentados hasta la etapa efectiva de prueba, los planes de prueba identifican las porciones especificas del sistema que va a ser probado,
- ✓ **De abajo hacia arriba,** que empieza probando las unidades atómicas,
- ✓ **De arriba hacia abajo,** considera la profundidad o la amplitud de la prueba,
- ✓ **Ejecutar las pruebas y reportar resultados,** describir los recursos que se necesitan para probar incluyendo a los recursos humanos involucrados. Se debe presentar resultados reales obtenidos durante la prueba, comparándolos con los resultados que se esperaba obtener con dicha prueba. Los resultados reportados junto con el plan deben ser archivados como parte de la documentación permanente del sistema.
- ✓ **Resolver los problemas cruciales,** los errores e irregularidades son identificados a partir de las pruebas que se llevan a cabo. Cuando dichos problemas ocurren, las pruebas tienen que ser rediseñadas en el plan de prueba y deben ser ejecutadas nuevamente hasta que se superen los errores detectados.

Las herramientas en la etapa de pruebas son fundamental, debe considerar al menos algunos puntos:

- ✓ Base de datos a relacionar,
- ✓ Modulo de captura de datos de entrada,
- ✓ Modulo de consultas,
- ✓ Generador de textos e informes,
- ✓ Asistencia en línea.

Las pruebas de cumplimiento se basan en evidencias obtenidas directa o indirectamente, para tener la seguridad razonable de que los procedimientos han sido cumplidos dentro el periodo bajo revisión.

4.2.2.2.5 Sustentar el riesgo

Una vez que se han establecido los elementos de riesgo, estos se combinan para formar una visión general del riesgo. El nivel de riesgo remanente una vez que los controles han sido aplicados se denomina riesgos residuales, que puede ser usado por la gerencia, para identificar las áreas en las que se requiere más control para reducir aún más los riesgos.

El objetivo de la sustentación del riesgo es dar soporte a la opinión profesional del auditor de sistemas e instar a la alta gerencia de las acciones inmediatas que deben emprender. Por lo que el ASI, debe considerar lo siguiente:

- ✓ Documentar los controles débiles y las amenazas resultantes y su vulnerabilidad,
- ✓ Identificar y documentar el impacto social,
- ✓ En caso de ser necesario, realizar la reingeniería del proceso en determinadas áreas de la organización.

Por último, revisar los objetivos de control para TI que concuerden con los objetivos de la auditoria trazados en la etapa de planeación, en base al marco referencial de la metodología COBIT.

4.2.2.2.6. Medición del riesgo

La evaluación del riesgo deberá asegurar que la información del análisis de la obtención o identificación del nivel de riesgos genere una medida cuantitativa y/o cualitativa.

4.2.2.3. Elementos de salida para los procesos

Los elementos de salida de la etapa de ejecución consisten en documentos bien elaborados (papeles de trabajo) con respecto a entrevistas, visitas, cheklist realizadas a

gerentes, empleados, usuarios, relativos a las fortalezas y debilidades de las áreas funcionales auditadas o falta de políticas, métodos y procedimientos para cumplir los objetivos de control. Esta documentación deberá entregarse a las autoridades respectivas para su aprobación.

4.2.3. Etapa de reportes de la auditoria

La Figura 4.10 muestra un plan de reportes de la auditoria

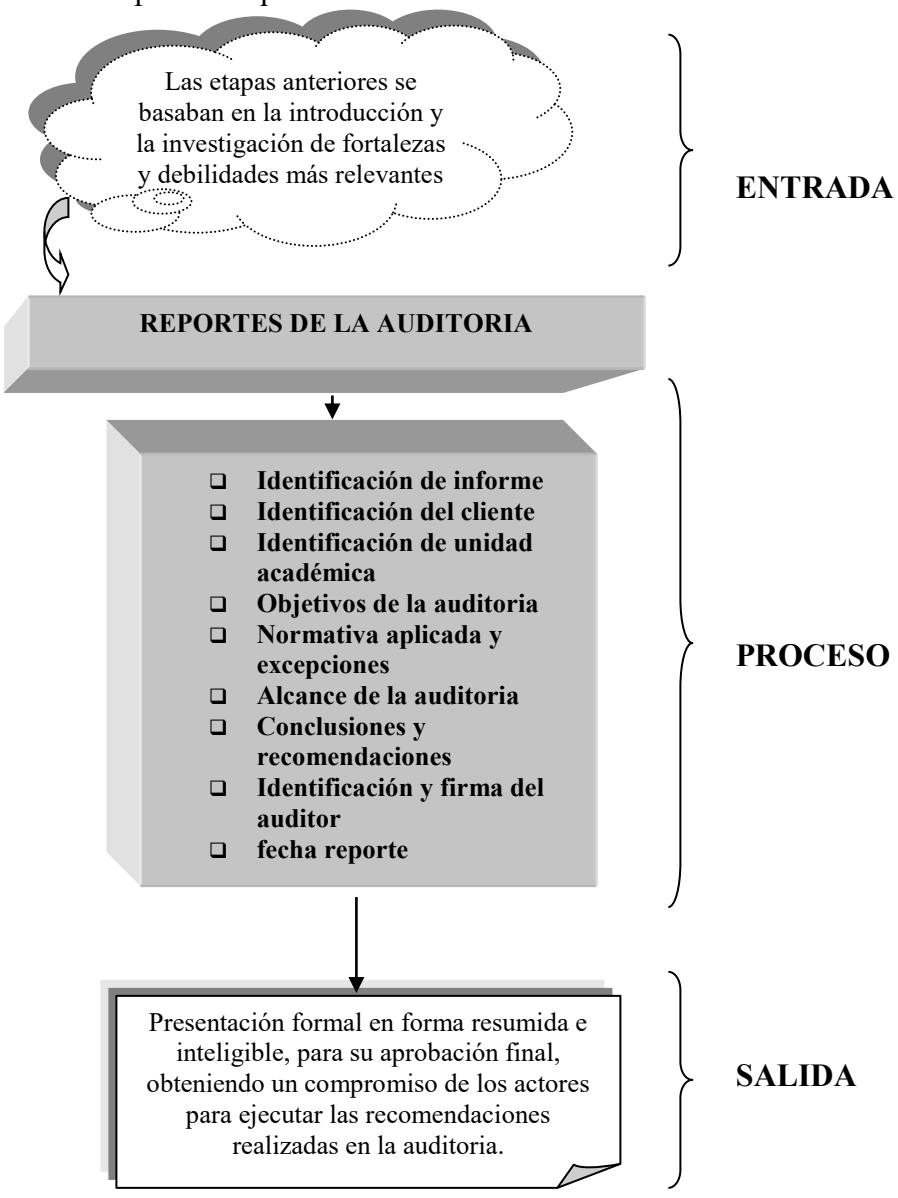


Fig.4.10 Etapa de reportes de auditoria

4.2.3.5 Elementos de entrada para los reportes

Los elementos de entrada para la etapa de reportes, están precedidos por un plan preliminar que se presenta a la alta gerencia y posteriormente en base a ese plan de acción realizar la investigación y evaluación correspondiente al cumplimiento de objetivos de control para detectar fortalezas y debilidades más relevantes.

4.2.3.6 Procesos de los reportes

Antes de comunicar los resultados de una auditoria a las autoridades superiores de la organización, se debe considerar discutir los hallazgos con la persona encargada de la administración de la Base de Datos. El objetivo de dicha discusión seria llegar a un acuerdo sobre los hallazgos y desarrollar un curso de acción a seguir para corregirlos.

Los reportes de auditoria son el producto final del trabajo de auditoria de Base de Datos Relacional, esto es la comunicación del auditor de sistemas de información a las autoridades jerárquicas de la organización, formal y, quizás, solemne, definiendo el alcance de la auditoria: objetivos, tiempo de cobertura, naturaleza y en algunos casos extensión del trabajo realizado y por ultimo los resultados y conclusiones de la auditoria de sistemas.

La redacción del reporte debe ser claro, adecuado, suficiente y comprensible, cuyo contenido y estructura [De la Peña, 2001] será la siguiente:

- ✓ **Identificación del informe,** contiene el título del reporte,
- ✓ **Identificación del cliente,** debe identificarse a la autoridad correspondiente de la unidad académica solicitante,
- ✓ **Identificación de la unidad auditada,** unidad académica objeto de la auditoria de Base de Datos Relacional
- ✓ **Objetivos de la auditoria de sistemas,** detalle de los objetivos para identificar su propósito, señalando objetivos incumplidos,

- ✓ **Normativa aplicada y excepciones,** identificación de métodos y procedimientos y el posible impacto en los resultados de la auditoria,
- ✓ **Alcance de la auditoria,** unidad auditada, tiempo de auditoria. Reportando limitaciones al alcance y restricciones de la unidad auditada,
- ✓ **Conclusiones,** reporte de opinión profesional respecto a si los controles y procedimientos examinados durante la auditoria son adecuados,

El reporte debe contener uno de los siguientes tipos de opinión:

- ➢ **Opinión favorable**, sin salvedades o limpia, deberá reportarse en forma clara y precisa,
- ➢ **Opinión con salvedades**, cuando sean significativas en relación con los objetivos de auditoria, argumentando en forma detallada las razones, por ejemplo: restricciones del auditado, contingencias no previstas en el alcance de la auditoria, incumplimiento de procedimientos.
- ➢ **Opinión desfavorable**, cuando se identifica irregularidades,
- ➢ **Opinión denegada**, cuando existe incertidumbre, irregularidades,
- ➢ **Resumen**, claro de la auditoria.

Si durante la auditoria se detecta debilidades, se debe comunicar a la alta gerencia lo antes posible, con los siguientes puntos:

- ➢ Detallar las debilidades encontradas en el proceso de revisión,
- ➢ Describir el criterio o instrumento de medida utilizado,
- ➢ Describir los efectos que sufriría el objeto analizado,
- ➢ Recomendar posibles soluciones, para eliminar la debilidad.

- ✓ **Fecha de reporte,** es importante para conocer el trabajo realizado, considerando fechas de inicio y fecha final,
- ✓ **Identificación y firma del auditor,** competente ya sea individual o perteneciente a una firma de socios auditores en sistemas de información.

La Paz, 19 de febrero 2016

Señores

EMPRESA CURTIEMBRE “CUEROBOL”

Presente.-

Para su consideración, remito el informe de Evaluación de la Base de Datos que es gestionada por el sistema “StockBase” para realizar el control de sus ventas y clientes, al 31 de diciembre del 2015.

El detalle es el siguiente:

I. Objetivo General
II. Alcance del trabajo
    a) Normativa utilizada;
    b) Procedimientos de auditoria;
    c) Revisión de los controles generales del Departamento de Sistemas y al diseño de la Base de Datos.
III. Conclusiones.

Nitza Sauter Estevez
AUDITORA DE SISTEMAS

I. Objetivo General

El objetivo es evaluar el flujo de información a través del Sistemas de Información "StockBase" y que generen información confiable, íntegra y oportuna y los mecanismos de seguridad implementados que minimicen los riegos tecnológicos.

No se pretende aplicar una Auditoría Informática rigurosa en la empresa "CUEROSBOL", únicamente se hace la evaluación sobre gestión de la información a través de los Sistemas de Información, considerando las mejores prácticas a nivel nacional e internacional.

II. Alcance del trabajo

La evaluación de la Base de Datos Relacional, gestionada a través del sistema "StockBase", pretende aplicar los conceptos y procedimientos generalmente aceptados, en cuanto a:

- ✓ Confidencialidad, integridad y confiabilidad de la información;
- ✓ Efectividad del control interno;
- ✓ Flujo de la información;
- ✓ Normas, procedimientos, planes de contingencia;

a) Normativa utilizada

- ✓ Modelo COBIT (Objetivos de Control para Tecnología de la Información y Tecnología Relacionada). Es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. COBIT permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización;
- ✓ Modelo ISO 27000. Este estándar ha sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. **BS ISO/IEC 27001** – Sistema de Gestión de Seguridad de la Información – Requisitos. **BS ISO/IEC 27002** – Código de práctica para la Gestión de la Seguridad de la información.

b) Procedimientos de auditoria

- ✓ Recopilación de normas, procedimientos y reglamentos inherentes a los recursos tecnológicos;
- ✓ Análisis de la estructura organizacional del Departamento de Sistemas;
- ✓ Identificación de personas clave;
- ✓ Entrevistas;
- ✓ Proceso de análisis, diseño, implementación, mantenimiento y pruebas del modelo conceptual;

- ✓ Seguridad física y lógica;
- ✓ Planes de contingencia.

c) Revisión de los controles generales del Departamento de Sistemas y Sistemas de Información

Es importante comprender la relación y la diferencia entre los controles de aplicación y los controles generales de Tecnología de la Información. De lo contrario, es posible que el alcance de una revisión del control de aplicación no se determine correctamente; lo que impactaría en la calidad de la auditoría y su cobertura.

Los Controles generales de TI se aplican a todos los componentes, procesos y datos de sistemas presentes en una organización o al entorno de sistemas. El objetivo de estos controles es garantizar el desarrollo y la implementación adecuada de las aplicaciones, así como también la integridad de los archivos de datos y programas y de las operaciones informáticas. Los controles generales de TI más comunes son:

- Controles de acceso lógico sobre la infraestructura, las aplicaciones y los datos;
- Controles de gestión de cambio de la Base de Datos;
- Controles sobre gestión de riesgos;
- Controles de respaldo y recuperación de datos y sistema.
- Controles de operaciones informáticas.

Dado que los controles se relacionan con las transacciones y los datos que reporta el sistema "StockBase". El objetivo de los controles de aplicación es garantizar la integridad y precisión de los registros y la validez de las entradas realizadas en cada registro, como el resultado del procesamiento de programas.

¿Qué son los controles de aplicación?

Son aquellos controles que corresponden al alcance de los procesos de negocio o sistemas de aplicaciones individuales, incluidos las ediciones de datos, la separación de funciones de negocio, el balanceo de totales de procesamiento, el registro de transacciones y la generación de informes de errores. Por lo tanto, el objetivo de los controles de aplicación es asegurar que:

- Los datos de ingreso sean precisos, completos, autorizados y correctos.
- Los datos se procesen según lo planeado en un período de tiempo aceptable.
- Los datos almacenados sean precisos y completos.
- Las salidas sean precisas y completas.
- Se mantenga un registro para realizar el seguimiento del proceso de datos desde el ingreso hasta el almacenamiento y la eventual salida.

Existen varios tipos de controles de aplicación. Estos incluyen:

- ✓ Controles de ingreso de datos;
- ✓ Controles de procesamiento;
- ✓ Controles de salida;
- ✓ Controles de integridad;
- ✓ Pistas para la dirección.

Recopilación de normas, procedimientos y reglamentos inherentes al Sistemas "StockBase"

La revisión de documentación proporcionada por el Departamento de Sistemas, relacionada a normas, políticas, procedimientos y reglamentos formalmente aprobados, se limitó a lo siguiente:

- ✓ Sistema de gestión (ventas de cueros de vaca para chamarras y calzados – compras materia prima - crédito institucional)
- ✓ Manual técnico y manual del usuario de los módulos del Sistema "StockBase". Estos manuales están desactualizados;
- ✓ Manual del diseño de la Base de Datos Relacional es empírico.

Ejecución de controles internos

En nuestra evaluación observamos, que no se realizan auditorias de sistemas y no se cuenta con una unidad de control interno o con un especialista en la ejecución de Auditorias de Sistemas; esto implica que las tareas de seguimiento, control y monitoreo de las diferentes actividades de la Entidad no se realizan, debilitándose el ambiente de seguridad.

Emigrar el sistema "StockBase" de licencia a plataformas de Software Libre

Se pudo evidenciar que en las estaciones de trabajo (PC) que interactúan con el servidor de aplicaciones, no cuentan con licencias de software. Por tanto, se convierten en el uso de software ilegal:

- Sistema Operativo Windows 7;
- Microsoft Office;
- Adobe.

Diseño, implantación y mantenimiento de la Base de Datos

Se evaluó la existencia del modelo conceptual (ver figura 4.11) en el diseño de la Base de Datos para satisfacer requerimientos de las áreas usuarias.

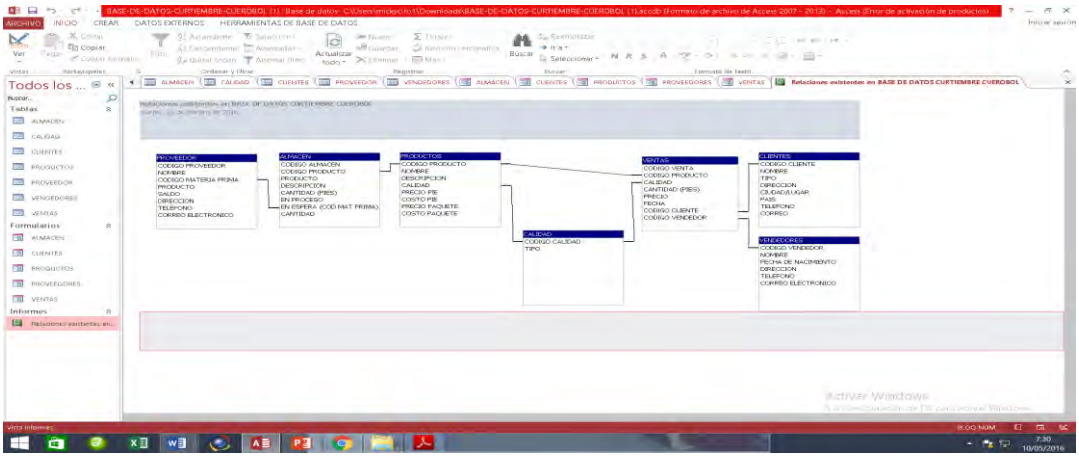
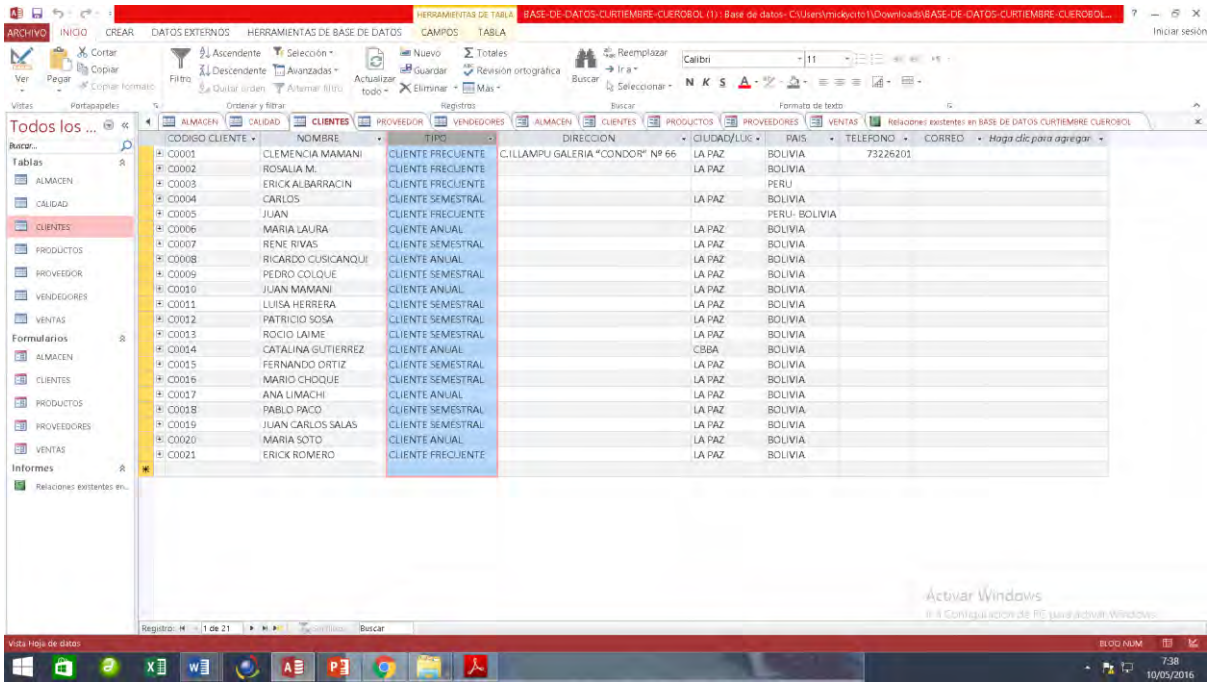


Fig.4.11 Relaciones entre entidades

El diseño de la entidad Clientes (ver figura 4.12), no contempla las Formas Normales, generando inconsistencias en los datos almacenados en la Base de Datos.



CODIGO CLIENTE	NOMBRE	TIPO	DIRECCION	CIUDAD/LUG	PAIS	TELEFONO	CORREO
C0001	CLEMENCIA MAMANI	CLIENTE FRECUENTE	C.ILLAMPU GALERIA "CONDOR" Nº 66	LA PAZ	BOLIVIA	73226201	
C0002	ROSALIA M.	CLIENTE FRECUENTE		LA PAZ	BOLIVIA		
C0003	ERICK ALBARRACIN	CLIENTE FRECUENTE			PERU		
C0004	CARLOS	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0005	JUAN	CLIENTE FRECUENTE			PERU- BOLIVIA		
C0006	MARIA LAURA	CLIENTE ANUAL		LA PAZ	BOLIVIA		
C0007	RENE RIVAS	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0008	RICARDO CUSICANQUI	CLIENTE ANUAL		LA PAZ	BOLIVIA		
C0009	PEDRO COLQUE	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0010	JUAN MAMANI	CLIENTE ANUAL		LA PAZ	BOLIVIA		
C0011	LUISA HERRERA	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0012	PATRICIO SOSA	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0013	ROCIO LAIME	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0014	CATALINA GUTIERREZ	CLIENTE ANUAL		CBBA	BOLIVIA		
C0015	FERNANDO ORTIZ	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0016	MARIO CHOQUE	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0017	ANA LIMACHI	CLIENTE ANUAL		LA PAZ	BOLIVIA		
C0018	PABLO PACO	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0019	JUAN CARLOS SALAS	CLIENTE SEMESTRAL		LA PAZ	BOLIVIA		
C0020	MARIA SOTO	CLIENTE ANUAL		LA PAZ	BOLIVIA		
C0021	ERICK ROMERO	CLIENTE FRECUENTE		LA PAZ	BOLIVIA		

Fig.4.12 Datos inconsistentes en la tabla Clientes

El modelo COBIT, en **PO2 Definir la arquitectura de información**, indica que la función de los sistemas de información debe crear y actualizar de forma regular un

modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.

En **PO4.4 IT Administración de la integridad,** señala claramente que se debe definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

En **PO9 Evaluar y administrar los riesgos de TI,** indica crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia.

Asimismo, en **PO9.1 Alineación de la administración de riesgos de TI y del negocio** Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización **PO9.2 Establecimiento del contexto del riesgo** Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos. **PO9.3 Identificación de eventos** Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información. **PO9.4 IT Evaluación de riesgos** Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio. **PO9.5 Respuesta a los riesgos** Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los

niveles de tolerancia de riesgos definidos. **PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos** Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

Seguridad física y lógica

Se evaluó la existencia de normas, políticas y procedimientos formalmente aprobada por instancias correspondientes relacionadas a seguridad informática, como el uso de estándares internacionales: ISO 9126, ISO 17799 o ISO 27000, que contemple la administración de cuentas de usuario, perfiles de usuario (altas, bajas y modificaciones), gestión de accesos al sistema; administración de copias de respaldo incluyendo periodicidad y frecuencia, medios de almacenamiento masivo, etiquetado y responsable de la actividad. Asimismo, se evaluó las licencias de software como antivirus, antispyware, sistemas operativos, Office y Adobe.

Con relación a la seguridad física, se evaluó procedimientos de control de accesos al Centro de Cómputo, existencia de alarmas, sensores, cableado estructurado, aire acondicionado, ups que brindan seguridad a los servidores de archivos, servidores de Bases de Datos, Servidores de Correo Institucional.

Se detectó los principales riesgos:

NRO.	ÁREA FUNCIONAL DE TI	DESCRIPCIÓN DEL RIESGO
1	**Seguridad de la Información**	Falta de una persona responsable de la seguridad física y lógica
	Seguridad de la Información	No existe programa para manejar exhaustivamente riesgos cibernéticos.
	Seguridad de la Información	No se emplea un marco de seguridad global a través de Compañía para identificar, controlar y mitigar proactivamente los riesgos de seguridad TI.
	Base de Datos	No se cumple con estándares en el diseño de Base de Datos, relacionados a la integridad referencial, cardinalidad, formas normales. Etc.
	Protección de Privacidad & Datos	En la Compañía se manejan información sensible. Existe el riesgo de que las prácticas de seguridad y privacidad no esta de acuerdo con normas de seguridad y privacidad.
	Adquisición e Integración de TI	Existe un riesgo de que la confiablidad, integración y confidencialidad no se lleve a cabo de una manera controlada.

Entrevistas al personal
Personal del Departamento de Sistemas

Se realizaron una serie de entrevistas planificada al Lic. Marco Sempetegui. Responsable del Sistema, referente a la gestión de riesgos en el diseño de la Base de Datos Relacional.

Usuarios de la institución

Se realizó entrevista a algunos empleados de la institución referente al sistema **"StockBase"**, grado de interoperabilidad, confiabilidad, interfaz de usuario. Asimismo, valorar el punto de vista individual sobre el la versatilidad del correo institucional, apoyo efectivo de parte del personal de sistemas sobre algunas contingencias.

Planes de contingencia

Durante nuestra revisión, observamos que la Entidad no cuenta con un plan de contingencias formalmente establecido para el Departamento de Sistemas. Si bien, se cuenta con procedimientos de contingencias operativos, estos no han sido consolidados y formalizados a través de un plan.

III. **Conclusiones**

- ✓ El sistema **"StockBase",** que es una licencia comercial, cuenta con un grado aceptable de confidencialidad integridad y confiabilidad;
- ✓ El diseño de Base de Datos Relacional con que cuenta la empresa no cumple estándares generalmente aceptadas, incrementando el riesgo;
- ✓ Se utiliza aplicaciones, como el sistema operativo Windows 7, office, adobe sin haber adquirido la licencia, corriendo el riesgo de utilizar software "pirata";

4.2.3.7. Elementos de salida para los reportes

Los elementos de salida para los reportes es la tarea más importante para el supervisor y el auditor de sistemas de información, después de aplicar las anteriores etapas en forma rigurosa se espera la aprobación formal del trabajo de auditoria de sistemas realizada a una determinada unidad del negocio. El documento presentado es un resumen claro, contundente e inteligible.

5.1. Conclusiones

Las amenazas y vulnerabilidades se deben a incidentes de inseguridad relacionadas a Tecnología de Información, a falta de un referente metodológico. El trabajo de Proyecto de Grado está orientado al desarrollo de un método de Gestión de Riegos para la Auditoria de Base de Datos aplicable a la Empresa de cueros "CUEROBOL" cumpliendo normas y procedimientos generalmente aceptados.

Este método está dirigida a ejecutar controles efectivos, que luego, permita emitir una opinión profesional sobre el estado de TI y tomar las acciones preventivas, detectivas y correctivas adecuadas con el fin de minimizar riegos. Este método aplica los dominios de COBIT 4.1

Es importante resaltar que cada vez que se incorpora una nueva herramienta o negocio de TIC a la entidad se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos y, por supuesto, considerando la regla básica de Riesgo de TI *vs.* Control *vs.* Coste, es decir, minimizar los riesgos con medidas de control ajustadas y considerando los costes del control.

La metodología propuesta, contribuye a fomentar las actividades de protección de la información en la Empresa de cueros "CUEROBOL", mejorando su seguridad de la información, su imagen y generando confianza frente a terceros.

- ✓ La metodología propuesta, cumple con los objetivos planteados;
- ✓ La seguridad y gestión de riesgos se basa en las personas;
- ✓ Las personas responsables de la gestión de riesgos en la Empresa de cueros "CUEROBOL", al utilizar el método, podrán evaluar el contenido de las diferentes actividades y aplicar los controles que considere necesario en forma sistemática y disciplinada con el objetivo de minimizar los riesgos.

5.2. Recomendaciones

Es recomendable aplicar en forma rigurosa métodos de gestión de riesgos para la auditoría de Bases de Datos Relacional bajo el paraguas del modelo COBIT. Pero, esto no significa que con la aplicación de este método, se garantice la gobernabilidad efectiva de la información. Todo dependerá del cambio de actitud cultural de los diferentes actores de la institución.

La gestión de riesgos en ambientes tecnológicos, bajo estándares internacionales, es relativamente nueva. Por lo que se sugiere las siguientes recomendaciones:

- ✓ La primera que debo recomendar es actualizar el trabajo;
- ✓ Las organizaciones deben definir una estrategia de seguridad basada en el negocio y no en la tecnología.
- ✓ En futuros trabajos se recomienda implementar la ISO 30000 e ISO 31000;
- ✓ Se recomienda implementar modelos como MAGERIT e ITIL
- ✓ Se debe tomar conciencia de parte de la gerencia, que los ambientes donde se procesa información cuente con un plan de contingencias, que este contemplado como objetivos generales de la institución.

REFERENCIAS BIBLIOGRÁFICAS

AENOR *Sistemas de gestión de la calidad*. ISO 9001-2000. Madrid: AENOR, 2000.

[Hernández 2005] Hernández, R., 2005: Metodología de la Investigación, 505 pp. Editorial McGraw-Hill.

[Piattini,2001] Piattini Velthuis, Mario G. Auditoría Informática: un enfoque práctico. Segunda Edición. ISBN: 84-7897-293-5.

[Elmasri, 2009] Elmasri, Ramez. Navathe, Shamkant. Fundamentos de Sistemas de Bases de Datos. Tercera Edición. ISBN: 84-7829-051-6.

En línea:

http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0041430&PDF=Si

[Acceso, enero 2016] Asociación Española de Normalización y Certificación – AENOR UNE 71504:2008: Metodología de análisis y gestión de riesgos para los sistemas de Información.

http://ciberconta.unizar.es/LECCION/SEGURO/inicio.html

[Acceso, Agosto 2015] Riesgos y seguridad en los sistemas de información. Auditoría informática.

http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx
Instituto de Administración de las Tecnologías de la Información – ITGI
Objetivos de control para la información y tecnologías relacionadas – CoBiT 4.1

http://aechile.cl/wp-content/uploads/2015/01/COSO-in-the-Cyber-Age_FULL_r11-11.pdf

[Acceso, enero 2016] COSO IN THE CYBER AGE

http://www.coso.org/guidance.htm

http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

http://doc.contraloria.gob.pe/Control-Interno/Normativa_Asociada/coso_2013-resumen-ejecutivo.pdf