Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

CONTROL DE LA TECNOLOGÍA DE LA INFORMACIÓN (COBIT) APLICADO A LA REALIZACIÓN DE AUDITORÍA DE SISTEMAS DE BASES DE DATOS RELACIONALES

Marlon Francisco Orellana López

Asesorado por: Inga. Elizabeth Domínguez Alvarado

Guatemala, octubre de 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

CONTROL DE LA TECNOLOGÍA DE LA INFORMACIÓN (COBIT) APLICADO A LA REALIZACIÓN DE AUDITORÍA DE SISTEMAS DE BASES DE DATOS RELACIONALES

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

MARLON FRANCISCO ORELLANA LÓPEZ
ASESORADO POR: INGA. ELIZABETH DOMINGUEZ ALVARADO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA,OCTUBRE DE 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE LA JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia Garcia Soria
VOCAL II	Lic. Amahán Sánchez Alvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
EXAMINADOR	Inga. Florisa Felipa Avila Pesquera
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

CONTROL DE LA TECNOLOGÍA DE LA INFORMACIÓN (COBIT)
APLICADO A LA REALIZACIÓN DE AUDITORÍA
DE SISTEMAS DE BASES DE DATOS RELACIONALES,

tema que fuera asignado por la Coordinación de la Carrera de Ingeniaría en Ciencias y Sistemas de la Facultad de Ingeniería, con fecha 20 de agosto de 2005.

Marlon Orellana

Digitally signed by Marlon Orellana
DN: cn=Marlon Orellana, c=GT, o=USAC-SISTEMAS, ou=Universidad de San Carlos, email=MarlonOrellana2005@gmail.com
Date: 2006.10.24 10:22:37 -06'00'

Marlon Francisco Orellana López

Guatemala, 8 de Agosto de 2006

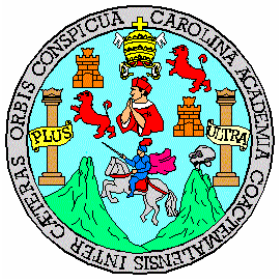
Ing. Carlos Alfredo Azurdia Morales
Coordinador de Privados y Trabajo de Graduación
Escuela de ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Ing. Azurdia:

Por medio de la presente hago de su conocimiento que he tenido a bien revisar el trabajo de graduación de **MARLON FRANCISCO ORELLANA LÓPEZ,** titulado "Control de la tecnología de la información (COBIT) aplicado a la realización de auditoría de sistemas de bases de datos relacionales", por lo cual me permito recomendar dicho trabajo final para la respectiva revisión por parte de la comisión de tesis de la escuela de Ciencias y Sistemas.

Sin otro particular, me suscribo atentamente,

Inga. Elizabeth Domínguez
Asesora



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 23 de Agosto de 2006

Ingeniero
Jorge Armín Mazariegos
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Mazariegos:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **MARLON FRANCISCO ORELLANA LÓPEZ,** titulado: "CONTROL DE LA TECNOLOGÍA DE LA INFORMACIÓN (COBIT) APLICADO A LA REALIZACIÓN DE AUDITORÍA DE SISTEMAS DE BASES DE DATOS RELACIONALES", y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

El Director de La Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor con el visto bueno del Revisor y Licenciado en Letras, del trabajo de graduación titulado: **"CONTROL DE LA TECNOLOGÍA DE LA INFORMACIÓN (COBIT) APLICADO A LA REALIZACIÓN DE AUDITORÍA DE SISTEMAS DE BASES DE DATOS RELACIONALES"** , presentado por el estudiante universitario **Marlon Francisco Orellana López**, aprueba el presente trabajo y solicita la autorización del mismo.

ID Y EÑSENAD A TODOS

Ing. Jorge Armín Mazariegos
DIRECTOR
INGENIERIA EN CIENCIAS Y SISTEMAS

Guatemala, Octubre de 2006

Ref. DTG-374-2006

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de Graduación titulado: "CONTROL DE LA TECNOLOGÍA DE LA INFORMACIÓN (COBIT) APLICADO A LA REALIZACIÓN DE AUDITORÍA DE SISTEMAS DE BASES DE DATOS RELACIONALES", presentado por el estudiante universitario, Marlon Francisco Orellana López, procede a la autorización para impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olimpo Paiz Recinos
DECANO

Guatemala, 30 de Octubre de 2006

/lmcb.

ACTO QUE DEDICO A:

Dios:	Por su infinita misericordia, luz y sabiduría para conmigo.
Virgen santísima:	Por ser manantial de bendiciones en mi vida.
Mis padres:	Por su ejemplo, amor y tiempo que hacen de mi una persona de bien.
Mi hermano:	Por que juntos formemos triunfos en nuestra familia.
Mis abuelos:	Por su apoyo, comprensión y sus enseñanzas.
Mi familia:	Por estar conmigo en mi formación.
Universidad de San Carlos de Guatemala	Tricentenaria casa de estudios, en cuyas aluas se forman profesionales de éxito.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

Aplicaciones	Suma de procedimientos, manuales y programas.
Autentificación	Representa dar fe de la legalidad de un objeto, acción o hecho.
Autodescriptivo	Descripción propia de un objeto.
Arquitectura	Estructura lógica y física de los componentes de un computador.
Backend	Equipo cliente en un esquema cliente-servidor.
Bitácora	Archivo representativo de las acciones realizadas por el usuario sobre una aplicación determinada.
Capa	División de tecnología que se comunica con otra de diferente arquitectura para conformar un sistema único.
Checklist	Cuestionario utilizado para evaluar

	aspectos de auditaje de recursos TI.
Cifrado	Escritura en donde se usan signos o letras convencionales y solo puede entenderse conociendo la clave
Criptografía	Arte de escribir con clave secreta la información.
COBIT	*“Control Objectives for information and related Technology”;* objetivos de control en la tecnología de la información.
Coherencia	Estado de un sistema cuando sus componentes aparecen en conjuntos solidarios.
Control	Comprobación, inspección, fiscalización Intervención.
COSO	*“Committee of sponsoring organizations”* comisión de estudios de controles internos.
DBMS	Sistema de administración de base de datos.

DDL	Lenguaje de definición de datos.
Dictamen	Opinión o juicio que se emite sobre algo.
DML	Lenguaje de manipulación de datos.
Estándar	Modelo, norma o patrón de referencia.
Frontend	Equipo servidor en un esquema cliente-servidor.
Inconsistencia	Falta de consistencia de los elementos que conforman algo.
Inferir	Consecuencia o deducción algo de otra cosa.
Interfaz	Conexión física y funcional entre dos aparatos o sistemas independientes.
ISACF	*“Information Systems Audit and Control Foundation”.*
Jerarquía	Gradación de los valores de un objeto.
KGI	Indicadores clave de resultados.
KPI	Indicadores clave de desempeño.

Hardware	Conjunto de componentes físicos que integran la parte material de una computadora.
Lineamiento	Dirección o tendencia.
Log	Archivo plano que almacena las operaciones ejecutadas sobre el DBMS, conformando una bitácora de las mismas.
Modelo	Arquetipo o punto de referencia para imitarlo o reproducirlo.
Pragmático	Establecimiento de relaciones entre los usuarios y las circunstancias de comunicación entre ellos.
Performance	Rendimiento o efectividad de respuesta.
Privilegio	Derecho de acceso a un objeto o servicio bajo condiciones especificas de uso.
Razonabilidad	Arreglado, justo, conforme a la razón**.**
Restricción	Limitación o reducción impuesta sobre el acceso a un producto o servicio**.**

Requerimiento	Examinar el estado en el que se halla algo.
Roles	Conjunto de privilegios asignados a un usuario determinado sobre un objeto dado.
Rutina	Secuencia invariable de instrucciones que forma parte de un programa y se puede utilizar repetidamente.
Script	Archivo de texto que contiene la definición de una base de datos en forma estructurada.
SCF	Factores críticos de éxito.
SGBD	Sistema de gestión de base de datos
Software	Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en computadoras.
Tablespaces	Espacio físico donde es almacenado las bases de datos correspondiente a un manejador de base de datos específico.
TI	Tecnología de la información.

RESUMEN

Se evalúan los temas específicos que se aplican sobre una auditoría de sistemas de base de datos, empezando por una descripción a nivel general sobre el tema; se definen los antecedentes de la auditoría, las clases que existen, definiciones específicas sobre un (Sistema de Base de Datos) DBMS relacional, aspectos clave de auditaje, los tipos de controles que se pueden realizar en el sentido informático, la aplicación de los objetivos de control sobre el desarrollo de una auditoría de sistemas, y las utilidades y beneficios que se pueden realizar con una correcta utilización de las herramientas aplicados a un DBMS.

Para concretar una explicación más específica, los conceptos que se manejan en las diferentes áreas donde se puede aplicar una auditoría a los DBMS relacionales, así como también, los recursos de tecnología de la información (TI) donde son aplicables la auditoría de un DBMS relacional.

Como parte central, se expone y aplica el concepto de una metodología denominada COBIT, que son los objetivos de control en las tecnologías de información, aplicado al auditaje DBMS relacionales; utilizado como estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnologías de Información.

COBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos puramente técnicos y riesgos de negocio. Este habilita el desarrollo de una política clara y de buenas prácticas de control de TI, a través de organizaciones.

Se establece lo que es la auditoría por objetivos de control, su historia y la necesidad de contar con una unión entre el área gerencial y el soporte de sistemas.

La aplicación de COBIT en el auditaje de un sistema de base de datos involucra la aplicación de los objetivos de control asociados al control de los recursos TI de un DBMS.

El auditaje de un DBMS relacional, aplicando los objetivos de control asociados de COBIT a los recursos de TI de información de una organización, describen aspectos como:

- El apoyo que brinda sobre el auditaje del DBMS.
- Planeación y organización de objetivos de control sobre un DBMS relacional
- La construcción de un modelo de madurez para un DBMS relacional.
- Impacto de la aplicación de objetivos de control sobre un DBMS relacional.

OBJETIVOS

- **General**

  Evaluar las ventajas que brinda aplicar COBIT en la realización de una auditoría de un DBMS relacional.

- **Específicos**

1. Identificar los procedimientos básicos, utilizados en una auditoría de DBMS relacionales y los objetivos de control asociados.

2. Examinar la disponibilidad de la base de datos conforme a la implementación de los objetivos de control para el auditaje de usuarios, procesos y los indicadores apropiados para limitar los efectos de las fallas en los elementos del DBMS relacionales.

3. Identificar los beneficios de COBIT en el auditaje de DBMS relacionales.

4. Establecer los procesos de TI en un sistema DBMS relacional que requieran ser evaluados regularmente en relación a los tiempos de ejecución, calidad y cumplimiento de los requerimientos de control y su alcance.

INTRODUCCIÓN

Para muchas organizaciones, la información y la tecnología que la respalda, representan algunos de los activos más valiosos de la empresa, por lo que la administración de los riesgos asociados de la tecnología de información, o gobernabilidad de tecnología de la información (TI), ha ganado notoriedad en tiempos recientes como un aspecto clave de la gobernabilidad corporativa, dada su capacidad de proporcionar valor agregado al negocio, balanceando la relación entre el riesgo y el retorno de la inversión sobre de TI y sus procesos.

Los objetivos de control de información (COBIT) representan una herramienta que permite organizar, administrar y evaluar la calidad del soporte de TI actual de la organización, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan y los requerimientos sobre la información de los primeros; a la vez permite definir las metas desde el punto de vista de seguridad y control que le serán de utilidad alcanzar a la organización para cada uno de sus procesos, ejecutando un plan de acción que permita identificar los lineamientos que sustenten un proceso de monitoreo y mejora continua sobre las soluciones implementadas desde el punto de vista de métricos del proceso de implementación.

La auditoría, de sistemas de bases de datos (DBMS) relacionales se instituye como la verificación de la exactitud, consistencia y confiabilidad de la información y con la privacidad y confidencialidad de los datos.

La aplicación de COBIT en la ejecución de una auditoría de un DBMS relacionales agrupan dominios de control de alto nivel, que cubren tanto los aspectos de información, como de tecnología que la respalda, facilitando la generación y procesamiento de la información masiva, cumpliendo así con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

1. AUDITORÌA DE SISTEMAS DE BASES DE DATOS RELACIONALES

1.1 Antecedentes

Conforme se expandía el comercio, después de pasar por el trueque primero en pueblos, ciudades, estados y finalmente, en continentes y motivados por su constante crecimiento, tanto en volumen como en el monto de operaciones comerciales, los incipientes comerciantes tuvieron la necesidad de establecer mecanismos rudimentarios de registro que le permitieran dominar las actividades mercantiles que realizaban.

Desde tiempos históricos, la auditoría evaluaba los ingresos y gastos producidos por un establecimiento u organización, practica utilizada por civilizaciones antiguas. Su verdadero nacimiento fue a finales del siglo XV cuando la clase alta de España, Inglaterra, Holanda, Francia y los países poderosos de Europa, recurrían a revisores de cuentas quienes verificaban las cuentas manejadas por los administradores de sus bienes y se aseguraban que no existieren malversaciones en los reportes presentados.

En la década de 1800, las empresas habían alcanzado gran auge en las actividades fabriles y mercantiles, lo cual trajo un gran crecimiento de sus operaciones y género esto la necesidad de evaluar el registro de las operaciones y resultados financieros por profesionales ajenos a la empresa que emitieran un dictamen imparcial a la situación de dicha evaluación.

La aplicación de la auditoría se ha extendido a otros campos profesionales para ampliar su revisión, siendo incluyente en las diversas actividades de la empresa. Con la aparición de la primera generación de computadoras en la década de los cincuentas, la informática se convierte en una herramienta muy importante en las labores de la auditoría financiera. Con esto se establecen los inicios de una “auditoría de sistemas”. Alrededor de los años sesentas, los sistemas de información se hacen presentes en las empresas cada vez con mayor frecuencia; a finales de esta década, se empieza a reconocer la necesidad de auditar los sistemas de información a la vez también se funda la asociación de auditores del proceso electrónico de datos.

Al implementarse los sistemas de información de la organización cada vez más dependientes de los procesos computarizados, nace la necesidad de auditar el correcto funcionamiento de los sistemas informáticos. A finales de la década de los 90’s, se descubren algunos casos de fraude cometidos con la ayuda del computador. Surge con esto una nueva especialidad híbrida, que contenga los conceptos de un auditor con los conocimientos técnicos del manejo de sistemas de información. En la actualidad, uno de los principales activos de las organizaciones, es la información y los sistemas de administración de la misma, representando su principal ventaja estratégica competitiva.

1.2 Auditoría

Auditoría es la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación.

La auditoría se desarrolla como una actividad especializada que puede ejecutarse solo por quienes están capacitados profesionalmente para ello. Sin embargo es necesario que estos profesionales cuenten con los conocimientos, experiencias, actitudes y aptitudes necesarios para realizar este tipo de trabajo, a fin de cumplirlo tal y como demandan las empresas y la sociedad.

El resultado final de una auditoría es un informe de la misma, en donde el auditor, con absoluta libertad y profesionalismo y totalmente fundamentado en la aplicación de sus técnicas, herramientas y conocimientos de auditoría, informa sobre los resultados obtenidos durante su revisión; para ello emite una opinión profesional e independiente, que plasma en un documento formal, llamado dictamen en el cual asienta todas las desviaciones y los demás aspectos observados durante su evaluación, para que los interesados conozcan el estado que guardan las actividades y operaciones de la empresa o el área auditada; siendo este el objetivo final de la auditoría.

1.2.1 Clases de auditoría

Dentro de la auditoría, se pueden diferenciar distintos enfoques. Por consiguiente, la auditoría se puede clasificar de la siguiente forma:

a. Auditorias por su lugar de aplicación

Refiere a la forma en que se realiza este tipo de trabajos y como se establece la relación laboral donde se llevara a cabo la auditoría.

- **Auditoría externa**

  Es la revisión independiente que realiza un profesional de auditoría, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como de la razonabilidad en la emisión de sus resultados financieros. La relación del trabajo del auditor es ajena a la institución donde se aplicara la auditoría y esto le permite emitir un dictamen libre e independiente.

- **Auditoría interna**

  Es la revisión que realiza un profesional de auditoría, cuya relación de trabajo es directa subordinada a la institución donde se aplicara la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, proveyendo finalmente con un dictamen interno sobre las actividades de toda la empresa.

b. Auditorias por su área de aplicación

Este tipo de auditoría refiere al ámbito específico donde se llevan a cabo las actividades y operaciones que serán auditadas, ubicando a cada tipo de auditoría de acuerdo con el área de trabajo e influencia de la rama o especialidad que será evaluada.

- **Auditoría financiera**

  Es la revisión sistemática, explorativa y critica que realiza un profesional de la contabilidad a los libros y documentos contables, a los controles y registros de las operaciones financieras y la emisión de los estados financieros de la empresa con el fin de evaluar y opinar sobre la razonabilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros obtenidos durante un periodo especifico o un ejercicio fiscal.

- **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 exhaustiva, sistemática y específica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo sus operaciones, cualquiera que estas sean, tanto en el establecimiento y cumplimento de los métodos técnicas y procedimientos de trabajos necesarios para el desarrollo de sus operaciones, en coordinación con los recursos disponibles.

- **Auditoría integral**

  Es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas la actividades y operaciones de una empresa, con el propósito de evaluar, de manera integral, el correcto desarrollo de las funciones en todas sus áreas administrativas, cualesquiera que estas sean así como de evaluar sus resultados conjuntos y sus relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objetivo institucional.

- **Auditoría gubernamental**

  Es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental, cualquiera que sea la naturaleza de las dependencias y entidades de la administración publica federal.

Esta revisión se ejecuta con el fin de evaluar el correcto desarrollo de las funciones de todas las áreas y unidades administrativas de dichas entidades, así como los métodos y procedimiento que regulan las actividades necesarias para cumplir con los objetivos gubernamentales, estatales o municipales.

- **Auditoría informática**

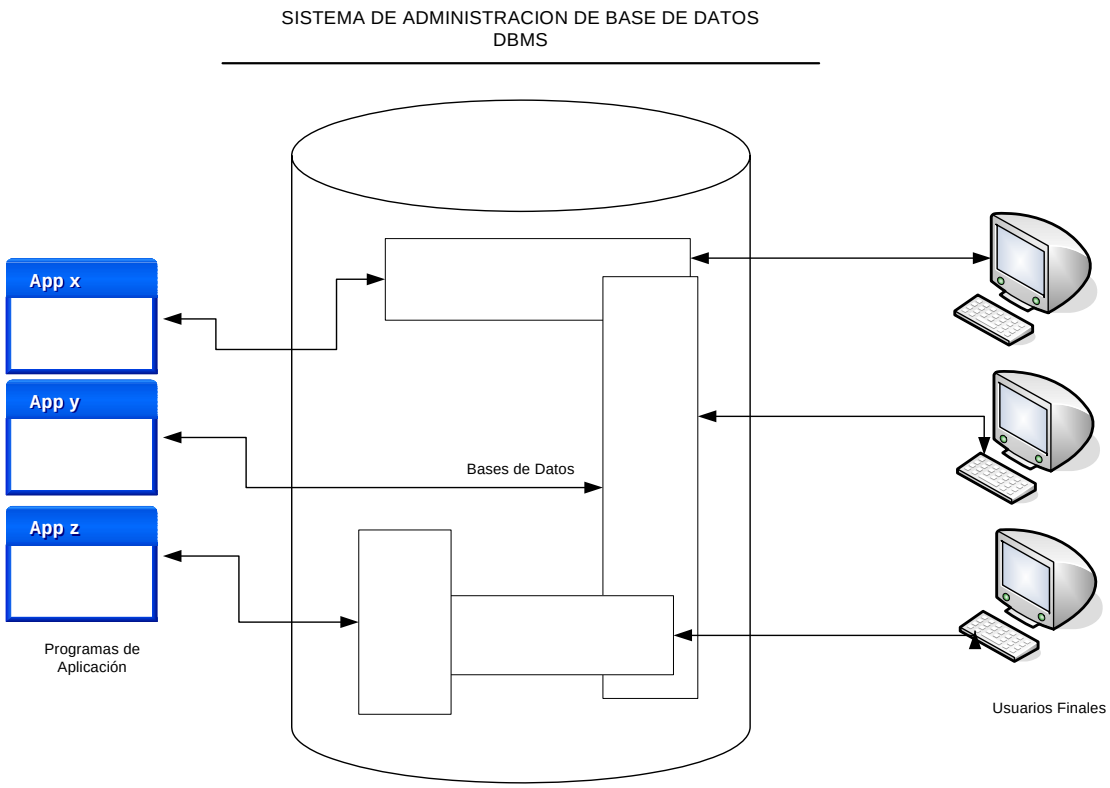
  Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o redes así como sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. El propósito fundamental es evaluar el uso adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

1. 3 Sistemas de bases de datos relacionales

1.3.1 Bases de datos

Conocido como DBMS, básicamente es un sistema computarizado que guarda registros de información y permite a los usuarios recuperar y actualizar dicha información, con base a peticiones. La información en cuestión puede ser cualquier cosa que sea de importancia para el individuo u organización; en otras palabras todo lo que sea necesario para auxiliarle en el proceso general de administración.

Figura 1 Sistema de base de datos



Un sistema de base de datos comprende cuatro componentes principales:

A. Datos

Un sistema de base de datos registra la información (colección de datos) en un repositorio de información organizado denominado base de datos, almacenada en un sistema centralizado multiusuario en el que los usuarios pueden tener acceso simultáneo a la misma. Los datos dentro la base de datos se encuentra de forma integrada y compartida; integrados dado que definen a la base de datos como una unificación de diversos archivos de información con una redundancia entre ellos parcialmente eliminada.

B. Hardware

Los componentes de hardware del sistema constan de:

- Los volúmenes de almacenamiento secundario, principalmente discos magnéticos que se emplean para la contención de datos almacenados junto a los dispositivos asociados.

- Los procesadores hardware y la memoria principal para apoyar la ejecución del software del sistema de base de datos.

C. Software

Entre la base de datos física, es decir los datos como están almacenados físicamente y los usuarios del sistema existe una capa de software conocida como el administrador de la base de datos o servidor de la base de datos comúnmente conocida como sistema de administración de la base de datos (DBMS).

D. Usuarios

En un sistema de base de datos, se contemplan tres grandes clases de usuarios:

a. **Programadores de aplicaciones:** son los responsables de escribir los programas de aplicación de base de datos en algún lenguaje de programación.

b. **Usuarios finales:** son quienes interactúan con el sistema de estaciones de trabajo o terminales en línea.

c. **Administrador de base de datos (DBA):** Es el responsable del control general del sistema a nivel técnico.

1.3.2 Bases de datos relacionales

Una base de datos relacional es un conjunto autodescriptivo de registros integrados. Es autodescriptiva dado que contiene una descripción de su propia estructural; definida en un diccionario de datos. Una base de datos posee una jerarquía de elementos de datos constituida por:

a.- Una jerarquía de los elementos de datos en el procesamiento de archivos.

b.- Una jerarquía de elementos de datos en el procesamiento de la base de datos.

Una base de datos relacional constituye un modelo de la realidad o alguna parte de la realidad, que esta relacionada con un negocio, cuyos componentes denotan: entidades, propiedades, identificadores, relaciones, diagramas entidad-relación, datos y modelos de datos.

1.3.2.1 Entidades

Una entidad es algo que puede identificarse en el ambiente de trabajo de los usuarios, es algo importante para los usuarios del sistema que se va a desarrollar. Las entidades se agrupan en clases de entidades o conjuntos de entidades del mismo tipo. Existen múltiples ocurrencias de una entidad en una clase de entidad.

1.3.2.2 Propiedades

Las entidades tienen atributos o como se les denomina en ocasiones, propiedades que describen las características de una entidad. En el modelo entidad relación los atributos pueden ser de valor único o múltiple o bien compuestos.

1.3.2.3 Identificadores

Las ocurrencias de una entidad tienen nombres que las identifican; el identificador de una ocurrencia de entidad es uno o más de sus atributos, un identificador puede ser único o no serlo. Si es único, su valor identificara una y solo una ocurrencia de entidad. Pero si no es único, el valor identificara un conjunto de ocurrencias.

1.3.2.4 Relaciones

Las entidades pueden asociarse una con otra en relaciones. El modelo E-R contiene clases de relaciones y ocurrencias de las relaciones. Las clases de relaciones son asociaciones entre las clases de entidades y ocurrencias de relaciones son asociaciones entre las ocurrencias de entidades. Las relaciones pueden tener múltiples atributos.

Una relación puede incluir muchas entidades; la cantidad de entidades en una relación determina el grado de la relación. El modelo E/R permite relaciones de cualquier grado que la mayoría de aplicaciones del modelo solo consideran relaciones de grado 2. Cuando son de tal tipo las relaciones se denominan binarias.

Existen tres tipos de relaciones binarias:

- **Relación 1-1:** tipo de relación que identifica una ocurrencia de una entidad única de un tipo se relaciona con una ocurrencia de entidad única de otro tipo.

- **Relación 1-N:** tipo de relación que identifica que la ocurrencia de una entidad se relaciona con muchas ocurrencias de otra entidad ajena.

- **Relación N- M:** tercer tipo de relación binaria; identifica que las ocurrencias de una entidad determinada se relaciona con las ocurrencias de otra entidad ajena.

1.3.2.5 Diagramas entidad-relación

Se denominan diagramas entidad-relación a los diagramas estandarizados en forma muy abierta, de acuerdo con este estándar, las clases de entidades se muestran con rectángulos; las relaciones mediante diamantes y la cardinalidad máxima de la relación aparece dentro el diamante. El nombre de la entidad se muestra dentro del rectángulo y el nombre de la relación cerca del diamante.

1.3.2.6 Datos y modelo de datos

En la fase de requerimientos para representar la realidad del negocio el objetivo centra en la creación de un modelo de datos del usuario; dicho modelo identifica las cosas que se van almacenar en la base de datos y define sus estructuras y relaciones entre ellas. El desarrollo de una base de datos ser complica proporcionalmente a la cantidad de requerimientos existentes.

Cuando los usuarios afirman que necesitan formas y reportes con datos y estructuras específicas, su petición implica un modelo del mundo que perciben. La gente de desarrollo debe inferir a partir de los requerimientos de los usuarios, la estructura y las relaciones de las cosas almacenadas en la base de datos. Después los analistas registran estas inferencias en un modelo de datos que se transforma en un diseño de base de datos y ese diseño se implementa utilizando un sistema de administración de base de datos DBMS relacional.

Desarrollar un modelo de datos es un proceso de inferencia, por lo que la inferencia y trabajo inverso a las estructuras y relaciones de la información son parte del trabajo de los analistas. La calidad del modelo es importante, si el modelo de datos documentado refleja con precisión el modelo de datos en la mente del usuario hay una cercanía de la representación de la realidad del negocio modelado. El modelo de base de datos debe documentarse para la resolución de diferencias y un mejor entendimiento de los analistas y desarrolladores. El modelo de la base de datos se transforma en una unión lógica de las piezas de un modelo de un grupo de trabajo o de la organización.

1.3.2.7 Administración de datos y administración de bases de datos relacional

La implicación de la administración de información organizacional es delgada la responsabilidad del control centralizado sobre los datos a una persona. Esa persona es el administrador de datos (DA) conceptualizado bajo un nivel de administración superior, y es el quien decide en que datos deben ser almacenados en la base de datos así como el establecimiento de políticas para mantener y manejar esos datos una vez almacenados.

El técnico responsable de implementar las decisiones del administrador de datos es el administrador de base de datos (DBA), siendo este un profesional TI, y su trabajo consiste en crear la base de datos real e implementar los controles técnicos necesarios para hacer cumplir las diversas decisiones de las políticas hechas por el administrador de datos.

1.3.2.8 Beneficio del enfoque de bases de datos relacional

Como parte de un control centralizado que brinda se especifican diferentes ventajas específicas que determinan el enfoque relacional:

1. **Compartimiento de datos:** denota la capacidad de que las aplicaciones organizacionales compartan la información de la base de datos y ala vez el desarrollo de nuevas aplicaciones que operen sobre los mismos datos.

2. **Reducción de redundancia:** conducción de una redundancia considerable de los datos almacenados, con el consecuente desperdicio de espacio de almacenamiento.

3. **Evitar inconsistencia:** representación de actualización de entidades vinculadas en donde ambas están totalmente actualizadas y consistentes.

4. **Manejo de transacciones:** una transacción es una unidad de trabajo lógica que regularmente comprende varias operaciones de la base de datos por lo que representa atomicidad de operaciones en la misma, es decir la realización completa o nula de transacciones sobre la base de datos.

5. **Manejo de integridad:** Asegura que los datos de la base de datos este correctos es decir especificar que se cumplan las restricciones de integridad (reglas del negocio).

6. **Cumplir con las restricciones de seguridad:** Definiciones de canales de acceso a la base de datos a través de la cual se definen las reglas de seguridad que verifican la sensibilidad de acceso a los datos.

7. **Equilibrio de requerimientos en conflicto:** Configuración de acceso a los datos por parte del DBA para el acceso rápido por parte de las aplicaciones.

8. **Estandarización:** Aplicabilidad de estándares para la representación de datos, para el intercambio de datos o para el movimiento de datos entre sistemas.

1.3.3 Arquitectura

La arquitectura de un sistema de base de datos relacional se basa en el estándar ANSI/SPARC y divide en tres niveles la estructura del mismo siendo estos: nivel interno, conceptual y externo respectivamente.

1.3.3.1 Nivel interno

Nivel conocido como físico, y cuyo acercamiento esta en el entorno físico de almacenamiento; tiene que ver con la forma en que los datos están almacenados físicamente.

1.3.3.2 Nivel externo

Conocido como el nivel lógico del usuario, y se denota como el nivel con cercanía al usuario. Se desarrolla con la forma en que los usuarios visualizan los datos.

1.3.3.3 Nivel conceptual

Conocido como el nivel lógico, cuya función es de indireccion entre lo otros dos niveles.

Figura 2 Arquitectura de un DBMS

1.3.4 Sistema de administración de base de datos

El DBMS (sistema de administración de base de datos) es el software que maneja todo acceso a la base de datos; y actúa bajo la siguiente lógica:

- El usuario emite una petición de acceso, utilizando algún sublenguaje de datos especifico.
- El DBMS intercepta la petición y la analiza.
- El DBMS inspecciona en su momento el esquema externo para ese usuario, la transformación externa/conceptual correspondiente, el esquema conceptual, la transformación conceptual/interna y la definición de la estructura de almacenamiento.
- El DBMS ejecuta las operaciones necesarias sobre la base de datos almacenada.

Complementa su estructura un conjunto de funciones del DBMS siendo estas: definición de datos, manipulación de datos, optimización y ejecución, seguridad e integridad, recuperación de datos y concurrencia, diccionario de datos y rendimiento.

1.3.4.1 Definición de datos

El DBMS es capaz de aceptar definiciones de datos (esquemas externos, el esquema conceptual, el esquema interno y todas las transformaciones respectivas) en la forma fuente y convertirla a la forma objeto correspondiente. Este incluye entre sus componentes un procesador DDL (Lenguaje de definición de datos) o compilador DDL.

1.3.4.2 Manipulación de datos

El DBMS debe ser capaz de manejar peticiones pare recuperar, actualizar o eliminar datos existentes en la base de datos o agregar nuevos datos a esta, con un componente procesador DML (Lenguaje de manipulación de datos).

En general, las peticiones DML pueden ser “planeadas” o “no planeadas” definidas de la siguiente forma:

- Una petición planeada es aquella cuya necesidad fue prevista antes del momento de ejecutar una petición.

- Una petición no planeada es una consulta adhoc; es decir una petición para la que no se previo por adelantado a su necesidad, si no en vez de ello, surgió sin pensarlo.

1.3.4.3 Diccionario de datos

Considerado como la base de datos del sistema. El diccionario contiene datos sobre los datos (metadatos). En particular, todos los esquemas fuentes y objetos estarán almacenados en el diccionario.

1.3.4.4 Rendimiento

Puede decirse en síntesis que la función global del DBMS es proporcionar la "interfaz de usuario" al sistema de base de datos que se encuentre disponible a un alto rendimiento a las peticiones que recibe el DBMS ejecutando consultas en tiempo adhoc.

1.3.4.5 Administrador de comunicaciones de datos

El data communication manager (DCM) es un componente de software que no es parte del DBMS, pero debe de trabajar con el, ya que es quien organiza los "mensajes de comunicación" hacia y desde la base de datos.

1.3.4.6 Arquitectura cliente-servidor

Desde un nivel muy alto, un sistema de base de datos puede considerarse que tiene una estructura de dos partes muy simple, que consiste de:

- Un servidor (backend)
- Un conjunto de clientes (frontends)

Las aplicaciones del tipo cliente-servidor están categorizidas de la siguiente manera:

- user-written applications
- vendor-provided applications
- escritores de reportes
- subsistemas gráficos de negocio
- procesadores de lenguaje natural
- paquetes estadísticos
- generadores de aplicaciones
- productos CASE.

1.3.4.7 Utilerías

Son los programas designados para ayudar al DBA en las diferentes tareas de administración. Las utilerías están categorizadas de la siguiente manera:

- Rutinas de cargado
- Rutinas de descarga/recargado
- Rutinas de reorganización
- Rutinas estadísticas
- Rutinas de análisis.

1.3.4.8 Procesamiento distribuido

Distintas máquinas pueden estar conectadas en una red de comunicación tal que una sola tarea de procesamiento de datos puede ocupar muchas máquinas en la red.

En general, cada servidor puede servir a muchos clientes, y cada cliente puede acceder a muchos servidores.

Un sistema de base de datos distribuido es cuando un cliente puede acceder muchos servidores simultáneamente. Es decir, que una sola petición a "la base de datos" puede combinar datos de varios servidores.

1.4 Auditoría de sistemas de bases de datos

1.4.1 Pasos de la metodología tradicional de auditaje del DBMS

La obtención del inventario de recursos (Hardware, software, orgware y liveware) y la información relevante para apoyar el examen que el equipo de auditoría realizara sobre el DBMS y el resultado de esta recopilación se organiza en un archivo de papeles de trabajo denominado archivo permanentemente o expediente continuo de auditoría.

Los pasos de un auditaje tradicional se denotan descritos bajos los siguientes puntos:

I. Conocimiento del negocio y del sistema.

Información sobre la empresa y su objeto social, sobre sus políticas y normas. Además toda la información referente al sistema de bases de datos, aspectos tales como:

1. Políticas y normas del negocio en relación con las actividades apoyadas con el sistema de bases de datos.

2. Información de objetos de las bases de datos (tablas, vistas, procedimientos almacenados, triggers, etc.).

3. Diagrama de sistema y de redes del servidor de bases de datos, servidores de replicación y servidores de aplicaciones. Todas las conexiones clientes a la base de datos incluyendo interfaces de red, direcciones IP, conexiones LAN y WAN.

4. Listado de usuarios de la base de datos con sus roles y privilegios.

5. Documentación de las aplicaciones sobre la base de datos

6. Cuadros organizacionales y descripción de funciones y procedimientos del personal que soporta las bases de datos.

7. Políticas de administración y procedimientos sobre la base de datos incluyendo procedimientos de seguridad, programas de backup y procedimientos de recover o restauración.

8. Documentación de pruebas de recovery o restauraciones.

9. Documentación de espacio en disco, tablas de espacio y monitoreo.

10. Archivos de arranque de bases de datos.

11. Script de utilidades.

12. Archivos de configuración.

13. Listados a través de sistema operativo de los directorios de la base de datos mostrando propietarios y permisos hasta el nivel de archivos.

14. Listados a través de sistema operativo de los directorios de programas de aplicación que accedan las bases de datos, mostrando propietarios y permisos hasta el nivel de archivos.

15. Listado de archivos de usuarios y grupos de usuarios.

16. Listado de información de archivos de logs.

17. Listado de los servicios habilitados

II. Definición del alcance de auditoría.

El alcance de la auditoría, representa la extensión de desarrollo de la misma haciendo explicito los recursos, procesos de TI que cubrirá la misma.

III. Definición de grupos de riesgos

Los escenarios de riesgos existentes en un sistema de bases de datos relacional se detallan conforme a la orientación de componentes, programas, planes, accesos u objetos que posee el mismo, entre los cuales podamos mencionar:

a . Objetos de la base de datos y reportes

- Permiso en SGBD
- Permisos SO
- Información fuera de tablas Export/Import.
- Privacidad y confidencialidad.
- Informes.
- DBA
- Acceso a los datos fuera de DBMS
- Políticas de seguridad

b. Programas de aplicación y utilitarios

- Acceso lógico
- Permiso en SGBD
- Permisos sistema operativo
- Datos en programas
- Modificaciones a aplicaciones
- Estándares de desarrollo
- Documentación cambios
- Autorización a cambios, pruebas y puesta en marcha.
- Acceso a fuentes.
- Copias de los nuevos programas.
- Adicionar rutinas de auditoría

c. Auditoría y seguimiento

- Logs.
- Riesgos logs muy grandes.
- Desconocimiento de la información.

d. Planes de respaldo y contingencia

e. **Metadatos**

f. **Seguridad en la red**

g. **Acceso a través de Internet**

h. **Seguridad Instalaciones y acceso físico**

i. **Diseño de la base de datos**

- Llaves primarias lógicas
- Integridad referencial o mecanismos
- Normalización
- Triggers mal diseñados

j. **Eficiencia y economía de recursos**

k. **Almacenamiento.**

IV. Agrupación

Se denotan los riesgos potenciales con un mayor nivel de riesgo y se agrupan para una evaluación simplificada y efectiva en la auditoría basándose en los siguientes criterios:

a. Problemas por seguridad en instalaciones y acceso físico.

b. Riesgos relacionados con el acceso lógico y la privacidad a las bases de datos causados por la relación el SO y el DBMS.

c. Riesgos asociados a las aplicaciones y utilitarios.

d. Problemas relacionados con el diseño de la base de datos.

e. Asuntos concernientes al diccionario de datos y documentación.

f. Problemas con el respaldo y planes de contingencia.

g. Riesgos por personal y organización.

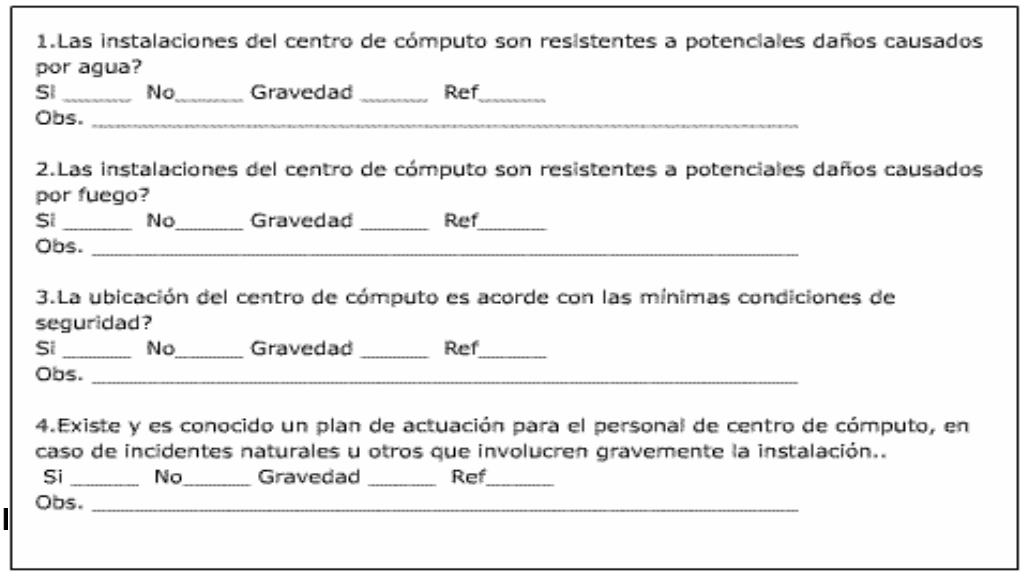
V. Evaluación del control interno

Objetivos de la evaluación para cada grupo de riesgos preguntando para cada objetivo gravedad, probabilidad, impacto, referencias observaciones, denotando el auditor las evaluaciones a ejecutar correspondientes al DBMS y su entorno, definiendo los siguientes tipos de evaluaciones:

a. Evaluaciones de seguridad en instalaciones y acceso físico.

- Evaluar la seguridad de las instalaciones contra diferentes riesgos.
- Evaluar la existencia e planes de acción ante siniestros que involucren las instalaciones.
- Evaluar las medidas existentes para el control de acceso físico a las instalaciones.

Figura 3 checklist de objetivos de problemas de seguridad en instalaciones y acceso físico.



1.Las instalaciones del centro de cómputo son resistentes a potenciales daños causados por agua?
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____

2.Las instalaciones del centro de cómputo son resistentes a potenciales daños causados por fuego?
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____

3.La ubicación del centro de cómputo es acorde con las mínimas condiciones de seguridad?
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____

4.Existe y es conocido un plan de actuación para el personal de centro de cómputo, en caso de incidentes naturales u otros que involucren gravemente la instalación..
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____

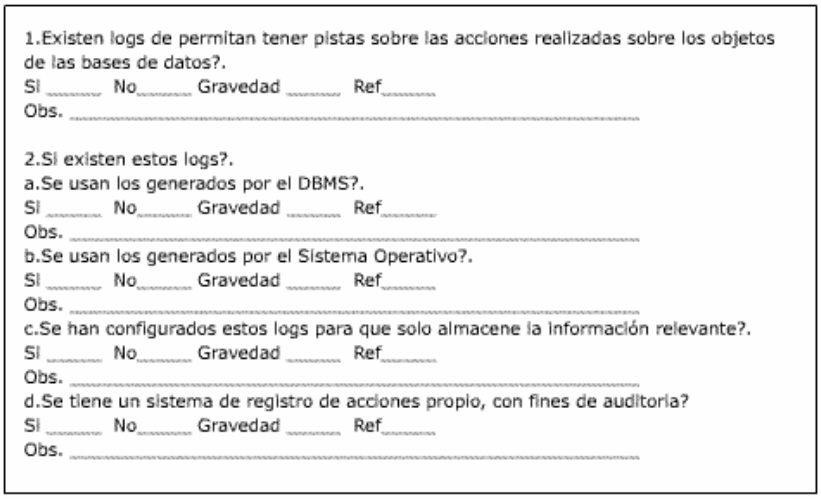
b. Otras evaluaciones

Dentro de otros aspectos a evaluar cabe mencionar los siguientes puntos:

- Riesgos relacionados con el acceso lógico y la privacidad a las bases de datos.
- Riesgos asociados a las aplicaciones y utilitarios.
- Problemas relacionados con el diseño de la base de datos.
- Investigar sobre la metodología de diseño usada.
- Evaluar la integridad y consistencia de los datos.
- Evaluar si el sistema respeta y apoya las reglas del negocio.
- Asuntos concernientes al diccionario de datos y documentación.
- Problemas con el respaldo y planes de contingencia.
- Riesgos por personal y organización.
- Evaluar las funciones del DBA.
- Evaluar si el sistema respecta la segregación de funciones.
- Evaluar las condiciones del personal involucrado con el DBMS.

Figura 4 checklist de objetivos de problemas

de seguridad en instalaciones y acceso físico.



1.Existen logs de permitan tener pistas sobre las acciones realizadas sobre los objetos de las bases de datos?.
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____

2.Si existen estos logs?.
a.Se usan los generados por el DBMS?.
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____
b.Se usan los generados por el Sistema Operativo?.
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____
c.Se han configurados estos logs para que solo almacene la información relevante?.
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____
d.Se tiene un sistema de registro de acciones propio, con fines de auditoria?
Si _____ No_____ Gravedad _____ Ref_____
Obs. _____

Los pasos anteriores son base para determinar la naturaleza y extensión de las pruebas de auditoría que deban efectuarse. Las pruebas de auditoría, son de dos tipos:

- De cumplimiento
- Sustantivas

Las pruebas de auditoría buscan obtener evidencia que los controles establecidos existen en realidad y se utilizan y ejecutan correctamente. Al conjunto de pruebas resultante se denomina programa de auditoría. El modo en que se verifica cada respuesta de los cuestionarios, debe ser incluido en los checklist.

Es un trabajo de escritorio donde se especifica la instalación a evaluar, el número de la prueba, el objetivo de la misma, las técnicas a emplear, el tipo de prueba (de cumplimiento o sustantiva), los recursos necesarios para aplicarla, en cuanto a información, software, hardware y personal.

VI. Ejecución de pruebas

Su propósito es obtener evidencia sobre los controles establecidos, su utilización, y el entendimiento y ejecución de los mismos por parte de las personas. Para cada prueba ejecutada deben adjuntarse los soportes correspondientes.

VII. Análisis de efectos de debilidades

a. Identificación de debilidades del DBMS

b. Impacto del mal funcionamiento del DBMS

c. Costo de perdidas y adicionales del DBMS

d. Probabilidad de ocurrencia.

VIII. Diseño de controles

Determinar y evaluar medidas de seguridad adicionales presentando los siguientes documentos de sustentación:

- Informe final
- Informe de seguimiento

1.4.2 Alcance de la auditoría

El auditaje a los métodos de acceso, seguridad y la salvaguarda de la información organizacional son aspectos claves definibles para el alcance de una auditoría a un DBMS como:

- Planes de prevención contra contingencias en el funcionamiento del DBMS, en la información y datos de la organización y en los demás bienes informáticos asociados y de las demás áreas que estén vinculadas con el DBMS.

- Identificación de accesos, almacenamiento y custodia de la información, sistemas operativos, lenguajes y archivos de programas institucionales.

- Evaluación de controles y sistemas de seguridad, protección de los programas, información, instalaciones, empleados y usuarios del sistema computacional.

- Planes contra contingencia para seguridad y protección de los programas información, instalaciones, empleados y usuarios del DBMS.

- Sistemas de control de accesos lógicos al DBMS y a las bases de datos.

- Sistemas de control de accesos físicos al centro de cómputo.

1.4.3 Auditoría de la seguridad lógica

Para la realización de la auditoría que evalué la seguridad a nivel lógico en el DBMS se deben considerar los siguientes aspectos claves:

- Estándares, medidas de seguridad y métodos establecidos para la consulta de datos y salida de información del DBMS.

- Evaluación de métodos de acceso, consulta, uso manipulación y modificación de información y datos contenidos en las bases de datos del sistema así como los procesos y operación del mismo.

- Existencia y aplicación de normas, políticas y procedimientos para el control de acceso de datos, para su procesamiento y salida del sistema computacional.

- Administración adecuada de la seguridad de las bases de datos e información institucional, así como la existencia y periodicidad de respaldos de información.

- Administración de niveles de accesos, contraseñas, privilegios de manejo de información y medidas de seguridad para proteger las bases de datos de los sistemas de la empresa.

1.4.3.1 Auditoría de la administración del DBMS

Para ejecutar una evaluación sobre el control y administración se denotan aspectos como evaluación de los usuarios y objetos del DBMS.

1.4.3.1.1 Administración de usuarios

Es clave denotar que para una adecuada administración de usuarios y evaluación de los mismos se procede a evaluar aspectos de nombres de usuarios, claves de acceso (contraseña) y perfiles asociados. Pueden también ser evaluados los roles que serán concedidos a los estos según sus funciones.

El aseguramiento y evaluación de los procesos de usuarios deben ser autorizados y autenticados en la base de datos.

1.4.3.1.2 Administración de objetos

En una evaluación de objetos del DBMS se denotan las políticas del sistema operativo, bases de datos, tablas, vistas, triggers, procedimientos almacenados, registros de bitácora, informes, y políticas de seguridad.

1.4.4 Auditoría del performance del DBMS

El banco de datos es el conjunto de datos que guardan entre si una coherencia temática independiente del medio de almacenamiento. La cantidad de información que contiene un banco de datos suele ser en el orden de millones de datos.

Considerando que una base de datos organizacional, debe facilitar el acceso, recuperación y actualización de datos, dicho banco de datos refiere a una estructura activos de datos valiosos de información prescindible para la toma de decisiones y historialmente representativa.

El sistema de administración de base de datos (DBMS) esta representando por un conjunto de programas que administran las bases de datos facilitando:

- Actualizar y recuperar información en tiempos considerables de respuesta de una base de datos en tiempos de respuesta considerables.

- Administración efectiva de solicitudes de múltiples de usuarios.

- Tiempos de respuesta considerables balanceando la carga de las solicitudes de los usuarios.

- Almacenamiento de información centralizada o distribuidamente según el tipo de configuración del DBMS.

- Eliminación de redundancia en los archivos.

2. OBJETIVOS DE CONTROL EN TECNOLOGÍA DE INFORMACIÓN COBIT

2.1 Antecedentes al objetivo de control

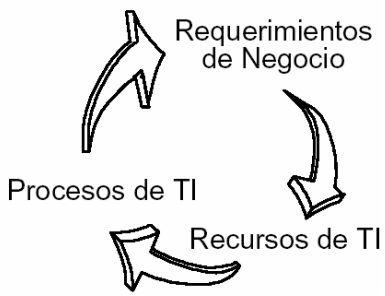
COBIT está basado en los objetivos de control existentes de la Information Systems Audit. and Control Foundation (ISACF); ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de tecnología informática. Los objetivos de control resultantes, aplicables y aceptados en forma generalizada, han sido desarrollados para ser aplicados a los sistemas de información de toda la empresa.

Como estándar, se tiene un producto independiente de la plataforma técnica de tecnología informática, que tiende a ser pragmático, relativamente pequeño y que responda a las necesidades del negocio. La provisión de indicadores de performance (normas, reglas, etc.) ha sido identificada como prioridad para las futuras mejoras que se realicen en la estructura.

2.2 Marco referencial de COBIT

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en tecnología de información se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la tecnología de información, que deben ser administrados por procesos de TI.

Figura 5 Marco referencial de COBIT

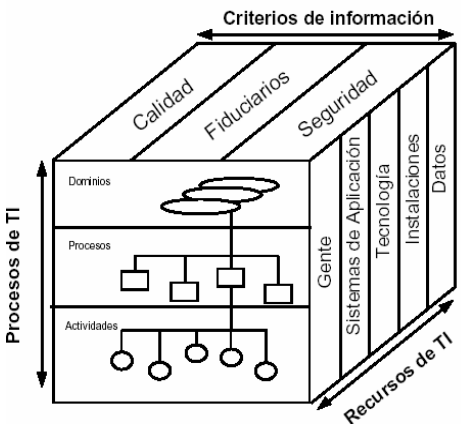


El marco referencial conceptual puede ser enfocado desde tres puntos estratégicos:

1.- Recursos de TI
2.- Requerimientos de negocio para la información y
3.- Procesos de TI.

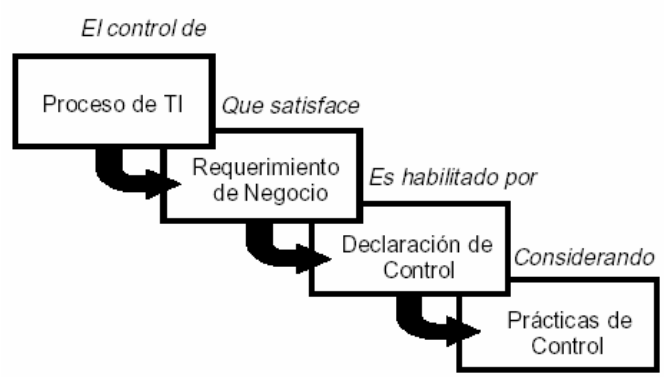
Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

Figura 6 Punto de vista estratégico del marco referencial de COBIT



También deberá tomarse en cuenta que los objetivos de control COBIT han sido definidos en una manera genérica, por ejemplo, sin depender de la plataforma técnica, aceptando el hecho de que algunos ambientes de tecnología especiales pueden requerir una cobertura separada para objetivos de control.

Figura 7 Cobertura de los objetivos de control



2.2.1 Establecimiento del la escena

En años recientes, ha sido cada vez más evidente para los legisladores, usuarios y proveedores de servicios la necesidad de un marco referencial para la seguridad y el control de tecnología de información (TI). Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de TI relacionada la criticalidad del control emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información

- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las “amenazas cibernéticas” y la guerra de información

- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información

- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología.

Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

La administración debe decidir la inversión razonable en seguridad y control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. La administración necesita un marco referencial de prácticas de seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente de TI, tanto el existente como el planeado.

Existe una creciente necesidad entre los usuarios en cuanto a la seguridad en los servicios TI, a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados. Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan una base general a ser establecida como primer paso.

2.2.2 Principios del marco referencial

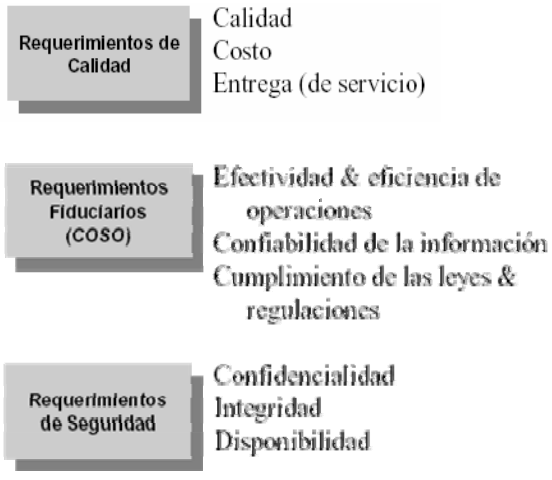
El marco referencial de los objetivos de control de la tecnología de la información esta conformado por:

I. Modelos de control

Existen dos clases distintas de modelos de control disponibles actualmente; aquellos de la clase del “modelo de control de negocios” (por ejemplo COSO) y los “modelos más enfocados a TI” . COBIT se posiciona como una herramienta más completa para la administración y para operar a un nivel superior que los estándares de tecnología para la administración de sistemas de información. COBIT es el modelo para el gobierno de TI.

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos.

Figura 8 Criterios de COBIT



La calidad ha sido considerada principalmente por su aspecto ‘negativo’ (no fallas, confiable, etc...), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo, atractivo, “ver y sentir”, desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de objetivos de control de TI.

La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la calidad está cubierto por los criterios de efectividad.

Para los requerimientos fiduciarios, COBIT utiliza las definiciones de COSO para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, confiabilidad de información fue ampliada para incluir toda la información, no sólo información financiera.

Con respecto a los aspectos de seguridad, COBIT identifica la confidencialidad, integridad y disponibilidad como los elementos clave, estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

II. Definición de trabajo

A partir de los requerimientos de negocios para la información y tomando en cuenta cada unos de ellos, se pueden extraer siete categorías distintas, ciertamente superpuestas a las cuales, se llamarán definiciones de trabajo de COBIT, las cuales se listan a continuación:

- **Efectividad:** se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

- **Eficiencia:** se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

- **Confidencialidad:** se refiere a la protección de información sensible contra divulgación no autorizada.

- **Integridad:** se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

- **Disponibilidad:** se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro.

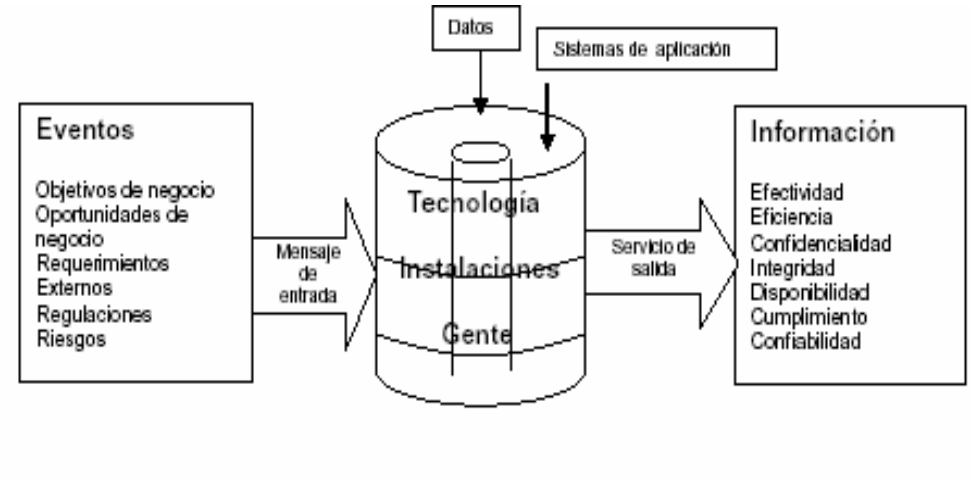
- **Cumplimiento:** se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto.

- **Confiabilidad de la Información:** se refiere a la provisión de información apropiada para la administración, con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

III. Recursos de TI

Una forma de ver la relación de los recursos de tecnología de información, respecto a la entrega de servicios es que la información que los procesos de negocios necesitan es proporcionada a través del empleo de recursos de tecnología de información. Con el fin de asegurar que los requerimientos de negocios para la información son satisfechos, deben de definirse, implementarse y monitorearse medidas de control adecuadas para éstos recursos, el cual se ilustra en la siguiente gráfica.

Figura 9 Recursos de TI



Los recursos de tecnología de información se pueden explicar o definir de la siguiente manera:

1. Datos: los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

2. Aplicaciones: se entiende como sistemas de aplicación la suma de procedimientos manuales y programas.

3. Tecnología: la tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

4. Instalaciones: recursos para alojar y dar soporte a los sistemas de información.

5. Personal: habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

IV. Procesos de TI

El marco referencial consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación.

La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI, al considerar la administración de sus recursos. Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control).

Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.

V. Dominios

Con lo anterior como marco de referencia, los dominios son identificados empleando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización.

Cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo. Las definiciones para los dominios mencionados son las siguientes:

- **Planeación y organización:** este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma, en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.

- **Adquisición e implementación:** para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio.

- **Entrega y soporte:** en este dominio, se hace referencia a la entrega de los servicios requeridos, que comprende desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- **Monitoreo:** todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia, en cuanto a los requerimientos de control.

2.2.3 Utilización del marco referencial

El marco referencial conceptual puede ser enfocado desde tres puntos estratégicos:

1) Recursos de TI
2) Requerimientos de negocio para la información y
3) Procesos de TI.

Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente. El marco referencial COBIT ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de TI particular, cuyo logro es posible a través de un establecimiento de controles, para el cual deben considerarse controles aplicables potenciales.

Los objetivos de control de TI han sido organizados por proceso/actividad, pero también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista para facilitar enfoques combinados, tales como instalación e implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de TI por un proceso.

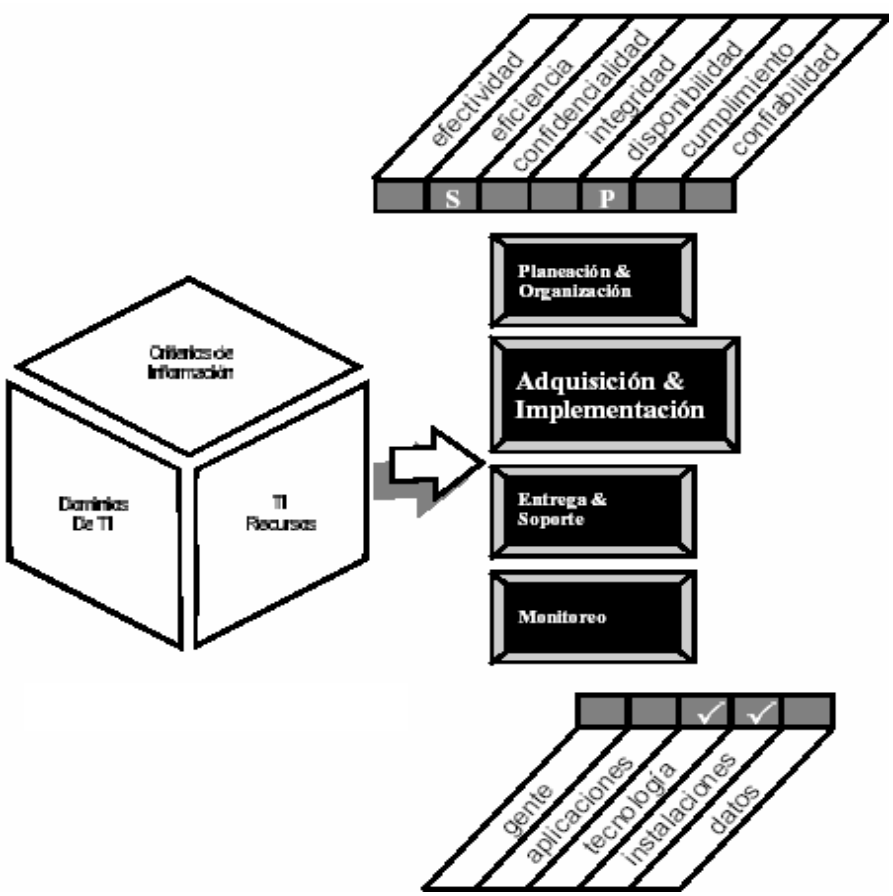
2.2.4 Ayuda de navegación

Para facilitar el empleo eficiente de los objetivos de control como soporte a los diferentes puntos de vista, se proporcionan ayudas de navegación como parte de la presentación de los objetivos de control de alto nivel. Se proporciona una ayuda de navegación para cada una de las tres dimensiones del marco referencial COBIT procesos, recursos y criterios.

Como un índice de navegación para el manejo de los objetivos de control se denotan el manejo de los mismos a través de los siguientes pasos:

- **Identificación de dominios**

Figura 10 Dominios de COBIT



- **Identificación de criterios**

  La clave para el criterio de información será proporcionada por la matriz superior en la sección de objetivos de control la cual identifica el criterio y en qué grado (primario o secundario) es aplicable a cada objetivo de control de TI de alto nivel.

- **Identificación de recursos TI**

  Una segunda “mini” matriz en inferior identifica los recursos de TI que son administrados en forma específica por el proceso bajo consideración no aquellos que simplemente toman parte en el proceso.

- **Principios de los objetivos de control**

  COBIT refleja el compromiso continuo por mejorar y mantener el cuerpo común de conocimientos requeridos para apoyar la actividad de la auditoría y control de sistemas de información. Así como el marco de referencia de COBIT (COBIT Framework) que se encuentra enfocado a controles de alto nivel para cada proceso.

Los objetivos de control alinean el marco de referencia general con los objetivos de control detallados a partir de treinta y seis (36) fuentes primarias que comprenden estándares internacionales de hecho y de derecho y las regulaciones relacionadas con TI.

Este contiene la relación de los resultados o propósitos deseados que desean alcanzarse a través de la implementación de procedimientos de control específicos dentro de una actividad TI y de esta manera proporciona una política clara y una mejor practica para el control de TI organizacional.

Los objetivos de control están dirigidos a la gerencia y al personal de servicios de información, controles, funciones de auditoría y lo mas importante a los propietarios de procesos de negocios. Permiten la traducción de los conceptos presentados en el marco de referencia en controles específicos aplicables para cada proceso TI.

2.3. Modelo de madurez de COBIT

El modelo de madurez de COBIT ofrece las bases para el entendimiento y la evaluación de las condiciones actuales de seguridad y control de los procesos del ambiente de TI de una organización. Este modelo provee las bases para la evaluación de las principales funciones del área de TI, a través de la consideración de cada uno de sus procesos clave, a los cuales se les asignará un valor de cero (0) a cinco (5), indicando así el nivel de esfuerzo ("madurez") que se sugiere invertir en la actividad de control de dicho proceso, de forma de garantizar una buena relación costo beneficio al asegurar el nivel de seguridad estrictamente requerido.

Las principales características que identifican a cada nivel son las siguientes:

0. Inexistente: Ausencia total de cualquier proceso o control reconocible. La organización no ha reconocido la necesidad del proceso o control.

1. Inicial: Existe evidencia de que la organización ha reconocido la necesidad de mejorar los procesos o controles. No existen procesos

estandarizados, pero se realizan procedimientos “ad hoc” que tienden a aplicarse en casos individuales. La forma en que la gerencia enfrenta estos temas no se encuentra organizada.

2. Repetible: Se han desarrollado procesos donde se siguen procedimientos similares por diferentes personas para la misma tarea. No se ha formalizado la capacitación o la comunicación de los procedimientos en forma estándar, ni la responsabilidad es de cada individuo. Hay un alto grado de confianza en el conocimiento individual, por lo que los errores son más frecuentes.

3. Definido: Los procedimientos han sido estandarizados y documentados y son comunicados a través de la capacitación. Sin embargo, se deja a los individuos el seguimiento de los procesos, por lo que resulta poco probable que se detecten desviaciones. Los procedimientos no son sofisticados pero existe formalización de las prácticas existentes.

4. Gestionado o administrado: Es posible monitorear y medir el cumplimiento de los procedimientos y tomar acciones cuando los procesos no están funcionando efectivamente. Los procesos se encuentran constantemente bajo mejora y proveen buenas prácticas. Se utilizan automatización y herramientas de una forma limitada o fragmentada.

5. Optimizado: Los procesos han sido redefinidos al nivel de las mejores prácticas, basados en los resultados de mejoras continuas y el modelo de madurez con otras organizaciones. TI se utiliza de una forma integrada para automatizar el workflow, proveyendo herramientas para mejorar la calidad y la efectividad, con una rápida adaptación.

Mejorando el nivel de madurez de los controles asociados a cada uno de los procesos de TI, según las necesidades reales de éstos, la organización logrará mejorar el nivel de control interno de los mismos.

En este caso se obtendrán, al menos, un incremento de la eficiencia operativa y la formalización de los procesos. Trabajando en base al modelo de madurez deseado, se seleccionarán los objetivos de control que deberán aplicarse a los efectos de evaluar la situación actual de cada uno de los procesos de TI de la organización; de esta manera se obtendrá el grado de cumplimiento de cada proceso tomando como marco de referencia los estándares provistos por COBIT, pero guiados por los requerimientos reales de la organización.

Figura 11 Modelo de madurez de COBIT

El modelo de madurez representa entonces, “a dónde la organización desea llegar”, mientras que el resultado de la evaluación (aplicando el marco COBIT) representa “dónde la organización está”. Las posibles brechas detectadas entre ambas situaciones serán los disparadores del plan de acción para implementar las soluciones que se requiera para mejorar la estructura de control interno en el grado deseado.

De lo anterior se deduce que es tan importante fijar adecuadamente “hasta dónde se desea llegar” (grado de madurez), cómo seleccionar los objetivos de control que permitirán realizar la evaluación. Este es un aspecto clave para poder proseguir con una implantación de COBIT exitosa alineada a las necesidades de la organización.

Existen otros aspectos que conforman el modelo de madurez COBIT, que se definen a continuación:

1. **Factores críticos de éxito (SCF):** Definen los asuntos más importantes o las acciones que debe llevar adelante la gerencia para alcanzar el control sobre los procesos de TI. Deben ser lineamientos de implementación orientados a la administración y que identifiquen las principales acciones a realizar, desde el punto de vista estratégico, técnico, organizacional y procedimental.

2. **Indicadores clave de resultados (KGI):** Define métricas que le indican a la gerencia –después de ocurrido- si un proceso de TI ha alcanzado sus requerimientos de negocio, usualmente expresados en términos de los criterios de información de COBIT:

   - Disponibilidad de la información necesaria para soportar los requerimientos del negocio
   - Ausencia de riesgos de integridad y confidencialidad
   - Eficiencia en los costos de procesos y operaciones
   - Confirmación de confianza, efectividad y cumplimiento

3. **Indicadores clave de desempeño (KPI):** Define métricas para determinar cuán bien se desempeña el proceso de TI para alcanzar la meta. Son los indicadores principales para saber si es probable o no que se alcance una meta y son buenos indicadores de capacidades, prácticas y habilidades.

3. APLICACIÓN DE COBIT EN LA AUDITORÍA DE UN DBMS

3.1 Mejores prácticas en el auditaje del DBMS aplicando COBIT

Los recursos asociados al control de los componentes de un sistema de base de datos: programas y datos deben ser controlados y verificados de forma objetiva bajo la utilización de COBIT para dictaminar sobre la situación actual del DBMS.

Para ello, se distingue entre las medidas para restringir y controlar el acceso a dichos recursos asociando los objetivos de control asociados a cada caso presentado vinculado con los recursos evaluados, así como los procedimientos para asegurar la fiabilidad del software (tanto operativo como de gestión) y los criterios a considerar para garantizar la integridad de la información.

3.1.1 Control de acceso

Sistemas de identificación, asignación y cambio de derechos de acceso, control de accesos, restricción de terminales, desconexión de la sesión, limitación de reintento.

3.1.2 Software de la base de datos

Control de cambios y versiones, control de uso de programas de utilidad, control de uso de recursos y medición del “performance”’ o rendimiento.

3.1.3 Software de aplicación

Concierne al software de aplicación, es decir, todo lo relativo a las aplicaciones de gestión, sean producto de desarrollo interno de la empresa o bien sean paquetes estándar adquiridos en el mercado.

3.1.4 Desarrollo de software

En el desarrollo de software se evalúan los siguientes aspectos claves:

- Metodología: existe, se aplica, es satisfactoria. Documentación: existe, esta actualizada, es accesible.
- Estándares: se aplican, como y quien lo controla. Involucración del usuario.
- Participación de personal externo.
- Control de calidad.
- Entornos real y de prueba.
- Control de cambios.

3.1.5 Adquisición de software estándar

Metodología, pruebas, condiciones, garantías, contratos, capacitación, licencias, derechos, soporte técnico.

3.1.6 Datos

Los datos es decir, la información que se procesa y se obtiene son la parte más importante de todo el sistema informático y su razón de ser. Un sistema informático existe como tal desde el momento en que es capaz de tratar y suministrar información. Sin ésta, se reduciría a un conjunto de elementos lógicos sin ninguna utilidad.

En la actualidad la inmensa mayoría de sistemas tienen la información organizada en sendas bases de datos. Los criterios que se citan a continuación hacen referencia a la seguridad de los sistemas de gestión de bases de datos (SGBD) que cumplan normas ANSI, si bien muchos de ellos pueden ser aplicables a los archivos de datos convencionales.

3.1.7 Diseño de bases de datos

Es importante la utilización de metodologías de diseño de datos. El equipo de analistas y diseñadores deben hacer uso de una misma metodología de diseño, la cual debe estar en concordancia con la arquitectura de la base de datos elegida jerárquica, relacional, red, o bien orientada a objetos.

Debe realizarse una estimación previa del volumen necesario para el almacenamiento de datos basada en distintos aspectos tales como el número mínimo y máximo de registros de cada entidad del modelo de datos y las predicciones de crecimiento.

A partir de distintos factores como el número de usuarios que accederá a la información, la necesidad de compartir información y las estimaciones de volumen se deberá elegir el SGBD más adecuado a las necesidades de la empresa o proyecto en cuestión. En la fase de diseño de datos, deben definirse los procedimientos de seguridad, confidencialidad e integridad que se aplicarán a los datos.

Procedimientos para recuperar los datos en casos de caída del sistema o de corrupción de los archivos. Procedimientos para prohibir el acceso no autorizado a los datos. Para ello deberán identificarlos.

Procedimientos para restringir el acceso no autorizado a los datos. Debiendo identificar los distintos perfiles de usuario que accederán a los archivos de la aplicación y los subconjuntos de información que podrán modificar o consultar. Procedimientos para mantener la consistencia y corrección de la información en todo momento. Básicamente existen dos niveles de integridad: la de datos, que se refiere al tipo, longitud y rango aceptable en cada caso, y la lógica, que hace referencia a las relaciones que deben existir entre las tablas y reglas del negocio.

3.1.8 Creación de bases de datos

Debe crearse un entorno de desarrollo con datos de prueba, de modo que las actividades del desarrollo no interfieran el entorno de explotación. Los datos de prueba deben estar dimensionados de manera que permitan la realización de pruebas de integración con otras aplicaciones, de rendimiento con volúmenes altos.

En la fase de creación, deben desarrollarse los procedimientos de seguridad, confidencialidad e integridad definidos en la etapa de diseño:

- Construcción de los procedimientos de copia y restauración de datos.
- Construcción de los procedimientos de restricción y control de acceso.

Existen dos enfoques para este tipo de procedimientos:

- Confidencialidad basada en roles, que consiste en la definición de los perfiles de usuario y las acciones que les son permitidas (lectura, actualización, alta, borrado, creación/eliminación de tablas, modificación de la estructura de las tablas).

- Confidencialidad basada en vistas, que consiste en la definición de vistas parciales de la base de datos, asignándolas a determinados perfiles de usuario.

Construcción de los procedimientos para preservar la integridad de la información. En los SGBD actuales, la tendencia es la implantación de estos procedimientos en el esquema físico de datos, lo cual incide en un aumento de la fiabilidad y en una disminución del coste de programación, ya que el propio gestor de la base de datos controla la obligatoriedad de los atributos de cada entidad, dominio o rango de los datos y las reglas de integridad referencial.

3.1.9 Explotación de bases de datos

Es importante la realización de inspecciones periódicas que comprueben que los procedimientos de seguridad, confidencialidad e integridad de los datos funcionan correctamente. Para ello, existen diversos métodos y utilidades:

- Registro de accesos y actividad (archivos lógicos). Los SGBD actuales suelen tener archivos de auditoría, cuya misión es registrar las acciones realizadas sobre la base de datos, haciendo referencia a nombre de objetos modificados, fecha de modificación, usuario que ha realizado la acción, en fin lo datos más relevantes para poder llevar a cabo seguimiento de las acciones efectuadas.

- Registro de modificaciones realizadas por la aplicación. Una aplicación bien diseñada debería grabar información necesaria para detectar incidencias o fallos. Estos atributos, también llamados pistas de auditoría, pueden ser la fecha de creación o de ultima modificación de un registro, el responsable de la modificación, la fecha de baja lógica de un registro en general registrar todos los datos relevantes para poder llevar un seguimiento de las modificaciones efectuadas.

- Mantenimiento periódico de la base de datos. Periódicamente, el administrador de datos debe controlar el crecimiento y la evolución de los archivos de la base de datos a fin de tomar las medidas necesarias para mejorar el rendimiento del sistema.

- Mantenimiento de la base de datos; dado que la base de datos es un objeto cambiante, periódicamente debe efectuarse su mantenimiento, ya que su estructura, volumen, comportamiento, apariencia se modifican con el paso del tiempo. Asimismo, deben revisarse los roles de los usuarios para adecuarlos a los posibles cambios que se vayan produciendo.

En la etapa de selección de una metodología, el equipo de desarrollo debe de elegir la que más se acerque a la problemática del sistema, indudablemente que no todas las metodologías son las adecuadas a cada problema, es aquí donde la ingeniería de software ayuda, sugiriendo diferentes metodologías, e inclusive la combinación de estas. La visión de un desarrollador de software se debe de centrar en la idea de que es lo mas importante para la empresa, teniendo como antecedente de que ambas partes (principalmente el usuario) deben de estar de acuerdo en la solución al problema.

Tomando en cuenta lo anterior y en los problemas mencionados en la justificación, se aplico una combinación de metodológicas entre el ciclo de vida clásico y el sistema de análisis estructurado.

Sobre la metodología de ciclo de vida, se utilizo la fase, “Determinación de los requerimientos”, ya que es de suma importancia conocer las necesidades del cliente u posibles problemas y para la recopilación de datos se aplica la entrevista y el cuestionario entre otros. Considerando las ventajas y desventajas que cada técnica ofrece se aplico la entrevista, por ser una de las más seguras y aplicables a un numero menor de personas.

El principal objetivo de recabar información es para determinar el tamaño del sistema de estudio, debido a esto se determino que se trataba de un sistema pequeño por la cantidad de procesos, el flujo de información y la complejidad de los cálculos estadísticos que maneja la empresa. En lo que se refiere al sistema de análisis estructurado, es considerable permitir el manejo de sistemas de menor complejidad, desarrollar programas de software e incorporar conceptos de bases de datos.

El uso de las bases de datos permite almacenar gran cantidad de información además de las siguientes ventajas:

- Permite tener un mejor control sobre la información que se almacena.
- Una gran velocidad sobre la consulta de información.
- Respaldo de información, dando una mayor seguridad de la misma.
- Flexibilidad en el traslado de la información

- Manejo de reportes inmediatos, obteniendo el numero de copias necesarias en corto tiempo.

Cada uno de los elementos que se incorporan en el análisis y diseño de esta metodología ayudan a identificar y comprender los procesos que se aplican, los elementos están involucrados, el agrupamiento mas adecuado de los datos, encontrar la duplicidad de la información, establecer una relación entre agrupamientos de la organización sobre la programación del software, así como un mantenimiento que asegure el funcionamiento adecuado del sistema.

El análisis estructurado de sistemas, es utilizado en sistemas no muy grandes y de poca complejidad, incorpora un lenguaje gráfico para representar sus modelos de sistemas a manipular más fácilmente la información. Esta se basa en los siguientes puntos:

a. Diagrama

El símbolo entidad puede representar a una empresa, una persona o una máquina, donde cada uno de estos puede ser fuente o destino de datos. La flecha representa como la información se traslada de una entidad a otra, la punta de la flecha indica el destino de los datos. Si se desea indicar transformaciones de los datos, se utiliza un rectángulo con esquinas redondeadas, donde la información que sale será diferente de la que entra.

El símbolo de almacenamiento de datos, indica donde la información puede ser consultada, sirve también para indicar donde se puede almacenar o guardar la información. El analista puede representar un sistema desde su forma más general hasta llegar a detallar la parte de interés en el desarrollo del sistema.

b. Diccionario de datos

El uso de un diccionario de datos ayuda a determinar cuales son los elementos de un sistema, además de que ayuda a detallarlo. Los elementos se deben de definir y de indicar en que parte son utilizados. Como primer paso se deben de agrupar según la información que se obtenga, determinar en que grupos son repetidos los diferentes elementos. El uso de un diccionario de datos debe primero ser generado durante la fase de análisis, y además un segundo diccionario durante la fase de diseño, ambos diccionarios de datos son importantes, ya que mientras en la fase de análisis sirvió para identificar los elementos del sistema, en la fase de diseño permitirá organizar la información que será almacenada por medio de la computadora en algún dispositivo de almacenamiento secundario.

c. Representaciones lógicas

Una representación lógica es principalmente utilizada para explicar los procesos que utiliza el instituto, estos procesos pueden ser representados por medio de lenguaje estructurado, por árboles de decisión o por diagramas de flujo: la técnica del lenguaje estructurado es la mas recomendable para que el usuario entienda si los procesos son correctos, se recomienda utilizar el español para explicar los procesos, ayudándose de estructuras de control como si entonces, hacer mientras etc.

d. Diseño estructurado

Es uno de los más utilizados y recomendados por los expertos en el desarrollo de sistemas de cómputo, además de que es una consecuencia del sistema de análisis estructurado, el diseño estructurado esta compuesto por las siguientes herramientas:

- **Diccionario de datos** El diccionario de datos que se diseñara, deberá tener como base el diccionario de datos que se realizo durante el análisis, además de tomar en cuenta las estructuras que fueron resultantes durante la fase de técnicas de estructuración de almacenamiento de datos.

- **Mapa de relaciones** Esta herramienta tiene como base las estructuras que fueron resultantes durante el desarrollo de la aplicación de las técnicas de estructuración de almacenamiento de datos, añadiendo la forma en que las estructuras están relacionadas, tomando como base la asignación de llaves, que permiten la identificación de cada relación y la forma en que estas pueden ser identificadas, una flecha indica que la relación será de una a una, doble flecha podrá indicar una a muchas, muchas a una, o muchas a muchas, la forma en que se representen deberá ser respetada por el quipo de trabajo, ya que es así como se realizara la programación.

3.2 Elementos de apoyo del COBIT en el DBMS

3.2.1 Claves primarias

Los objetivos de control asociados a la evaluación de llaves primarias dentro de las bases de datos que administra el DBMS se encuentran representados por:

P011 Administración de la calidad

Satisfacción de los requerimientos del cliente por medio de uso de identificadores principales a las relaciones definidas en el modelo relacional, normalizando las mismas a la primera forma normal.

DS05 Garantizar la seguridad del sistema

Salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, esto se hace posible a través de controles de acceso lógico que aseguran que el acceso a sistemas y programas este restringido a usuarios autorizados.

Al evaluar la seguridad del DBMS se toma en consideración lo siguiente:

- Autorización de acceso.
- Autentificación de acceso
- Acceso
- Perfiles de usuario
- Manejo de reportes y seguimiento de incidentes(Logs)
- Diccionario/ directorio de datos
- Lenguaje de datos
- Software de seguridad
- Sistema de almacenamiento, respaldo y recuperación
- Reporteadores
- SQL
- WebServer Software

3.2.2 Dominios de atributos

Los objetivos de control asociados a la evaluación de los dominios de los atributos de las relaciones dentro de las bases de datos que administra el DBMS se encuentran representados por:

PO2 Definición de la arquitectura de la información

Organiza de mejor manera las bases dentro del DBMS. La creación y mantenimiento de un de un modelo relacional de negocios, asegurando que se definan sistemas apropiados para optimizar la utilización de esta información.

Al evaluar la definición de la arquitectura se considera lo siguiente:

- Documentación
- Diccionario de datos
- Reglas de sintaxis de datos
- Propiedad de información

3.2.3 Reglas de integridad

Los objetivos de control asociados a la evaluación de reglas de integridad de las relaciones dentro de las bases de datos que administra el DBMS se encuentran representados por:

PO2 Definición de la arquitectura de la información

Organiza de mejor manera las bases dentro del DBMS. La creación y mantenimiento de un de un modelo relacional de negocios, asegurando que se definan sistemas apropiados para optimizar la utilización de esta información.

Al evaluar la definición de la arquitectura se considera lo siguiente:

- Documentación
- Diccionario de datos
- Reglas de sintaxis de datos
- Propiedad de información

P011 Administración de la calidad

Satisfacción de los requerimientos del cliente por medio de uso de identificadores principales a las relaciones definidas en el modelo relacional, normalizando las mismas a la primera forma normal.

3.2.4 Reglas de integridad del negocio

Los objetivos de control asociados a la evaluación de reglas de integridad de un negocio implementado a las bases administradas a un DBMS se encuentran representados por:

P8 Aseguramiento de cumplimiento de requerimientos externos

El objetivo de control provee un control para el cumplimiento de obligaciones legales, regulatorias y contractuales. Haciendo esto posible a través de la identificación y el análisis de los requerimientos externos en cuanto a su impacto en TI y llevando a cabo las medidas apropiadas para cumplir con ellos.

Para ello se evalúan las siguientes consideraciones:

- Leyes, regulaciones y contratos.
- Monitoreo de evoluciones legales, y regulatorios
- Revisiones regulares en cuanto a cambios.
- Búsqueda de asistencia legal y modificaciones
- Seguridad y ergonomía
- Privacidad
- Propiedad intelectual
- Flujo de datos

P9 Desarrollo y mantenimiento de procedimientos relacionados con tecnología de información

El objetivo de control asegura el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas, a través de un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones de usuarios, requerimientos de servicio y material de entrenamiento.

Evaluando para dicho objetivo de control lo siguiente:

- Procedimientos y controles de usuarios
- Procedimientos y controles operacionales
- Materiales de entrenamiento.

3.2.5 Consultas y vistas

Los objetivos de control asociados a la evaluación de manejo de consultas y vistas de las bases administradas a un DBMS se encuentran representados por:

PO2 Definición de la arquitectura de la información

Organiza de mejor manera las bases dentro del DBMS. La creación y mantenimiento de un de un modelo relacional de negocios, asegurando que se definan sistemas apropiados para optimizar la utilización de esta información.

Al evaluar la definición de la arquitectura se considera lo siguiente:

- Documentación
- Diccionario de datos
- Reglas de sintaxis de datos
- Propiedad de información

P011 Administración de la calidad

Satisfacción de los requerimientos del cliente por medio de uso de identificadores principales a las relaciones definidas en el modelo relacional, normalizando las mismas a la primera forma normal.

DS3 Administrar desempeño y calidad

El objetivo de control asociado pretende asegurar que la calidad adecuada este disponible y que se este haciendo el mejor uso de ella para alcanzar el desempeño deseado, a través de controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos.

Evaluando los siguientes aspectos asociados a dicho objetivo de control a tomar en consideración:

- Requerimientos de disponibilidad y desempeño
- Monitoreo y reporte
- Herramientas de modelado
- Administración de capacidad
- Disponibilidad de recursos

DS4 Asegurar continuidad de servicio

El objetivo de control satisface el mantener la continuidad del servicio y su disponibilidad de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, esto se logra teniendo un plan de continuidad probado y funcional, que este alineado con el plan de continuidad del negocio y relacionado con los requerimientos del negocio.

Tomando en consideración para realizar todo esto:

- Clasificación de la severidad
- Plan Documentado
- Procedimientos alternativos
- Respaldo y recuperación
- Pruebas y entrenamiento sistemáticos y regulares

DS11 Administrar la información

El objetivo de control pretende asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento, haciéndolo posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI, tomando en consideración:

- Diseño de formatos
- Controles de documentos fuente
- Controles de entrada

- Controles de procesamiento
- Controles de salida
- Identificación, movimiento y administración de la librería de
- medios.
- Administración, almacenamiento y respaldo de medios.
- Autentificación e integridad.

3.2.6 Perfiles de usuario y acceso a los objetos del DBMS

Los objetivos de control asociados al control de usuarios y los objetos de las bases de datos administradas a un DBMS se encuentran representados por:

DS05 Garantizar la seguridad del sistema

Salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, esto se hace posible a través de controles de acceso lógico que aseguran que el acceso a sistemas y programas este restringido a usuarios autorizados.

Al evaluar la seguridad del DBMS se toma en consideración lo siguiente:

- Autorización de acceso.
- Autentificación de acceso
- Acceso
- Perfiles de usuario
- Manejo de reportes y seguimiento de Incidentes(Logs)

P07 Administración de recursos humanos

El objetivo de control satisface el maximizar las contribuciones del personal a los procesos de TI, a través de técnicas sólidas para administración de personal.

Tomando en consideración los aspectos a controlar:

- Reclutamiento y promoción
- Procedimientos de acreditación
- Evaluación objetiva y medible del desempeño

3.2.7 Criptografía de datos

Los objetivos de control asociados al manejo de la criptografía en las bases de datos administradas a un DBMS se encuentran representados por:

PO2 Definición de la arquitectura de la información

Organiza de mejor manera las bases dentro del DBMS. La creación y mantenimiento de un de un modelo relacional de negocios, asegurando que se definan sistemas apropiados para optimizar la utilización de esta información.

Al evaluar la definición de la arquitectura se considera lo siguiente:

- Documentación
- Reglas de sintaxis de datos
- Propiedad de información

P11 Administración de la calidad

Satisfacción de los requerimientos del cliente por medio de uso de identificadores principales a las relaciones definidas en el modelo relacional, normalizando las mismas a la primera forma normal.

DS05 Garantizar la seguridad del sistema

Salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, esto se hace posible a través de controles de acceso lógico que aseguran que el acceso a sistemas y programas este restringido a usuarios autorizados.

Al evaluar la seguridad del DBMS se toma en consideración lo siguiente:

- Autorización de acceso.
- Autentificación de acceso
- Acceso
- Perfiles de usuario
- Manejo de reportes y seguimiento de Incidentes(Logs)

DS11 Administrar la información

El objetivo de control pretende asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento, haciéndolo posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI, tomando en consideración:

- Diseño de formatos
- Controles de documentos fuente
- Controles de entrada
- Controles de procesamiento
- Controles de salida
- Autentificación e integridad.

3.2.8 Disparadores o triggers

Los objetivos de control asociados al manejo de los disparadores o triggers en las bases de datos administradas a un DBMS se encuentran representados por:

A16 Administración del cambio

Objetivo de control asociado a minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, por medio de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual.

El objetivo de control toma en consideración:

- Identificación de los cambios
- Procedimientos de categorización, priorización y emergencia.
- Evaluación de impacto
- Autorización de cambios
- Manejo de liberación
- Distribución de software

DS13 Administración de operaciones

Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Logrando dichos objetivos por medio de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades.

El objetivo de control evalúa:

- Manuales de procedimientos de operaciones
- Documentación de procedimientos
- Registro de eventos

M1 Monitoreo de proceso

El objetivo de control asegura el logro de los objetivos establecidos para los procesos de TI. El monitoreo de los procesos se hace por definición por parte de la gerencia de reportes e indicadores de desempeño gerenciales, la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Tomando en consideración los siguientes aspectos:

- Indicadores clave de desempeño
- Factores críticos de éxito
- Evaluación de satisfacción de clientes

3.2.9 Backups

Los objetivos de control asociados al manejo de los backups en las bases de datos administradas por el DBMS se encuentran representados por:

P1 Definición de un plan estratégico de tecnología de información

El objetivo de control permite aprovechar un balance óptimo entre las oportunidades de tecnología de información en el DBMS necesario y los requerimientos de TI de negocio, así como para asegurar sus logros futuros, haciéndolo posible a través de un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo.

Los planes a largo plazo deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo. Tomando en consideración lo siguiente:

- Definición de objetivos del negocio y necesidades de TI
- Inventario de soluciones tecnológicas e infraestructura actual.
- Servicios de vigilancia tecnológica.
- Estudios de factibilidad oportunos
- Evaluación de sistemas existentes.

A12 Adquirir y mantener software de la aplicación

El objetivo asociado proporciona funciones automatizadas que soporten efectivamente al negocio, haciéndolo posible a través de la definición de declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros evaluando lo siguiente:

- Requerimientos de usuario
- Requerimientos de archivo de entrada, proceso y salida
- Interfase usuario-máquina
- Personalización de paquetes
- Pruebas funcionales
- Controles de aplicación y requerimientos funcionales
- Documentación

A13 Adquirir y mantener la arquitectura tecnológica

Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios. La evaluación del desempeño de hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema considerando:

- Evaluación de la tecnología
- Mantenimiento preventivo de hardware
- Seguridad de software del sistema, instalación, mantenimiento y control de cambios.

DS10 Administrar problemas e incidentes

Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia, ejecutándolo por medio de un sistema de manejo de problemas que registre y de seguimiento a todos los incidentes considerando:

- Suficientes pistas de auditoría de problemas y soluciones
- Resolución oportuna de problemas reportados.
- Procedimientos de escalamiento
- Reportes de Incidentes

DS11 Administrar la información

El objetivo de control pretende asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento, haciéndolo posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI, tomando en consideración:

- Controles de documentos fuente
- Controles de entrada
- Controles de procesamiento
- Controles de salida
- Administración de almacenamiento y respaldo de medios.
- Autentificación e integridad.

DS13 Administrar la operación

El objetivo de control asegura que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada, por medio de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Evaluando los siguientes aspectos:

- Manual de procedimientos de operaciones
- Documentación de procedimientos de arranque
- Calendarización de personal y cargas de trabajo
- Registro de eventos del DBMS

3.3 Modelo de madurez de COBIT para un DBMS

El modelo de madurez de COBIT ofrece las bases para el entendimiento y la evaluación de las condiciones actuales de seguridad de un DBMS y control de los procesos del ambiente de TI de una organización que están vinculados con el DBMS.

Este modelo provee las bases para la evaluación de las principales funciones del área de TI en cuanto a recursos de información se refiere sobre un DBMS, a través de la consideración de cada uno de sus procesos clave, a los cuales se les asigna un valor de cero (0) a cinco (5), indicando así el nivel de esfuerzo (“madurez”) que se sugiere invertir en la actividad de control de dicho recurso, de forma de garantizar una buena relación costo beneficio al asegurar el nivel de seguridad estrictamente requerido.

El modelo de madurez representa entonces, “a dónde la organización desea llegar”, mientras que el resultado de la evaluación (aplicando el marco COBIT) representa “dónde la organización está”. Las posibles brechas detectadas entre ambas situaciones serán los disparadores del plan de acción para implementar las soluciones que se requiera para mejorar la estructura de control interno en el grado deseado.

De lo anterior se deduce que es tan importante fijar adecuadamente “hasta dónde se desea llegar” (grado de madurez), cómo seleccionar los objetivos de control que permitirán realizar la evaluación. Este es un aspecto clave para poder proseguir con una implantación de COBIT exitosa alineada a las necesidades de la organización.

3.3.1 Nivel de madurez inexistente

Refiere a la ausencia total de cualquier proceso o control reconocible. La organización no ha reconocido la necesidad del proceso o control.

3.3.2 Nivel de madurez inicial

Existe evidencia de que la organización ha reconocido la necesidad de mejorar los procesos o controles. No existen procesos estandarizados, pero se realizan procedimientos “ad-hoc” que tienden a aplicarse en casos individuales. La forma en que la gerencia enfrenta estos temas no se encuentra organizada.

3.3.3 Nivel de madurez repetible

Se han desarrollado procesos donde se siguen procedimientos similares por diferentes personas para la misma tarea. No se ha formalizado la capacitación o la comunicación de los procedimientos en forma estándar, ni la responsabilidad es de cada individuo. Hay un alto grado de confianza en el conocimiento individual, por lo que los errores son más frecuentes.

3.3.4 Nivel de madurez definido

Los procedimientos han sido estandarizados y documentados y son comunicados a través de la capacitación. Sin embargo, se deja a los individuos el seguimiento de los procesos, por lo que resulta poco probable que se detecten desviaciones. Los procedimientos no son sofisticados pero existe formalización de las prácticas existentes.

3.3.5 Nivel de madurez gestionado o administrado

Es posible monitorear y medir el cumplimiento de los procedimientos y tomar acciones cuando los procesos no están funcionando efectivamente. Los procesos se encuentran constantemente bajo mejora y proveen buenas prácticas. Se utilizan automatización y herramientas de una forma limitada o fragmentada.

3.3.6 Nivel de madurez optimizado

Los procesos han sido redefinidos al nivel de las mejores prácticas, basados en los resultados de mejoras continuas y el modelo de madurez con otras organizaciones.

TI se utiliza de una forma integrada para automatizar el workflow, proveyendo herramientas para mejorar la calidad y la efectividad, con una rápida adaptación.

Mejorando el nivel de madurez de los controles asociados a cada uno de los procesos de TI, según las necesidades reales de éstos, la organización logrará mejorar el nivel de control interno del DBMS.

En el modelo de madurez se obtendrán, al menos, un incremento de la eficiencia operativa y la formalización de los procesos en el DBMS.

Trabajando en base al modelo de madurez deseado, se seleccionarán los objetivos de control que deberán aplicarse a los efectos de evaluar la situación actual de cada uno de los procesos de TI de la organización. De esta manera se obtendrá el grado de cumplimiento de cada proceso tomando como marco de referencia los estándares provistos por COBIT, pero guiados por los requerimientos reales de la organización.

Existen otros aspectos que conforman el modelo de madurez COBIT aplicados al DBMS, que se definen a continuación:

Factores críticos de éxito (SCF) Definen los asuntos más importantes o las acciones que debe llevar adelante la gerencia para alcanzar el control sobre los procesos de TI en el DBMS. Deben ser lineamientos de implementación orientados a la administración y que identifiquen las principales acciones a realizar, desde el punto de vista estratégico, técnico, organizacional y procedimental.

Indicadores clave de resultados (KGI) Definen métricas que le indican a la gerencia después de ocurrido si un proceso de TI ha alcanzado sus requerimientos de negocio implementados al DBMS, usualmente expresados en términos de los criterios de información de COBIT:

- Disponibilidad de la información necesaria para soportar los requerimientos del negocio
- Ausencia de riesgos de integridad y confidencialidad
- Eficiencia en los costos de procesos y operaciones
- Confirmación de confianza, efectividad y cumplimiento

Indicadores clave de desempeño (KPI) Define métricas para determinar cuan bien se desempeña el proceso de TI para alcanzar la meta. Son los indicadores principales para saber si es probable o no que se alcance una meta y son buenos indicadores de capacidades, prácticas y habilidades sobre el DBMS.

3.4 Impacto de la aplicación COBIT en el DBMS

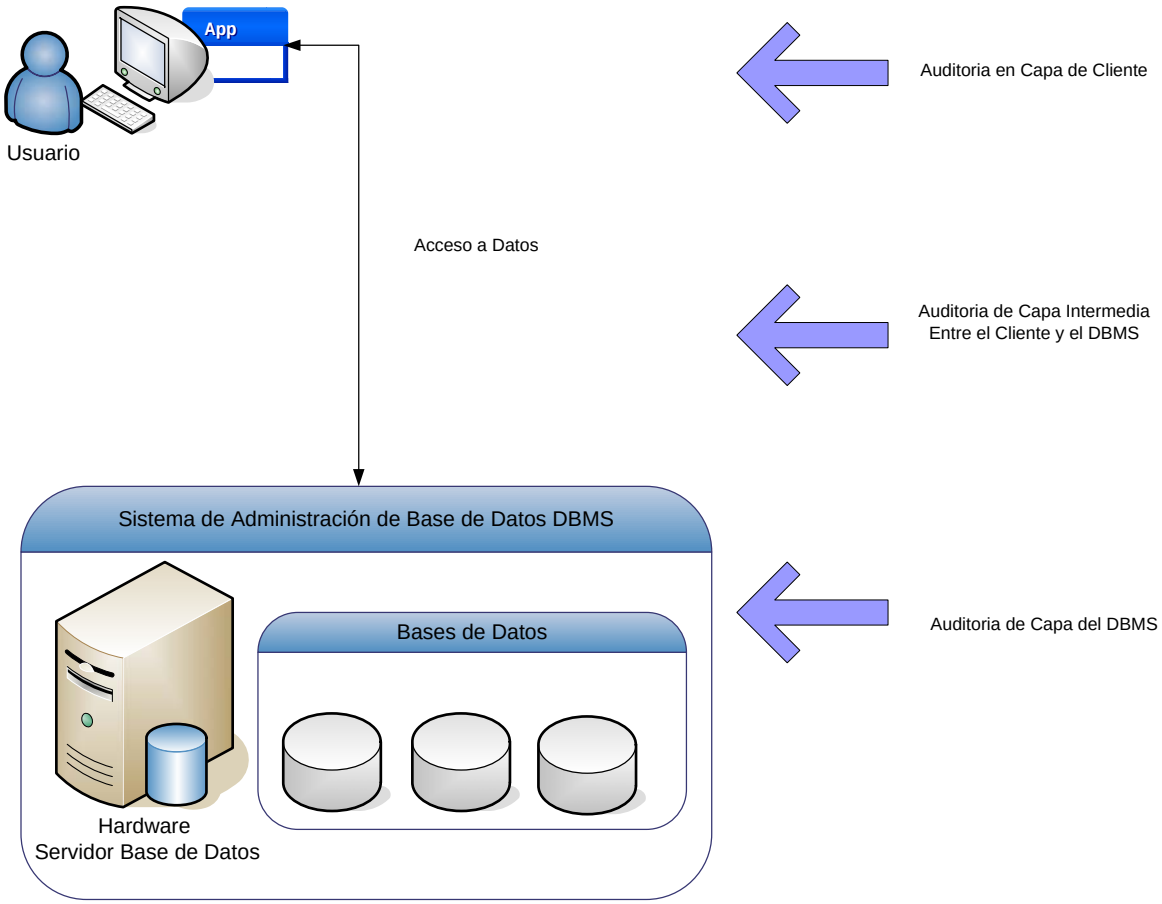
Eventualmente, una organización puede tener formalizados algunos procedimientos, aplicando distintos marcos de referencia, ya que no todos desarrollan con igual nivel de detalles todos los aspectos vinculados al control de los recursos informáticos.

En particular COBIT es una herramienta que permite evaluar la calidad del soporte de TI actual de la organización y en los sistemas asociados a esta, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan en especial a los sistemas de administración de base de datos, y los requerimientos sobre la información de los primeros.

Establecido el diagnóstico permite definir las metas desde el punto de vista de seguridad y control que le serán de utilidad alcanzar a la organización para cada uno de sus procesos, pudiendo entonces establecer un plan de acción para lograr estas mejoras, y posteriormente identificar los lineamientos para sustentar un proceso de monitoreo y mejora continua sobre las soluciones implementadas. El aplicar COBIT sobre el auditaje de los sistemas de administración de base de datos DBMS impacta a graves de 3 capas de arquitectura de la siguiente manera:

1. Auditaje de la capa del cliente
2. Auditaje de capa intermedia entre el cliente y el DBMS
3. Auditaje de la capa del DBMS

Figura 12 Desarrollo del auditaje de un DBMS



- **Auditaje en la capa del cliente**

  - Disponibilidad de seguimiento de la actividad del usuario
  - Adaptación de herramientas a todo acceso a datos.
  - Imposibilidad de estar el 100% seguro
  - Implementación de herramientas 100% autorizadas.

- **Auditaje de capa intermedia entre el cliente y el DBMS**

    - Puesta en protección continua de datos del DBMS
    - Funcionalidad de auditaje limitada
    - Inconsistencia entre los tipos de DBMS del mercado
    - Penalidad en el performance del DBMS

- **Auditaje de capa del DBMS**

    - Monitoreo entre las conversaciones cliente-DBMS
    - La tecnología difiere entre los diferentes tipos de DBMS para un control eficiente.
    - Existencia de diferentes tipos de monitoreos cliente-DBMS
    - Implementaciones de control del tipo de:
    - Alcance
    - Calidad
    - Usabilidad de los resultados
    - Performance

3.4.1 Monitoreo de procesos del DBMS

El monitoreo de los procesos del DBMS incluyen los siguientes aspectos:

- El acceso de los archivos de datos deberá ser restringido en una vista de datos lógica, a nivel de tipo de campo. La seguridad en el campo será dada de acuerdo al contenido del campo.

- Control de acceso al acceso del diccionario de datos.

- Control de acceso al DBMS.

- La bitácora de auditoría debe reportar los accesos al diccionario de datos y a las bases de datos.

- Las modificaciones de capacidades desde el DBMS para las bases de datos deberán limitarse al personal apropiado.

3.4.2 Adecuación del control interno con el DBMS

Cuando se realizar una revisión de la seguridad lógica del control interno, se debe evaluar y probar los siguientes controles para minimizar los riesgos:

- Control de acceso a los programas y a la información.
- Control de cambios.
- Bitácoras de auditoría.

La evaluación de todos los tipos de software deberá asegurar que los siguientes objetivos sean cumplidos:

- El acceso a funciones, datos y programas asociados con el software debe estar restringido a individuos autorizados y debe ser consistente con documentos esperados.

- Todos los cambios del software deben ser realizados de acuerdo con el manejo del plan de trabajo y con la autorización del usuario.

- Se debe de mantener una bitácora de auditoría de todas las actividades significativas.

Una auditoría de seguridad lógica puede ser realizada de diferentes formas. La auditoría puede enfocarse en áreas de seguridad que son aplicables a todo tipo de software y pueden cubrir la instalación, el mantenimiento y la utilización de software.

También debe tomarse en cuenta las características de seguridad del software, incluyendo el control de acceso, la identificación del usuario y el proceso de autentificación del usuario, ejecutado por el software.

3.4.3 Disposición de auditoría interna del DBMS

El software de auditoría especializado puede ser usado para revisar todos los cambios y asegurarse que son ejecutados de acuerdo con los procedimientos probados por la gerencia evaluando los siguientes aspectos:

I. Control de acceso

Entre las consideraciones de auditoría para el control de acceso están:

- Diseño y administración.
- Procedimientos de identificación de usuario.
- Procedimientos de autentificación de usuario.
- Recursos para controlar el acceso.
- Reportes de vigilancia del software de control de acceso reportando y vigilando.

II. Diseño y administración de los datos

Al auditar el diseño y administración del DBMS debe ser revisado los siguientes elementos:

- Localización de archivos de seguridad y tablas para asegurar que los archivos del software de control de acceso estén protegidos.

- Uso de recursos o controles de acceso a nivel de usuario para asegurar que el software de control de acceso protege datos y recursos en un nivel correcto.

- Limitaciones de acceso para los archivos de seguridad que contienen descripciones y passwords.

- Limitaciones de acceso a archivos de seguridad a través de la administración de comandos de seguridad en línea o utilerías.

- La jerarquía de seguridad

- Los usuarios encargados de la administración de la seguridad.

- Métodos y limitaciones sobre los archivos de seguridad o modificación de tablas.

- Definición de parámetros de seguridad.

III. Procedimientos de identificación de usuario

Las siguientes situaciones proveen un beneficio que impacta en el DBMS por un apropiado nivel de dirección de la siguiente manera:

- Las identificaciones del usuario para verificar que sean individuales y no compartidas.
- Probar la reovación de los usuarios inactivos
- El despliegue de la ultima fecha y hora en algún ID especifico que fue usado.
- Revocación de identificaciones del usuario siguiendo un número específico inválido.
- El uso de comienzo y fin de fechas para id de usuario de empleados contratados.
- El uso de grupos de usuario para el recurso de acceso a los archivos.
- Propietarios de datos y recursos para asegurar que ellos son los responsables apropiados.

IV. Procedimientos de autentificación del usuario

Los beneficios de evaluar los procedimientos de autentificación del usuario al DBMS se enlistan de la siguiente manera:

- Evaluación del uso de passwords o información personal durante la sesión.

- Deberá ser identificada la disponibilidad de automatizar funciones una vez identificado el usuario así como la autentificación de procedimientos.

- Los procedimientos para el uso de passwords para asegurarse que este esta protegido cuando es usado por el usuario.

- La mascara del password para asegurarse que el área de los caracteres no se desplieguen.

- Mantenimiento de la historia del password.

- Procedimientos para suplir identificaciones de usuarios y password por procesos batch.

V. Recursos para controlar el acceso

Los beneficios de evaluar los recursos que controlan el acceso al DBMS se enlistan de la siguiente manera:

- Posibles niveles de acceso
- Niveles de acceso por default, particularmente para usuarios o jobs que no tienen un ID de usuario.
- El acceso del usuario a archivos de seguridad.
- Que la seguridad sea implantada en el nivel correcto.
- Procedimientos para asegurar la protección automática.
- Procedimiento para la protección de recursos.
- Uso de rutas rápidas o funciones aceleradas a través de controles.
- Controles de acceso sobre aplicaciones locales o remotas.
- Restricciones de acceso sobre recursos críticos del sistema.

VI. Reportes de vigilancia del DBMS

Los beneficios de evaluar los reportes de vigilancia del DBMS se enlistan de la siguiente manera:

- Login, identificación de acceso autorizado al sistema y el uso de los recursos.
- Las identificaciones de acceso no autorizado
- La identificación de archivos de seguridad, mantenimiento a tabla y el uso de comandos sensibles.
- El login de usuarios privilegiados y sus actividades
- Las restricciones de acceso a archivos de log del sistema.
- Sistema operativo o software de control de acceso existente.
- Las violaciones a la seguridad.
- Los archivos de seguridad y la generación de reportes de las actividades de usuario para asegurar que los propietarios de datos y recursos son notificados de los eventos de seguridad en un periodo determinado.

CONCLUSIONES

1. COBIT brinda como ventaja un marco de referencia que permite la evaluación de los objetivos de control asociados a los recursos evaluados en un DBMS.

2. El modelo de madurez COBIT, es clave para la administración TI, de los recursos de la organización, evaluando el control interno actual de la organización y la proposición de objetivos de control asociados que ayuden a los procesos TI de la organización.

3. Los procedimientos asociados a la auditoría de un DBMS relacional conllevan la evaluación del control existente, la ejecución de pruebas sobre los recursos TI del DBMS y el análisis de las debilidades sobre el mismo.

4. El beneficio directo que proporciona la aplicación de los objetivos de control sobre el auditaje del DBMS obedece a la disposición de los recursos de TI auditados bajo objetivos claves que responden a aspectos claves de funcionamiento y administración TI de la organización.

5. Los procesos de almacenamiento, respaldo, registro de procedimientos, administración de personal y registro de información de las operaciones del DBMS constituyen la evaluación primordial de la aplicación de los objetivos de control en el auditaje del DBMS.

RECOMENDACIONES

1. Evaluar la necesidad de formación de equipo de evaluación y control constante de los procedimientos de que involucran la administración del servidor de base de datos y las capas externas con las cual interactúa el mismo.

2. Implementar la generación y presentación de reportes mensuales sobre la actividad que se produce en materia de información a la alta gerencia para la evaluación de controles sobre los procesos y recursos TI asociados a los objetivos clave de la organización.

3. Adquisición e implementación de software que monitoree los procesos del DBMS relacional y audite los archivos transaccionales del mismo, así como herramientas de firewall actualizables que respondan a ataques directos al DBMS relacional.

4. Considerar las directrices planteadas por la auditoría y, desarrollar un conjunto de herramientas como los formularios de control basados en COBIT, para evaluar el desarrollo y utilización de los recursos y procesos TI de la organización.

5. Registrar y controlar los procesos TI de la organización, para fomentar el desarrollo de una cultura organizacional dispuesta a un control interno efectivo bajo indicadores clave de control.

BIBLIOGRAFÍA

1. Alonzo Rivas, Gonzalo. **Auditoría Informática**. 2ª ed. España. Ediciones Díaz de Santos S.A. 1988. 185pp.

2. Alta Dirección. **La Auditoría en la era de la informática**. España. Ediciones Nauta. S.A. 1982. 163pp.

3. CASIC. **Curso de Auditoría de Sistemas de Información Computarizada**. Guatemala. Centro de adiestramiento de personal. 1981. 115pp.

4. Piattini, Mario Gerardo y Emilio del Peso Navarro. **Auditoría Informática**: un enfoque práctico. 3ª ed. España. Editorial Alfa– Omega. 1998. 605pp.

5. Robert Murdick y Jhon Munson. **Sistemas de Información Administrativa**. 2ª ed. México. Editorial Prentice-Hall S.A. 1988 722pp.

6. Carlos Muñoz Razo. **Auditoría en Sistemas Computacionales.** 2ª ed. México. Editorial Pearson S.A. 2002 796pp.

7. **Auditoría de sistema de bases de datos.** http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capiulo4.html Agosto de 2005.

8. **Mejores prácticas y objetivos de control para la información y la tecnología.** http://www.pc-news.com/detalle.asp?sid=&id=10&Ida=2016 Agosto de 2005.

9. **Trabajo de auditoría: normas cobit.**
http://www.monografias.com/trabajos14/auditoríasistemas/auditoríasistemas.shtml
Agosto de 2005.

10. **Auditoría de sistemas de bases de datos.**
http://www.auditoríasistemas.com
Agosto de 2005.

11. **Conceptos de auditorias de sistemas.**
http://www.monografias.com/trabajos14/auditoría/auditoría.shtml
Agosto de 2005.

12. **Arquitectura de los sistemas de bases de datos.**
http://alarcos.inf-r.uclm.es/doc/bda/doc/trab/T9900_Ogonzalez.pdf
Agosto de 2005.

13. **Auditaje de datawarehousing.**
http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo5.html
Agosto de 2005.

14. **Seguridad y normalización de los sistemas de información.**
http://www.aicpa.org/assurance/systrust/index.htm
Agosto de 2005.

15. **Metodologías de auditorias de sistemas.**
http://www.inei.gob.pe/web/metodologias/attach/lib605/DOC4-4.htm
Agosto de 2005.

16. **Manual de auditaje de sistemas de información.**
http://www.ilustrados.com/publicaciones/AuditajeInformatico.php
Agosto de 2005.

17. **Auditoría y control de sistemas e informática.**
www.moyasevich.cjb.net
Agosto de 2005.

18. Information systems audit and control foundation
www.isaca.org
Agosto de 2005.