

**REPUBLICA BOLIVARIANA DE VENEZUELA  
UNIVERSIDAD CATÓLICA ANDRÉS BELLO  
VICERRECTORADO ACADÉMICO  
DIRECCION GENERAL DE ESTUDIOS DE POSTGRADO  
POSTGRADO EN SISTEMAS DE INFORMACION**

**MODELO DE AUDITORÍA Y CONTROL  
DE INFORMACION Y TECNOLOGIAS RELACIONADAS  
CASO: BANCO SOFITASA**

**Proyecto de Trabajo Especial de Grado para optar al Título de  
Especialista en Sistemas de Información**

**Autor: Elixender Lamprea L.**

**Tutor: Jaime A. Vélez Laguado**

**San Cristóbal, Julio de 2004**

**REPUBLICA BOLIVARIANA DE VENEZUELA  
UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

**MODELO DE AUDITORÍA Y CONTROL  
DE INFORMACION Y TECNOLOGIAS RELACIONADAS**

**Autor: Elixender Lamprea L.**

**San Cristóbal, Julio de 2004**

## **APROBACIÓN DEL TUTOR**

En mi carácter de Tutor del Trabajo Especial de Grado, presentado por el ciudadano Elixender Lamprea León, para optar al grado de Especialista en Sistemas de Información, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En la ciudad de San Cristóbal, a los quince días del mes de Septiembre de dos mil cuatro.

---

Jaime A. Vélez Laguado

C.I.: V-11.499.462

A

**Alicia y Manuel,**

Desde algún lugar de la eternidad me guían y esperan...

**Rubiela y José del Carmén,**

Creadores de mi vida;

**Gloria Cecilia,**

Mi fiel esposa y compañera;

**Sergio David, Jean Ibrahim, Gloria Elixandra,**

Mis hijos, motores de cada día nuevo;

Todos los que amo...

Elixender.

## ÍNDICE DE CONTENIDO

	pp.
LISTA DE CUADROS	vii
LISTA DE GRAFICOS	viii
RESUMEN	ix
INTRODUCCION	10
CAPITULO	
I EL PROBLEMA	12
Contexto o Marco Referencial	12
Planteamiento del Problema	13
Objetivos	17
Importancia del Estudio	17
II MARCO TEÓRICO	20
Antecedentes	20
Bases Teóricas	28
Modelo	29
Metodología	29
Auditoría	30
Clases de Auditoría	32
Informática	33
Dato e Información	34
COBIT	35
Requerimientos de Información	37
Recursos de TI	38
Procesos de TI	39
Dominios de TI	40
Gobierno de TI	59
Control	59
Objetivos de Control	60
Estructura COBIT	63

Guías de Auditoría	65
Definición de Términos	66
III MARCO METODOLÓGICO	69
Tipo de Investigación	69
Diseño de la Investigación	69
Población	70
Muestra	71
Técnicas e Instrumentos de recolección de datos	71
Análisis e Interpretación de resultados	73
IV PROPUESTA	83
CONCLUSIONES	125
RECOMENDACIONES	127
REFERENCIAS	128
ANEXOS	130
A Instrumento de Recolección de datos 1	
B Instrumento de Recolección de datos 2	
C Instrumento de Recolección de datos 3	
D Resumen de Objetivos de Control COBIT	
E Currículum Vitae	

## LISTA DE CUADROS

<b>CUADRO</b>		pp
1	Elementos fundamentales del concepto de auditoría	32
2	Clases de auditoría	33
3	Valoración de relevancia de los procesos de TI	77
4	Valoración del desempeño de los procesos de TI	77
5	Evaluación del Gobierno de los Procesos de TI por Dominio	78
6	Unidades Ejecutoras de Procesos de TI	79
7	Estado de los Procesos de TI respecto a Auditoría y Formalización	80
8	Unidades responsables del Gobierno de TI	81
9	Riesgos asociados a los Procesos PO1 y DS6 por Grupo de Riesgos	82

## LISTA DE GRAFICOS

<b>GRAFICO</b>		<b>PP</b>
1	Relación de los principios básicos de cobit	36
2	Información, recursos de ti y procesos del negocio	39
3	Relación de dominios, procesos y actividades cobit	40
4	Navegación en cascada de objetivos de control	61
5	Relación de Procesos (Objetivos de Control de Alto Nivel), Criterios de Información y Recursos de TI.	62
6	Cubo COBIT Dimensiones Conceptuales de COBIT	63
7	Procesos de TI definidos dentro de los cuatro dominios y su relación con los criterios de información y los recursos de TI	64
8	Escala de evaluación del desempeño de procesos de TI	87
9	Escala de valoración de Relevancia de los procesos y objetivos de TI	87
10	Escala de evaluación de los Objetivos de Control específicos de los procesos de TI	89
11	DFD contextual (Nivel 0) del Modelo Metodológico de Evaluación y Auditoría de TI	91
12	DFD (Nivel 1) del Modelo Metodológico de Evaluación y Auditoría de TI	92
13	Implantación del diseño físico de la base de datos del modelo	95
14	Diseño relacional de la base de datos del modelo	99
15	Formatos de Entrada / Salida	101

**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**  
**VICERRECTORADO ACADÉMICO**  
**DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO**  
**ESPECIALIZACIÓN EN SISTEMAS DE INFORMACIÓN**

**Modelo de Auditoría y Control de Información y Tecnologías Relacionadas**  
**Caso: Banco Sofitasa**

Trabajo especial de grado, presentado para optar al título de Especialista  
en Sistemas de Información

Autor: Elixender Lamprea L.  
Tutor: Jaime A. Vélez Lagüado  
Año: 2004

**RESUMEN**

El aumento significativo y relevante que el uso de la información tiene para las organizaciones actuales determina que todos los procesos relativos a la producción, administración y gerencia de Tecnologías de Información (TI) deben ser óptimamente controlados para asegurar la calidad de la información, soporte del cumplimiento de los objetivos del negocio. Los procesos de información requieren la aplicación de técnicas y medidas de control que garanticen la reducción de vulnerabilidad a amenazas generadoras de riesgo que pongan en peligro la estabilidad del sistema organizacional y del sistema del negocio. El presente trabajo desarrolla un estudio del problema de control y seguridad de la información y las tecnologías relacionadas, fundamentándose teóricamente en la investigación Cobit (Control Objectives for Information Technology), que resume estos requerimientos siguiendo las mejores prácticas de aceptación internacional en materia de gobierno de las TI. El estudio diagnostica el problema en el Banco Sofitasa, una organización que fundamenta sus procesos de negocio en los procesos de información y TI, con una alta infraestructura tecnológica, determinándose la factibilidad de aplicación del Modelo Metodológico de Auditoría de Información y Tecnologías Relacionadas, propuesto como proyecto factible por la presente investigación. El modelo propuesto, fundamentado en el Marco Referencial COBIT, intenta principalmente la promoción de la cultura de control y seguridad de TI en las organizaciones, suministrando una sencilla, práctica y sistémica manera de evaluar los procesos de TI, permitiendo determinar índices de evaluación de procesos, objetivos de control, riesgos asociados y aplicar guías y procedimientos de auditoría para facilitar la emisión de los informes de opinión.

## INTRODUCCION

Las organizaciones actuales requieren mantenerse activas y efectivas en la competencia global; las presiones del entorno, producto del avance tecnológico, las estrategias competitivas, las exigencias de los clientes y todas las variables endógenas y exógenas, determinan un singular juego de oportunidades y amenazas que deben ser oportunamente valoradas. En todo esto, la información y las tecnologías relacionadas que la soportan, producto de las operaciones del negocio, poseen un singular y alto grado de importancia y relevancia como activos de gran valor para la organización y la empresa. Esa información y los procesos de Tecnología de la Información que la planifican y organizan, la generan y administran, y la gerencian y evalúan, deben ser controlados a través de la implantación de técnicas de control efectivas, en procura del cumplimiento de objetivos de control que garanticen la calidad y satisfacción de los procesos alineados con los objetivos del negocio.

La complejidad creciente de las plataformas informáticas, múltiples sistemas de hardware y software, redes globales de comunicación de datos, comercio y negocio electrónico, capacidad de delinquir de los usuarios, generan nuevas amenazas de riesgo para los sistemas de información del negocio. Por todo esto, es necesario, como parte de los planes en materia de gobierno de TI, establecer en las organizaciones una estructura de relaciones y procesos dirigida a controlar la información para alcanzar los objetivos del negocio, adicionando valor mientras se mantiene un balance equilibrado de los riesgos sobre la Tecnología de Información y sus procesos.

La presente investigación plantea en el Capítulo I, un estudio del problema de control y seguridad de la información y las tecnologías relacionadas; en el Capítulo II

se presenta un estudio documental de antecedentes de investigación en esta línea y bases teóricas, resaltando el papel fundamental de la investigación adelantada desde el año 1996 por la ISACF (Información System Audit and Control Foundation) y el IT Governance Institute que ha producido el proyecto COBIT, resumiendo las mejores prácticas de aceptación universal para el tratamiento del problema de control de TI. En el Capítulo III se presenta el Marco Metodológico de la presente investigación, aplicada como caso de estudio real, al Banco Sofitasa, una organización bancaria de reconocida trayectoria y estructura organizacional, que por la complejidad y madurez de sus proyectos informáticos, gobernados desde la Vicepresidencia de Tecnología y en coordinación con la Gerencia de Auditoría de Sistemas permitió la aplicación de los instrumentos para la presente investigación y la realización del diagnóstico situacional referido al problema en estudio.

Finalmente, en el Capítulo IV, se presenta la propuesta factible de desarrollo del *Modelo Metodológico de Auditoría de Información y Tecnologías Relacionadas* que fundamentado en el proyecto COBIT, propone la aplicación de una serie de métodos y técnicas a través de varias fases, para el tratamiento del problema de evaluación y auditoría, facilitando la comprensión y promoción de la estructura COBIT como modelo práctico a seguir. Se incluye, el diseño lógico y físico del prototipo estructural de software que permite visualizar el enfoque metodológico para el desarrollo de una aplicación orientada al uso de los usuarios finales en las áreas gobierno y auditoría de TI.

## CAPITULO I

### EL PROBLEMA

#### Contexto o Marco Referencial

Para resaltar la relevancia y significado que los procesos de información y las tecnologías relacionadas tienen para las organizaciones actuales en procura del logro de los objetivos del negocio, resulta muy apropiada la mención de O'Brien (1998) a este aspecto: "La tecnología de la información se ha convertido en una necesidad estratégica, crea en ella, actúe con base en ella o conviértase en un acontecimiento tangencial en la historia".

La revolución tecnológica aplicada a la gestión de la información ha crecido a pasos agigantados en los últimos años. Las organizaciones como sistemas abiertos que son, están relacionadas con su entorno; las empresas y organizaciones están sometidas a presiones e influencias de órdenes económicos, industriales y sociales en los que se encuentran inmersas; en consecuencia, si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adaptarse rápidamente a las nuevas circunstancias para sobrevivir. Como cita Rodríguez (1998) en la presentación de Piattini y Del Peso (1998) "Una de las tendencias actuales más significativas es la que nos ha dirigido desde una Sociedad Industrial hacia una llamada Sociedad de Información".

Los cambios suceden muy rápido respecto a los procesos de adaptación de las organizaciones; están afectando al mundo entero, y su comprensión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los *Sistemas de Información (SI)* y *Tecnologías de la Información y las Comunicaciones (TIC)*.

Aunque los avances tecnológicos han sido constantes y espectaculares, en los últimos veinte años se ha producido una verdadera revolución tecnológica de gran impacto para la propia industria informática, así como de consecuencias importantes para el resto de los sectores.

En consecuencia, cada vez, un mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes. De igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información sobre los procesos de datos e información y sobre la tecnología relacionada son indispensables.

En este sentido, la gerencia debe establecer un sistema de *Control Interno* adecuado que minimice los riesgos producidos por la aplicación de la tecnología informática. Tal sistema debe soportar debidamente los procesos del negocio a través de la garantía de seguridad de los sistemas de información. Por lo tanto, el nivel o estado de la seguridad de información y las tecnologías relacionadas en una organización, es un objetivo a evaluar de primer orden. El cumplimiento de este objetivo, es la función principal de la evaluación y el control informáticos.

### **Planteamiento del Problema**

El continuo y creciente desarrollo de sistemas de información basados en el uso de computadoras y otras tecnologías de procesos, gestión y comunicación de información, ha convertido al computador en una herramienta indispensable en las organizaciones, proporcionándole un control más efectivo sobre sus recursos y operaciones, como también en la ejecución propia de esas operaciones. Sin embargo, esos mismos sistemas tienen cada vez, un mayor número de personas preocupadas debido a que el control computarizado de los activos, el fácil acceso a la información y la creciente dependencia de la tecnología pueden convertir a las organizaciones en entes más vulnerables que nunca, cuestionándose en este sentido en qué medida están sus sistemas de información adecuadamente controlados contra los riesgos informáticos.

A pesar de los grandes adelantos tecnológicos y de su aplicación al procesamiento de datos y gestión de información en lo que se ha llamado Tecnologías de la Información y las Comunicaciones (TIC), la incorporación de este importante recurso a las operaciones y gestión de la información en la organizaciones ha generado una problemática particular que se ha hecho evidente en múltiples organizaciones alrededor del mundo. Como lo cita Rodríguez (1998) presidente de la Organización de Auditoría Informática, Capítulo español de ISACA, (Information Systems Audit And Control Association), en la presentación de Piattini y del Peso (1998),

*“...la situación actual de los sistemas de información en las organizaciones se caracteriza frecuentemente por una falta de asimilación de las nuevas tecnologías, por una infrautilización de los equipos informáticos, por un descontento generalizado de los usuarios, por una obsolescencia de las aplicaciones informáticas actuales, por una falta de planificación de los Sistemas de Información, y por soluciones planteadas parcialmente que, al no estar integradas, producen islotes de mecanización y de procesos manuales, en muchos casos redundantes e/o incoherentes, difíciles de controlar y caros de mantener. En definitiva, por una falta de estándares y metodologías, y por una falta de formación y cultura generalizada, sobre todo en los aspectos de control y de seguridad informática. La auditoría informática ha aportado soluciones, en el pasado, para estos problemas; pero se ha realizado frecuentemente, hasta ahora, solo en grandes empresas y, en la mayoría de los casos, como un complemento de la auditoría financiera...”*

Cada día, son mayores las inversiones en tecnologías de información y mayor la dependencia del negocio de las estructuras informáticas; los sistemas de control y seguridad de la información exigen mayor rigurosidad en áreas tan diversas como la planificación de proyectos, la organización de la unidad de informática, la dirección y gestión de los recursos informáticos, la administración y control de infraestructuras e instalaciones, el desarrollo y mantenimiento de aplicaciones, la explotación de los sistemas de información, las bases de datos, las comunicaciones y redes, la ofimática, la seguridad general y particular, los recursos humanos y la calidad.

La globalización ha impuesto nuevos retos de competencia, las organizaciones se deben reestructurar hacia operaciones cada vez más competitivas y, como

consecuencia deben aprovechar los avances de las tecnologías de los sistemas de información para mejorar su situación competitiva. Hoy en día se habla de reingeniería de negocios y de procesos, de calidad total, de procesos distribuidos, de organizaciones planas, de múltiples tipos de sistemas de información: MIS (Management Information System), EIS/DSS (Executive Information System)/Decision Support Systems), ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) y otros, como cambios que generan un impacto en la manera en que operan las organizaciones privadas y públicas. Estos cambios están teniendo y continuarán teniendo implicaciones profundas para la gestión y para las estructuras de control en todas las organizaciones.

Todo lo anterior deriva en qué la previsión, el control, la seguridad, y la reducción de costos, implicados en los sistemas de información mecanizados son una estrategia fundamental de las organizaciones actuales. La automatización de las funciones y procesos de la organización, por su propia naturaleza, genera una mayor dependencia de mecanismos de control en las computadoras y redes desde el punto de vista del hardware y del software. La aplicación de la informática al proceso del negocio crea o genera unos riesgos informáticos de los que hay que proteger y preservar a la organización con un conjunto de controles, y la calidad y eficacia de estos controles es el objetivo central a evaluar para poder identificar los puntos débiles y mejorarlos. Esta es una de las funciones de la Auditoría Informática.

Para estar a la altura de las circunstancias, es necesario que los usuarios se pongan al día en cuanto a la tecnología y entorno de la Auditoría Informática, y para acceder a este nuevo paradigma debe tratarse el problema de minimizar la complejidad de los procesos de evaluación y control de los entornos de aplicación de las tecnologías de la información. En tal sentido, un modelo de registro de planes, recursos, procesos, riesgos, controles y guías de evaluación y control de los sistemas de información y sus tecnologías, favorecerá y facilitará la función de Evaluación y Auditoría Informática en la Organización. En resumen, se plantean entonces los siguientes interrogantes:

¿Conocen los usuarios de Sistemas de Información basados en TI, los elementos involucrados en el control y seguridad de la información?

¿Existen registros de los planes en materia de aplicación de TI?

¿Las soluciones de información basadas en TI se adquieren e implementan en función de los objetivos del negocio?

¿Esta controlada la seguridad del servicio de información para la ejecución de las operaciones del negocio?

¿Existen mecanismos de registro y evaluación de los procesos basados en la aplicación de TI?

¿Como acceder de manera sistémica y sencilla al conocimiento y aplicación, por parte de los usuarios ejecutivos de negocios, profesionales de TI y auditores de sistemas de información, de una estructura que facilite la Auditoría de los procesos de Tecnología Informática en concordancia con los objetivos del negocio?

¿Como saber en que medida de control se encuentra la organización respecto a la planificación, desarrollo, uso y evaluación de la TI?

## **Objetivos**

### **Objetivo General**

Diseñar un modelo metodológico de evaluación y Auditoría aplicable a los procesos de información y tecnologías relacionadas.

### **Objetivos Específicos**

1. Diagnosticar la necesidad de Evaluación y Auditoría Informática en una organización.
2. Seleccionar el enfoque metodológico para desarrollar la propuesta de solución al problema de evaluación y auditoría informática.
3. Diseñar el esquema conceptual del modelo de aplicación de evaluación, auditoría y control de procesos de información y tecnologías afines.
4. Integrar al modelo de auditoría, técnicas de valoración cuantitativa que permitan la obtención de valores de medidas de riesgo y control.
5. Estructurar el diseño lógico de la herramienta automatizada para la aplicación del modelo de auditoría, evaluación y control propuesto.

### **Importancia y Justificación del Estudio**

La importancia del estudio que intenta desarrollar el presente proyecto se fundamenta en cuatro aspectos característicos de la información como activo empresarial y en la conceptualización y aplicación de la estructura de la arquitectura

de información y de los procesos soportados en Tecnología de Información (TI) en las organizaciones actuales. Estos aspectos son:

**1. El Valor de la Información en las Organizaciones:** si se parte del conocimiento previo de qué la Información representa un activo de singular valor para las organizaciones, y que todos los procesos del negocio se sustentan en el procesamiento de datos y administración de información para soportar la toma de decisiones y mantener la estabilidad y rentabilidad del negocio, es necesario entender que la tecnología relacionada con la información y sus procesos representa un punto de enfoque de especial importancia para la estabilidad empresarial.

Existen principios generalmente aceptados en las buenas practicas, reconocidas internacionalmente por los expertos en la materia de *Control y Auditoría de Información y Tecnologías relacionadas*; por tal razón, toda investigación que esté sustentada en el marco referencial de las mejores prácticas y persiga la aplicabilidad de sus principios, está dotada de una singular importancia.

Las metodologías de Auditoría informática deben cubrir todos los aspectos de la información y de la tecnología que la soporta. *Los Objetivos de Control* deben encararse con referencia a las políticas y estándares de la empresa, el propietario del proceso del negocio debe asegurar que se provee un sistema de control adecuado para el ambiente de tecnología informática.

**2. Integración de los Recursos de los Sistemas de Información:** el presente estudio esta orientado a obtener un producto, que permitirá aplicar modelos de evaluación y control sobre las diferentes actividades y/o tareas, procesos y áreas de aplicación de las Tecnologías de Información bajo el enfoque de aplicación de los diferentes objetivos de control formulados para cada ámbito integrando los recursos y/o componentes de un sistema de información: personas, datos, software (programas), hardware (equipos y facilidades), redes y comunicaciones, información, actividades, conocimiento y bases de conocimiento, retroalimentación (autocontrol), procedimientos e instalaciones físicas.

**3. Requerimientos de información:** Los recursos anteriores se integran para satisfacer los requerimientos del negocio en cuanto a la calidad, aspectos financieros

y seguridad (control de riesgos) sobre los criterios de información para optimizar su uso. Comenzando el análisis desde los requerimientos amplios de calidad, financieros y seguridad, se deben contemplar las características de la información que satisfacen los criterios de *efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad*.

**4. La Estructura de Cobertura Global de la TI:** los procesos básicos de información basados en la aplicación de tecnología informática comienzan en las actividades y tareas necesarias para lograr un resultado mensurable. Las actividades tienen un concepto de ciclo de vida mientras que las tareas son consideradas más discretas. El concepto *ciclo de vida* tiene requerimientos típicos de control diferentes de las actividades discretas. Ejemplos de la primera categoría son las actividades de desarrollo de sistemas, administración de la configuración y administración de los cambios. La segunda categoría incluye tareas realizadas en soporte de planeamiento estratégico de Tecnología Informática, evaluación de riesgos, planeamiento de calidad, administración de capacidad y performance. Al más alto nivel, los procesos son agrupados naturalmente en dominios, su agrupamiento natural es a menudo confirmado como dominios de responsabilidad en una estructura organizacional y está en línea con el ciclo de administración o ciclo de vida aplicable a los procesos de Tecnología Informática.

La observancia en todos los aspectos mencionados anteriormente para el diseño de un modelo de auditoría, evaluación y control de los procesos de información y de la tecnología relacionada con estos procesos, permitirá la generación de una estructura conceptual y metodológica de fácil conocimiento y aplicación por parte de los usuarios ejecutivos de negocios, profesionales de TI y auditores de sistemas de información, para saber en que medida de control se encuentra la organización respecto a la planificación, desarrollo, uso y evaluación de la TI y en consecuencia, fortalecer o corregir los planes de acción en concordancia con los objetivos del negocio.

## **CAPITULO II**

### **MARCO TEORICO**

#### **Antecedentes**

En el marco de referencia de estudios precedentes sobre el estudio y/o aplicación de modelos o enfoques metodológicos de procesos de evaluación y control de Auditoría orientada a los sistemas de información y a las tecnologías relacionadas con estas áreas del conocimiento, hoy conocidas como tecnologías de la información (TI), se pueden encontrar múltiples referencias que han dado origen a las hoy conocidas Metodologías de Auditoría Informática, de las cuales, se presentará más adelante una referencia teórica a las más importantes por su uso y aporte al desarrollo de esta área del conocimiento denominada Auditoría Informática y como antecedentes, propiamente dichos, se citaran algunos estudios que se han sustentado en la aplicación de dichas metodologías para la solución de problemas de control y evaluación de TI y otros que han provisto aportes para la creación, uso y aplicación de nuevos enfoques, modelos o herramientas de aplicación de las metodologías preexistentes.

**García (1990)**, plantea la problemática de generación de novedosas formas de fraudes, delitos informáticos y fracasos de organizaciones como resultado del creciente uso del recurso computador que incorpora nuevas amenazas y riesgos en el tratamiento de la información y propone que frente a esta situación la respuesta no puede ser no utilizarlo; la solución debe ser canalizar adecuadamente su utilización, reconociendo, identificando, avizorando estas novedosas formas de fraudes y generadoras de fracasos. También plantea la existencia de información previa en obras de Auditoría de Sistemas, revistas especializadas, presentaciones de trabajos en

congresos y seminarios de corte internacional, realizados por importantes figuras del área, destacando aspectos estadísticos de robos y fraudes por computador y contribuyendo a alertar y generar conocimiento en la importante función de Auditoría de Sistemas. Según Garcia (ob. cit.) “...Sin embargo, el Auditor no dispone de una herramienta metodológica que le permita formular y aplicar programas de revisión y auditaje”. Junto a esta necesidad, como base conceptual para conformar la motivación de su investigación y presentación de su enfoque metodológico, Garcia presenta su enfoque metodológico en seis fases: (a) organización y planificación del programa de auditoría, (b) identificación y descripción de recursos y procesos, (c) simulación, identificación y descripción de amenazas y riesgos, (d) identificación y descripción de controles, (e) análisis de cobertura, y (f) prueba de los controles.

Este trabajo es importante como antecedente porque se ubica en una época, inicio de la década de los noventa, en la que la Auditoría de Sistemas es incipiente metodológicamente y presenta una opción de aplicación sistémica de evaluación y control de los recursos, procesos, amenazas y riesgos en los sistemas de información para evaluar los controles existentes y proponer una serie de controles pertinentes de acuerdo con el grado de requerimientos de control en los sistemas evaluados. Su aporte, aparte de la intención metodológica, es la clasificación y aplicación del concepto amplio de control en el contexto de los sistemas de información. La desventaja de esta investigación radica en que para su época, los conceptos de sistemas de información gerencial, la estrategia y objetivo del negocio, las tendencias abiertas de las tecnologías de la información y las comunicaciones no son contempladas ni incorporadas en el estudio.

La **ISACF (1996)**, Information Systems Audit and Control Foundation, Fundación para el Control y Auditoría de los Sistemas de Información, ha desarrollado y publicado con el apoyo de IT Governance Institute (Instituto para el Gobierno de Tecnologías de Información) el *Proyecto de Investigación COBIT*, acrónimo en ingles de Control Objectives for Information and related Technologies, (Objetivos de Control para la Información y las Tecnologías afines o relacionadas).

*COBIT* ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). *COBIT* es la herramienta innovadora para el gobierno de TI. *COBIT* se fundamenta en los *Objetivos de Control* existentes de la *Information Systems Audit and Control Foundation* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento.

Los *Objetivos de Control* resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término “**generalmente aplicable y aceptado**” es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, “*buenas prácticas*” significa consenso por parte de los expertos. El desarrollo de *COBIT* ha traído como resultado la publicación del Marco Referencial general y de los *Objetivos de Control* detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación *COBIT*. El desarrollo de *COBIT* ha resultado en la publicación de:

1. *Resumen Ejecutivo*: que consiste en una Síntesis Ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de *COBIT*) y el Marco Referencial que identifica los cuatro dominios de *COBIT* y los correspondientes 34 procesos de TI
2. *Marco Referencial*: que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TI que son impactados en forma primaria por cada objetivo de control
3. *Objetivos de Control*: los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 318 objetivos de control detallados y específicos a través de los 34 procesos de TI definidos en el marco referencial.

4. *Directrices de Auditoría:* las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 318 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o una recomendaciones de mejoramiento
5. *Conjunto de Herramientas de Implementación:* el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo. El Conjunto de Herramientas de Implementación incluye la *Síntesis Ejecutiva*, proporcionando a la alta gerencia conciencia y entendimiento de COBIT.

Las investigaciones y publicaciones sobre *COBIT* han sido posibles gracias a contribuciones de múltiples organizaciones como Unysis, Unitech Systems, Inc., MIS Training Institute, Zergo, Ltd., y Coopers & Lybrand. El Forum Europeo de Seguridad (European Security Forum –ESF-) amablemente puso a disposición material para el proyecto. Otras donaciones fueron recibidas de capítulos miembros de ISACA de todo el mundo.

En la historia de la investigación *COBIT* muchas fuentes han contribuido al aporte de consolidación de la misma. Entre ellas tenemos: (a) estándares técnicos de ISO, EDIFACT, otros; (b) códigos de conducta establecidos por el Council of Europe, OECD, ISACA, otros; (c) criterios de calificación para sistemas y procesos de TI: ITSEC, TCSEC, ISO 9000, SPICE, TICKIT, Common Criteria, otros; (d) estándares profesionales para control interno y auditoría: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, otros; (e) requerimientos y prácticas de foros de la industria: ESF, I4 y plataformas auspiciadas por gobiernos como IBAG, NIST, DTI; y (f) requerimientos específicos de industrias emergentes de sectores como banca, comercio electrónico, y manufactura de TI. (Las definiciones de los términos y/o acrónimos citados pueden verse más adelante en la definición de términos.

Estos antecedentes del Proyecto de investigación *COBIT* son importantes, en general, por cuanto presentan el basamento estructural de apoyo de los más recientes trabajos de investigación y aplicación en el área de Auditoría en Tecnologías de la Información, y en particular porque sustentan el desarrollo del presente proyecto de investigación.

Las referencias específicas a los contenidos conceptuales de *COBIT* y a su estructura serán presentadas más adelante en el contenido de las bases teóricas donde se ampliarán suficientemente los conceptos necesarios para soportar su aplicación en el presente estudio.

*MEYCOR Cobit Control Self Assessment (CSA)*, de **Datasec (1999)**, ha sido apoyado por el Gobierno de Uruguay en Suramérica. Buscando sacar provecho de la experiencia de los profesionales en el campo de la ciencia y la tecnología y promover la apertura de negocios estratégicos de mercado en esta área, decide apoyar proyectos innovadores en el Programa de Desarrollo Tecnológico (PDT) auspiciado por el Banco Interamericano de Desarrollo (BID).

Después de definir los requerimientos para los procesos de las propuestas, PDT aprobó un proyecto para soportar el desarrollo de software relacionado con el gobierno (gestión) de Tecnologías de Información (TI) basado en el modelo *COBIT* desarrollado por ISACF y el IT Governance Institute. El proyecto de investigación y desarrollo fue completado por *DATASEC S.R.L.*, una firma de consultores y desarrolladores de software. Después de una intensa investigación y acumulación de experiencia con aplicaciones de *COBIT* y metodologías de análisis cualitativo de riesgos como la francesa *MARION* y la inglesa *CRAMM*, el primer producto de software basado en *COBIT* fue llamado *MEYCOR Cobit Control Self Assessment (CSA)*, es un software que fue puesto al uso de clientes de la consultoría. Después el mismo ha sido mejorado, siendo utilizado por varias compañías en Uruguay y otras partes. A través de su investigación y desarrollo, Datasec ha impuesto a Meycor CSA los siguientes propósitos:

1. Permitir la funcionalidad Cobit no solo para grandes compañías, sino también para organizaciones de medio y pequeño tamaño.
2. Permitir la entrada en múltiples niveles de usuarios; a causa de la flexibilidad de la herramienta, puede ser introducida en las empresas al nivel de supervisores de operaciones, CIO's, directores, interventores, expertos de seguridad IT, auditores y asesores.
3. Generar automáticamente recomendaciones con enlace a gráficos que permitan a la organización el monitoreo de sus logros en cada proceso *COBIT*.
4. Asegurar una conexión entre objetivos de control con categorías primarias de seguridad en TI y a bajo nivel establecer requisitos de seguridad en múltiples plataformas.
5. Incluir la referencia a guías que permiten la comprobación de respuestas de los usuarios considerando el estado de cada objetivo de control.

Muchas de las organizaciones que han incorporado actividades de gestión de TI han conseguido logros sobresalientes. Entre estas, el Banco de la Republica Oriental del Uruguay (BROU), la institución financiera más importante del país, con más de diez empleados CISA's (Certified Information Systems Audit.) en su plantilla de personal, apoyados en Cobit ha conseguido un valor significativo.

Además de BROU, también se puede citar a Ancap (compañía de aceites), Montevideo Stock Exchange, Tribunal de Cuentas y otras organizaciones que han depositado en el proyecto de Datasec su confianza para darle soporte nacional y seguir la investigación y aplicación de herramientas basadas en la estructura *COBIT* como apoyo a la oportunidad otorgada por PDT y el BID, bajo la tutela del Ministerio de Educación y Cultura de Uruguay.

Este antecedente, respalda la importancia de la estructura *COBIT* en el tratamiento del problema de control en la aplicación de la Tecnología de Información en las organizaciones.

**Cubillos (2003)**, desarrolló el *Modelo de Evaluación de Riesgos AUDIRISK*, titulado “Evaluación de Riesgos Operacionales en Procesos de Negocio y Servicios Automatizados” en el cual se habla sobre la identificación y valoración de riesgos potenciales y expresa que para valorar o medir el nivel de exposición a riesgos potenciales en cualquier proceso de negocio o de tecnología de información o sistema sujeto a diseño de controles, es necesario tener en mente los siguientes supuestos:

1. Todos los riesgos aplicables al proceso o sistema sujeto a diseño de controles no son igualmente importantes, desde el punto de vista del impacto que podrían causar en caso de llegar a presentarse. Por consiguiente, para ser eficientes y efectivos en el proceso de diseño de controles, es necesario establecer prioridades para atacar los riesgos asociados con cada proceso o sistema.

2. Los recursos que se asignen para prevenir o mitigar los riesgos potenciales (tiempo, financieros, personas y tecnología) de cada proceso o sistema, deberían aplicarse con mayor énfasis a los riesgos críticos, es decir, a los que podrían generar las pérdidas o problemas operacionales más significativos en caso de presentarse.

3. Para priorizar los esfuerzos de protección que requieren los riesgos potenciales y definir los controles requeridos, es necesaria la participación de los funcionarios de niveles estratégico, táctico y operativo que intervienen en el manejo de las operaciones y la toma de decisiones en el negocio o sistema sujeto a diseño de controles.

Continúa el estudio, explicando que para establecer cuales riesgos pueden presentarse en cada proceso de negocio o sistema de información sujeto a diseño de controles, es necesario utilizar como punto de partida un modelo de riesgos típicos, de los varios que difunden y utilizan las asociaciones internacionales de profesionales en controles y Auditoría, las firmas de consultoría en seguridad, los analistas de riesgos y las firmas de auditores. También pueden utilizarse como punto de partida los diferentes modelos de riesgos existentes como son: (a) el modelo de FitzGerald J. (1991), (b) el modelo de Robert H. Courtney, publicado por el National Bureau of

Standard, (c) el modelo propuesto por el Instituto Canadiense de Contadores Públicos (CICA). (d) el modelo propuesto en el estudio SAC del Instituto de Auditores Internos de USA (IIA) y (e) el modelo *AUDIRISK*, propuesto por AUDISIS, su empresa. Este último utiliza como base el concepto que *"riesgo es el valor de las pérdidas que experimenta una organización como consecuencia de la ocurrencia de una ó más causas de riesgo o amenazas contra la seguridad"*, Cubillos (2003).

El modelo *AUDIRISK* agrupa el universo de riesgos potenciales en ocho (8) categorías de riesgos típicos. Estos son: (a) pérdidas por hurto / fraude, (b) pérdidas por daño y destrucción de activos, (c) pérdidas por sanciones legales, (d) pérdidas por baja credibilidad pública o pobre reputación, (e) pérdidas por desventaja competitiva, (f) pérdidas de ingresos por causas accidentales, (g) pérdidas por exceso de pagos, por causas accidentales, y (h) pérdidas por decisiones erróneas de la gerencia. La aplicabilidad de estas categorías de riesgo está comprobada para cualquier tipo de organización, sin importar el tamaño, el sector a que pertenezcan y el grado de sofisticación tecnológica que presenten sus operaciones automatizadas.

Una ventaja que ofrece el reducido número de categorías de riesgo de este modelo es la facilidad y simplicidad de análisis. Entre mayor número de riesgos utilice el modelo, mayor será la complejidad del análisis y será menor la eficiencia en el trabajo de diseño o revisión de controles.

Este modelo, como los referenciados por él, permiten valorar y justificar el enfoque y nombre de *"modelo metodológico"* en los trabajos de investigación y desarrollo en esta área de aplicación de metodologías al proceso de Auditoría y Evaluación de Tecnologías de Información y en general en la Auditoría de Sistemas Informáticos.

**Arima (1990)**, en su tesis doctoral de la Facultad de Economía, Administración y Contaduría de la Universidad de Sao Paulo, presenta la propuesta de un modelo metodológico y una herramienta automatizada de Auditoría de sistemas, enmarcado dentro del ciclo de vida del sistema de información de Contabilidad Computarizada

fundamentado en que el objetivo fundamental de la Auditoría de sistemas es como cita textualmente en el resumen "... revisar y evaluar el control interno de un determinado sistema de información...". El desenvolvimiento del modelo lo presenta constituido en seis etapas, a saber: (a) planeación del proyecto de Auditoría de sistemas de información, (b) levantamiento de información del sistema a ser auditado, (c) identificación e inventario de puntos de control, (d) priorización y selección de los puntos de control del sistema en Auditoría; (e) revisión y validación de los puntos de control, y (f) acompañamiento y/o conclusiones de la Auditoría. La propuesta automatizada requirió de un análisis funcional de la metodología que fue compuesta de los siguientes módulos: (a) administración de proyectos de Auditoría, (b) monitoreo de puntos de control, (c) aplicación de técnicas de Auditoría, y (d) gerencia de indicadores de Auditoría. En el modelo metodológico propuesto, los módulos indicados constituyen los programas de computación, aplicaciones, que deben permitir la estructuración y recuperación adecuada de información del banco de datos de la Auditoría, de acuerdo con las necesidades de operacionales del área auditada, también como de la alta administración relacionada.

Esta referencia permite observar que la propuesta de un *modelo metodológico* fundamentado en las variables, relaciones y procedimientos o procesos a desarrollar, puede plasmarse en una herramienta de software que permita demostrar la validez del modelo aplicado a cualquier organización, dado que todas las organizaciones que utilizan sistemas de información basados en TI manejan variables similares.

### **Bases Teóricas**

El basamento teórico de la presente investigación se fundamenta en los conceptos y definiciones relativas o referenciadas al marco de aplicación de las tecnologías de información (TI) en las organizaciones. Si entendemos las TI como el conjunto de todos los elementos necesarios para la generación, establecimiento, uso y

evaluación de sistemas de información, y a esto añadimos todos los elementos necesarios para la evaluación y control de la seguridad de la información y la tecnología relacionada, tendremos todo el marco referencial teórico requerido.

## **Modelo**

*“Un modelo puede ser definido como la representación idealizada de un sistema de la vida real”* UNA (1989). El sistema puede existir físicamente o ser una idea concebida que espera por su ejecución, como es el caso de un modelo propuesto para la evaluación, mediante su aplicación, de un sistema. En el primer caso, el objetivo del modelo es proveer los medios para analizar el comportamiento del sistema. “En el segundo caso, el objetivo es definir la estructura de un sistema futuro que incluya las interrelaciones funcionales entre sus componentes, y entre el sistema y su medio ambiente”, UNA (ob. cit).

Los modelos pueden ser icónicos, representan el sistema mediante modelos a escala como un avión en un túnel de viento. Los modelos analógicos como las graficas en un plano cartesiano representan las distancias modeladas de los objetos ubicados relativamente. Los modelos simbólicos o matemáticos emplean símbolos para representar las variables de decisión del sistema y las relaciones entre las variables se representan por medio de funciones.

Un modelo también permite presentar un diseño esquematizado para seguir procesos por una línea de acción predefinida que permitan evaluar el comportamiento del sistema estudiado con la aplicación del modelo, como es el caso de los modelos metodológicos.

## **Metodología**

Según el diccionario de la Lengua de la Real Academia Española (1939) “*método* es el modo de decir o hacer con orden una cosa”. Asimismo define la palabra *metodología* como “conjunto de métodos que se siguen en una investigación

científica o en una exposición doctrinal”. Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad y que es llamada metodología.

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde sus diseños de ingeniería hasta el desarrollo del software y la Auditoría de los sistemas de información.

Respecto a la aplicación de metodologías Piattini M., Del Peso E. (1998:45) expresan “Las metodologías usadas por un profesional dicen mucho de su forma de entender y hacer su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de acierto/error”.

Las metodologías son necesarias para que los equipos de profesionales en áreas específicas del conocimiento alcancen resultados homogéneos tal como si lo hiciera uno solo, por lo que resulta habitual y práctico el uso de metodologías siguiendo las prácticas desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

## **Auditoría**

La Auditoría en su acepción más general y original es definida por el diccionario General de la lengua Española VOX como el “Proceso que recurre al examen de libros, cuentas y registros de una empresa para precisar si es correcto el estado financiero de la misma, y si los comprobantes están debidamente presentados”.

Este concepto de Auditoría se ajusta más a la aplicación del área contable financiera que a las áreas técnicas como la informática y los sistemas de información, sin embargo, el objetivo de control general de salvaguarda de los activos empresariales está explícito en él y por tanto es aplicable a la información.

Según Echenique (1985) es frecuente encontrar la palabra *auditoría* empleada incorrectamente y considerada como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a acuñar la frase “tiene *auditoría*” como

sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio; no sólo detecta errores, sino que es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

Un concepto más actualizado y generalizado, aplicable a los diferentes tipos de Auditoría, es el emitido por Piattini y Del Peso (1998):

*“Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas”.*

En general, la palabra Auditoría viene del latín auditórius, y de esta proviene auditor, que tiene la virtud de oír, y el diccionario lo define como “revisor de cuentas colegiado”. El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es la evaluación de la eficiencia y la eficacia de las operaciones del negocio, para señalar cursos alternativos de acción que apoyen la toma de decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Esta orientación de la función de auditoría es la que justifica el desarrollo de metodologías y modelos de aplicación de evaluación y auditorías en general y de auditorías de información, en particular, por cuanto, como se conoce, la información constituye un activo de singular valor para las organizaciones.

La descomposición del concepto de Auditoría, permite obtener los elementos fundamentales presentados en el **Cuadro 1**.

## Cuadro 1

### Elementos Fundamentales del Concepto de Auditoría

<b>Elemento</b>	<b>Característica</b>
1) Contenido:	Una <b>opinión</b>
2) Condición:	<b>Profesional</b>
3) Justificación:	Sustentada en determinados <b>procedimientos</b>
4) Objeto:	Una determinada <b>información</b> obtenida en un cierto soporte
5) Finalidad:	Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su <b>fiabilidad</b>

*Nota:* Análisis conceptual de elementos tomado de Piattini y Del Peso (1998)

En general y en todo caso, la auditoría es una función que se realiza a posteriori, respecto a procesos o actividades ya ejecutados o realizadas, sobre las que hay que emitir una opinión.

### Clases de Auditoría

Los elementos 4) y 5) del concepto anterior presentado en el **Cuadro 1**, distinguen de que clase o tipo de Auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte y la finalidad con que se realiza el estudio, definen el tipo de Auditoría de que se trata. Ilustrativamente, Piattini y Del Peso (1998) presentan la clasificación mostrada en el **Cuadro 2**, a continuación:

## Cuadro 2

### Clases de Auditoría

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, otros	Operatividad eficiente y según normas establecidas
Gestión	Opinión	Dirección	Eficacia, eficiencia, economicidad
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas

*Nota:* Clasificación tomada de Piattini y Del Peso (1998)

### Informática

El concepto de informática es más amplio que el simple uso de equipos de cómputo o bien de procesos electrónicos. Etimológicamente, la palabra informática, deriva del francés *informatique*. Este neologismo proviene de la conjunción de *information* (información), y *automatique* (automática). Según la CIFCA (1983), su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de *proceso de datos*.

Hacia principios de los años setenta ya eran claras las limitaciones de esta definición, sobre todo por el hincapié en el uso de las maquinas. El principal esfuerzo por redefinir el concepto de informática lo realizó en esa época el IBI, Oficina Intergubernamental de Informática, en aquel tiempo órgano asociado a la UNESCO, que formuló la definición: “Aplicación racional, sistemática de la información para el desarrollo económico, social y político...ciencia de la política de la información”, IBI-UNESCO (1975).

Este último concepto tiene especial importancia por el realce y enfoque social del valor de la información, lo cual redundará en la justificación de la necesidad de los procesos de auditoría informática en las organizaciones como mecanismos de control y aseguramiento de la calidad de la información.

### **Dato e Información**

Es común confundir el concepto de dato con el de información. La información es una serie de datos clasificados y ordenados con un objetivo común y con un significado dentro de un contexto particular. El dato se refiere únicamente a un símbolo, signo, abstracción o a una serie de signos, letras o números sin significado de extensión o contexto. El proyecto *COBIT*, ISACF (1996), considera a los datos en sentido más amplio como todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos y otras representaciones concretas.

En general la información está orientada a reducir la incertidumbre del receptor y tiene características de poder duplicarse prácticamente sin costo, y no se gasta, no existe por sí misma, sino que debe expresarse en algún objeto explícito (papel, cinta, video, otros); de otra manera puede desaparecer o deformarse como sucede con la comunicación oral, la cual hace que la información deba ser controlada debidamente por medio de adecuados sistemas de seguridad, confidencialidad y respaldo, surgiendo el importante concepto de *control de la información*.

El control de la información debe asegurar que esta pueda comunicarse, y para ello hay que lograr que los medios de seguridad sean llevados a cabo después de un adecuado examen sobre la forma de transmisión, la eficiencia de los canales de comunicación, el transmisor, el receptor, el contenido de la comunicación, la redundancia y el ruido. Todos estos aspectos son relevantes en los procesos de Evaluación y Auditoría de la Información y de las Tecnologías que soportan el proceso de la misma.

## **COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)**

El proyecto de investigación *COBIT* de **ISACF (1996)**, representa la base teórica fundamental del presente trabajo sobre el modelo metodológico de auditoría de información y tecnologías relacionadas; en este sentido y tal como se presentó en los antecedentes, los conceptos, aspectos y componentes de la estructura *COBIT* representan la piedra angular. Los demás conceptos o bases teóricas que no se independizan en este trabajo están inmersos en la estructura *COBIT* que se presenta a continuación.

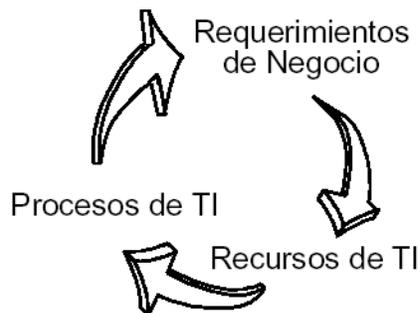
*COBIT* es una herramienta de gobierno (administración) de TI que ha cambiado la forma en que trabajan los profesionales de TI vinculando tecnología informática y prácticas de control, *COBIT* consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

*COBIT* se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. Según cita la propia ISACF en la publicación oficial del Marco Referencial *COBIT* (Cobit FrameWork) su misión es: *“Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y generalmente aceptados para el uso cotidiano de gerentes de empresas y auditores”*. *COBIT* esta dirigido a múltiples usuarios:

1. **La Gerencia:** para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
2. **Los Usuarios Finales:** quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

3. **Los Auditores:** para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
4. **Los Responsables de TI:** para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Las principales características de *COBIT* son: (a) orientado al negocio, (b) alineado con estándares y regulaciones "de facto", (c) basado en una revisión crítica y analítica de las tareas y actividades en TI, (c) alineado con estándares de control y auditoría como (COSO, IFAC, IIA, ISACA, AICPA), (d) los principios básicos de *COBIT*, **Gráfico 1**, están fundamentados en el enfoque del control en TI que 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 las TI que deben ser administrados por procesos de TI. A continuación se presentan las bases teóricas de la estructura *COBIT* que fundamentan el desarrollo del presente estudio.



**Gráfico 1. Relación de los Principios Básicos de COBIT.**  
*Fuente:* Marco Referencial COBIT. ISACF (2000)

## Requerimientos de Información COBIT (ob. cit.)

Los *requerimientos de la información* del negocio se definen como los criterios que la información necesita satisfacer para alcanzar los requerimientos del negocio. Estos criterios son: (a) *requerimientos de calidad*: - calidad, costo y entrega -, (b) *requerimientos fiduciarios*: - efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento de leyes y regulaciones -, y (c) *requerimientos de seguridad*: - confidencialidad, integridad y disponibilidad -. Estos requerimientos de información del negocio explicados por *COBIT* se definen como:

1. **Efectividad**: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
2. **Eficiencia**: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
3. **Confiabilidad**: proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
4. **Cumplimiento**: de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
5. **Confidencialidad**: Protección de la información sensible contra divulgación no autorizada
6. **Integridad**: Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
7. **Disponibilidad**: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

No todos los anteriores requerimientos de información son satisfechos o tienen impacto en el mismo grado por los diferentes objetivos de control de alto nivel: COBIT clasifica este grado de relación como:

1. **Primario (P)**: es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

2. **Secundario (S):** es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.
3. **Blanco (vacío):** podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

### **Recursos de TI COBIT (op. cit.)**

*COBIT* establece los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

1. **Recurso Humano:** Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.
2. **Datos:** Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos y otros objetos.
3. **Aplicaciones:** entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
4. **Tecnología:** incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
5. **Instalaciones:** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

Los procesos de negocio requieren de información, la cual a su vez es producida por un conjunto de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorearse medidas de control para estos recursos y procesos asociados. Estas relaciones se presentan en el **Gráfico 2** en la página siguiente.



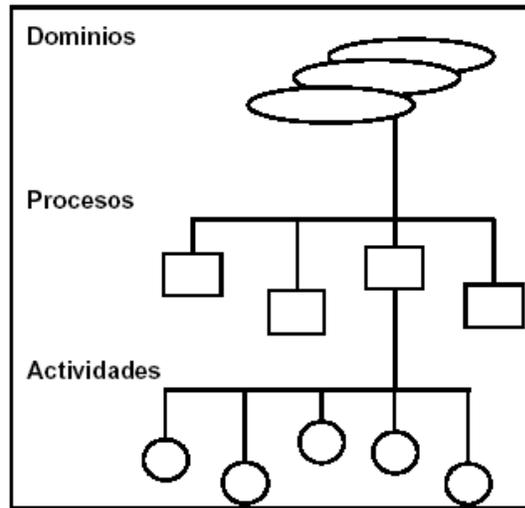
**Gráfico 2: Información, Recursos de TI y Procesos del Negocio.**

*Fuente:* Marco Referencial COBIT. ISACF (2000)

### Procesos de TI (ob. cit.)

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos" (ob. cit.). *COBIT* se divide en tres niveles: Dominios, Procesos y Actividades:

1. **Dominios:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. **Actividades:** Acciones requeridas para lograr un resultado medible. Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. El **Gráfico 3** muestra la relación entre dominios, procesos y actividades.



**Gráfico 3. Relación de Dominios, Procesos y Actividades COBIT.**  
*Fuente:* Marco Referencial COBIT. ISACF (2000)

**Dominios COBIT (ob. cit.)**

**Dominio: Planificación y Organización (PO).** 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. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas. Los procesos de este dominio son:

**PO1: Definición de un plan estratégico.** Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros. Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

1. La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
2. El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
3. Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI
4. Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos

**PO2: Definición de la arquitectura de información.** Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

1. La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
2. El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.
3. La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

**PO3: Determinación de la dirección tecnológica.** Aprovechar al máximo la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de

negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

1. La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
2. El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
3. Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
4. Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

**PO4: Definición de la organización y de las relaciones de TI.** Prestación de servicios de TI. Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

1. El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
2. Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
3. Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
4. Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

5. Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas
6. La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
7. Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.
8. El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

**PO5: Manejo de la inversión.** Tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

1. Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.
2. El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información
3. La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

**PO6: Comunicación de los objetivos y directivas de la alta gerencia.** Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la

comunidad de usuarios, necesiándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

1. Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
2. Las directrices tecnológicas
3. El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
4. El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
5. Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

**PO7: Administración de recursos humanos.** Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

1. El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
2. Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera
3. La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.

4. La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

**PO8: Asegurar el cumplimiento de los requerimientos externos.** Cumplir con obligaciones legales, regulatorias y contractuales. Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

1. Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continuo de los mismos.
2. Leyes, regulaciones y contratos
3. Revisiones regulares en cuanto a cambios
4. Búsqueda de asistencia legal y modificaciones
5. Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
6. Privacidad
7. Propiedad intelectual
8. Flujo de datos externos y criptografía

**PO9: Evaluación de riesgos.** Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI. Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

1. Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI de manera de que se pueda determinar como los riesgos deben ser manejados a un nivel aceptable.

2. Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos.
3. Actualización de evaluación de riesgos
4. Metodología de evaluación de riesgos
5. Medición de riesgos cualitativos y/o cuantitativos
6. Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
7. Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

**PO10: Administración de proyectos.** Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión. Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

1. Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.
2. El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
3. Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.

4. Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
5. Presupuestos de costos y horas hombre
6. Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
7. Plan de administración de riesgos para eliminar o minimizar los riesgos.
8. Planes de prueba, entrenamiento, revisión post-implementación.

**PO11: Administración de calidad.** Satisfacer los requerimientos del cliente. Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

1. Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.
2. Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, Auditorías, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.
3. Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
4. Documentación de pruebas de sistemas y programas
5. Revisiones y reportes de aseguramiento de calidad

**Dominio: Adquisición e Implementación (AI).** 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. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes. Sus procesos son:

**AI1: Identificación de soluciones automatizadas.** Asegurar el mejor enfoque para cumplir con los requerimientos del usuario. Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

1. Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
2. Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
3. Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
4. Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
5. Pistas de Auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)
6. Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
7. Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología específica a ser proporcionada.

**AI2: Adquisición y mantenimiento de software de Aplicación.** Proporciona funciones automatizadas que soporten efectivamente al negocio. Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

1. Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
2. Requerimientos de archivo, entrada, proceso y salida.
3. Interfase usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
4. Personalización de paquetes

5. Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
6. Controles de aplicación y requerimientos funcionales
7. Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

**AI3: Adquisición y mantenimiento de la infraestructura tecnológica.**

Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios. Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

1. Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
2. Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
3. Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

**AI4: Procedimientos de Desarrollo y Mantenimiento.** Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas. Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

1. Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
2. Manuales de Operaciones y controles, de manera que estén en permanente actualización.

3. Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

**AI5: Instalación y aceptación de sistemas.** Verificar y confirmar que la solución sea adecuada para el propósito deseado. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

1. Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
2. Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
3. Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
4. Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
5. Revisiones post implementación con el objeto de reportar si el sistema proporcione los beneficios esperados de la manera mas económica.

**AI6: Administración de cambios.** Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través 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 y toma en consideración:

1. Identificación de cambios tanto internos como por parte de proveedores
2. Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
3. Evaluación del impacto que provocaran los cambios.
4. Autorización de cambios
5. Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

6. Distribución de software, estableciendo medidas de control específicas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

**Dominio: Entrega y Soporte (DS: Delivery & Support).** En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Comprende los siguientes procesos:

**DS1: Definición de niveles de servicio.** Establecer una comprensión común del nivel de servicio requerido. Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

1. Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
2. Definición de las responsabilidades de los usuarios y de la función de servicios de información
3. Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
4. Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de

desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

5. Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.
6. Garantías de integridad
7. Convenios de confidencialidad
8. Implementación de un programa de mejoramiento del servicio.

**DS2: Administración de servicios prestados por terceros.** Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos. Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

1. Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
2. Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
3. Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
4. Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

**DS3: Administración de capacidad y desempeño del sistema.** Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado. Para ello se realizan 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 y toma en consideración:

1. Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
2. Monitoreo y reporte de los recursos de tecnología de información
3. Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
4. Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño
5. Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

**DS4: Aseguramiento de la Calidad del Servicio.** Mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones. Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

1. Planificación de Severidad
2. Plan Documentado
3. Procedimientos Alternativos
4. Respaldo y Recuperación
5. Pruebas y entrenamiento sistemático y singulares

**DS5: Establecimiento de pautas para la seguridad de sistemas.** Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

1. el acceso lógico junto con el uso de los autenticación y Autorización, recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso
2. Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario
3. Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
4. Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
5. Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
6. Firewalls si existe una conexión con Internet u otras redes de Utilización públicas en la organización

**DS6: Identificación e imputación de costos.** Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados. Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

1. Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
2. Campañas de toma de conciencia, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento

3. Técnicas de toma de conciencia proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

**DS7: Educación y capacitación de los usuarios.** Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI. Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

1. Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios
2. Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de computo y aseguren el trato justo de los departamentos usuarios y sus necesidades
3. Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

**DS8: Asistencia y asesoramiento a los clientes de TI.** Asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente. Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

1. Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda
2. Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas
3. Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias

**DS9: Administración de la configuración.** Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios. Para ello se realizan

controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

1. Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición
2. Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración
3. Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización
4. Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

**DS10 Administración de problemas e incidentes.** Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder. Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

**DS11 Administración de datos.** Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen los errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o

detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

**DS12: Administración de las instalaciones.** Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

**DS13: Administración de las operaciones.** Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una programación de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

**Dominio: Monitoreo (M).** Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio. Este dominio comprende los siguientes procesos:

**M1: Monitoreo del proceso.** Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte

así como la atención regular a los reportes emitidos. Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

**M2: Evaluación de la adecuación del control interno.** Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI. Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

**M3: Obtención de aseguramiento independiente.** Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo. Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

**M4: Provisión de auditoría independiente.** Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de Auditorías independientes

desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de Auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la Auditoría. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta Auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de Auditoría.

Según COBIT, la función de Auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoría, período de cobertura, naturaleza y trabajo de Auditoría realizado, como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de Auditoría llevado a cabo.

Los 34 procesos propuestos se concretan en los objetivos de control de alto nivel detallados anteriormente.

### **Gobierno de TI (IT Governance)**

El Marco referencial *COBIT* y el IT Governance Institute definen el Gobierno de TI como una estructura de relaciones y procesos dirigida a controlar la organización para alcanzar los objetivos del negocio adicionando valor mientras se mantiene un balance equilibrado de los riesgos sobre la Tecnología de Información y sus procesos.

### **Control**

Se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que

los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran y corregirán" (ob. cit.)

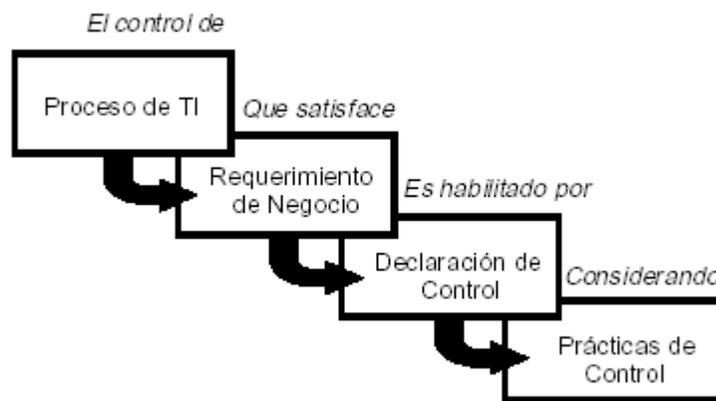
## **Objetivos de Control**

Se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI" (ob. cit.). Los objetivos expuestos en cada uno de los 34 procesos asociados a los 4 dominios explicados anteriormente corresponden a *Objetivos de Control Generales o de Alto Nivel*. Complementariamente, para cada uno de los 34 procesos, se definen de 3 a 30 *Objetivos Detallados de Control Específicos* asociados con cada uno de los procesos de TI. En la versión de *COBIT(1996)* el número de Objetivos Detallados de Control llegaba a 304; posteriormente en la última versión *COBIT(2000)*, el número de estos objetivos llega a 318 con la incorporación de nuevos criterios de control sobre los procesos definidos. Estos objetivos están contenidos en el documento del IT Governance Institute y ISACF denominado "Objetivos de Control Detallados" que complementa al documento "Marco Referencial" que contiene a los Objetivos de Control de Alto Nivel.

La distribución de Objetivos de Control por cada proceso de TI asociado a los diferentes dominios esta definida así: (a) Planificación y Organización – 100 Objetivos -, (b) Adquisición e Implementación – 68 Objetivos, (c) Entrega y Soporte – 126 Objetivos, y (d) Monitoreo con 24 Objetivos para un total de 318 en la versión de *COBIT(2000)*.

Todos los objetivos de control han sido definidos de una manera genérica, sin depender de la plataforma o arquitectura técnica, aceptando el hecho real de que diferentes ambientes de TI pueden requerir la cobertura separada de objetivos de control.

El **Gráfico 4**, en la página siguiente, muestra la navegación en cascada de los objetivos de control que facilita su aplicación. Un resumen de los 318 Objetivos de Control Específicos, Versión *COBIT(2000)*, se presenta en el (Anexo D).



**Gráfico 4. Navegación en cascada de Objetivos de Control.**

*Fuente:* Marco Referencial COBIT. ISACF(2000)

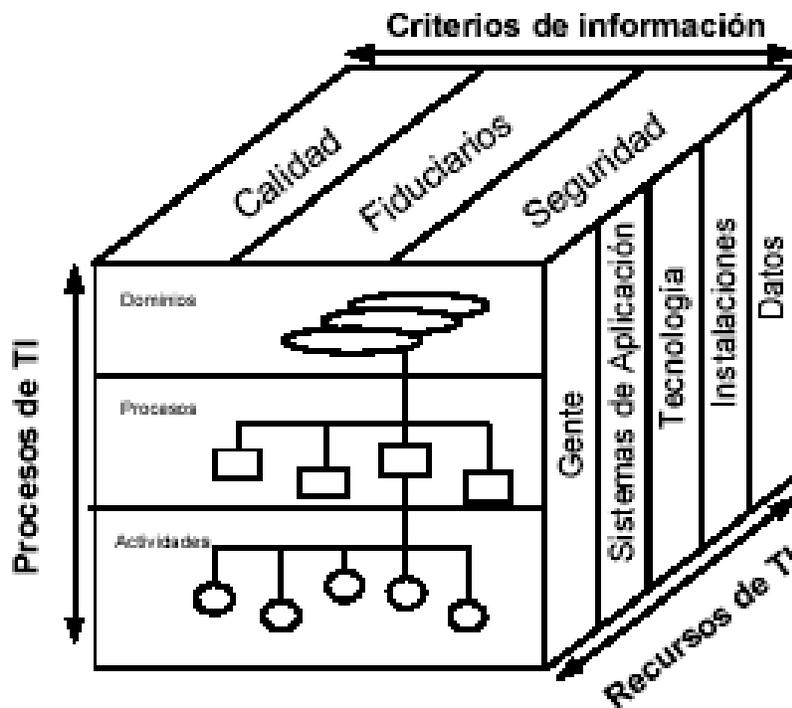
En la pagina siguiente, el **Gráfico 5**, indica por proceso y dominio de TI, cuales criterios de información tienen impacto (P)rimario, (S)ecundario o (V)acío de los 34 objetivos de control de alto nivel, así como una relación de cuales recursos de TI son aplicables.



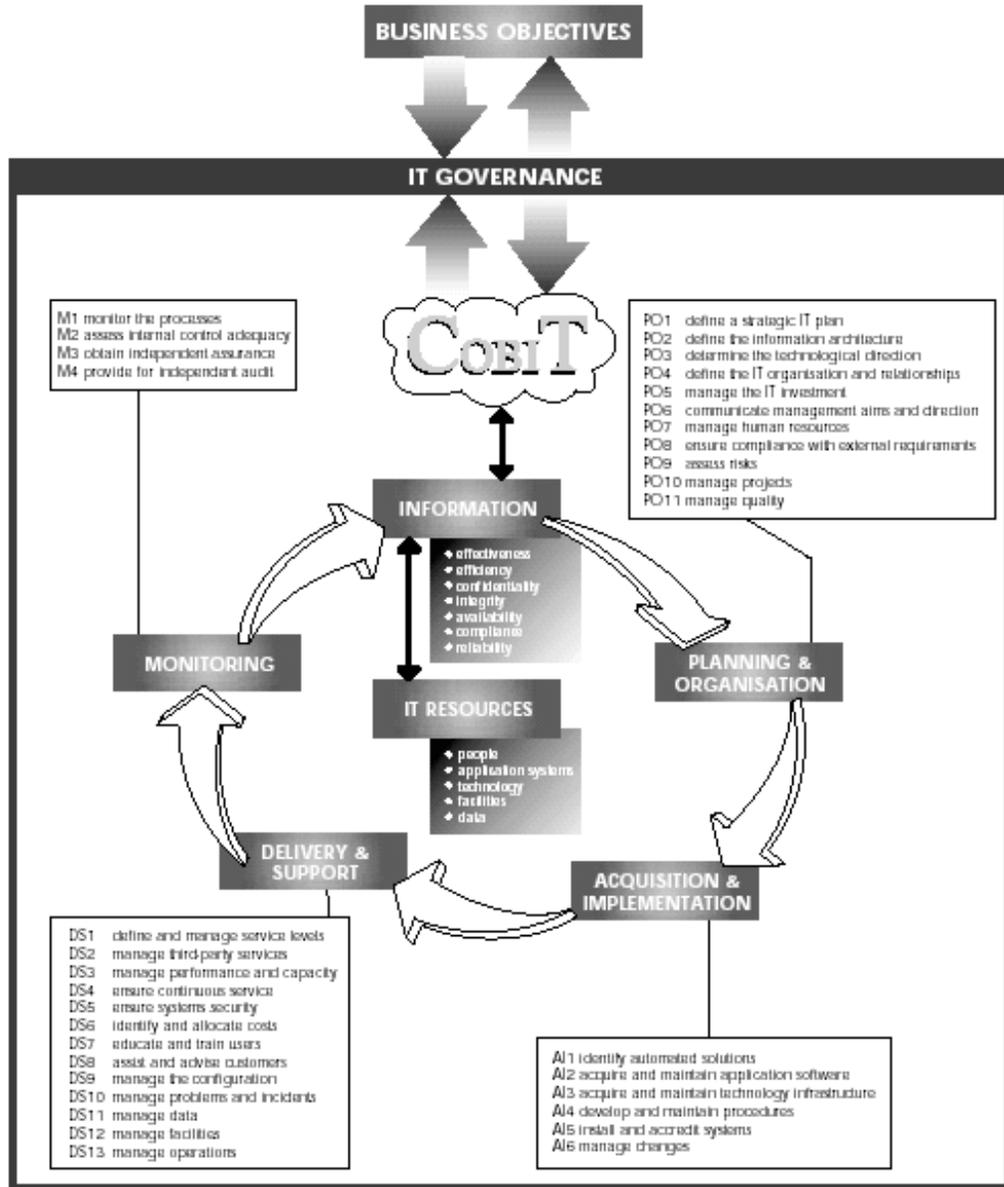
## Estructura COBIT (ob. cit.)

En resumen, la estructura conceptual de *COBIT* se enfoca desde tres puntos de vista: (a) los recursos de las TI, (b) los criterios empresariales que deben satisfacer la información y (c) los procesos de TI.

Estos tres puntos estratégicos constituyen las dimensiones conceptuales de la estructura *COBIT* y se muestran en el **Gráfico 6**, conocido como Cubo *COBIT*, y en el **Gráfico 7**, que presenta su estructura global con los procesos de TI definidos dentro de los cuatro dominios de agrupación natural de estos procesos.



**Gráfico 6. Cubo COBIT. Dimensiones Conceptuales de COBIT.**  
Fuente: Marco Referencial COBIT. ISACF(2000)



**Gráfico 7: Procesos de TI definidos dentro de los Cuatro Dominios y su relación con los Criterios de Información y los Recursos de TI.**

*Fuente:* Marco Referencial COBIT. ISACF(2000)

## Guías de Auditoría COBIT (ob. cit.)

Conjunto de pautas para analizar, valorar, apreciar, interpretar, reaccionar e implementar procesos que permitan alcanzar las metas y objetivos mediante la auditoría constante y consistente de los procedimientos. Las Guías de Auditoría perfilan, esbozan y sugieren actividades para desarrollar auditoría de cada uno de los 34 Objetivos de Control de Alto Nivel, mientras sustentan el riesgo de los objetivos de control no satisfechos. Las guías de auditoría, comprenden fundamentalmente cuatro actividades:

1. **Obtener y comprender:** las actividades del negocio y los controles existentes en el lugar de ejecución. Para ello deben realizarse entrevistas a los gerentes apropiados y al personal de staff para obtener y comprender: (a) Los requerimientos del negocio y los riesgos asociados, (b) La estructura de la Organización, (c) Los roles y responsabilidades, (d) Las políticas y procedimientos, (e) Leyes y regulaciones, (f) Medidas de control en el sitio, (g) Informes gerenciales, (h) Indicadores Claves de Desempeño (**KPI**: Key Performance Indicators).
2. **Evaluar los Controles:** (a) valorar la efectividad o grado en el cual el objetivo de control es alcanzado. Básicamente decidiendo que, en que caso y como evaluarlo. (b) Evaluar la medida de control para los procesos objeto de estudio identificando los criterios y mejores prácticas estándares de la industria, Factores Críticos de Éxito (**CSF**: Critical Success Factors) de las medidas de control y aplicación de juicios de auditoría profesional.
3. **Conformidad de valoración:** (a) asegurar que las medidas de control establecidas corresponden a la prescripción consistentemente y continuamente y concluir sobre el apropiado ambiente de control. (b) Obtener directa o indirectamente evidencia para los ítems y periodos que aseguren que los procedimientos han sido cumplidos. (c) Determinar el nivel de pruebas sustantivas y trabajo adicional requerido para asegurar que los procesos de TI son adecuados a los objetivos del negocio.

4. **Confirmar y verificar riesgos:** (a) desarrollar la confirmación del riesgo del objetivo de control no cumplido por el uso de técnicas analíticas y/o fuentes alternativas de consulta. El objetivo es soportar la opinión y promover a la gerencia para la acción. (b) Los auditores deben ser creativos en encontrar y presentar la información sensitiva y confidencial. (c) Documentar la debilidad de los controles, amenazas y vulnerabilidades. (d) Identificar y documentar el actual y potencial impacto de los riesgos asociados.

### **Definición de Términos**

**AICPA** Instituto Americano de Contadores Públicos Certificado. (*American Institute of Certified Public Accountants*)

**CCEB** Criterios comunes para seguridad en tecnología de información. (*Common Criteria for Information Technology Security*)

**CICA** Instituto Canadiense de Contadores. (*Canadian Institute of Chartered Accountants*)

**CISA** Auditor Certificado de Sistemas de Información. (*Certified Information Systems Auditor*)

**COSO** Comité de Organizaciones Patrocinadoras de la Comisión de Intercambio. "Tradeway" (*Committee of Sponsoring Organisations of the Tradeway Commission*).

**DRI** Instituto Internacional de Recuperación de Desastres. (*Disaster Recovery Institute International*)

**DTI** Departamento de Comercio e Industria del Reino Unido. (*Department of Trade and Industry of the United Kingdom*)

**EDIFACT** Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria (*Electronic Data Interchange for Administration, Commerce and Trade*)

**EDPAF** Fundación de Auditores de Procesamiento Electrónico de Datos (*Electronic Data Processing Auditors Foundation*), ahora **ISACF**.

**ESF** Foro Europeo de Seguridad (*European Security Forum*), cooperación de 70+ multinacionales europeas principalmente con el propósito de investigar problemas de seguridad y control comunes de TI.

**GAO** Oficina General de Contabilidad de los EUA. (*U.S. General Accounting Office*)

**I4** Instituto Internacional de Integridad de Información. (*International Information Integrity Institute*), asociación similar a ESF, con metas similares, pero con base principalmente en los Estados Unidos y dirigida por el Instituto de Investigaciones de Stanford (*Stanford Research Institute*)

**IBAG** Grupo Consultivo de Negocios Infosec (*Infosec Business Advisory Group*), representantes de la industria que asesoran al Comité Infosec. Este Comité está compuesto por funcionarios de los gobiernos de la Comunidad Europea y asesora a la Comisión Europea sobre cuestiones de seguridad de TI.

**IFAC** Federación Internacional de Contadores. (*International Federation of Accountants*)

**IIA** Instituto de Auditores Internos. (*Institute of Internal Auditors*)

**INFOSEC** Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (*Advisory Committee for IT Security Matters to the European Commission*)

**ISACA** Asociación para la Auditoría y Control de Sistemas de Información. (*Information Systems Audit and Control Association*)

**ISACF** Fundación para la Auditoría y Control de Sistemas de Información. (*Information Systems audit and Control Foundation*)

**ISO** Organización de Estándares Internacionales. (*International Standards Organisation*)

**ISO9000** Estándares de manejo y aseguramiento de la calidad definidos por ISO.

**ITIL** Biblioteca de Infraestructura de Tecnología de Información. (*Information Technology Infrastructure Library*)

**ITSEC** Criterios de Evaluación de Seguridad de Tecnología de Información (*Information Technology Security Evaluation Criteria*). Combinación de los criterios de Francia, Alemania, Holanda y Reino Unido, soportadas consecuentemente por la Comisión Europea (ver también TCSEC, el equivalente en los Estados Unidos).

**NBS** Departamento Nacional de Estándares de los Estados Unidos (*National Bureau of Standards of the U.S.*)

**NIST (antes NBS)** Instituto Nacional de Estándares y Tecnología. (*National Institute of Standards and Technology*), con base en Washington D.C.

**NSW** Nueva Gales del Sur, Australia. (*New South Wales, Australia*)

**OECD** Organización para la Cooperación y el Desarrollo Económico. (*Organisation for Economic Cooperation and Development*)

**OSF** Fundación de Software Público (*Open Software Foundation*)

**PCIE** Consejo Presidencial de Integridad y Eficiencia. (*President's Council on Integrity and Efficiency*)

**TCSEC** Criterios de Evaluación de Sistemas Computarizados Confiables. (*Trusted Computer System Evaluation Criteria*), conocido también como "*The Orange Book*". Criterios de evaluación de seguridad para sistemas computarizados definidos originalmente por el Departamento de Defensa de los Estados Unidos. Ver también ITSEC, el equivalente europeo.

**TickIT** Guía para la Construcción y Certificación de Sistemas de Administración de Calidad. (*Guide to Software Quality Management System Construction and Certification*)

## **CAPITULO III**

### **MARCO METODOLOGICO**

#### **Tipo de Investigación**

El estudio que se realizará consiste en una investigación que se ubica en la modalidad conocida como Proyecto Factible, la cual según Barrios (1998), consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo, en este caso, modelo metodológico, viable para la solución de problemas, requerimientos o necesidades de organizaciones o grupos sociales; referido a la formulación de políticas, programas, tecnologías, métodos o procesos. Estos aspectos serán cubiertos en el ambiente de aplicación de Sistemas de Información y las Tecnologías Relacionadas con los procesos de información en las organizaciones actuales.

#### **Diseño de la Investigación**

El diseño de la investigación es considerado por Balestrini (1998:118) como "... el plan global que integra de un modo coherente y adecuadamente correcto, técnicas de recogidas de datos a utilizar, análisis previstos y objetivos...". Esta investigación se sustenta en fuentes mixtas por originarse en investigación documental (referencias de materiales impresos y de información publicada en paginas web, documentos y/o bibliografía existente que sirven de base al estudio y al fundamento teórico, principalmente toda la información relacionada con las publicaciones *COBIT*) y de campo (a través de la cual se adquieren conocimientos y datos que no están plasmados en ninguna bibliografía sino que se obtienen estando en

el lugar donde se desarrollaran las actividades, procesos o hechos que fundamentan los conocimientos empíricos).

La investigación documental se centra en el estudio del problema de control de la información y las tecnologías que la soportan dentro de las organizaciones. La investigación de campo esta centrada en el análisis sistemático del problema en una organización específica; en este estudio se tomará como representante de la realidad a la empresa Banco Sofitasa, con el propósito de interpretar el problema del control de la información en sus procesos, haciendo uso de métodos de diagnostico y evaluación relacionados con la estructura *COBIT*.

## **Población**

Una población es definida por Martínez (2000: 711) como "...conjunto de unidades o elementos que representan una característica común". En este caso de estudio, la población esta representada por los niveles directivos de la más alta gerencia en materia de Tecnología de Información y Auditoría de Sistemas dentro de la Organización objeto de estudio. Esto representa en cierta forma una limitante para el levantamiento de información pero también asegura la calidad de la información recogida por cuanto los usuarios propietarios de los datos requeridos para la investigación representan a su vez las unidades organizacionales que gobiernan la tecnología de información y su evaluación, seguridad y control. La naturaleza de los cargos gerenciales determina una confidencialidad particular de los datos de los procesos a estudiar, por su acceso restringido y su valor estratégico y funcional. Esto determina que la población objeto de estudio este limitada a un número muy reducido de personas por la jerarquía de su ubicación dentro de la organización; las unidades organizacionales hacia las cuales esta orientada la aplicación de las técnicas de recolección de datos son la Vicepresidencia de Tecnología y la Gerencia de Auditoría de Sistemas del Banco Sofitasa, sede San Cristóbal, Estado Táchira. El personal autorizado para suministrar los datos esta limitado a los cargos directivos en cada una de las áreas seleccionadas lo cual no excede las 3 o 4 personas, a lo sumo 2 por cada

área, los cuales no suministrarán los datos en forma independientemente sino lo harán en un *workgroup* para suministrar información de consenso sobre los importantes aspectos de *Gobierno de TI*.

## **Muestra**

Una muestra es definida por Martínez (2000:715) como “...una parte de la población o subconjunto de elementos que resulta de la aplicación de algún proceso, generalmente de selección aleatoria, con el objeto de investigar todas o parte de las características de estos elementos.”

Por las características expuestas para la población en estudio, el muestreo aleatorio o probabilístico no tiene aplicación, dado el reducido tamaño de la población, la cual además, unida en un *workgroup*, representa una unidad homogénea de información consensuada; en consecuencia, se opta por aplicar los instrumentos de recolección de datos al grupo directivo como una sola unidad de información tomada como muestra bajo el enfoque de opinión de expertos, en este caso directivos de Tecnología de Información en la organización objeto de estudio, en cuyo caso se le da un tratamiento de censo, definido por Martínez (2000:714) como “la enumeración total de una población en un tiempo dado”

## **Técnicas e Instrumentos de Recolección de Datos**

Las técnicas de recolección de datos son distintas formas o maneras de obtener la información, son ejemplos de técnicas; la observación directa, la encuesta en sus dos modalidades (entrevista o cuestionario), el análisis documental, análisis de contenido entre otras. Los instrumentos según Perdomo (1983:20) “... son el conjunto de elementos o medios de que se sirve el investigador en búsqueda del conocimiento”. Los instrumentos de recolección de datos son los medios materiales que se emplean para recoger y almacenar la información, son ejemplos de

instrumentos; los formatos de cuestionario, guías de entrevista, listas de cotejo (checklist), entre otros.

En el presente estudio, se emplean el análisis documental y de contenidos de las referencias bibliográficas y en línea para la sustentación de las bases teóricas de interés para la investigación. En el estudio de campo dentro del Banco Sofitasa, específicamente en la Vicepresidencia de Tecnología, se desarrollaron entrevistas y se aplicaron cuestionarios en el grupo de trabajo bajo los formatos estructurados de listas de cotejo. La entrevista según Tamayo y Tamayo (1986:117) es la “Obtención directa de respuestas de un sujeto por parte del investigador, el cual las anota”, la entrevista es del tipo estructurada, ya que facilita la comunicación entre el investigador y el entrevistado a través de la aplicación de un cuestionario predefinido organizado en forma de listas de chequeo o comprobación, de esta forma se obtienen datos directos de las personas que forman parte del proceso, debido a que se tienen preguntas previamente formuladas. Las listas de cotejo o técnicamente como son conocidas en el ámbito de la Auditoría Informática, checklist, son instrumentos estructurados que permitirán valorar las respuestas por pesos de preguntas en escala o por valores duales o binarios (dicotómicos) para obtener de forma más precisa los valores de las variables del estudio.

Para la recolección de datos se han utilizado tres instrumentos denominados: (a) “Checklist para Identificar las Necesidades de Servicios en Evaluación y Auditoría de Información y Tecnologías Relacionadas” (Anexo A), (b) “Autoevaluación del Gobierno de los Procesos de Tecnología de Información” (Anexo B), y (c) “Matriz de Evaluación de Procesos de Tecnología de Información y Grupos de Riesgos Asociados” (Anexo C). El primer instrumento tiene como objetivo determinar un análisis diagnóstico de la situación actual de la organización respecto al requerimiento de servicios de evaluación y auditoría de la información y las tecnologías relacionadas. El segundo permite valorar la importancia o relevancia de los 34 procesos *COBIT* y su desempeño en alineación con los objetivos del negocio. Estos valores de relevancia y desempeño, permiten establecer una relación de riesgo de cada proceso; a su vez se identifica por cada proceso, la unidad organizacional

ejecutora, el estado de auditoria y la formalidad estructurada del proceso. El tercer instrumento tiene por finalidad verificar la correspondencia o afinidad de los riesgos estimados por el negocio para los procesos *COBIT* y la clasificación estándar de los grupos de riesgos establecidos por las mejores practicas en materia de evaluación de riesgos.

### **Análisis e Interpretación de los Datos**

Los datos y/o información que se recopiló con la aplicación de las técnicas e instrumentos se organizaron y codificaron para su análisis e interpretación según el tipo de cada uno de ellos; en el caso de las checklist, los datos se clasifican de acuerdo a la categoría de contenido y/o tipo de pregunta, asignándosele una calificación o cuantificación según el tipo de dato. En el caso de las matrices de evaluación, algunos ítems se valoran por respuestas en escala numérica de (1-5) y otros por valores ambivalentes o binarios tipo marcaje X.

En las entrevistas de aplicación de los instrumentos, además de llevar el control de las respuestas del grupo de trabajo entrevistado, también se anotaron los comentarios y observaciones que pudieron realizar los integrantes del grupo de expertos, según su experiencia, afinidad y conocimiento del tema, para posteriormente contrastar la información estructurada con la información complementaria y enriquecer el contexto de aplicación del análisis situacional. Complementariamente, el estudio diagnostico se enriqueció con información proveniente de documentos de la organización pertinente sobre normas, procedimientos, políticas de seguridad y control de la información y las tecnologías relacionadas.

Específicamente, el análisis de cada uno de los instrumentos aplicados permitió obtener los siguientes resultados clasificados por categorías de contenido y áreas de interes. En el Instrumento 1, "*Checklist para Identificar las Necesidades de Servicios de Evaluación y Auditoria de Información y Tecnologías Relacionadas*", se clasifican los contenidos en las siguientes categorías de datos:

1. **Recurso Humano asignado al área de IT:** 40 personas clasificadas como tecnólogos, ingenieros, especialistas en telecomunicaciones y otros como operadores, transcritores y personal de apoyo; lo que permite definir a la organización como de tamaño medio respecto a la función de IT.
2. **Plataformas de Hardware y Software:** 4 plataformas de sistemas operativos interconectadas en red, 3 motores de bases de datos, 500 equipos activos de red, servicio de Internet con acceso controlado por perfil de usuario e Intranet para mensajería interna, servidor Exchange de correo electrónico, Firewalls ubicados en diferentes segmentos de la red, 8 servidores de archivos, 2 Mainframes, 500 Microcomputadoras y un Data Warehouse en implementación en la actualidad. Esta arquitectura de Hardware y Software determina que en la organización hay una *alta complejidad* de los procesos de TI.
3. **Sistemas de Información y Aplicaciones:** principalmente cabe resaltar aquí, los 3 grandes sistemas y sus módulos componentes principales, (a) SIAF – Sistema Integral de Administración Financiera, con los módulos de Crédito, Contabilidad, Fideicomiso, Cuentas Corrientes, Cuentas de Ahorro, Cobranza y Política Habitacional -, (b) UNICARD – Sistema de Tarjetas de Crédito -, y (c) SBE – Sistema de Cajeros Automáticos-. Se observa aquí, la relevancia de los sistemas de gestión financiera por la propia naturaleza de la organización que define los objetivos del negocio.
4. **Portafolio de Aplicaciones en Producción y su Importancia:** Esta categoría de datos se valora bajo tres aspectos y modalidades: relevancia (1-Menor relevancia, 5-Mayor), Herramientas de Desarrollo, y existencia de programas fuentes. Los resultados obtenidos permiten determinar en el primer aspecto que todas las aplicaciones son de relevancia para la organización ubicadas en el rango 4 y 5 (Alta importancia, es obvio que de ellas depende la información sensitiva del negocio), en el segundo aspecto se observa que aproximadamente el 66 % de las aplicaciones son desarrolladas en OS/400 y el resto 34% en LINC, esto favorece la

estandarización y compatibilidad de los procesos porque no hay múltiples herramientas de desarrollo. En el tercer aspecto, todas las aplicaciones poseen programas fuentes, lo que significa un aseguramiento de los procesos de mantenimiento de aplicaciones y ausencia de riesgos por procesos de “*caja negra*”, sin conocimiento de código lógico.

5. **Actividades de Procesamiento de Datos:** Esta categoría de datos, de valor ambivalente (marcaje X) permite conocer que en la organización, todas las actividades de procesamiento de datos se desarrollan o ejecutan y que todo el ciclo de aseguramiento de procesos se toma en cuenta, garantizando la continuidad de las operaciones, a saber: (a) Captura de datos, (b) Control de entradas y salidas, (c) Proceso y actualización de archivos, (d) Ayuda de escritorio, (e) Soporte a usuarios, (f) Mantenimiento de hardware, (g) Administración de bases de datos, (h) Administración de seguridad lógica, (i) Planeación estratégica de sistemas, (j) Administración de contratos con terceros, (k) Definición e implementación de políticas de seguridad corporativas, (l) Análisis y diseño de sistemas, (m) Construcción de programas, (n) Mantenimiento de aplicaciones y (o) Aseguramiento de la calidad. El cumplimiento de todas estas actividades reduce la vulnerabilidad de los procesos a eventuales riesgos, quedando pendiente la valoración de cada una de estas actividades.
6. **Servicios Contratados con Terceros:** De las 16 actividades o servicios de procesamiento de datos enumeradas en el punto anterior, solo 3 son desarrolladas con participación de terceros externos (Outsourcing) (a) Mantenimiento de hardware, (b) Programación de aplicaciones, y (c) Planeación de contingencias en sistemas de información, es decir solo el 18,75% de los procesos; estas actividades son controladas por procedimientos internos documentados y estructurados lo que reduce la vulnerabilidad de riesgos.
7. **Servicios de Control Interno y Seguridad de Sistemas de interés:** Según los datos obtenidos en esta categoría, se determina el interés de la dirección

de TI y la dirección de Auditoría de Sistemas de la organización en los servicios de (a) Asesoría para la implantación de estándar COBIT (Control Objectives for Information and Related Technology), (b) Aseguramiento de la calidad del software, y (c) Capacitación en controles y seguridad en sistemas de información. Esta opinión evidencia el requerimiento de la organización en el conocimiento y aplicación de estándares y las mejores prácticas en materia del gobierno de las TI en alineación con los procesos del negocio.

8. **Servicios de Auditoría de Sistemas de interés:** Las respuestas en esta categoría de datos, están en concordancia con las del punto anterior y complementan la justificación del requerimiento de la organización en los servicios de (a) Auditoría al plan de contingencias de sistemas de información (Aseguramiento de la continuidad del negocio) y (b) Asesoría para implantar el enfoque de Auditoría de Sistemas orientada al riesgo.

En el Instrumento 2, “*Autoevaluación del Gobierno de los Procesos de Tecnología de Información*”, se clasifican los contenidos en las categorías definidas por *COBIT* para los 4 dominios y los 34 procesos (Objetivos de Control de Alto Nivel) organizando los datos en 4 grupos de parámetros de evaluación por cada proceso: (a) Pesos de Relevancia y Desempeño, (b) Unidad Organizacional Ejecutora del Procesamiento, (c) Estado del Proceso respecto a Auditoría y Formalización, y (d) Unidad Organizacional Responsable del Gobierno del proceso. Cada uno de los 4 parámetros suministra información particular sobre el diagnóstico situacional de los procesos de TI en alineación con los objetivos del negocio de la Organización. Cada parámetro es evaluado de forma particular y combinada. A continuación se exponen los criterios de evaluación de cada grupo de parámetros y los resultados obtenidos:

1. **Relevancia y Desempeño:** particularmente, la relevancia mide la calidad o condición de importancia y significación del proceso de TI en función de su contribución al logro de los objetivos del negocio. Cada proceso es autoevaluado en la escala de (1 – 5) siendo la interpretación cualitativa de

los valores de este rango, la mostrada en el **Cuadro 3**. Particularmente, el desempeño mide el nivel y calidad de cumplimiento (performance) esperado de la ejecución del proceso de TI en el rango (0 – 5), siendo la interpretación la mostrada en el **Cuadro 4**.

### **Cuadro 3**

#### **Valoración de relevancia de los procesos de TI**

<b>Relevancias</b>	
<b>Relevancia</b>	<b>Descripción</b>
1	No Relevante
2	Poco Relevante
3	Medianamente Relevante
4	Relevante
5	Muy Relevante

*Fuente:* propia

### **Cuadro 4**

#### **Valoración del desempeño de los procesos de TI**

<b>Desempeños</b>		
<b>Desempeño</b>	<b>Descripción</b>	<b>Comentario</b>
0	No existe	Proceso no Aplicado o no Definido
1	Inicial	Proceso Ad-hoc y Desorganizado
2	Regular	Proceso Rutinario de Curso Regular
3	Definido	Proceso Documentado y Comunicado
4	Gerenciado	Proceso Monitoreado y Evaluado
5	Optimizado	Proceso bajo las Mejores Practicas y Automatizado

*Fuente:* propia (enfoque de valoración basado en el modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software)

En forma combinada, estos dos valores, relevancia y desempeño, permiten estimar un indicador de fortaleza o debilidad respecto a la vulnerabilidad de riesgo del proceso. Por ejemplo, un proceso valorado con relevancia 5 (muy

relevante) y con desempeño 3 (apenas documentado y comunicado, no monitoreado ni evaluado, no ejecutado bajo las mejores prácticas) es un proceso altamente vulnerable con un alto indicador de riesgo. En cambio, un proceso con relevancia 2 o 3 (poco o medianamente relevante) y desempeño 3 (definido) es un proceso estable, muy poco vulnerable a riesgos. De acuerdo con este análisis valorativo de relevancia y desempeño se obtuvieron los resultados por Dominio *COBIT* presentados en el **Cuadro 5**.

### Cuadro 5

#### Evaluación del Gobierno de los Procesos de TI por Dominio

PROCESOS	REL.	DES.	RIESGO
<b>DOMINIO: PO – Planificación y Organización (11 Procesos)</b>			
5: PO2,PO3,PO9,PO10,PO11	4	4	1 : Moderado
3: PO4,PO5,PO7	4	5	1,25: Bajo
1: PO1	5	3	<b>0,6: Alto (*)</b>
1: PO8	5	4	<b>0,8: Alto</b>
1: PO6	5	5	1: Moderado
<b>DOMINIO: AI – Adquisición e Implementación (6 Procesos)</b>			
6: Todos	4	4	1: Moderado
<b>DOMINIO: DS – Entrega y Soporte (13 Procesos)</b>			
1: DS6	4	3	<b>0,75: Alto</b>
9: DS1,DS5,DS7 a DS13	4	4	1: Moderado
1: DS2	4	5	1,25: Bajo
1: DS4	5	4	<b>0,8: Alto</b>
1: DS3	5	5	1: Moderado
<b>DOMINIO: M – Monitoreo (4 Procesos)</b>			
4: Todos	4	4	1: Moderado

*Nota: Fuente Propia. Datos tomados del Instrumento No. 2.* Los procesos identificados por su nomenclatura COBIT son agrupados y contados en cada dominio por grupos de puntajes de Relevancia y Desempeño iguales. El riesgo autoevaluado se estima como la razón entre el desempeño y la relevancia: < 1: Alto, 1: Moderado, > 1: Bajo.

De acuerdo con los datos obtenidos en el Cuadro 5, puede observarse que la autoevaluación determina al proceso PO1: Planificación y Organización como el proceso más crítico con riesgo Alto, con la mayor relevancia (5) y el menor desempeño (3). Complementariamente, deben considerarse otros indicadores de vulnerabilidad de riesgo como la provisión o ausencia de auditoría (interna y/o externa) del proceso y el grado de formalización del

proceso (existencia de contratos, convenios, acuerdos de niveles de servicio, documentación formal).

2. **Procesamiento:** esta categoría de contenido en el Instrumento 2, permite determinar la Unidad Ejecutora del Proceso de TI entre las unidades de Tecnología, Otras unidades, Terceros o No Informado obteniéndose los siguientes resultados:

### Cuadro 6

#### Unidades Ejecutoras de Procesos de TI

DOMINIOS	PROC.	TI	OTR.	EXT.
PO: Planificación y Organización	11	11	4	1
AI: Adquisición e Implementación	6	6	2	3
DS: Entrega y Soporte	13	13	5	3
M: Monitoreo	4	4	2	1
<b>Total Procesos Ejecutados</b>	<b>34</b>	<b>34</b>	<b>13</b>	<b>6</b>

*Nota: Fuente Propia. Datos tomados del Instrumento No. 2.* Los 34 procesos definidos por COBIT son ejecutados con participación directa de la Vicepresidencia de TI, El procesamiento de 13 procesos es compartido con otras unidades y 6 procesos comparten su ejecución con terceros externos.

Puede observarse en esta categoría de datos que la Vicepresidencia de Tecnología ejecuta todos los procesos y comparte la ejecución con las unidades usuarias en los procesos PO7 a PO10, AI5, AI6, DS1, DS3 a DS6, M1 y M2, particularmente estos dos últimos con la Gerencia de Auditoría de Sistemas. Los procesos ejecutados por terceros son PO4, “Definición de la Organización y de las relaciones de TI”, que merece una referencia especial por cuanto en la actualidad, el Banco Sofitasa, adelanta estudios sobre la alineación del negocio con la estrategia de TI a través de procesos de Outsourcing con firmas especializadas en consultoría del área. El análisis de la ejecución de procesos permite observar que en la organización existe una conciencia especial respecto al valor de aplicación del concepto de Gobierno de TI.

3. **Estado:** en esta categoría de contenido del Instrumento 2, se evidencia la aplicación de procedimientos y programas de Control Interno en todos los procesos de TI (Auditoría Interna) y solo 9 procesos poseen o han recibido Auditoría Externa, lo cual deja una brecha o vacío importante en la aplicación de procedimientos de Evaluación y Auditoría bajo enfoques de Gobierno de TI por parte de terceros que puedan apreciar con objetividad el estado actual de la Organización en estos procesos. Finalmente, en esta categoría, se obtiene información sobre el estado de formalización del

proceso, determinándose qué de los 34 procesos, solo 24 poseen documentación formal. En el caso de procesos que hayan sido valorados con Relevancia (4 o 5), la ausencia de formalización implica un alto grado de vulnerabilidad de riesgos, mayor aún cuanto más bajo sea la valoración del desempeño; según esta relación los procesos PO1: “Definición de un plan estratégico de TI y DS6: “Identificación e imputación de Costos”, no formalizados y con (5,3) y (4,3) de Relevancia y Desempeño respectivamente representan los Procesos de TI (Objetivos de Control de Alto Nivel) de estado crítico respecto al riesgo, y por lo tanto, los procesos sobre los que habría que apuntalar procedimientos de Evaluación y Auditoría. Los valores obtenidos se representan a continuación:

### Cuadro 7

#### Estado de los Procesos de TI respecto a Auditoría y Formalización

<b>DOMINIOS</b>	<b>PROC.</b>	<b>AUI</b>	<b>AUE</b>	<b>FOR.</b>
PO: Planificación y Organización	11	11	1	7
AI: Adquisición e Implementación	6	6	3	5
DS: Entrega y Soporte	13	13	2	8
M: Monitoreo	4	4	3	4
<b>Totales:</b>	<b>34</b>	<b>34</b>	<b>9</b>	<b>24</b>

*Nota: Fuente Propia. Datos tomados del Instrumento No. 2. Todos los procesos tienen Auditoría Interna, solo 9 han recibido Auditoría Externa y hay 24 procesos formalizados. En el dominio PO, uno de los procesos no formalizados es el PO1 y en el dominio DS, no está formalizado el proceso DS6.*

- 4. Responsables del Gobierno de TI:** en esta categoría de contenido del Instrumento 2, se identifican los responsables del Gobierno de TI para cada uno de los procesos y de acuerdo con los resultados puede calcularse la distribución de responsabilidad de los procesos de TI en las unidades organizacionales responsables, obteniéndose los resultados por dominio presentados en el **Cuadro 8**.

## Cuadro 8

### Unidades responsables del Gobierno de TI

Unidades Responsables	PO	AI	DS	M	TOT.
Dirección Ejecutiva	2				2
Gerencia de TI	6	5	10		21
Gerencia de Auditoria de Sistemas	1	1	1	4	7
Gerencia de Recursos Humanos	1				1
Gerencia de Seguridad			2		2
Gerencia de Riesgos	1				1
<b>TOTALES</b>	<b>11</b>	<b>6</b>	<b>13</b>	<b>4</b>	<b>34</b>

*Nota: Fuente Propia. Datos tomados del Instrumento No. 2. Distribución de responsabilidad del Gobierno de TI para los 34 procesos COBIT.*

De estos resultados se determina que el 61.7 % del Gobierno de los procesos de TI, son responsabilidad de la Vicepresidencia de TI, el 20.5 % son responsabilidad de la Gerencia de Auditoria de Sistemas, la Dirección Ejecutiva y la Gerencia de Seguridad, cada una con el 6% y un 2.9% para la Gerencia de Riesgos y la Gerencia de Recursos Humanos.

Con el Instrumento 3, “*Matriz de Evaluación de Procesos de Tecnología de Información y Grupos de Riesgos Asociados*” se encuentra una ratificación por parte de la dirección de tecnología del Banco Sofitasa, de la clasificación establecida por las referencias *COBIT* para los 34 procesos y los grupos de riesgos asociados. Lo importante aquí, es poder establecer la relación específica entre los procesos PO1 y DS6, diagnosticados como los procesos con más alta vulnerabilidad de riesgo, y los riesgos particulares asociados a estos procesos. Estas relaciones se presentan en el **Cuadro 9**.

**Cuadro 9.**

**Riesgos asociados a los Procesos PO1 y DS6 por Grupo de Riesgos**

PROCESO	DIRECCION					INTER/INTRA					SOLUCIONES					CLIEN/SERV.							
Número > de Riesgo	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
<b>PO1</b>	X		X										X		X			X		X			X
<b>DS6</b>					X																		

*Nota: Fuente Propia. Datos tomados del Instrumento No. 3. Abstracción de los riesgos asociados a los procesos PO1 y DS6, determinados como más vulnerables en la autoevaluación diagnóstica del Gobierno de TI.*

De acuerdo con los resultados de la autoevaluación del Gobierno de TI para los procesos definidos por COBIT y los grupos de riesgos asociados se determinan las siguientes relaciones:

- Riesgos del Proceso PO1:** (a) De Dirección, 01- Iniciativas de TI alineadas con la estrategia del negocio, 03 - Utilización de la TI para obtener ventajas competitivas; (b) De Soluciones Empresariales, 13 – Fracaso al alcanzar los requerimientos de usuario, 15 - Incompatibilidad con la infraestructura técnica; y (c) De Arquitectura Cliente / Servidor, 18 - Fracaso en los requerimientos de coordinación, 20 - Incompatibilidad con la infraestructura técnica, 23 - Elevados costos de propiedad.
- Riesgos del Proceso DS6:** (a) De Dirección, 05 - Reducción de costos de la propiedad de TI; y (b) De Soluciones Empresariales, 17 - Implementación costosa/compleja.

## CAPITULO IV

### **PROPUESTA: MODELO METODOLOGICO DE EVALUACION Y AUDITORIA DE INFORMACION Y TECNOLOGIAS RELACIONADAS**

#### **Definición del Modelo Metodológico.**

El Modelo Metodológico de Evaluación y Auditoría de Información y Tecnologías Relacionadas considera la definición y aplicación de los siguientes elementos:

1. El Marco Referencial COBIT (*COBIT Framework*) con capacidad definible de relaciones abiertas entre los elementos: procesos, requerimientos o criterios de información y recursos de TI.
2. El conjunto de Objetivos de Control Específicos relacionados con el Marco Referencial *COBIT*.
3. El conjunto de las Guías de Auditoría *COBIT* por Objetivo de Control de Alto Nivel.
4. El Plan de Evaluación y Auditoría definido por el usuario del modelo.
5. Los alcances a ser cubiertos por el proceso de Evaluación y Auditoría.
6. La evaluación de los procesos (Objetivos de Control de Alto Nivel).
7. La evaluación de los Objetivos de Control Específicos detallados por proceso.
8. La información detallada resultado de la aplicación de las Guías de Auditoría por proceso que sustentan el Informe de Evaluación y Auditoría.
9. La opinión del Auditor sobre la aplicación y resultados del Plan de Evaluación y Auditoría con las observaciones y recomendaciones.
10. La emisión del Informe de Evaluación y Auditoría.

Para la definición del Modelo Metodológico de Evaluación y Auditoría de Información y Tecnologías Relacionadas, a continuación se detalla cada uno de los elementos enumerados anteriormente; luego se presenta un esquema general de la aplicación del modelo propuesto reflejando con un diagrama de Flujo de Datos, los diferentes procesos, entidades interfaces, almacenes de datos y flujos de datos. Seguidamente, se presentan el diseño lógico conceptual de la aplicación de software propuesta para la ejecución y validación del modelo con datos de prueba para el Dominio PO: Planificación y Organización, proceso PO1: Definición de un Plan Estratégico de TI.

### **Elementos del Modelo**

1. **Marco Referencial COBIT (COBIT Framework).** Como se explicó en las bases teóricas de la presente investigación, el Marco Referencial *COBIT* presentado por ISACF y el IT Governance Institute(2000), es el fundamento teórico y estructural de la presente propuesta de aplicación metodológica. En resumen, se toman en cuenta: (a) 4 Dominios de procesos de TI: 1-PO: Planificación y Organización, 2-AI: Adquisición e Implementación, 3-DS: Entrega y Soporte, 4-M: Monitoreo; (b) 34 Procesos u Objetivos de Control de Alto Nivel organizados por dominio de correspondencia: 1-PO: 11 procesos, 2-AI: 6 Procesos, 3-DS: 13 procesos, M: 4 procesos; (c) 7 criterios de información del negocio: 1-Efectividad, 2-Eficiencia, 3-Confidencialidad, 4-Integridad, 5-Disponibilidad, 6-Cumplimiento, 7-Integridad; y (d) 5 Recursos de TI: 1-Personas, 2-Datos, 3-Aplicaciones, 4-Tecnología, 5-Instalaciones.
2. **Objetivos de Control Detallados por proceso de TI.** Los 318 Objetivos de Control Específicos organizados por cada dominio y proceso *COBIT* son tomados en cuenta dentro de la Base de Conocimiento del modelo. La carta resumen de este conjunto de Objetivos de Control es presentada en el (Anexo D), en el documento titulado *COBIT 3rd. Edition Control*

*Objectives* emitido por el Comité Directivo de COBIT – ISACA y el IT Governance Institute.

3. **Guías de Auditoría COBIT.** Para los efectos de aplicación de los Procedimientos de Auditoría posteriores a la evaluación de los procesos de TI, el modelo contempla la referencia, observación y aplicación de las guías de auditoría organizadas por proceso.
4. **Plan de Evaluación y Auditoría.** El modelo permite definir el Plan de Evaluación y Auditoría a ser desarrollado, indicando el periodo de la auditoría, los usuarios Auditor, Supervisor y Revisor, y las fechas de seguimiento. Este plan permitirá su vinculación con la definición de alcances del proceso de Evaluación y Auditoría.
5. **Alcance del Plan de Evaluación y Auditoría.** El modelo permite definir el alcance, especificando el marco de aplicación del Plan de Evaluación y Auditoría a través de los dominios, procesos (Objetivos de Control de Alto Nivel), criterios de información, recursos de TI por proceso y Objetivos de Control Específicos detallados por proceso.
6. **Evaluación de los procesos (Objetivos de Control de Alto Nivel).** La evaluación de los procesos seleccionados en el alcance, asociados a sus correspondientes dominios, se logra a través de la relación de dos variables denominadas *Relevancia* (mide el grado de significancia e importancia del proceso asignado por consenso entre el Gobierno de TI y el Auditor) y *Desempeño* (valora el grado de desempeño del proceso tomando en cuenta el modelo de madurez para la capacidad de desarrollo de software definido por el Software Engineering Institute. Estas escalas se representan en los **Gráficos 8 y 9**. Analíticamente, el índice de madurez del proceso se calcula mediante la relación (1):

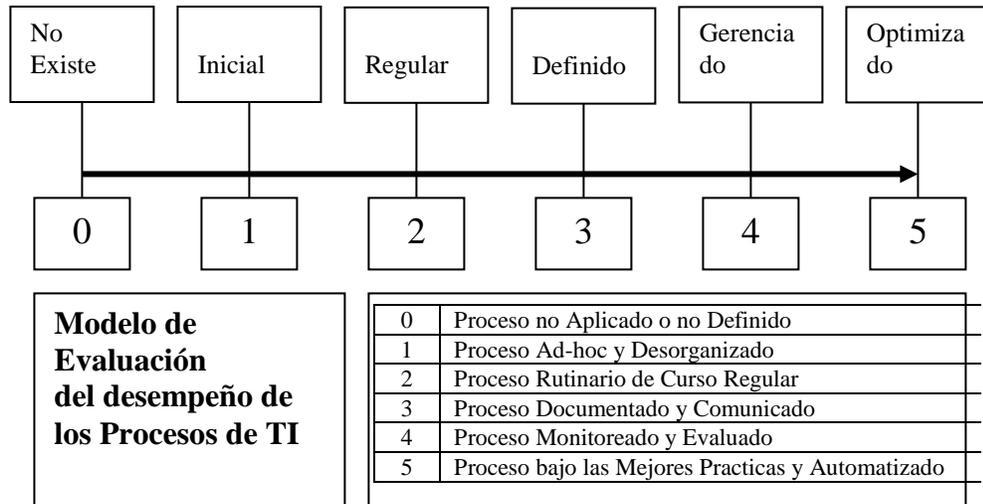
$$(1) \quad IM = D / R$$

Donde el Índice de Madurez (IM), representa una relación directamente proporcional al Desempeño (D) e inversamente proporcional a la Relevancia (R). El dominio de D es [0,5], el dominio de R es [1,5] obteniéndose un rango de [0,5] para IM.

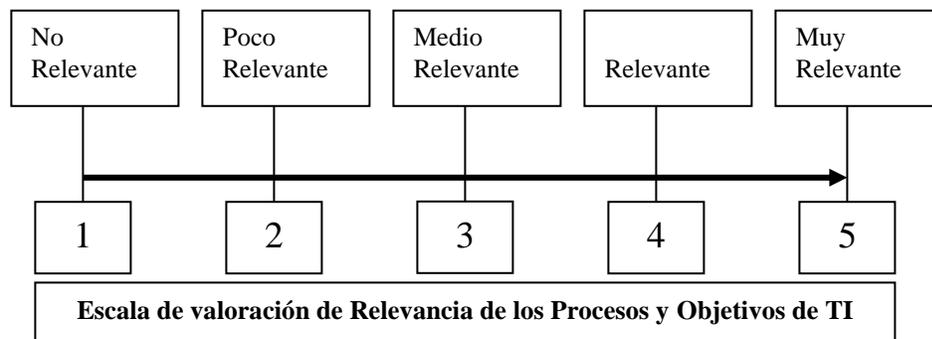
Una vez obtenidos los IM por cada uno de los procesos correspondientes al Dominio evaluado (en caso de la evaluación total del dominio), se obtienen los índices de evaluación del dominio a partir de sus procesos, con las siguientes expresiones analíticas:

- (2)  $SR = \sum R$  (Sumatoria de Relevancias del Dominio)
- (3)  $SRM = 5 * NP$  (Sumatoria de Relevancias Máxima,  
NP: Número de procesos del Dominio)
- (4)  $SD = \sum D$  (Sumatoria de Desempeños)
- (5)  $SDM = 5 * NP$  (Sumatoria de Desempeños Máxima)
- (6)  $IR = SR / SRM$  (Índice de Relevancias)
- (7)  $ID = SD / SDM$  (Índice de Desempeños)
- (8)  $IMD = ID / IR$  (Índice de Madurez del Dominio)
- (9)  $SIM = \sum IM$  (Sumatoria de IM de los procesos  
del Dominio)
- (10)  $PIM = SIM / NP$  (Promedio de IM del Dominio)
- (11)  $MD = PIM * IMD$  (Madurez del Dominio)

Finalmente, de acuerdo con su IM (Formula 1), los procesos del dominio se clasifican en *procesos críticos* (Riesgo Alto) si  $IM < 1$ , *procesos estables* (Riesgo Moderado) si  $IM = 1$ , y *procesos aceptables* si  $IM > 1$ . Cuanto más cerca esté el valor IM de cero, más crítico y mayor vulnerabilidad a riesgos tendrá. Cuanto más sea IM mayor que uno, más aceptable y seguro será respecto a amenazas que generen vulnerabilidad al riesgo. Estas mismas interpretaciones valen para el análisis del valor MD del dominio total.



**Grafico 8:** Escala de evaluación del desempeño de procesos de TI basada en el modelo de madurez definido por el Software Engineering Institute para la capacidad de desarrollo de software.



**Grafico 9:** Fuente propia. Escala de valoración de Relevancia de los procesos y objetivos de TI

7. **Evaluación de los Objetivos de Control Específicos.** La evaluación de los objetivos control específicos detallados por cada proceso seleccionado en el alcance, se obtiene mediante la aplicación de dos variables denominadas *Relevancia* (mide el grado de significancia e importancia del cumplimiento del objetivo de control específico, para el cumplimiento del objetivo de control de alto nivel del proceso) y *Valoración* (asigna el grado de cumplimiento o ausencia del objetivo de control específico para el proceso). La escala de Relevancia es la misma utilizada para la evaluación de los procesos y mostrada en el **Gráfico 9**. La escala para la Valoración se representa en el **Gráfico 10**. Analíticamente, el valor del Índice de Evaluación asociado al objetivo de control esta determinado por el producto:

$$(12) \quad IE = R * V$$

Donde el Índice de Evaluación (IE), representa una relación directamente proporcional a la Relevancia (R) y a la Valoración (V). El dominio de R es [1,5], el dominio de V es [0,1] obteniéndose un rango de [0,5] para IE.

Una vez obtenidos los IE por cada uno de los objetivos correspondientes al proceso evaluado (en caso de la evaluación total del proceso), se obtienen los índices de evaluación del proceso a partir de sus objetivos de control específicos, con las siguientes expresiones analíticas:

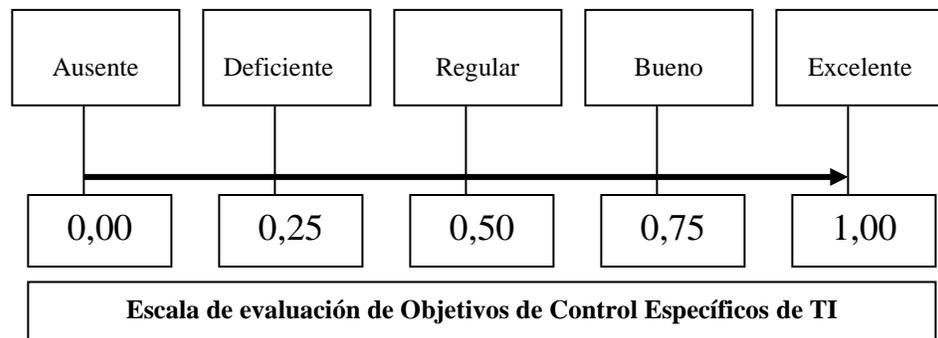
$$(13) \quad SR = \sum R \quad (\text{Sumatoria de Relevancias del Proceso})$$

$$(14) \quad SRM = 5 * NO \quad (\text{Sumatoria de Relevancias Máxima, NO: Número de Objetivos del Proceso})$$

$$(15) \quad IR = SR / SRM \quad (\text{Índice de Relevancias del Proceso})$$

- (16)  $SIE = \sum IE$  (Sumatoria de IE de los Objetivos del Proceso)
- (17)  $PIE = SIE / NO$  (Promedio de IE del Proceso)
- (18)  $ICP = PIE / 5,00$  (Indice de Control del Proceso  $\rightarrow$  % de Control del Proceso)

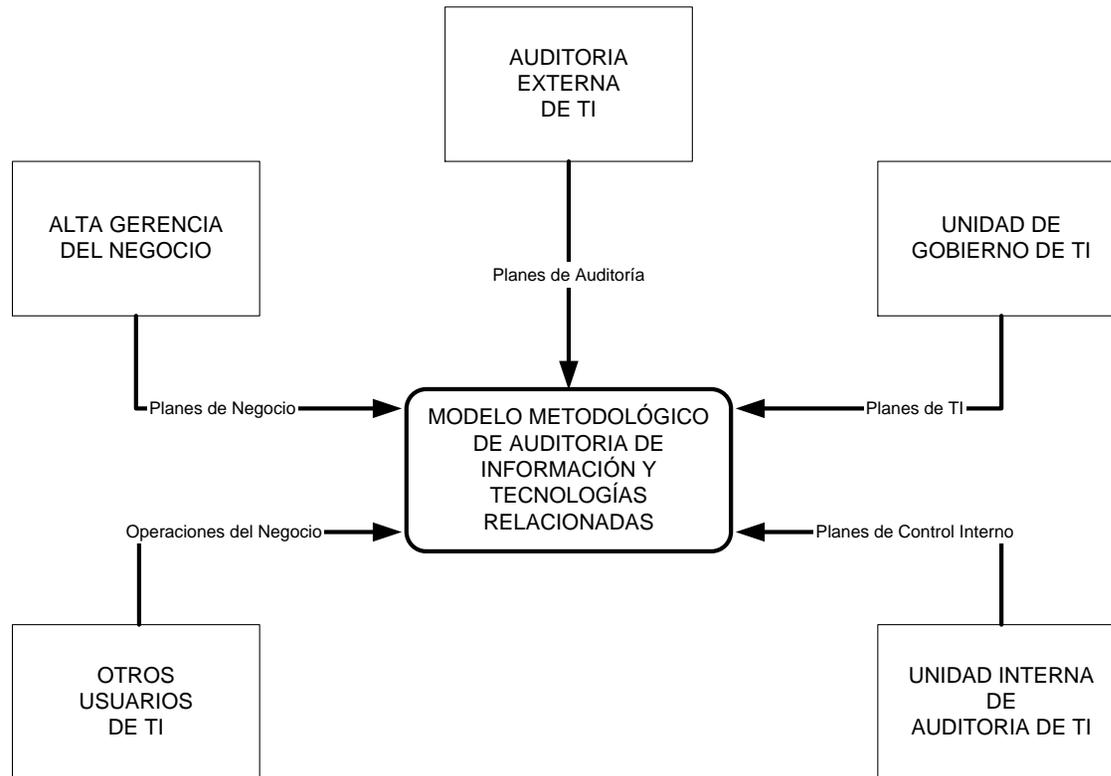
Finalmente, de acuerdo con su IE (Formula 12), los objetivos específicos del proceso se clasifican en *objetivos críticos* (Riesgo Alto con Debilidades de Control) si  $IE < PIE$ , *objetivos estables* (Riesgo Moderado) si  $IE = PIE$  y *objetivos aceptables* (Riesgo Bajo con Fortalezas de Control) si  $IE > PIE$ . Cuanto más cerca esté el valor IE de cero, más crítico y generador de vulnerabilidad a riesgos por la falta de control. Cuanto más sea IE cercano a 5,00, más efectivo será el control respecto a amenazas que generen vulnerabilidad al riesgo. Estas mismas interpretaciones valen para el análisis del valor ICP del proceso total.



**Grafico 10:** Fuente propia. Escala de evaluación de los Objetivos de Control específicos de los procesos de TI

8. **Información de aplicación de las Guías de Auditoría.** Con referencia en las Guías de Auditoría *COBIT*, documentadas en el modelo por cada proceso del alcance del plan de auditoría, se registran los resultados de aplicación y desarrollo de los procedimientos de auditoría que sustentan el Informe de Evaluación y Auditoría. El modelo permite el registro de la información de:  
(a) Obtención y comprensión del negocio mediante el detalle de entrevistas, personas, fechas, temática, comentarios, referencias a instrumentos, cuestionarios, checklist e investigación documental pertinente al alcance de la auditoría, determinación de información sensitiva, indicadores claves de desempeño. referencias a documentos, análisis de entrevistas y observaciones complementarias; (b) Resultados de la evaluación de los controles de Alto Nivel (Procesos por Dominio) y de los Objetivos de Control Específicos por proceso con los indicadores de evaluación obtenidos por la aplicación de los métodos del modelo y estudio de los factores críticos de éxito mediante la aplicación de los principios de auditoría profesional; (c) Conformación de la valoración de la evaluación y auditoría mediante exámenes de pruebas de cumplimiento y sustantivas , correspondencia con las prescripciones, determinación de evidencias y justificativos de las evaluaciones con referencia a los papeles de trabajo de la auditoría; (d) Confirmación y verificación del riesgo con el desarrollo de actividades analíticas y/o complementarias con fuentes de consulta satisfactorias como soporte de la opinión, documentación sobre debilidades, amenazas y vulnerabilidades identificando y documentando las situaciones de impacto de los riesgos actuales y futuros detectados.
9. **Opinión del Auditor.** El modelo facilita el registro de información sobre la aplicación y resultados del Plan de Evaluación y Auditoría por cada proceso (Objetivo de Control de Alto Nivel) asociado a la definición del alcance, indicando las observaciones y recomendaciones para el Informe de Auditoría.
10. **Emisión del Informe.** La emisión del informe de Evaluación y Auditoría en cumplimiento del plan, incorporando el resumen de información contenida en el registro de opinión anterior.

DFD DE CONTEXTO DEL MODELO METODOLÓGICO DE AUDITORIA DE TI



**Gráfico 11.** Fuente propia, DFD contextual (Nivel 0) del Modelo Metodológico de Evaluación y Auditoría de TI

DFD DEL MODELO METODOLÓGICO DE AUDITORIA DE TI (Nivel 1)

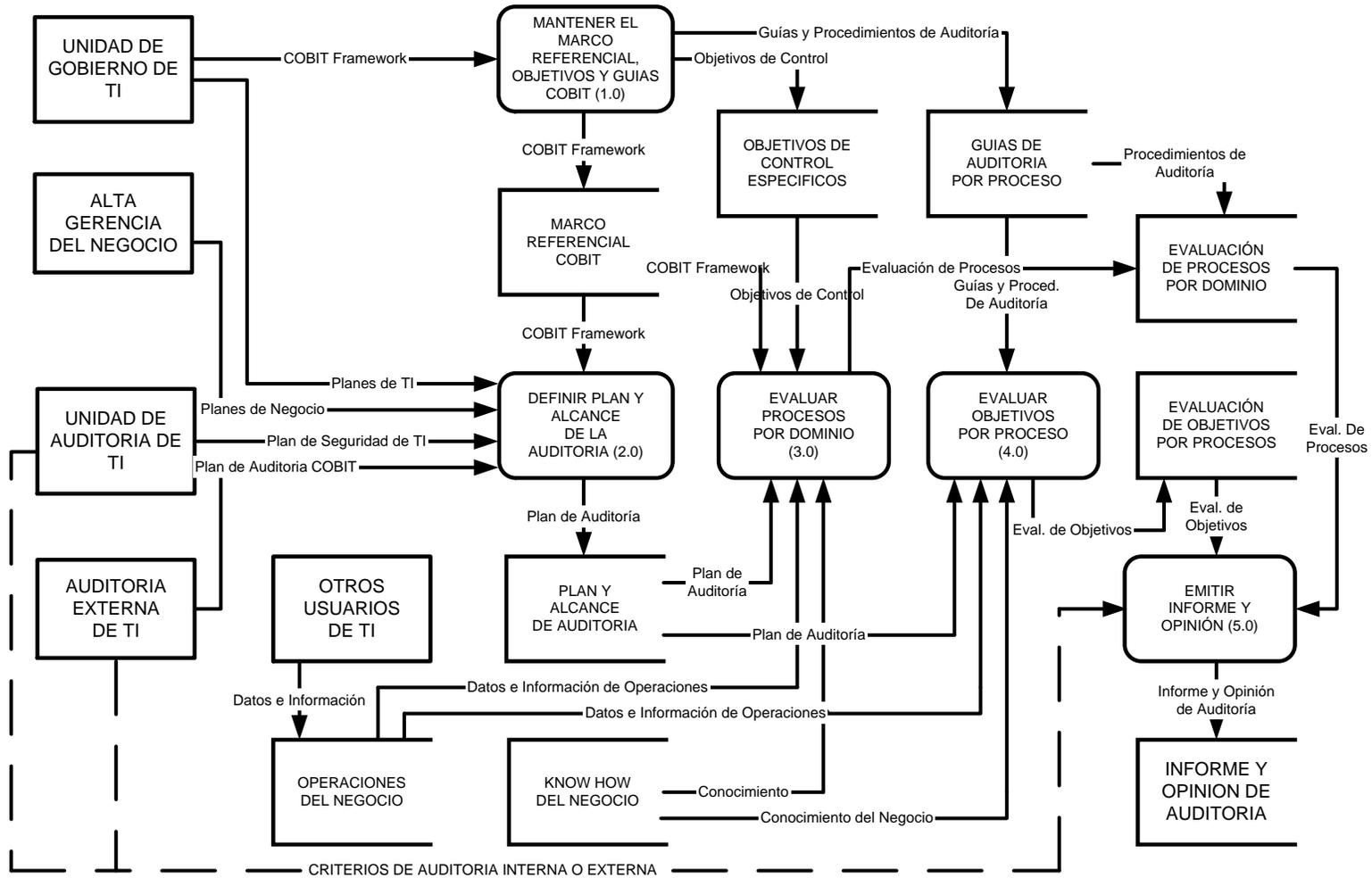


Gráfico 12. Fuente propia, DFD (Nivel 1) del Modelo Metodológico de Evaluación y Auditoría de TI

## **Diseño de la Propuesta de Software para la Implantación del Modelo**

Seguidamente, se presentan el diseño lógico conceptual de la aplicación de software propuesta para la ejecución y validación del modelo. A continuación y en este orden se presenta el modelo lógico de datos a nivel de entidades, el diseño físico de la base de datos (denominada COBIT), el modelo relacional de la base de datos, el diseño de formularios de captura y consulta, e informes de datos y resultados de los procesos de evaluación de procesos (Objetivos de Control de Alto Nivel) y Objetivos de Control Específicos por proceso. Para la implantación física de los componentes de software expuestos en el presente modelo se ha utilizado como herramienta de desarrollo e implantación el software Microsoft Access 2000. La muestra de diseño presentada no intenta representar la totalidad formal de una aplicación para el usuario final, sino la representación factible del modelo de software que puede desarrollarse para satisfacer los requerimientos de aplicación del *Modelo Metodológico de Auditoría de Información y Tecnología Relacionada*. Para facilitar su comprensión y visualización, se alimentaron las estructuras con datos de prueba para el Dominio PO: Planificación y Organización, proceso PO1: Definición de un Plan Estratégico de TI, considerando la importancia de las actividades, tareas y objetivos del proceso de planificación estratégica de TI para la alineación de los objetivos del negocio con los procesos de TI. También como referencia al resultado diagnóstico del presente caso de estudio, en el cual los procesos PO1 y DS6 resultaron ser autoevaluados como los procesos más sensibles al riesgo por parte del grupo de trabajo entrevistado. **Es importante**, mencionar en esta parte, que los datos de prueba que se presentan a continuación en el modelo de software, no corresponden estrictamente a la realidad del caso de estudio, los cuales, por la confidencialidad y sensibilidad de la información para la seguridad de la organización Banco Sofitasa, no son utilizados en toda su dimensión.

## Modelo Lógico Conceptual de Datos

### Entidades

Representación del Marco Referencial COBIT (COBIT Framework):

1. **Dominios:** Dominios COBIT
2. **Procesos:** Procesos (Objetivos de Control de Alto Nivel) por dominio
3. **Criterios:** Criterios o requerimientos de información del negocio indicando tipo de criterio (P)rimario, (S)ecundario
4. **Recursos:** Recursos de TI
5. **Procesos-Criterios:** Criterios de información asociados a procesos
6. **Procesos-Recursos:** Recursos asociados a procesos

Representación del Marco de Control:

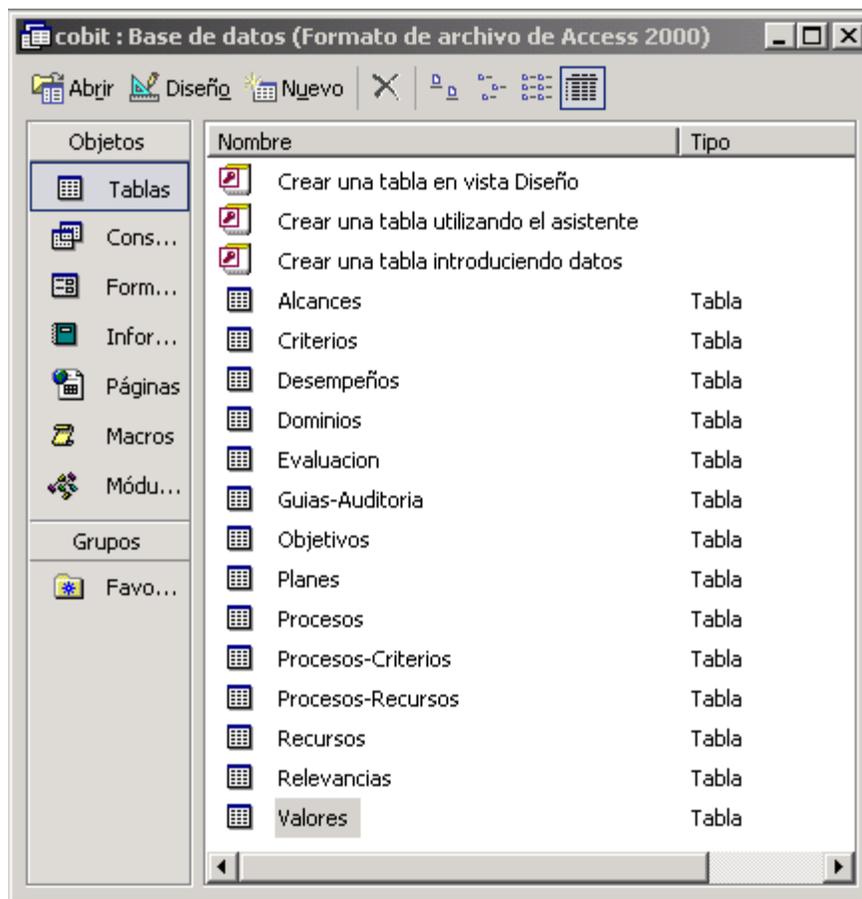
7. **Objetivos:** Objetivos de Control Específicos detallados por proceso
8. **Guías-Auditoria:** Guías de Auditoría por proceso

Representación del Modelo integrado al Marco Referencial y de Control:

9. **Planes:** Registro de planes o revisiones de evaluación y auditoría
10. **Alcances:** Registro de procesos y objetivos asociados al plan de auditoria con indicación de la evaluación por objetivo detallado
11. **Evaluación:** Registro de procesos asociados al plan de auditoria con indicación de la evaluación por proceso (Objetivo de Alto Nivel)
12. **Relevancias:** Escala de valores de significancia e importancia de procesos y objetivos detallados por proceso
13. **Desempeño:** Escala de valores del nivel de desempeño o madurez de los procesos u objetivos de control de alto nivel.
14. **Valores:** Escala de valoración del cumplimiento o ausencia de objetivos de control detallados por proceso

## Diseño Físico de Entidades (MS Access-2000)

El diseño físico de las entidades para el modelo propuesto se implantó utilizando el manejador de bases de datos de Microsoft Access 2000. Las tablas definidas en el modelo lógico de datos se diseñaron físicamente en una base de datos de nombre **cobit.mdb** como puede observarse en el **Gráfico 12**. Para los efectos de identificación del diseño físico de las tablas contenidas en esta base de datos, todos los esquemas gráficos de las tablas son referidos al Gráfico 12.



**Gráfico 13.** Implantación del diseño físico de la base de datos del modelo

Nombre del campo	Tipo de datos	Descripción
Dominio	Texto	Codigo del dominio
Nombre_Dominio	Texto	Descripción del dominio

Nombre del campo	Tipo de datos	Descripción
Dominio	Texto	Codigo de dominio
Proceso	Texto	Codigo de proceso
Nombre_Proceso	Texto	Descripción de proceso
Requerimiento	Memo	Requerimientos de información
Posibilidad	Memo	Se posibilita por...
Consideracion	Memo	Toma en consideración...

Nombre del campo	Tipo de datos	Descripción
Criterio	Texto	Numero de criterio
Nombre_Criterio	Texto	Descripción de criterio

Nombre del campo	Tipo de datos	Descripción
Recurso	Texto	Numero de recurso
Nombre_Recurso	Texto	Descripción de recurso

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Criterio	Texto	Numero de criterio
Tipo-Criterio	Texto	Tipo de criterio (P)rimario - (S)ecundario

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Recurso	Texto	Numero de recurso

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Objetivo	Texto	Codigo de objetivo de control
Nombre-Objetivo	Memo	Descripción del objetivo de control
Descripción-Control	Memo	Descripción de técnicas de control

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Entrevistando-A	Memo	Relación de personal a entrevistar
Obteniendo	Memo	Información que debe obtenerse
Considerando-Si	Memo	Consideraciones sobre la información
Examinando-Que	Memo	Exámenes que deben hacerse
Desarrollando	Memo	Actividades que deben desarrollarse
Identificando	Memo	Identificación de situaciones de riesgo

Nombre del campo	Tipo de datos	Descripción
Plan-Auditoria	Texto	Código del plan de auditoría
Empresa	Texto	Descripción de la empresa auditada
Auditor	Texto	Nombre del auditor responsable
Supervisor	Texto	Nombre del supervisor interno
Fecha-Inicio	Fecha/Hora	Fecha de inicio del plan
Fecha-Final	Fecha/Hora	Fecha de finalización del plan
Fecha-Seguimiento	Fecha/Hora	Fecha de la última revisión
Revisor	Texto	Nombre del revisor

	Nombre del campo	Tipo de datos	Descripción
🔑	Plan	Texto	Código del plan de auditoría
🔑	Proceso	Texto	Código del proceso a auditar
🔑	Objetivo	Texto	Código del objetivo a evaluar
	Valor	Número	Valoración del objetivo evaluado
	Relevancia	Número	Relevancia asignada al objetivo

	Nombre del campo	Tipo de datos	Descripción
🔑	Plan	Texto	Codigo del plan de auditoría
🔑	Proceso	Texto	Codigo del proceso evaluado
	Relevancia	Número	Relevancia asignada al proceso
	Desempeño	Número	Nivel de desempeño asignado al proceso
	Entrevistas	Memo	Detalle de entrevistas realizadas
	Obtenciones	Memo	Detalle de la información obtenida
	Consideraciones	Memo	Detalle de las consideraciones tomadas en cuenta
	Exámenes	Memo	Exámenes aplicados y papeles de trabajo
	Desarrollos	Memo	Actividades desarrolladas
	Identificaciones	Memo	Detalle de situaciones ed riesgo identificadas
	Opinión	Memo	Resumen de opinión del auditor para el informe

	Nombre del campo	Tipo de datos	Descripción
🔑	Relevancia	Número	Codigo de relevancia de procesos y objetivos
▶	Descripcion	Texto	Descripción de relevancia

	Nombre del campo	Tipo de datos	Descripción
🔑	Desempeño	Número	Codigo del nivel de desempeño de procesos
	Descripcion	Texto	Descripción breve del desempeño
	Comentario	Texto	Comentario amplio del nivel de desempeño

	Nombre del campo	Tipo de datos	Descripción
🔑	Valor	Número	Valor de evaluación de objetivos de control
▶	Descripcion	Texto	Descripción de la valoración de evaluación

## Diseño Relacional de la Base de Datos

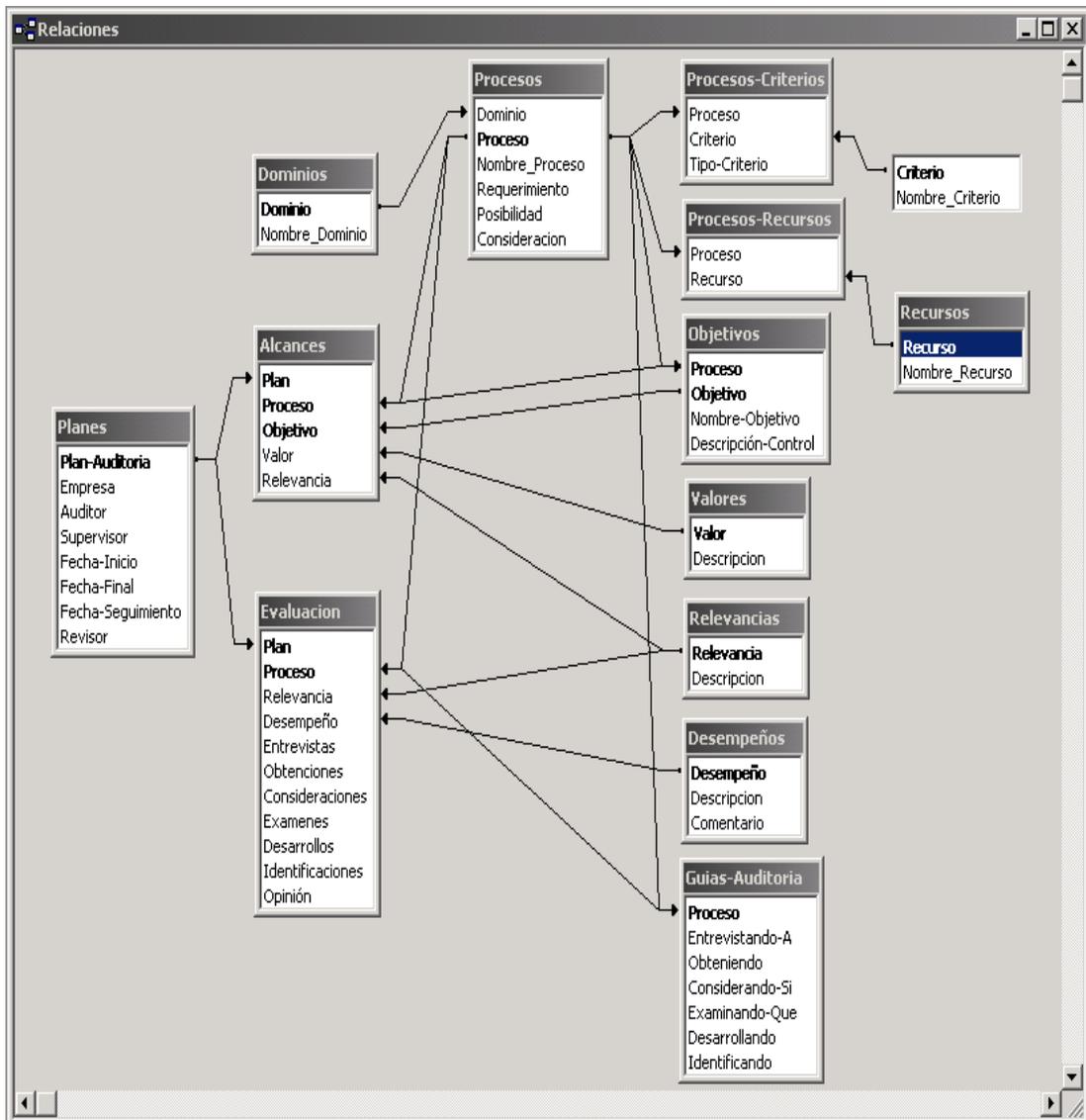


Gráfico 14: Diseño relacional de la base de datos del modelo

## **Diseño de Entrada y Salida**

Para los efectos de captura de datos de los registros de prueba del modelo se diseñaron formularios de entrada y consulta de datos y en el caso de datos extensos para ciertas categorías de información se diseñaron informes que permiten visualizar y comprender la ejecución del modelo de auditoría y control. Los datos de prueba se relacionaron con el dominio PO: Planificación y Organización, proceso PO1: Definición de un Plan Estratégico de TI, para el cual se asignaron en el alcance del modelo los 11 objetivos de control detallados y específicos al proceso en evaluación.

En los formularios que se presentan a continuación, se han hecho abstracciones de algunos registros de entrada para las diferentes categorías de datos e inmediatamente a continuación se presenta un formulario de consulta si son pocos los registros contenidos en la categoría de datos, o un informe si los datos de la categoría son extensos para ser presentados en una consulta. El objeto de las presentaciones siguientes, formularios e informes, es visualizar en la práctica las diferentes relaciones de datos del modelo propuesto y los mecanismos de evaluación y procedimientos de auditoría desde la fase de planificación hasta la fase de opinión pasando por la fase de evaluación y examen.

El orden de exposición de los elementos de entrada y salida se corresponde con el orden de ejecución del modelo según el DFD propuesto en el **Gráfico 11** que se resume en los siguientes procesos generales: (1) Mantenimiento del Marco Referencial COBIT (COBIT Framework): Dominios, Procesos, Criterios, Recursos; Mantenimiento de Objetivos de Control Detallados y Guías de Auditoría; (2) Mantenimiento de Planes de Auditoría; Definición de Alcance de la Auditoría a nivel de Procesos y Objetivos; (3) Evaluación de Procesos por Dominio; (4) Evaluación de Objetivos de Control Específicos Detallados por Proceso; (5) Aplicación de Auditoría según las Guías y Procedimientos y Emitir el Informe y Opinión. (Este último proceso consta del registro de la información y opinión para alimentar el informe).

Gráfico 15: Formatos de Entrada / Salida

The screenshot shows a window titled "Dominios". It contains two input fields: "Dominio" with the value "PO" and "Nombre\_Dominio" with the value "Planificación y Organización". At the bottom, there is a "Registro:" label followed by navigation buttons and the text "4 de 4".

The screenshot shows a window titled "Dominios Consulta : Consulta de selección" containing a table with two columns: "Dominio" and "Nombre\_Dominio". The table has four rows, with the last row selected. Below the table is a "Registro:" label with navigation buttons and the text "4 de 4".

Dominio	Nombre_Dominio
AI	Adquisición e Implementación
DS	Entrega y Soporte
M	Monitoreo
PO	Planificación y Organización

**Criterios**

**Criterio**

**Nombre\_Criterio**

Registro:       de 7

**Criterios Consulta : Consulta de selección**

	Criterio	Nombre_Criterio
▶	1	Efectividad
	2	Eficiencia
	3	Confidencialidad
	4	Integridad
	5	Disponibilidad
	6	Cumplimiento
	7	Integridad

Registro:       de 7

**Recursos**

Recurso:

Nombre\_Recurso:

Registro:       de 5

**Recursos Consulta : Consulta de selección**

	Recurso	Nombre_Recurso
<input checked="" type="checkbox"/>	1	Personas
<input type="checkbox"/>	2	Datos
<input type="checkbox"/>	3	Aplicaciones
<input type="checkbox"/>	4	Tecnología
<input type="checkbox"/>	5	Instalaciones

Registro:       de 5

**Dominios-Procesos**

**Dominio** PO

**Nombre\_Dominio** Planificación y Organización

**Procesos:**

**Control sobre el proceso de TI de:**

Definición de un Plan Estratégico de TI

**PO1**

**que satisface los requerimientos de negocio de:**

Lograr un balance óptimo entre las oportunidades de Tecnología de Información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.

**se hace posible a través de: (Declaración de Control)**

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

**y toma en consideración: (Prácticas de Control)**

- definición de objetivos de negocio y necesidades de TI
- inventario de soluciones tecnológicas e infraestructura actual
- servicios de vigilancia tecnológica

Registro: 1 de 11

Registro: 4 de 4

**Dominios-Procesos**

**Dominio** PO

**Nombre\_Dominio** Planificación y Organización

**Procesos:**

**Control sobre el proceso de TI de:**

Administración de calidad **PO11**

**que satisface los requerimientos de negocio de:**

Satisfacer los requerimientos del cliente

**se hace posible a través de: (Declaración de Control)**

La planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización

**y toma en consideración: (Prácticas de Control)**

- estructura del plan de calidad
- responsabilidades de aseguramiento de la calidad
- metodología del ciclo de vida de desarrollo de sistemas
- pruebas y documentación de sistemas y programas

Registro: 11 de 11

Registro: 4 de 4

**Dominios-Objetivos**

Dominio: PO  
 Nombre\_Dominio: Planificación y Organización

**Procesos:**

Proceso	Nombre_Proceso
PO1	Definición de un Plan Estratégico de TI
PO2	Definición de la Arquitectura de Información

Registro: 1 de 11

**Objetivos:**

Objetivo	Nombre-Objetivo
1.1	Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.
<b>Descripción del Objetivo de Control</b> La alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas de la organización. A este respecto, la alta gerencia deberá asegurar que los problemas de tecnología de información, así como las oportunidades, sean evaluados adecuadamente y reflejados en los planes a largo y corto plazo de la organización.	
1.2	Plan a largo plazo de Tecnología de Información

Registro: 1 de 6

Registro: 4 de 4

**Dominios-Objetivos**

Dominio: PO  
Nombre\_Dominio: Planificación y Organización

**Procesos:**

Proceso	Nombre_Proceso
PO1	Definición de un Plan Estrategico de TI
PO2	Definición de la Arquitectura de Información

Registro: 1 de 11

**Objetivos:**

Objetivo	Nombre-Objetivo
1.5	Planeación a corto plazo para la Función de Servicios de Información
<b>Descripción del Objetivo de Control</b> La Gerencia de la función de servicios de información deberá asegurar que el plan a largo plazo de tecnología de información sea traducido regularmente en planes a corto plazo de tecnología de información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de tecnología de información con una base consistente con el plan a largo plazo de tecnología de información. Los planes a corto plazo deberán ser reevaluados y modificados periódicamente según se considere necesario respondiendo a las	
1.6	Evaluación de Sistemas Existentes

Registro: 6 de 6

Registro: 4 de 4

**Crterios de Información por Proceso**

**Dominio** PO

**Nombre-Dominio** Planificación y Organización

**Procesos:**

Proceso	Nombre_Proceso
P01	Definición de un Plan Estrategico de TI
P02	Definición de la Arquitectura de Información

Registro: 1 de 11

**Crterios de Información:**

Crterio	Nombre-Crterio	Tipo-Crterio
1	Efectividad	P
2	Eficiencia	S

Registro: 3 de 3

Registro: 4 de 4

**Criterios de Información por Proceso**

**Dominio** PO

**Nombre-Dominio** Planificación y Organización

**Procesos:**

Proceso	Nombre_Proceso
P09	Evaluación de riesgos
P010	Administración de proyectos

Registro: 9 de 11

**Criterios de Información:**

Criterio	Nombre-Criterio	Tipo-Criterio
1	Efectividad	S
2	Eficiencia	S
3	Confidencialidad	P
4	Integridad	P
5	Disponibilidad	P
6	Cumplimiento	S
7	Integridad	S

Registro: 1 de 7

Registro: 4 de 4

## Criterios de Información por Proceso

Dominio / Procesos	Requerimiento	Criterios	Tipo
<b>PO Planificación y Organización</b>			
PO1	Definición de un Plan Estratégico de TI Lograr un balance óptimo entre las oportunidades de Tecnología de Información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.	1 Efectividad 2 Eficiencia	P S
PO2	Definición de la Arquitectura de Información Organizar de la mejor manera los sistemas de información	1 Efectividad 2 Eficiencia 3 Confidencialidad 4 Integridad	P S S S
PO3	Determinación de la dirección tecnológica Aprovechar la tecnología disponible o tecnología emergente	1 Efectividad 2 Eficiencia	P S
PO4	Definición de la organización y de las relaciones de TI Prestación de servicios de TI	1 Efectividad 2 Eficiencia	P S
PO5	Manejo de la inversión Asegurar el financiamiento y el control de desembolsos de recursos financieros	1 Efectividad 2 Eficiencia 7 Integridad	P P S
PO6	Comunicación de la dirección y aspiraciones de la gerencia Asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones	1 Efectividad 6 Cumplimiento	P S

<b>Dominio / Procesos</b>	<b>Requerimiento</b>	<b>Criterios</b>	<b>Tipo</b>
PO7	Administración de recursos humanos Maximizar las contribuciones del personal a los procesos de TI	1 Efectividad	P
		2 Eficiencia	P
PO8	Aseguramiento del cumplimiento de requerimientos Cumplir con obligaciones legales, regulatorias y contractuales	1 Efectividad	P
		6 Cumplimiento	P
		7 Integridad	S
PO9	Evaluación de riesgos Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI	1 Efectividad	S
		2 Eficiencia	S
		3 Confidencialidad	P
		4 Integridad	P
		5 Disponibilidad	P
		6 Cumplimiento	S
		7 Integridad	S
PO10	Administración de proyectos Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión	1 Efectividad	P
		2 Eficiencia	P
PO11	Administración de calidad Satisfacer los requerimientos del cliente	1 Efectividad	P
		2 Eficiencia	P
		4 Integridad	P
		7 Integridad	S

**Recursos por Proceso**

**Dominio** PO

**Nombre\_Dominio** Planificación y Organización

**Procesos:**

Proceso	Nombre_Proceso
P01	Definición de un Plan Estratégico de TI
P02	Definición de la Arquitectura de Información

Registro: 1 de 11

**Procesos-Recursos:**

	Recurso	Nombre_Recurso
▶ 1		Personas
2		Datos
3		Aplicaciones
4		Tecnología
5		Instalaciones
*		

Registro: 1 de 5

Registro: 4 de 4

**Recursos por Proceso**

**Dominio** PO

**Nombre\_Dominio** Planificación y Organización

**Procesos:**

Proceso	Nombre_Proceso
PO1	Definición de un Plan Estratégico de TI
▶ PO2	Definición de la Arquitectura de Información

Registro: 2 de 11

**Procesos-Recursos:**

	Recurso	Nombre_Recurso
▶	2	Datos
	5	Instalaciones
*		

Registro: 4 de 4

---

## Recursos por Proceso

---

Dominio / Procesos	Posibilidad	Recursos
<b>PO Planificación y Organización</b>		
PO1	Definición de un Plan Estratégico de TI	
	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	
		1 Personas
		2 Datos
		3 Aplicaciones
		4 Tecnología
		5 Instalaciones
PO2	Definición de la Arquitectura de Información	
	La creación y mantenimiento de un modelo de información de negocios y asegurando que se definan sistemas apropiados para optimizar la utilización de esta información	
		2 Datos
		5 Instalaciones
PO3	Determinación de la dirección tecnológica	
	La creación y mantenimiento de un plan de Infraestructura tecnológica	
		3 Aplicaciones
		4 Tecnología
PO4	Definición de la organización y de las relaciones de TI	
	Una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas	
		1 Personas
PO5	Manejo de la inversión	
	Presupuestos periódicos sobre inversiones y operación establecidos y aprobados por el negocio	
		1 Personas
		2 Datos
		3 Aplicaciones
		4 Tecnología

<b>Dominio / Procesos</b>	<b>Posibilidad</b>	<b>Recursos</b>
PO6	Comunicación de la dirección y aspiraciones de la gerencia	
	políticas establecidas y transmitidas a la comunidad de usuarios; además, se necesita estándares para traducir las opciones estratégicas en reglas de usuario prácticas utilizables	1 Personas
PO7	Administración de recursos humanos	
	Técnicas sólidas para administración de personal	1 Personas
PO8	Aseguramiento del cumplimiento de requerimientos externos	
	La identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, y llevando a cabo las medidas apropiadas para cumplir con ellos	1 Personas 2 Datos 5 Instalaciones
PO9	Evaluación de riesgos	
	La participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos	1 Personas 2 Datos 3 Aplicaciones 4 Tecnología
PO10	Administración de proyectos	
	Identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido	1 Personas 2 Datos 3 Aplicaciones 4 Tecnología
PO11	Administración de calidad	
	La planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por	1 Personas 2 Datos 3 Aplicaciones 4 Tecnología 5 Instalaciones

**Planes de Auditoria**

**Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT**

**Plan-Auditoria** 2004-08-1  
**Empresa** Banco X - DATOS DE PRUEBA SIN VALOR REAL -  
**Auditor** Auditor 1  
**Supervisor** Auditor Jefe  
**Fecha-Inicio** 01/08/2004  
**Fecha-Final** 31/08/2004  
**Fecha-Seguimiento** 15/08/2004  
**Revisor** Gerente de Auditoria

Registro: 1 de 3

**Planes Consulta : Consulta de selección**

Plan-Auditoria	Empresa	Auditor	Supervisor	Fecha-Inicio	Fecha-Final	Fecha-Segu	Revisor
▶ 2004-08-1	Banco X - DATOS DE PRUEBA SIN VALOR REAL -	Auditor 1	Auditor Jefe	01/08/2004	31/08/2004	15/08/2004	Gerente de Auditori
2004-12-1	Corporación Sur del Lago Azul	Auditor 3	Auditor Jefe	03/01/2005			Gerente de Auditori
2005-01-1	Technology Consulting	Auditor 1	Gerente de Riesgo	15/01/2005			Auditor de Sistema:
*							

Registro: 1 de 3

Planes-Procesos

### Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT

**Empresa** Banco X - DATOS DE PRUEBA SIN VALOR REAL -

**Plan-Auditoria** 2004-08-1 **Fecha-Inicio** 01/08/2004

**Auditor** Auditor 1 **Fecha-Final** 31/08/2004

**Supervisor** Auditor Jefe **Fecha-Seguimiento** 15/08/2004

**Revisor** Gerente de Auditoria

**Alcances a Nivel de Procesos: (Objetivos de Control de Alto Nivel)**

Proceso	Relevancia	Desempeño
P01 Definición de un Plan Estratégico de TI	5 Muy Relevante	3 Definido Procesos Documentados y Comunicados
P02 Definición de la Arquitectura de Información	4 Relevante	4 Gerenciado Procesos Monitoreados y Evaluados
P03 Determinación de la dirección tecnológica	4 Relevante	4 Gerenciado Procesos Monitoreados y Evaluados
P08 Aseguramiento del cumplimiento de requerimientos externos	5 Muy Relevante	4 Gerenciado Procesos Monitoreados y Evaluados

Registro: 1 de 11

Registro: 1 de 3

## Evaluación de Procesos

<b>Plan</b>		2004-08-1	<b>Empresa</b>		Banco X - DATOS DE PRUEBA SIN VALOR -
<b>Auditor:</b>		Auditor 1		<b>Fecha-Inicio</b>	01/08/2004
				<b>Fecha-Final</b>	31/08/2004
<b>Dominio / Proceso</b>		<b>Relevancia</b>	<b>Desempeño</b>	<b>Indice de Madurez</b>	
<b>Dominio: PO - Planificación y Organización</b>					
PO1	Definición de un Plan Estratégico de TI	5 Muy Relevante	3 Definido	0,6	
			Procesos Documentados y Comunicados		
PO2	Definición de la Arquitectura de Información	4 Relevante	4 Gerenciado	1	
			Procesos Monitoreados y Evaluados		
PO3	Determinación de la dirección tecnológica	4 Relevante	4 Gerenciado	1	
			Procesos Monitoreados y Evaluados		
PO4	Definición de la organización y de las elaciones de TI	4 Relevante	5 Optimizado	1,25	
			Procesos bajo las Mejores Practicas y Automatizados		
PO5	Manejo de la inversión	4 Relevante	5 Optimizado	1,25	
			Procesos bajo las Mejores Practicas y Automatizados		
PO6	Comunicación de la dirección y aspiraciones de la gerencia	5 Muy Relevante	5 Optimizado	1	
			Procesos bajo las Mejores Practicas y Automatizados		
PO7	Administración de recursos humanos	4 Relevante	5 Optimizado	1,25	
			Procesos bajo las Mejores Practicas y Automatizados		
PO8	Aseguramiento del cumplimiento de requerimientos externos	5 Muy Relevante	4 Gerenciado	0,8	
			Procesos Monitoreados y Evaluados		
PO9	Evaluación de riesgos	4 Relevante	4 Gerenciado	1	
			Procesos Monitoreados y Evaluados		
PO10	Administración de proyectos	4 Relevante	4 Gerenciado	1	
			Procesos Monitoreados y Evaluados		
PO11	Administración de calidad	4 Relevante	4 Gerenciado	1	
			Procesos Monitoreados y Evaluados		

---

## Evaluación de Procesos

---

<b>Plan</b>	2004-08-1	<b>Empresa</b>	Banco X - DATOS DE PRUEBA SIN VALOR -
<b>Auditor:</b>	Auditor 1	<b>Fecha-Inicio</b>	01/08/2004
		<b>Fecha-Final</b>	31/08/2004

---

<b>Dominio / Proceso</b>	<b>Relevancia</b>	<b>Desempeño</b>	<b>Indice de Madurez</b>
--------------------------	-------------------	------------------	--------------------------

---

### **Dominio: PO - Planificación y Organización**

<b>Totales del Dominio:</b>	<b>43/55</b>	<b>43/55</b>	<b>11,15</b>
<b>Indices del Dominio:</b>	<b>0,78</b>	<b>0,78</b>	<b>1,00</b>
<b>Promedio del Dominio:</b>			<b>1,01</b>
<b>Madurez del Dominio:</b>			<b>1,01</b>

### **Resumen: (Índices de Madurez de Procesos)**

#### **Procesos Críticos: (Riesgo Alto)**

PO1 = 0,6; PO8 = 0,8

#### **Procesos Estables: (Riesgo Moderado)**

PO2, PO3, PO6, PO9, PO10, PO11

#### **Procesos Aceptables: (Riesgo Bajo)**

PO4, PO5, PO7

**Planes-Alcances**

### Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT

**Empresa:** Banco X - DATOS DE PRUEBA SIN VALOR REAL -

**Plan-Auditoria:** 2004-08-1      **Fecha-Inicio:** 01/08/2004

**Auditor:** Auditor 1      **Fecha-Final:** 31/08/2004

**Supervisor:** Auditor Jefe      **Fecha-Seguimiento:** 15/08/2004

**Revisor:** Gerente de Auditoria

**Alcances a Nivel de Objetivos de Control Especificos:**

**Proceso:** PD1 Definición de un Plan Estrategico de TI

Objetivo de Control Especifico:	Relevancia	Valoración
1.4 Cambios al Plan a largo plazo de Tecnología de Información	2 Poco Relevante	0,00 Ausente
1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura	4 Relevante	0,25 Deficiente
1.2 Plan a largo plazo de Tecnología de Información	3 Medianamente Relevante	0,50 Regular

Registro: 1 de 6

Registro: 1 de 3

## Valoración de Objetivos de Control Detallados por Proceso

<b>Plan</b>	2004-08-1	<b>Empresa</b>	Banco X - DATOS DE PRUEBA SIN VALOR -		
<b>Auditor:</b>	Auditor 1			<b>Fecha-Inicio</b>	01/08/2004
				<b>Fecha-Final</b>	31/08/2004

**Proceso:** PO1 Definición de un Plan Estratégico de TI

<b>Objetivos:</b>	<b>Relevancia</b>	<b>Valoración</b>	<b>Índice de Evaluación</b>
1.1 Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.	5 Muy	0,75 Bueno	3,75
1.2 Plan a largo plazo de Tecnología de Información	3 Medianamente	0,50 Regular	1,50
1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura	4 Relevante	0,25 Deficiente	1,00
1.4 Cambios al Plan a largo plazo de Tecnología de Información	2 Poco	0,00 Ausente	0,00
1.5 Planeación a corto plazo para la Función de Servicios de Información	5 Muy	1,00 Excelente	5,00
1.6 Evaluación de Sistemas Existentes	5 Muy	0,75 Bueno	3,75

**Totales del Proceso:** 24/30 **15,00**

**Promedio Valoración de Control del Proceso:** 0,8 **2,50**

**Índice de Control del Proceso: (Promedio / Máximo Control)**  $\rightarrow 2,50 / 5,00 = 0,5 \rightarrow 50\%$

**Resumen: (Valoración de Objetivos de Control detallados)**

**Objetivos por debajo del Promedio: (Críticos) - Debilidades**

$$1.2: 2,50 - 1,50 = 1,00$$

$$1.3: 2,50 - 1,00 = 1,50$$

$$1.4: 2,50 - 0,00 = 2,50$$

**Objetivos en el Promedio: (Moderados) - Estables**

-

**Objetivos por encima del Promedio: (Aceptables) - Fortalezas**

$$1.1: 3,75 - 2,50 = 1,25$$

$$1.5: 5,00 - 2,50 = 2,50$$

$$1.6: 3,75 - 2,50 = 1,25$$

**Dominios-Guias** Modelo Metodológico de Evaluación y Auditoría de TI Basado en COBIT

**Dominio** PO Planificación y Organización

**Proceso** PO1 Definición de un Plan Estratégico de TI

**Los Objetivos de Control de Alto Nivel y los Objetivos de Control Específicos son Auditados por:**

**Obtención y Comprensión del negocio:**

**Entrevistando a:** Chief Executive Officer - CEO - Director Ejecutivo  
 Chief Operations Officer - COO - Director de Operaciones  
 Chief Financial Officer - CFO - Director Financiero  
 Chief Information Officer - CIO - Director de Información

**Obteniendo:** Políticas y procedimientos relacionados con la planificación de procesos  
 Roles y responsabilidades de las gerencias de dirección  
 Planes y objetivos organizacionales a corto y largo plazo  
 Planes y objetivos de TI a corto y largo plazo

**Evaluación de los Controles:**

**Considerando si:** Políticas de TI y/o del negocio y procedimientos dirigidos por una planificación estructurada que considere una metodología orientada a formular y modificar los planes cubren por lo mínimo:  
 - Misión de la Organización y Metas  
 - Iniciativas de TI para soportar la misión y metas de la organización  
 - Oportunidades para las iniciativas de TI  
 - Estudios de factibilidad de ed las iniciativas de TI  
 - Evaluación de riesgos de las iniciativas de TI

**Conformación de la Valoración:**

**Examinando que:** - Las agendas de las reuniones del comité de planificación y dirección reflejan los procesos de planificación  
 - Existe una metodología de planificación y cumple con las prescripciones  
 - Las iniciativas de TI relevantes son incluidas en los planes a corto y largo plazo, (cambios ed hardware, planificación de capacitación, arquitectura de información, desarrollo de nuevos sistemas o su obtención, planes de recuperación de desastres, instalación de nuevas plataformas de procesamiento, etc.)  
 - Las iniciativas de TI soportan los planes a corto y largo plazo y consideran requerimientos para investigación

**Confirmación y Verificación del Riesgo:**

**Desarrollando:** - Benchmarking de los planes estratégicos de TI contra organizaciones similares y/o estándares internacionales apropiados y reconocidos  
 - Las mejores practicas de la industria  
 - Una revisión detallada de los planes de TI para asegurar que las iniciativas de TI reflejan la misión y metas de la

**Identificando:** - Fallas de TI para alcanzar la misión y metas de la organización  
 - Fallas de TI para relacionar los planes a corto plazo con los planes a largo plazo  
 - Fallas en los proyectos de TI para cumplir los planes a corto plazo  
 - Fallas de TI para cumplir los lineamientos de costo y tiempo

Registro: 4 de 4

Planes-Guias

### Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT

Plan de Auditoria: 2004-08-1      Empresa: Banco X - DATOS DE PRUEBA SIN VALOR REAL -  
 Auditor: Auditor 1

Evaluacion-Guias

Proceso: PO1 Definición de un Plan Estratégico de TI

#### Notas para el Informe de Auditoria

**Obtención y Comprensión del negocio:**

**Entrevistas:** DETALLE DE ENTREVISTAS, PERSONAS, FECHAS, TEMATICA, COMENTARIOS, REFERENCIAS A INSTRUMENTOS, CUESTIONARIOS, CHECKLIST

**Información Obtenida:** DETERMINACION DE INFORMACION SENSITIVA, INDICADORES CLAVES DE DESEMPEÑO, REFERENCIAS A DOCUMENTOS, ANALISIS DE ENTREVISTAS, OBSERVACIONES COMPLEMENTARIAS

**Evaluación de los Controles:**

**Observaciones:** RESULTADOS DE LAS EVALUACIONES CON INDICADORES DE VALORACION POR OBJETIVOS DE CONTROL DE ALTO NIVEL Y OBJETIVOS ESPECIFICOS DETALLADOS, RESULTADOS DE LA APLICACIÓN DE LOS METODOS DE AUTOEVALUACION, VALORACION Y ESTUDIO DE LOS FACTORES CRITICOS DE ÉXITO MEDIANTE LA APLICACIÓN DE AUDITORIA PROFESIONAL

**Conformación de la Valoración:**

**Exámenes:** PRUEBAS DE CUMPLIMIENTO Y SUSTANTIVAS, CORRESPONDENCIA CON LAS PRESCRIPCIONES, DETERMINACION DE EVIDENCIAS Y JUSTIFICATIVOS DE LAS EVALUACIONES CON REFERENCIA A LOS PAPELES DE TRABAJO DE LA AUDITORIA

**Confirmación y Verificación del Riesgo:**

**Actividades Desarrolladas:** ACTIVIDADES ANALITICAS y/o COMPLEMENTARIAS CON FUENTES DE CONSULTA SATISFACTORIAS COMO SOPORTE DE LA OPINION, DOCUMENTACION SOBRE DEBILIDADES, AMENAZAS Y VULNERABILIDADES

**Situaciones Identificadas:** IDENTIFICACION Y DOCUMENTACION DE IMPACTO DE LOS RIESGOS ACTUALES Y FUTUROS DETECTADOS

Registro: 1 de 11

Registro: 1 de 3

**Proceso-Opinion**

### Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT

**Empresa** Banco X - DATOS DE PRUEBA SIN VALOR REAL -

**Plan-Auditoria** 2004-08-1      **Fecha-Inicio** 01/08/2004

**Auditor** Auditor 1      **Fecha-Final** 31/08/2004

**Supervisor** Auditor Jefe      **Fecha-Seguimiento** 15/08/2004

**Revisor** Gerente de Auditoria

**Opinión de Evaluación de Procesos:**

**Dominio** PO Planificación y Organización

**Proceso:** PO1 Definición de un Plan Estratégico de TI

**Opinión de Auditoría:**

OPINION DE AUDITORIA DEL PROCESO PO1: DEFINICION DE UN PLAN ESTRATEGICO DE TI

----- OPINION DEL AUDITOR SOBRE EL PROCESO PARA EL INFORME DE AUDITORIA -----

Registro: 1 de 11

Registro: 1 de 3

## CONCLUSIONES

En las Organizaciones empresariales es evidente la existencia del problema de control de la información y las tecnologías relacionadas con su proceso. Por el singular valor que tiene la información como activo del negocio, se hace necesaria la implantación de un entramado de medidas de control que garanticen el cumplimiento de los criterios de calidad de la información resumidos en: efectividad, eficiencia, confiabilidad, confidencialidad, integridad, disponibilidad

La estructura COBIT (Control Objectives for Información Technology) presenta la referencia más reconocida y aceptada internacionalmente para el uso de las mejores prácticas en el tratamiento del problema de control de los procesos de TI. Su conjunto de elementos permite el diseño de soluciones bajo un enfoque integral de los procesos de información alineados con los objetivos del negocio en lo que se conoce y se promueve como Gobierno de TI.

Se hace posible la difusión, promoción y aplicación de la estructura COBIT en las organizaciones, a través de diseños metodológicos sistémicos de fácil conocimiento y uso para promover la cultura de control y seguridad de la información entre los directivos del negocio, los gerentes administrativos y de gestión, los directores de TI, los auditores de sistemas y los usuarios de las aplicaciones informáticas para lograr organizaciones más eficientes en el uso de la TI.

Con la aplicación de la estructura COBIT, los análisis cualitativos y cuantitativos, obtenidos en la evaluación a nivel de procesos de TI (Objetivos de Alto Nivel) y a nivel de Objetivos de Control Específicos detallados por cada proceso, permiten concluir que existe evidentemente, una relación bien definida entre

dominios, procesos y objetivos detallados que permite la integración de estos elementos en un modelo metodológico de evaluación y auditoría para generar métodos de valoración de riesgos y control.

El Modelo Metodológico de Auditoría de Información y Tecnologías Relacionadas propuesto, permite su aplicación a través de herramientas de software aplicativo de uso sencillo e interactivo. Siguiendo el diseño propuesto, pueden desarrollarse y mejorarse versiones de aplicación de la estructura COBIT.

## RECOMENDACIONES

El diseño lógico propuesto que permitió el desarrollo del prototipo presentado para la aplicación del modelo, puede mejorarse y enriquecerse con la definición de otras relaciones de datos y procesos. Pueden desarrollarse aplicaciones de software instalables en configuraciones de escritorio, para su uso *Stand Alone* o pueden desarrollarse aplicaciones bajo arquitectura cliente/servidor para facilitar los procesos colaborativos de evaluación y auditoría en ambientes de Workgroup y Groupware, lo que redundaría en mejorar la cultura organizacional respecto al control y seguridad de los procesos de TI.

Una línea de investigación y desarrollo metodológico de aplicaciones, bajo el enfoque COBIT, debe considerar después de los elementos contemplados en el presente trabajo, variables conducentes a considerar las guías gerenciales COBIT, *Management Audit Guidelines*, que contemplan la extensión y aplicación integral del concepto de Gobierno de TI con la incorporación del modelo de madurez, definido con los siguientes elementos: Factores Críticos de Éxito (Critical Success Factors - CSFs), Indicadores Claves de Objetivos (Key Goal Indicators – KGIs) e Indicadores Claves de Desempeño – KPIs). Estos elementos entregan un marco de referencia especial para responder a las necesidades de la gerencia en materia de planificación y evaluación de los procesos de TI.

## REFERENCIAS BIBLIOGRÁFICAS

**Arima, H.(1990)**, Estudio de un Modelo Metodológico Automatizado de Auditoría de Sistemas Computarizados. Tesis doctoral de la Facultad de Economía, Administración y Contaduría de la Universidad de Sao Paulo. Disponible: en la Web <http://dedalus.usp.br:4500/ALEPH/POR/USP/USP/TES/FULL/0731774> [Consulta: 2004, Junio]

**Balestrini, M. (1998)**. Como se elabora el Proyecto de Investigación. BL consultores Asociados, Caracas

**Barrios, M. (1998)**. Manual de Trabajos de Grado de Especializaciones y Maestría y Tesis Doctorales. Editorial UPEL. Caracas.

**CIFCA (1983)**, Conferencia del Centro de Informática de la Facultad de Contaduría y Administración, Universidad Autónoma de México

**Cubillos M. (2003)**, Modelo de Evaluación de Riesgos AUDIRISK AUDISIS Ltda., Auditoría Integral y Seguridad en Sistemas de Información, Boletín Audideas Año 6 No. 2, Bogotá

**Datasec (1999)**, MEYCOR Cobit Control Self Assessment (CSA); Uruguay. Caso de Estudio en IT Governace Institute. Disponible: en la Web [http://www.itgi.org/Template\\_ITGI.cfm?Section=Case\\_Studies1&CONTENTID=9195&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.itgi.org/Template_ITGI.cfm?Section=Case_Studies1&CONTENTID=9195&TEMPLATE=/ContentManagement/ContentDisplay.cfm). [Consulta: 2004 Julio]

**Diccionario General de la lengua Española VOX**. Disponible en la Web: <http://www.diccionarios.com> [Consulta: Julio /2004]

**Echenique, J.A. (1985)**, Auditoría Informática. Ed. Mc-Graw Hill.

**Fitzgerald, J. (1991)**, Controles Internos para Sistemas de Computación Editorial Limusa.

**Garcia C. (1990)**, Un enfoque metodológico de Auditoría de sistemas San Cristóbal, UNET – Trabajo de Ascenso Docente

**ISACA (1987)**, General Standars for Information System Auditing,  
Information System Audit and Control Foundation (ISACA). Illinois, USA.

**ISACA(2000)** Information System Audit and Control Asociation (ISACA).  
Disponible en la Web <http://www.isaca.org>. [Consulta: 2004, Julio, Agosto]

**ISACF (1996-2000)**, COBIT, Control Objectives for Information and Related  
Technology, Information System Audit and Control Foundation (ISACA), 1996,  
1998, 2000. Illinois, 60008, USA

**ISACA A.L (2000)**, Information System Audit and Control Foundation (ISACA),  
Capítulo America Latina. Disponible en la Web <http://www.isaca.cl/cobit.html>  
[Consulta: 2004, Julio-Agosto]

**Piattini, M., Del Peso, E.(1998)**  
AUDITORÍA INFORMATICA, Un enfoque práctico,  
Ed. Alfaomega,

**O´Brien J. (1998)**, Sistemas de Información Gerencial,  
Ed., Mc Graw Hill

**Rodríguez R. (1998)**, Presentación en Piattini, M., Del Peso, E. (1998)  
Ed. Alfaomega,

**Tamayo y Tamayo (1986)**, El Proceso de la Investigación Científica, (ojo)  
Fundamentos de Investigación, Grupo Noriega Editores

**UNA. (1998)**, Universidad Nacional Abierta,  
AUDITORÍA y EVALUACION DE SISTEMAS, Caracas

## **ANEXOS**