



**UNIVERSIDAD AUTÓNOMA DEL ESTADO
DE HIDALGO**

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

**Objetivos de Control para la Información y
Tecnologías Relacionadas**

M O N O G R A F Í A

QUE PARA OBTENER EL TÍTULO DE:

LICENCIATURA EN SISTEMAS COMPUTACIONALES

P R E S E N T A :

P.D.L.S.C. KARINA LOZANO HERNÁNDEZ

Dirección:
M. en C. LUIS ISLAS HERNÁNDEZ

Pachuca de Soto, Hgo., Julio del 2008.

Agradecimientos

Doy gracias **A Dios**, por que me ha dado la existencia, el cuerpo y el alma, me conserva amorosamente y me ayuda a atesorar las oportunidades que me ofrece la vida.

También doy gracias a Dios por permitirme conocer a personas con una gran calidad humana, como a ti **M. C. C. Luís Islas Hernández**, mi Director de monografía por la disposición y el apoyo incondicional para la realización de esta misma.

Al **Ing. Alberto Alfonso Galindo Galindo**, por su dedicación y el tiempo que se tomó para sus respectivas correcciones de la monografía, aun más le agradezco por exigir excelencia en el trabajo y por su experiencia educativa y humana.

Agradezco a **M.G.A. Theira Irasema Samperio Monroy**, por aceptar en ser mi sinodal y sin escatimar el tiempo disponible para hacer las correcciones necesarias, asimismo agradezco a Dios por darle el privilegio de ser madre mil felicidades.

Al **M.C.C. Ismael Domínguez Jiménez**, gracias por los comentarios aportados para la mejora de esta tesis.

Al **M. en A. David Hernández Sánchez**, mil gracias por su apoyo incondicional y por las correcciones que realizo a mi trabajo de monografía,

A **DR.Luís Enrique ramos Velasco y DR. Enrique Escamilla Hernández**, gracias por los comentarios aportados a mi trabajo y por el tiempo destinado a el.

Al **Ing. Genaro Téllez Alcocer**, por brindarme su amistad y dar me todo el apoyo necesario durante la estancia de la licenciatura y doy gracias a Dios por tener privilegio de conocer personas como usted con grandes valores, mil gracias por todo y que Dios le de al ciento por uno de bendiciones.

Dedicatorias

A Dios:

Por que me ha permitido alcanzar una meta más en mi vida y se que nunca me a dejado sola, que en todo tiempo me tiene entre sus brazos, cuidándome y protegiéndome.

A mi Padre:

Prof. Braulio Lozano Hernández, por darme el mejor regalo que es la vida y la dicha de tenerte a mi lado por ser un padre responsable y estar al pendiente siempre de tus hijos y de tu nieto aun mas por ser un ejemplo de un hombre muy trabajador y de ser muy noble, caritativo y tener gran amor a Dios. **TE AMO PAPÁ.**

A mi Madre:

Sra Carito Hernández González, a ti te dedico todo ya que sin ti no seria nada, gracias mamá por ser mi gran amiga mi confidente, mi consuelo, y mi ejemplo a seguir por ser una mujer fuerte cuando lo amerita y tierna, mil gracias por darme la vida, por estar a mi lado en los momentos de alegría y de tristeza, de triunfos y fracasos de saber que siempre cuento con mi amiga incondicional. **TE AMO.** y no hay como pagarle a Dios por darme el mejor ángel como Madre, gracias por amar y de cuidar a tu nieto por que se que él es lo más importante para ti.

A mi Esposo:

Ing. Luís Enrique Mejía Gayosso, por el amor y apoyo incondicional que me das en cada momento de mi vida, porque junto a ti he encontrado la plenitud del amor y me has dado el privilegio de ser madre, **TE AMO**, con toda mi alma, mil gracias por existir en mi vida y por ser el padre cariñoso, tierno y responsable te Amamos tu hijo y yo, le doy gracias a Dios por marcar nuestro camino juntos **TE AMOOOOOOOOOO.**

A mi Hijo:

Iker Mejía Lozano, de mes y medio de edad, a ti te dedico mi trabajo ya que eres mi inspiración y mi fuerza para salir adelante porque cada vez que te observo me transmites mucha ternura, amor y paz, sabes que has llegado en el mejor momento de mi vida para tener el privilegio de ser madre, **TE AMO HIJO.**

A mi Hermano:

Ing. Braulio Lozano Hernández, Por ser el mejor ejemplo de mi vida, por tener ese corazón tan noble y generoso, gracias por todo el apoyo que me has brindado, pero aun mas por estar al pendiente de nuestros padres y ser un mejor hijo que cada días desea ser mejor y que Dios te bendiga y que sea muy feliz siempre. **TE QUIERO.**

A mi Hermana:

Téc. Irania Lozano Hernández, pues Dios nos dio un regalo muy grande que eres tu, ya que has dedicado tu tiempo al servicio de ÉL, gracias por ser mi hermanita que en todo momento se preocupa por nosotros y que con tus oraciones Dios no da muchas bendiciones, **TE QUIERO MUCHO.**

A mi Sobrino:

Brandón Lozano Cortes, se que no hemos tenido el tiempo suficiente para compartir pero quiero decirte que te quiero mucho y que siempre estas en mis oraciones y que Dios te cuide y te bendiga mi niño.

A mi abuelita:

Sra. Higinia González Santillán, por ser una persona muy fuerte y que se preocupa por todos y cuando necesitamos apoyo siempre estas tú abuelita mil gracias.

A mi abuelito:

Sr. Amador Lozano Gutiérrez, por ser un hombre muy sabio y que siempre esta pendiente de nosotros, por que se que somos sus consentidos te quiero mucho abuelito.

A mis tíos y tías, primos y primas:

Por su cariño incondicional que me brinda y el apoyo necesario que me han dado y doy gracias a Dios por tener el privilegio de pertenecer a esta familia hermosa **LOS QUIERO.**

Índice

AGRADECIMIENTOS	I
DEDICATORIAS	II
ÍNDICE	IV
JUSTIFICACIÓN.	I
OBJETIVOS.	II
OBJETIVO GENERAL.	II
OBJETIVOS PARTICULARES.	II
INTRODUCCIÓN.	III
CAPITULO 1 EVOLUCIÓN HISTÓRICA DE COBIT	1
1.1 DEFINICIÓN DE COBIT.	2
1.2 EVOLUCIÓN DE COBIT.	2
1.2.1 <i>Desarrollo de CoBIT.</i>	5
1.2.2 <i>Surgimiento de CoBIT.</i>	9
1.3 CLASIFICACIÓN DEL PRODUCTO COBIT.	10
1.3.1 <i>Primera edición.</i>	10
1.3.2 <i>Segunda Edición.</i>	10
1.3.3 <i>Tercera Edición.</i>	12
1.3.4 <i>Cuarta Edición.</i>	13
1.4 FUNCIONAMIENTO DEL SISTEMA COBIT.	15
1.5 COBIT Y OTRAS NORMAS.	18
CAPITULO 2 GOBIERNO DEL CONTROL DE TECNOLOGÍA INFORMÁTICA	20
2.1 TECNOLOGÍAS DE INFORMACIÓN (TI).....	21
2.2 RECURSOS DE LA TECNOLOGÍA DE LA INFORMACIÓN.....	23
2.2.1 <i>Niveles de Madurez.</i>	25
2.3 PROGRAMAS (DOMINIOS).....	27
CAPITULO 3 MARCO DE CONTROL DE COBIT	29
3.1 EL ROL DE LA AUDITORIA DE SISTEMAS.	30
3.2 ESTABLECIMIENTO DE UN MARCO DE CONTROL.	32
3.3 ESTÁNDARES DE AUDITORIA.	33
3.4 MODELO DE CONTROL.	34
3.5 RECURSOS DE TECNOLOGÍA INFORMÁTICA.	35
3.6 CRITERIOS DE INFORMACIÓN: (CALIDAD, FIDUCIARIOS, SEGURIDAD).....	37
CAPITULO 4 OBJETIVOS DE CONTROL	39
4.1 OBJETIVOS DE CONTROL.....	40
4.2 PRINCIPIOS DE LOS OBJETIVOS DE CONTROL.	42
4.3 MARCO DE REFERENCIA DE COBIT.	45
CAPITULO 5 DOMINIOS DE COBIT	48
5.1 DEFINICIÓN DE DOMINIOS.....	49
5.2 CLASIFICACIÓN DE DOMINIOS.....	49

5.2.1 Dominio de planificación y organización.....	49
5.2.2 Dominio de adquisición e implementación.....	50
5.2.2.1 Adquiera e Instrumento.....	51
5.2.3 Dominio de entrega de servicio y soporte.	51
5.2.4 Dominio de monitoreo.....	52
5.2.4.1 Monitor y Evaluación.....	52
CONCLUSIONES.....	55
GLOSARIO.....	59
BIBLIOGRAFÍA.....	63
CIBERGRAFÍA.....	64

Justificación.

Dentro de los sistemas de información el enfoque del control en Tecnología de Información y Comunicación (TIC), se lleva a cabo visualizando la información necesaria para dar soporte a los procesos y considerando a la información como el resultado de la aplicación combinada de recursos relacionados que deben ser administrados.

Desde el punto de vista de los recursos de la tecnología en la informática, CoBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de Tecnología Informática (TI). De amplio uso como herramienta de cumplimiento y de muchas otras normas internacionales.

CoBIT precede a las leyes de control que se están promulgando en todo el mundo. Es el fruto de 15 años de investigaciones y cooperación entre expertos mundiales en (TI) y negocios, y constituye un marco unificador internacional que integra las principales normas internacionales de tecnología de la información.

En este trabajo se pretende cubrir los componentes más relevantes de la tecnología de la información dentro de los recursos de CoBIT, como son la utilización, el funcionamiento, beneficio y las aplicaciones que se han desarrollado para obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

OBJETIVOS.

Objetivo general.

Presentar todos los componentes más relevantes de utilización, funcionamiento, beneficio y aplicación del sistema CoBIT.

Objetivos particulares.

- Mostrar la evolución de los sistemas TI
- Aplicar las buenas prácticas de control en TI
- Fundamentar la estructura de control de las TI
- Proporcionar los objetivos de control, dentro del marco referencial definido.
- Conocer las aplicaciones que se pueden obtener con este sistema.

Introducción.

Desde la década de 1960, el rápido desarrollo de los sistemas automatizados ha creado la expectativa de una apropiada respuesta de las áreas que se ocupan en gestionar la tecnología informática y sistemas de información.

Muchas organizaciones se están reestructurando a fin de modernizar sus operaciones y simultáneamente aprovechar los avances en tecnologías de información a fin de mejorar su posición competitiva. La reingeniería del negocio, el dimensionamiento correcto y el procesamiento distribuido, son todos cambios que afectan la forma en que operan las organizaciones.

La alta velocidad con la cual se procesan las transacciones; los sistemas de administración de las bases de datos; las redes de telecomunicaciones globales; el procesamiento distribuido de datos; la comunicación sobre Internet, y muchos otros factores, han causado que en toda organización, sin excepción alguna, la información y los datos en los cuales se apoya se tornen cada día más y más importantes.

Sin embargo, también han comprendido la importancia de conocer y administrar los riesgos asociados con la implementación de las nuevas tecnologías. En la Administración de Tecnología de Información (ATI), es hoy una oportunidad profesional para ampliar el espectro de aprovechamiento de la computación.

Utilizar estratégicamente la Tecnología de Información (TI) para mejorar las organizaciones, donde es común encontrar empresas que padecen el fenómeno del despilfarro computacional.

Este trabajo esta organizado de lo siguiente forma:

En el primer capítulo se habla del concepto, la evolución, el surgimiento, el desarrollo del sistema CoBIT, además, se comenta de la clasificación de las ediciones que han determinado el desarrollo y algunas otras normas.

En el segundo capítulo se habla del Control de Tecnología Informática (TIC), Sociedad de la Información (SI), los cuales se identificaron como elementos determinantes para el avance económico y la mejora de la productividad y la competitividad, en el desarrollo de CoBIT.

En el tercer capítulo se explicará el rol, los estándares de las auditorias, establecimientos, modelos dentro del marco de control en CoBIT, también se mencionan las diferentes definiciones de los recursos de TI.

En el cuarto capítulo analizaremos los objetivos, principios de control, asimismo se menciona cómo el marco de referencia se fundamenta dentro de los objetivos de control utilizados en CoBIT.

En el quinto capítulo se hace mención de la definición de dominio, también se describen 4 clasificaciones que determinan a los dominios de CoBIT, la organización, la implementación, el soporte y el monitoreo de la tecnología de la información. Y por ultimo se enlistan algunas clasificaciones dentro de los subdominios

CAPÍTULO I

Capitulo 1 Evolución histórica de CoBIT

En este capítulo se habla del concepto, la evolución, el surgimiento, el desarrollo del sistema CoBIT, Además, se comenta de la clasificación de las ediciones que han determinado el desarrollo de CoBIT y algunas otras normas.

1.1 Definición de CoBIT.

COBIT es en realidad un acrónimo formado por las siglas derivadas de Control Objectives for Information and Related Technology (objetivos de control para tecnología de información y tecnologías relacionadas). [C13].

En la actualidad se define como “Gobierno, Control y Auditoria para la Información y Tecnología Relacionadas”.

También es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoria y Control de Sistemas de Información. [C13]

1.2 Evolución de CoBIT.

El proyecto CoBIT se emprendió por primera vez en el año de 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así también de los controles de los sistemas de información implantados.

La primera edición de CoBIT, fue publicada en 1996 y fue vendida en 98 países de todo el mundo. La segunda edición publicada en Abril de 1998, desarrolla y

mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados (de forma detallada) objetivos de control de alto nivel, intensificando las líneas maestras de auditoría, introduciendo un conjunto de herramientas de implementación.

CoBIT evolucionará a través de los años y será el fundamento de investigaciones futuras, por lo que se generará una familia de productos. Al ocurrir esto, las tareas y actividades que sirven como la estructura para organizar los Objetivos de Control de TI, serán refinadas posteriormente, siendo también revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria.[C5]

Una temprana adición significativa visualizada para la familia de productos CoBIT, es el desarrollo de las Guías de Gerencia que incluyen Factores Críticos de Éxito, Indicadores Clave de Desempeño y Medidas Comparativas. identificarán los aspectos o acciones más importantes para la administración y poder tomar, así, dichas acciones o considerar los aspectos para lograr control sobre sus procesos de TI. Las medidas comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: determinar el nivel actual de madurez, de la empresa; determinar el nivel de madurez que se desea lograr, como una función de sus riesgos y objetivos; y proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición, proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de CoBIT. [C10]

Comenzando con el marco de CoBIT definido en la primera edición, el uso de estándares internacionales, las pautas y la investigación en las mejores prácticas condujeron al desarrollo de los objetivos de control. Las pautas de la intervención fueron desarrolladas después para determinar si estos objetivos del control están puestos en ejecución apropiadamente.

La investigación para las primeras y segundas ediciones incluyó la colección y el análisis de fuentes internacionales identificadas y fue realizada por los equipos en Europa (universidad libre de Amsterdam), los E.E.U.U. (universidad politécnica de California) y Australia (universidad de Nuevo Gales del Sur). Cargaron a los investigadores con la compilación, la revisión, el gravamen y la incorporación apropiada de los estándares técnicos internacionales, códigos de la conducta, estándares de calidad, estándares profesionales en la revisión, y las prácticas y los requisitos de la industria, como se relacionan con el marco y con los objetivos del control individual.

Después de la colección y del análisis, desafiaron a los investigadores a examinar cada dominio y a procesar profundizado y a sugerir los nuevos o modificados objetivos del control aplicables a ese detalle del proceso. La consolidación de los resultados fue realizada por el comité de dirección de CoBIT.

El proyecto de la edición de CoBIT ^{3ro} consistió en el desarrollar de las pautas de la gerencia y el poner al día de la edición de CoBIT ^{2do} basada en nuevas y revisadas referencias internacionales.

1.2.1 Desarrollo de CoBIT.

CoBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI), es pues, una herramienta innovadora para el gobierno de las TI. [C3]

CoBIT se fundamenta en los objetivos de control existentes de la Información Systems audit. and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulativos y específicos para la industria, tanto los ya existentes como los que están surgiendo en la actualidad. 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. [C5]

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades del negocio,

manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

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. [C3]

Se determinó que las mejoras a los objetivos de control originales deberían consistir en:

- El desarrollo de un marco referencial para el control en tecnologías de la información como fundamento para los objetivos de control en TI, y como una guía para la investigación consistente en auditoría y control de las tecnologías de la información;
- Una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho; Una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en tecnología de información y, cuando fuese posible, la especificación de indicadores de desempeño relevantes

- (normas, reglas, etc.), así como una revisión crítica y una actualización de las guías actuales para el desarrollo de auditorías de los sistemas de información.[C3]

En los últimos años, ha sido cada vez más evidente la necesidad de un marco referencial para la seguridad y el control de tecnología de información (TI). Las organizaciones exitosas requieren una apreciación y un entendimiento básico de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles adecuados.

La administración debe decidir cual es la inversión razonable en seguridad y en control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos, no los eliminan. Adicionalmente, el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

Finalmente, la Administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Juzgar cual puede ser el nivel tolerable, particularmente cuando se tiene en cuenta contra el costo, puede ser una decisión difícil para la Administración. Por esta razón, la Administración necesita un marco de referencia de las prácticas generalmente aceptadas de control y seguridad de TI para compararlos contra el ambiente de TI existente y planeado.

Existe una creciente necesidad entre los usuarios de los servicios de TI, de estar protegidos a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles y seguridades adecuadas. Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan que se establezca una base general como un primer paso. [C5]

Frecuentemente, los AUDITORES han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar su opinión acerca de los controles internos frente a la gerencia. Sin contar con un marco referencial, ésta se convierte en una tarea demasiado complicada. Incluso, la administración consulta cada vez más a los auditores para que la asesoren en forma proactiva en lo referente a asuntos de seguridad y control de TI.

1.2.2 Surgimiento de CoBIT.

Resulta imposible hablar de CoBIT sin citar a (ISACA), la entidad en cuyo seno vieron la luz los primeros “Objetivos de Control, y a ITGI (IT), el organismo que hoy día se ocupa.

ISACA es, actualmente, la organización profesional de referencia, a nivel mundial, en el ámbito de la auditoría Informática, que agrupa a más de cincuenta mil miembros en ciento cuarenta países. Cuenta, así mismo, con una red de ciento setenta capítulos -tres de ellos en España: Madrid, Barcelona y Valencia.

Por su parte, el Instituto para el Gobierno de TI (ITGI) -apéndice de ISACA- es la entidad encargada de las actividades de investigación de la asociación. Nació tras la segunda edición de CoBIT, en 1998, y desde ese momento, ha venido encargándose de su continua actualización y publicación. [C8]

1.3 Clasificación del producto CoBIT.

1.3.1 Primera edición.

Se publica por 1ra vez en Septiembre de 1996, CoBIT incluye un marco respetado a nivel internacional de gobierno generalmente aplicable y aceptado, al igual que las prácticas de control. Gracias a una construcción extensiva por medio de todos los componentes, la guía proporciona a los accionistas de la tecnología de la información un camino detallado para ayudar a las organizaciones a cumplir con las necesidades gubernamentales de tecnología de la información.

El Juego Empresarial Gubernamental IT está dirigido a todos los niveles de accionistas gubernamentales IT. Asumiendo los papeles que normalmente no desempeñan, los participantes consiguen una perspectiva global de los temas clave durante el ejercicio diario. Los materiales del juego están basados en CoBIT [C5]

1.3.2 Segunda Edición.

Un Resumen Ejecutivo, el cual consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de CoBIT. [C5]

Un Marco Referencial, el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios del CoBIT, e identifica los cuatro dominios describiendo en detalle, además, los 34 objetivos de control de alto nivel e identificando los requerimientos de negocio para la información y los recursos de las Tecnologías de la Información que son impactados en forma primaria por cada objetivo de control: [C5]

Se publica la 2a Edición en Abril de 1998, La segunda versión ampliada de CoBIT La sinopsis para la dirección, la estructura y los Objetivos de Control como un estándar abierto para intensificar el acceso a estas buenas prácticas para la TI generalmente aceptadas" ha dicho Patrick Stachtchenko, CISA, CA, presidente internacional de ISACA y socio de Deloitte Touche Tohmatsu, París, Francia. Se creó en 1998 para avanzar en el pensamiento internacional y los estándares en la dirección y control de la tecnología de control empresarial. El gobierno eficaz de la tecnología de la información ayuda a asegurar que IT soporta los objetivos empresariales, maximiza la inversión empresarial en tecnología de la información y gestiona de forma correcta los riesgos relacionados con la tecnología de la información y sus oportunidades. Para aprender más sobre el IT. [C5]

1.3.3 Tercera Edición.

Se publicó la 3ª Edición en Marzo de 2000, La nueva versión supone la primera gran actualización del contenido principal de CoBIT desde la presentación de su 3ª edición en 2000. Este nuevo volumen consta de cuatro secciones:

- La visión general ejecutiva
- La estructura
- El contenido principal (objetivos de control, directrices de gestión y modelos de madurez)
- Apéndice (asignaciones y referencias cruzadas, información adicional del modelo de madurez, material de referencia, una descripción del proyecto y un glosario)

CoBIT 4.0 no invalida el trabajo realizado con las versiones anteriores, pero en cambio se puede usar para mejorar las implementaciones existentes basadas en dichas versiones anteriores. Cuando la mayoría de actividades se planifican para iniciativas de gobierno de las TI, o cuando se anticipa una revisión de la estructura de control de la empresa, se recomienda empezar de nuevo con CoBIT 4.0. La nueva versión presenta las actividades de forma más práctica y directa, haciendo que la mejora continua del gobierno de las TI sea más fácil de conseguir que nunca. [C14]

- Analiza cómo pueden trazarse mapas de objetivos de control de los cinco dominios de gobierno IT para identificar vacíos potenciales.
- Armoniza y traza mapas entre CoBIT y otras normativas (ITIL, CMM, COSO, PMBOK, ISF e ISO 17799)
- Clarifica las relaciones entre el indicador de objetivo clave (key goal indicator, KGI) y el indicador de rendimiento clave (key performance indicator, KPI), identificando cómo los KPI permiten conseguir los KGI
- Enlaza los objetivos empresariales con los objetivos IT y los procesos IT (una investigación detallada en ocho sectores permite evaluar cómo los procesos COBIT facilitan el logro de objetivos IT específicos y, por extensión, de objetivos empresariales). [C14]

1.3.4 Cuarta Edición.

El (ITGI) anunció la publicación de CoBIT 4.1, una actualización de la guía CoBIT, que proporciona un estándar internacional de prácticas aprobadas mundialmente que ayuden a juntas directivas, ejecutivos y administradores a incrementar el valor de las TI y a reducir riesgos. Usado generalmente como herramienta para uso conjunto con Sarbanes-Oxley y otros estándares mundiales, COBIT se anticipa a la reglamentación que es decretada alrededor del mundo. Es el producto de 15 años de investigación y cooperación entre expertos mundiales en TI y negocios. [C11]

CoBIT 4.1 es una actualización significativa del marco mundial aprobado que asegura que las TI estén alineadas con los objetivos de negocio, sus recursos sean usados responsablemente y sus riesgos administrados de forma apropiada, también representa una mejora indiscutible del CoBIT 4.0 y puede usarse para perfeccionar el trabajo basado en versiones anteriores.

CoBIT ayuda a las organizaciones a reducir riesgos en el manejo de las TI e incrementar el valor derivado de su uso. Las actualizaciones incluyen: avances en la medición del desempeño; mejores objetivos de control; y una excelente alineación entre objetivos de negocio y de TI. [C1]

“CoBIT es el único marco administrativo que comprende el ciclo de vida completo de la inversión en TI. Considera los logros en los objetivos de negocio, asegura alineación de las TI con el negocio y mejora la eficiencia y efectividad de las TI,” afirma Roger Debrecey, Jefe del Comité de Manejo de CoBIT del ITGI. está creado como una guía práctica para administradores alrededor del mundo que lo utilizan para perfeccionar el gobierno de TI en sus organizaciones, así que ha sido probado y validado.[C11]

Además de CoBIT 4.1, ITGI lanzó tres publicaciones complementarias disponibles a través de la biblioteca ISACA.

1.- Dichas prácticas están orientadas a la acción y proveen argumentos dirigidos a la forma de obtener valor y limitar riesgos.

2.- Guía de Implementación de Gobierno TI: Uso de CoBIT y Val IT, 2da Edición -
Esta publicación proporciona un itinerario detallado para establecer efectivamente el gobierno de TI en una organización, con una guía que muestra como puede dar soporte a esta actividad. También ofrece una explicación detallada del alcance del proyecto de gobierno.

3.- Guía de Aseguramiento de TI: Uso de CoBIT – Al reemplazar la guía del aseguramiento, este libro ofrece una guía de cómo CoBIT puede dar soporte a una gran variedad de acciones de aseguramiento y cómo una revisión del mismo puede ser desarrollada para cada uno de los procesos de TI. [C11]

1.4 Funcionamiento del sistema CoBIT.

CoBIT, es una herramienta de gobierno de las Tecnologías de la información que ha cambiado de igual forma que lo ha hecho el trabajo de los profesionales de TI.

La misión del CoBIT: buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores. [C10]

Dicho de una forma menos formal, señalaremos que CoBIT ayuda a salvar las brechas existentes entre los riesgos de negocio, necesidades de control y

aspectos técnicos. Además, proporciona "prácticas sanas" a través de un Marco Referencial (*Framework*) de dominios y procesos, y presenta actividades en una estructura manejable y lógica. Las "prácticas sanas" del CoBIT representan el consenso de los expertos (ayudarán a los profesionales a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo que serán juzgados si las cosas salen mal). [C10]

El tema principal que trata CoBIT es la orientación a negocios. Éste, está diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. De forma creciente, las prácticas de negocio comprenden la completa autorización de los procesos propios de negocio, con lo que poseen una total responsabilidad para todos los aspectos de dichos procesos. La norma CoBIT, proporciona una herramienta para los procesos propios de negocio que facilitan la descarga de esta responsabilidad.

En orden de proporcionar la información que la organización necesita para llevar a cabo sus objetivos, los requisitos de las tecnologías de la información necesitan ser gestionados por un conjunto de procesos agrupados de forma natural. [C4]

Esta estructura, abarca todos los aspectos de la información y de la tecnología que la mantiene. Mediante la dirección de estos 34 objetivos de control de alto nivel, los procesos propios de negocio pueden garantizar la existencia de un sistema de control adecuado para los entornos de las tecnologías de la

información. En suma, cada uno de los 34 objetivos de control de alto nivel correspondiente, es una directiva de revisión o seguridad para permitir la inspección de los procesos de las tecnologías de la información en contraste con los 302 objetivos de control detallados en el CoBIT para el suministro de una gestión de seguridad, así como de un aviso para la mejora. La norma contiene un conjunto de herramientas de implementación el cual aporta una serie de lecciones de aprendizaje, con las que las organizaciones podrán aplicar de forma rápida y satisfactoria esta norma a sus entornos de trabajo. [C4]

En definitiva, CoBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio, asimismo habilita el desarrollo de una política clara y de buenas prácticas de control de TI, a través de organizaciones a nivel mundial es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. Por lo tanto, CoBIT esta orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con las tecnologías de la información y con las tecnologías relacionadas. [C4]

1.5 CoBIT y otras normas.

Las dos normas internacionales usadas hoy son CoBIT Y ISO/IEC 17799:2005. fue liberado y usado principalmente por la comunidad TI. En 1998, las Directrices de Dirección fueron añadidas, y CoBIT se hizo el marco internacionalmente aceptado para la gobernación TI y el control. ISO/IEC 17799:2005 (el Código de práctica para la Seguridad de Información la Dirección) es también un estándar internacional y es la mejor práctica para poner en práctica la dirección de seguridad. Las dos normas no compiten el uno con el otro y en realidad complementan el uno al otro. CoBIT típicamente cubre una más amplia área mientras ISO/IEC 17799 profundamente es enfocado (concentrado) en el área de seguridad.

En la tabla 1 se describe la interrelación de las dos normas así como ISO/IEC 17799 puede ser integrado con CoBIT. [C8]

COBIT DOMINIO	1	2	3	4	5	6	7	8	9	10	11	12	13
El plan y Organiza	-	+	-	-	++	+	+	-	-	0	.	.	.
Adquiera y el Instrumento	+	0	0	-	0	+
Entregue y el Apoyo	-	+	0	+	+	.	+	0	0	0	+	0	0
El monitor y Evalúa	-	0	-	0

Tabla 1 Interrelación de dos normas

(+) El marcar bueno (más de dos ISO/IEC 17799:2005 los objetivos fueron trazados un mapa de un proceso de COBIT)

(0) En parte el marcar (un o dos ISO/IEC 17799:2005 objetivos fue trazado un mapa de a un proceso de COBIT)

(-) No o el marcar menor (ningún ISO/IEC 17799:2005 el objetivo fue trazado un mapa de a un proceso de COBIT)

(.) No existe [C8]

CoBIT se acerca al control de TI por mirar la información no la información solamente (justo) financiera que es necesario para apoyar exigencias de negocio y los recursos asociados TI y procesos. COSO objetivos de control enfocan la eficacia de operaciones, el reportaje confiable financiero, y el cumplimiento con leyes y regulaciones. COBIT es ampliado para cubrir la calidad y exigencias de seguridad en siete categorías de traslape, que incluyen la eficacia, confidencialidad, la integridad, la disponibilidad, el cumplimiento, y la fiabilidad de información. [C8]

Estas categorías forman la fundación para los objetivos de control de CoBIT, COSO es útil para la dirección en general, mientras CoBIT es útil para la dirección, usuarios, e interventores. CoBIT expresamente es enfocado (concentrado) en mandos de TI. A causa de estas diferencias, interventores no deberían esperar una relación de uno a uno entre los cinco componentes de control de COSO y los cuatro dominios de CoBIT. [C2]

CAPÍTULO III

Capitulo 2 Gobierno del Control de Tecnología Informática

En este capítulo se habla del Control de Tecnología Informática (TIC), Sociedad de la Información (SI), los cuales se identificaron como elementos determinantes para el avance económico y la mejora de la productividad y la competitividad, en el desarrollo de CoBIT.

2.1 Tecnologías de Información (TI).

La TI se definen como la estructura de relaciones y procesos que dirigen y controlan la organización en orden de conseguir sus objetivos institucionales añadiendo valor, balanceado, riesgos contra beneficios.

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

1. Recursos de TI,
2. Requerimientos institucionales (objetivos) para la información y
3. Procesos de TI.

Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente. En Los procesos que pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel institucional, otros al nivel de la función de servicios de información, otros al nivel del responsable de cada proceso. Como se explica en la Figura 1 [C6].

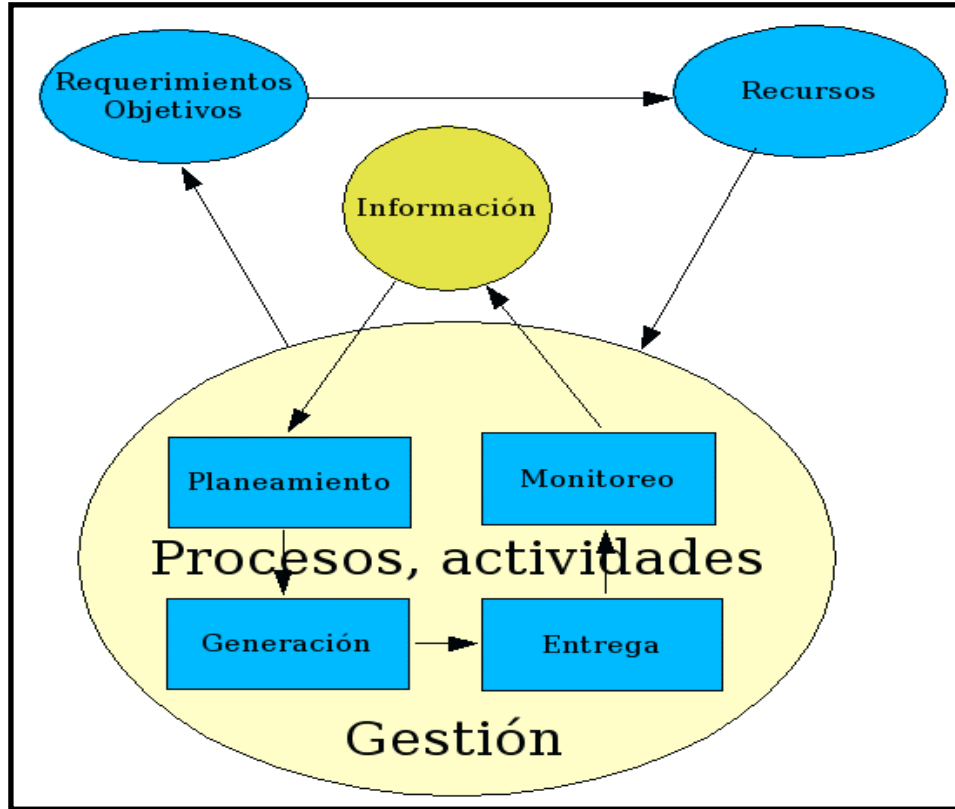


Figura 1 Los procesos a nivel institucional. [C6]

Los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos). Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control. Estos tres puntos estratégicos son descritos en el Cubo CoBIT que se muestra a continuación en la Figura 2. [C7]

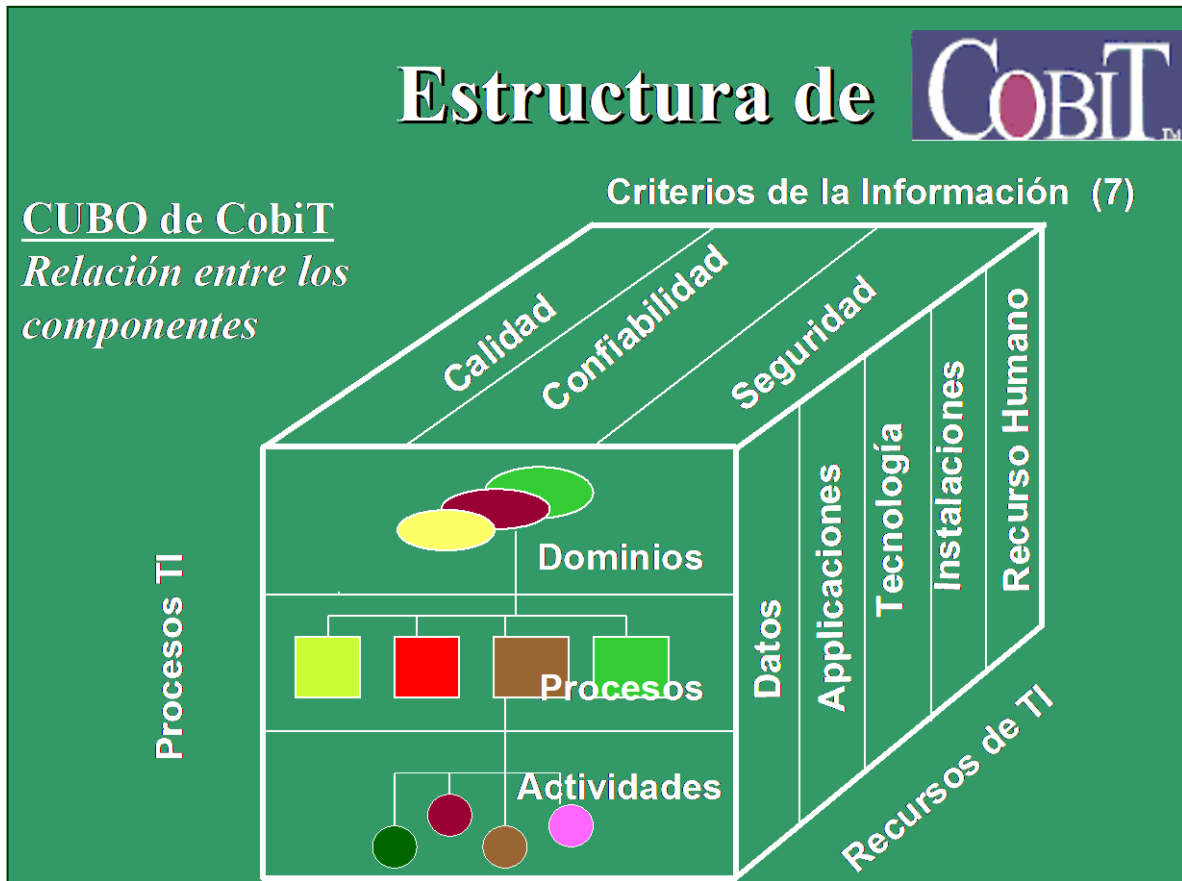


Figura 2 Cubo de CoBIT. [C7]

2.2 Recursos de la tecnología de la información

Los recursos pueden explicarse o definirse como se indica a continuación:

- **Datos:** Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc. Se empezó a crear los primeros diccionarios de datos, como son el sistema de lugares, el de organizaciones, personas, bienes, etc.

- **Aplicaciones:** Se entiende como sistemas de aplicación, la suma de procedimientos manuales y programados. Se ha comenzado a desarrollar el sistema Monitoreo, utilizando tecnología Ekeko y Software Libre, creando software bajo la GPL
- **Tecnología:** La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- **Instalaciones:** Recursos para alojar y dar soporte a los sistemas de información. Se cuenta con instalaciones relativamente apropiadas, si bien debiéramos incrementar la organización, comodidad, condiciones de temperatura para los equipos, etc.
- **Habilidades de la planta TIC:** conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios
- **Sistemas de información.** Se están organizando charlas de difusión y coordinación todas las semanas.
- **Habilidades de los usuarios** de la comunidad universitaria para adaptarse y usar las herramientas TIC. [C14]

El dinero o capital no es considerado como un recurso para la clasificación de objetivos de control para TI debido a que puede definirse como la inversión en cualquiera de los recursos mencionados anteriormente y podría causar confusión con los requerimientos de auditoría financiera. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuras de controles de compensación en cualquier área específica en revisión.

Otra forma de ver la relación de los recursos de TIC con respecto a la entrega de servicios se observan, en la Figura 3. [C14]

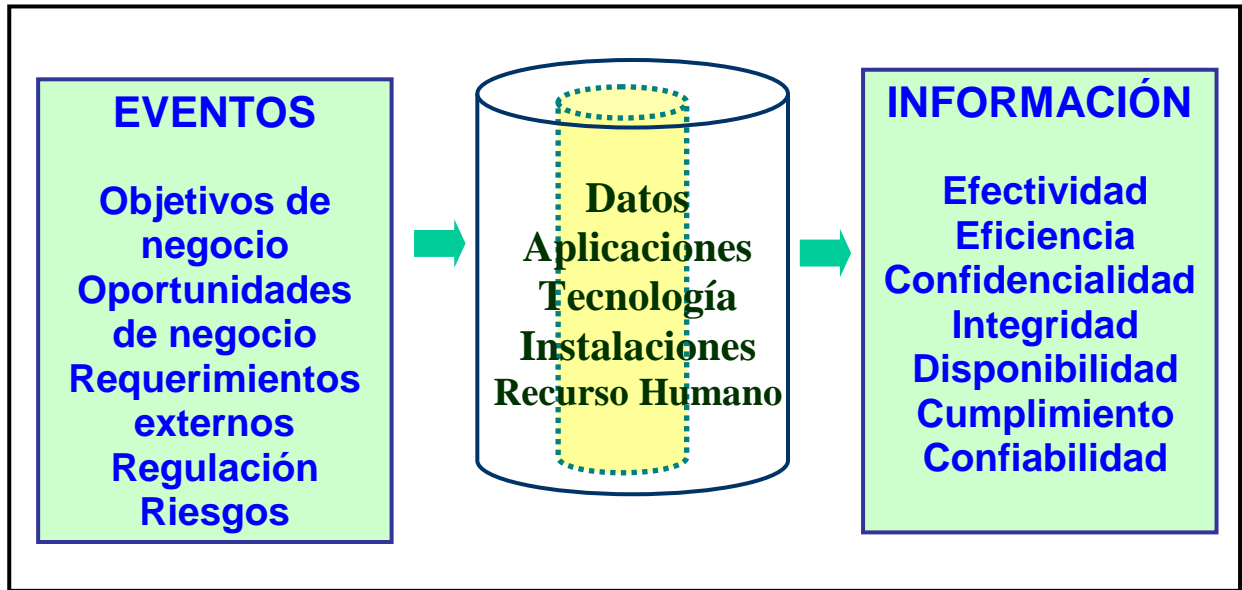


Figura 3. Relación de los recursos de TIC. [C14]

2.2.1 Niveles de Madurez.

Si bien existen acciones que expresan líneas de acción y su consecuente expresión en proyectos y programas, falta el hilo conductor que podría surgir de una planificación que formule objetivos comunes y desarrolle en forma integrada las distintas vías de concreción.

Tiene conformado un mecanismo específico para la planificación ni un sistema articulado con las otras unidades que englobe las políticas, enlace los diagnósticos

y vincule las estrategias en la universidad como un todo. Por su parte, la elaboración presupuestaria no se realiza en función de planes estratégicos o prioridades. [C14]

Cada actividad puede evaluarse y ser ubicada en un determinado nivel de madurez.

Características de cada nivel:

1. No hay proceso reconocible, la institución ni siquiera reconoce la cuestión.
2. La institución reconoce el problema, hay enfoques ad-a.C. para el caso por caso, no hay enfoque global coordinado, plantel desorganizado
3. Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
4. Los procesos están documentados y comunicados mediante entrenamiento. Sin embargo queda a cargo de cada individuo el seguir los procesos. Los procedimientos no son sofisticados pero las prácticas están formalizadas.
5. Se puede medir y monitorear el cumplimiento de los procesos y se toman acciones cuando hay desviaciones. Los procesos están bajo constante mejora. Se usan herramientas automatizadas en forma fragmentaria.

6. Los procesos están en el nivel de mejor práctica. Se usa la tecnología para automatizar el flujo de trabajo, se tiene herramientas para mejorar la calidad y la eficiencia, la organización se adapta rápidamente. [C14]

2.3 Programas (dominios).

Los Objetivos de Control muestran su interrelación con los objetivos institucionales y están definidos con una orientación a los procesos.

- **Control:** las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos institucionales serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.
- **Objetivo de control en TIC:** resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TIC particular.

La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TIC al considerar la administración de sus recursos. Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta típicamente con requerimientos de

control diferentes a los de actividades discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. [14]

La segunda categoría incluye tareas llevadas a cabo como soporte para el planeamiento estratégico de TI, evaluación de riesgos, planeamiento de la calidad, administración de la capacidad y el desempeño. Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios o programas. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TIC. [C14]

CAPÍTULO III

Capitulo 3 Marco de control de CoBIT.

Dentro del siguiente capítulo se explicará el rol, los estándares de las auditorías, establecimientos, modelos dentro del marco de control en CoBIT, también se mencionan las diferentes definiciones de los recursos de TI.

3.1 El rol de la auditoria de sistemas.

La automatización de las funciones organizacionales está determinando la incorporación de mecanismos de control más potentes en los sistemas de información, en los sistemas operativos, las redes, y el *hardware*. Además, las características estructurales de estos controles están evolucionando al mismo ritmo y de igual manera que estas tecnologías. [C12]

Para un número creciente de organizaciones y principalmente las de corte financiero, la seguridad de sus sistemas sigue siendo un aspecto importante a controlar y proteger, hasta el punto de que en algunas de ellas se creó inicialmente la función de Auditoría Informática para revisar la seguridad, aunque después se haya ido ampliando el alcance y los objetivos de esta, en función de la gran relevancia que ha pasado a tener esta tarea por la automatización de la mayoría de los procesos de negocio. [C12]

Pero en la actualidad, debemos ir hablando más de "Auditoría de Sistemas de Información" que sólo de Auditoría Informática, por la extensión de las áreas que llega a cubrir. En todo caso, la auditoria de sistemas de información se ha convertido en el control del ambiente de controles. [C12]

Esta denominación abarca la necesidad de controlar globalmente a los sistemas de información, es decir, desde su planificación a su implementación; observando

también su alineación con las estrategias de la organización, ya que es cierto que en muchos casos tan necesario o más que la protección de la información, es que las inversiones en los sistemas de información y la tecnología informática estén alineadas con las estrategias de la alta dirección, escapando al inadecuado enfoque de la tecnología por la tecnología. [C12]

También la Auditoría de Sistemas de Información debe contemplar el control del aprovechamiento que se hace de las tecnologías informáticas y si éstas aportan ventajas competitivas, además de la adecuación de la gestión de los recursos tecnológicos y de la seguridad que otorgan. [C12]

Debe evaluarse en la Auditoría de Sistemas de Información, si los modelos de seguridad están en consonancia con las nuevas arquitecturas y las distintas plataformas, porque no se puede auditar con conceptos, técnicas o recomendaciones de hace algunos años atrás. Así, el enfoque tradicional de la auditoría ha ido evolucionando. Se ha vuelto más participativa, priorizando un enfoque preventivo e intentando actuar antes o durante el hecho. La tendencia actual, en el ámbito de la Auditoría de Sistemas de Información apunta a participar más activamente en todos los proyectos y decisiones relacionados con los sistemas de información y la tecnología informática dentro de la organización. [C12]

3.2 Establecimiento de un marco de control.

En este contexto de cambios acelerados, si los gerentes, especialistas en sistemas de información y auditores han de desempeñar realmente sus roles con efectividad, sus habilidades deben evolucionar con la misma rapidez que lo hacen la tecnología y el ambiente de negocio. Deben comprender acabadamente la tecnología de los controles y su naturaleza cambiante; si han de aplicarse criterios razonables y prudentes para evaluar las prácticas de control presentes en las organizaciones. [C12]

La alta dirección de cualquier organización necesita poder comprender y contar con un conocimiento básico de los riesgos que introduce la incorporación y utilización de la tecnología informática, para así proveer una dirección eficaz y poner en práctica todos los mecanismos necesarios para la puesta en marcha de los controles adecuados. Tiene que decidir cuál es el grado de inversión razonable en seguridad y control, y cómo alcanzar un balance razonable entre el nivel de riesgo y la inversión en los controles. Planteadas anteriormente muchas de las nuevas exigencias para el incremento de los controles, surge la necesidad de contar con una metodología para organizar las actividades de la Auditoría de Sistemas de Información, la cual contribuya a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos; que sea aplicable a todos los tamaños y tipos de organización, y que esté dirigida no sólo a auditores de sistemas, sino también a la administración y a los usuarios; que

permita además, determinar el alcance de la tarea de auditoría e identificar los controles mínimos, y que pueda utilizarse como una herramienta de auto-evaluación del área de tecnología informática. [C12]

3.3 Estándares de auditoría.

En los últimos años se ha incrementado la atención sobre los controles internos, tanto para los auditores, los gerentes, los contadores, como para las entidades reguladoras en general. Como resultado de un continuo y trabajoso esfuerzo, se han desarrollado varios documentos para definir, valorizar, reportar y mejorar el control interno y ser utilizados como marco de referencia en las organizaciones, en resumen, éstos es:

- Informe COSO - (Committee of Sponsoring Organizations), de la Comisión de Estudios de Controles Internos.
- SAC - (Systems Auditability and Control), de la Fundación de Investigación del Instituto de Auditores Internos.
- SAS 55 y SAS 78 - Consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros, del Instituto Americano de Contadores Públicos (CPA)
- CoBIT (Control Objectives for Information and related Technology), de la Fundación de Auditoría y Control de Sistemas de Información.

Cada uno de ellos ha sido definido para una audiencia en particular: el "COSO" fue diseñado para la Gerencia; el "SAC" para los auditores internos; los SAS 55 y SAS 78 para los auditores externos, y finalmente el "CoBIT" enfocado principalmente para los auditores de sistemas de información. Este último es el que desarrollaremos más ampliamente. [C12]

3.4 Modelo de control.

El concepto que apunta la estructura CoBIT es que el control en Tecnología Informática es enfocado mirando hacia la información que se necesita en los procesos del negocio y hacia la información resultante de la aplicación combinada de recursos relacionados con Tecnología Informática, que requieren ser administrados mediante procesos de Tecnología Informática.

La información que los procesos de negocio necesitan es proporcionada a través del empleo 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 adecuadas para estos recursos. [C12]

3.5 Recursos de tecnología informática.

Requerimientos de Calidad, Financieros y de Seguridad Comenzando el análisis, se extrajeron siete categorías distintas, seguramente superpuestas, según el siguiente detalle:

Efectividad: trata con información relevante y pertinente al proceso de negocios, así como entregada de una manera oportuna, correcta, consistente y útil.

Eficiencia: concierne a la provisión de información mediante el uso óptimo (más productivo y económico) de los recursos.

Confidencialidad: concierne a la protección de la información sensible respecto de la disposición no autorizada.

Integridad: se relaciona con la precisión de la información así como con su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por el proceso del negocio, ahora y en el futuro. También concierne a la salvaguarda de los recursos necesarios y las capacidades asociadas.

Cumplimiento: trata con el cumplimiento de aquellas leyes, regulaciones y arreglos contractuales a los cuales está sujeto el proceso del negocio.

Confiabilidad de la información: se relaciona con la provisión de información apropiada a la gerencia para operar la entidad y también para ejercer sus responsabilidades de elaboración de informes financieros y de cumplimiento. [C7]

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que CoBIT hace referencia como requerimientos de negocio para la información como se muestra en la figura 4. Al establecer la lista de requerimientos, CoBIT combina los principios contenidos en los modelos. [C7]

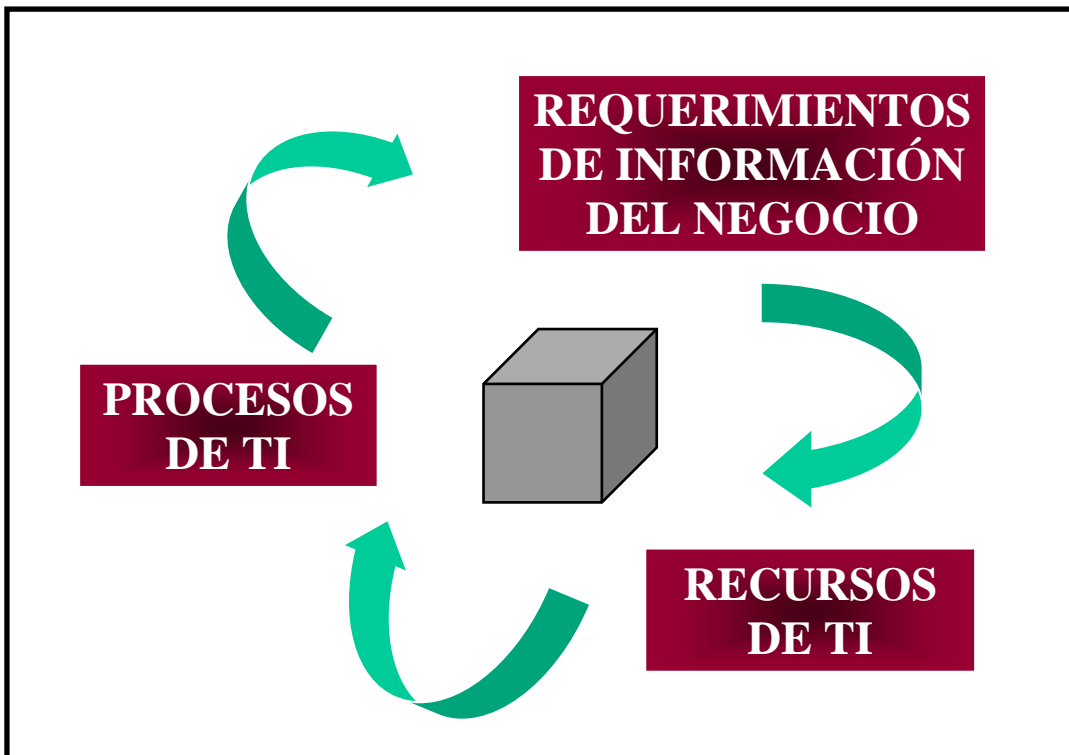
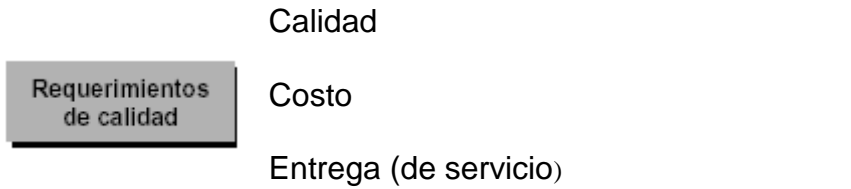
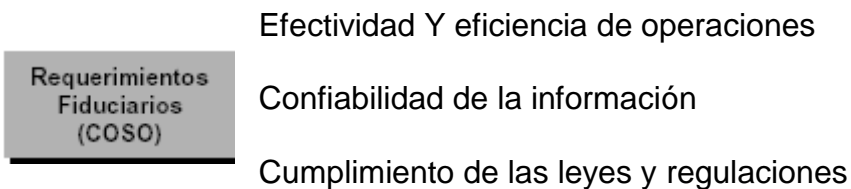


Figura 4. Requerimientos de negocio. [C7]

3.6 Criterios de Información: (calidad, fiduciarios, seguridad)

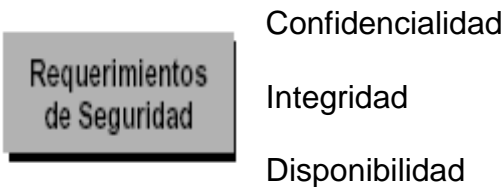


- **Calidad y Entrega:** Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
- **Costo:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.



- **Confiabilidad (fidelidad) de la información:** calidad y entrega. Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

- **Eficiencia de las operaciones, costo:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- **Cumplimiento: leyes, regulaciones y acuerdos, muchas veces externos:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.



- **Confidencialidad:** Se refiere a la protección de información sensible contra divulgación no autorizada.
- **Integridad:** precisión y suficiencia. Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- **Disponibilidad de la información.** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas. [C9]

CAPÍTULO IV

Capitulo 4 Objetivos de control.

En el siguiente capítulo analizaremos los objetivos, principios de control, así mismo se menciona cómo el marco de referencia se fundamenta dentro de los objetivos de control utilizados en CoBIT.

4.1 Objetivos de control

Los Objetivos de Control se distribuyen entre los 34 Subdominios y su objetivo es poder realizar una revisión de segundo nivel en la práctica de la gestión de tecnología. [C13]

Es claro que no todas las medidas de control necesariamente satisfacen el mismo grado de los distintos requerimientos del negocio en materia de información. [C8]

Dentro de la estructura CoBIT realiza una clasificación basada en un riguroso proceso de ingreso de datos de investigadores, expertos y revisores, con las definiciones estrictas establecidas anteriormente. [C12]

- **Primario** es el grado al cual el Objetivo de Control definido satisface completamente el requerimiento de información concerniente.
- **Secundario** es el grado al cual el Objetivo de Control definido sólo satisface con una menor extensión o indirectamente el requerimiento de información concerniente.
- **Blanco** podría ser aplicable; pero sin embargo, los requerimientos se satisfacen más apropiadamente por otro criterio en este proceso y/o por otro proceso.[C12]

Debe tomarse en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel corporativo, otros al nivel de la función de servicios de información, otros al nivel del propietario de los procesos de negocio.

También debe ser tomado en cuenta que el criterio de efectividad de los procesos que planean o entregan soluciones a los requerimientos de negocio, cubrirán algunas veces los criterios de disponibilidad, integridad y confidencialidad, en la práctica, se han convertido en requerimientos del negocio. Por ejemplo, el proceso de “identificar soluciones automatizadas” deberá ser efectivo en el cumplimiento de requerimientos de disponibilidad, integridad y confidencialidad. Resulta claro que las medidas de control no satisficieran necesariamente los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación dentro del marco referencial CoBIT basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente. Similarmente, todas las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de CoBIT indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración (no por aquellos que simplemente toman parte en el proceso). Esta clasificación es hecha dentro el Marco Referencial de CoBIT basado en el mismo proceso riguroso de información proporcionada por los investigadores, expertos y revisores, utilizando las definiciones estrictas indicadas previamente. [C12]

4.2 Principios de los objetivos de control.

El concepto fundamental del marco referencial CoBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI. Como se muestra en la Figura 5 [C6]

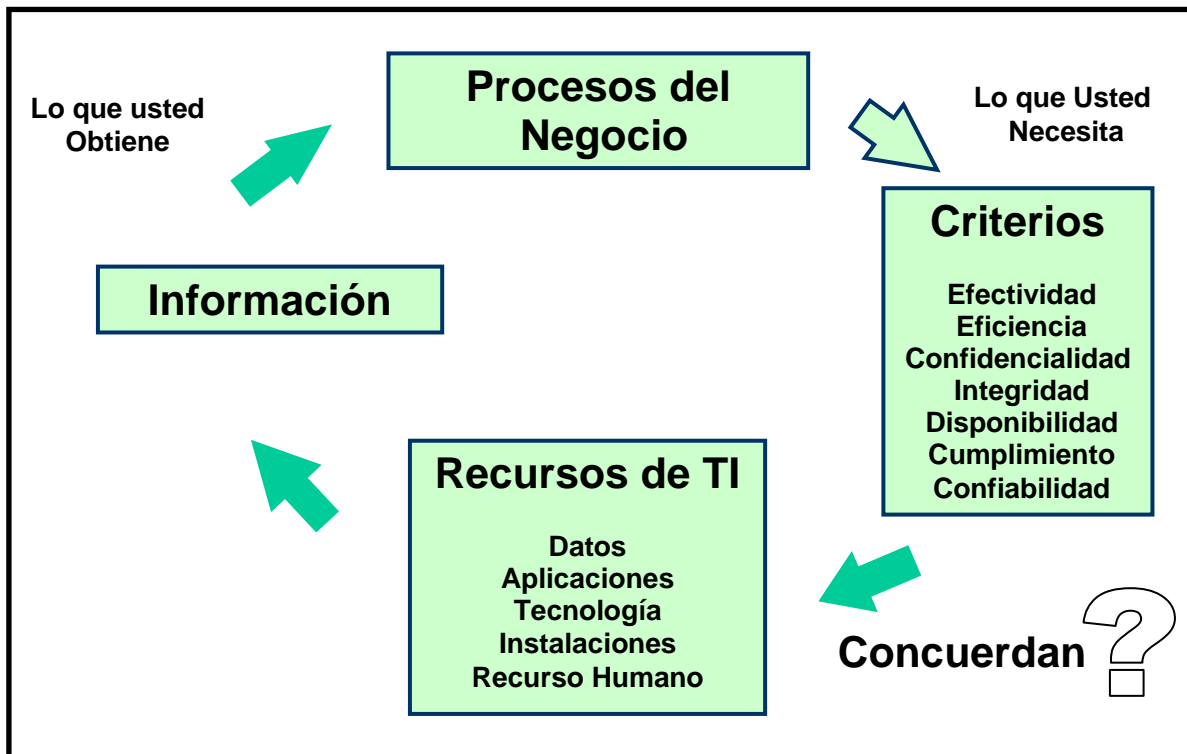


Figura 5. Principios del Marco de Trabajo. [C6]

Un "Objetivo de Control", es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática y sistemas de información. Los objetivos de control muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso dentro de toda la organización y más allá del uso exclusivo de los auditores.

Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. Estos objetivos de control de tecnología informática han sido organizados por proceso / actividad, pero también se facilita la entrada a partir de cualquier punto de vista estratégico, además para lograr enfoques combinados o globales, tales como instalación / implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de tecnología informática por un proceso. Para mayor facilidad los Objetivos de Control, dentro del CoBIT han sido definidos en una manera genérica, sin depender de la plataforma técnica.

Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría o de aseguramiento que permite la revisión de los procesos de tecnología informática, contra los 302 objetivos detallados de control recomendados por CoBIT para proporcionar la certeza de su cumplimiento y/o una recomendación para su mejora. Como se muestra en la figura 6 [C11]

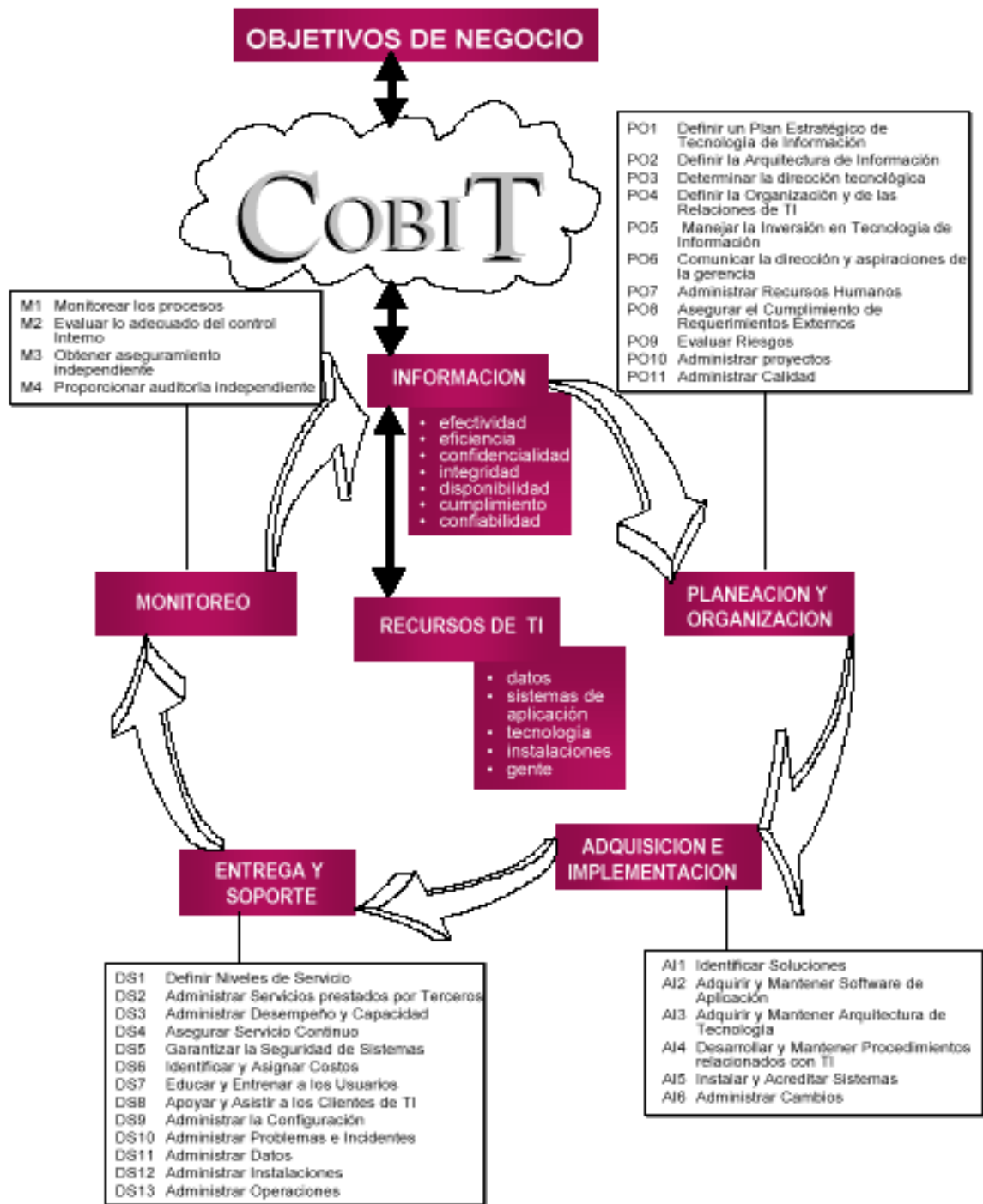


Figura 6 Objetivos de Control

4.3 Marco de referencia de CoBIT.

Uno de los estándares que más se están utilizando en el mundo para ser tomado como base para realizar una metodología de control interno en el ambiente de tecnología informática y sistemas de información, es el denominado CoBIT, el cual es un marco de referencia y se fundamenta en los objetivos de control existentes de la (ISACF), y que ha sido mejorado a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria. [C12]

El marco de referencia CoBIT otorga especial importancia al impacto sobre los recursos de tecnología informática, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el marco de referencia proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con tecnología de información. [C12]

La orientación a negocios es el tema principal de CoBIT. Está diseñado no sólo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y otorgamiento de autoridad de los dueños de procesos para que éstos posean total responsabilidad de todos los

aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados y herramientas al propietario de procesos de negocio que faciliten el cumplimiento de esta responsabilidad. [C12]

El desarrollo del marco de referencia CoBIT ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de tecnología informática particular, cuyo logro es posible a través del establecimiento de controles, para el cual deben considerarse controles aplicables potenciales. [C12]

Es aquí donde se requiere de un sano marco referencial de Objetivos de Control para TI como se muestra en la Figura 7. [C6]

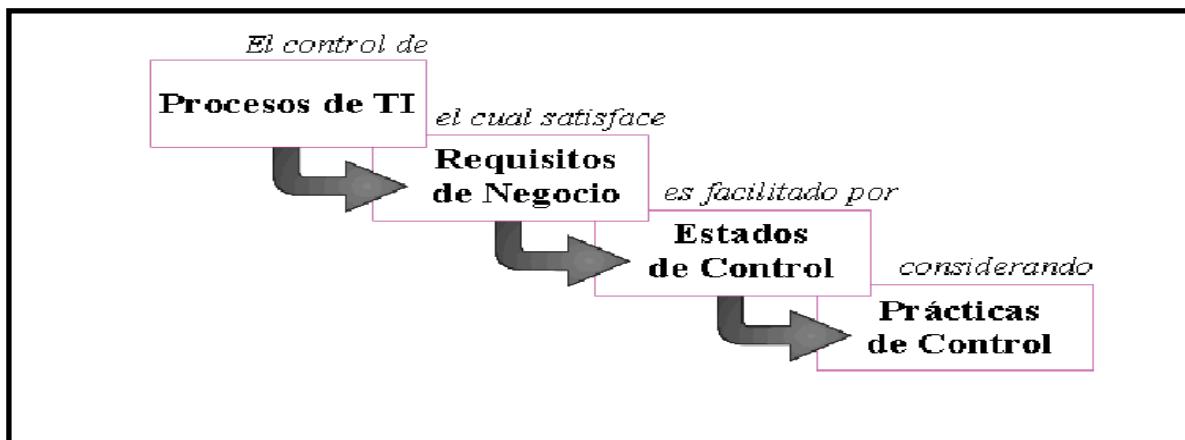


Figura 7 Organización del Marco Referencial.[C6]

El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos. [C6]

CAPÍTULO V

Capitulo 5 Dominios de CoBIT.

Dentro de este capítulo se hace mención de la definición de dominio, también se describen 4 clasificaciones que determinan a los dominios de CoBIT, la organización, la implementación, el soporte y el monitoreo de la tecnología de la información. Y por ultimo se enlistan algunas clasificaciones dentro de los subdominios.

5.1 Definición de dominios.

Es una agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional. [C1]

5.2 Clasificación de dominios.

Por lo tanto, se mencionan cuatro grandes dominios que son identificados y explicados a continuación: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo

5.2.1 Dominio de planificación y organización.

Este Dominio cubre la estrategia y las tácticas y le concierne la identificación de la forma en que la tecnología informática puede contribuir mejor al logro de los objetivos del negocio. Más aún, la realización de la visión estratégica necesita planearse, comunicarse y administrarse desde diferentes perspectivas. Finalmente, debe instalarse una organización apropiada así como una infraestructura tecnológica. [C13]

La Planificación y el dominio de Organización cubren el empleo de tecnología y como mejor, esto puede ser usado en una empresa ayudar alcanzar los objetivos de la empresa y objetivos. Esto también destaca la forma de organización e infraestructural TI debe tomar para alcanzar los resultados óptimos y generar la mayor parte de ventajas del empleo de TI. La mesa siguiente cataloga los objetivos de control nivel altos para el dominio de Organización y la Planificación.

Una buena planificación debe de realizar planes estratégicos de alta tecnología de información, definir arquitectura de la información y determinar la dirección tecnológica. [C2]

5.2.2 Dominio de adquisición e implementación.

Para comprender la estrategia de Tecnología Informática, las soluciones de Tecnología Informática necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en el proceso del negocio. Además, se cubren en este Dominio los cambios en y el mantenimiento de los sistemas existentes.

[C13]

5.2.2.1 Adquiera e Instrumento

Identificación de sus exigencias TI, adquiriendo la tecnología, y poniéndolo en práctica (realización) dentro de los procesos de negocio corrientes de la empresa. Este dominio también dirige el desarrollo de un plan de mantenimiento que una empresa debería adoptar para prolongar la vida de un sistema TI y sus componentes. La mesa siguiente cataloga los objetivos de control nivel altos para el dominio de Puesta en práctica y la Adquisición.

Se puede adquirir y mantener software de aplicación e instalar y acreditar sistemas, modificar soluciones y administrar cambios. [C2]

5.2.3 Dominio de entrega de servicio y soporte.

A este Dominio le concierne la entrega real de los servicios requeridos, que cubre desde las operaciones tradicionales sobre aspectos de seguridad y continuidad hasta el entrenamiento. Para brindar servicios deben instalarse los procesos de soporte necesarios. Este Dominio incluye el procesamiento real de los datos por los sistemas de aplicación, a menudo clasificados como controles de las aplicaciones. [C13]

5.2.3.1 Entrega y Apoyo

La entrega y el dominio de Apoyo enfocan en los aspectos de entrega de la tecnología de información. Esto cubre áreas como la ejecución de los usos dentro del sistema TI y sus resultados, así como, los procesos de apoyo que permiten la ejecución eficaz y eficiente de estos sistemas TI. Estos procesos de apoyo incluyen cuestiones de seguridad y educación (entrenamiento). La mesa siguiente cataloga los objetivos de control nivel altos para el dominio de Apoyo y la entrega.

[C2]

5.2.4 Dominio de monitoreo.

Todos los procesos de Tecnología Informática necesitan ser evaluados regularmente en el tiempo en su calidad y cumplimiento con los requerimientos de control.

5.2.4.1 Monitor y Evaluación

La Supervisión y el dominio de Evaluación tratan con la estrategia de una empresa en la evaluación de las necesidades de la empresa y si realmente la corriente TI el sistema todavía encuentra los objetivos para los cuales fue diseñado y los mandos necesarios de cumplir con exigencias reguladoras. La supervisión también cubre la cuestión de una evaluación independiente de la eficacia de sistema TI en su capacidad de encontrar objetivos de negocio y los procesos de control de la

empresa por interventores internos y externos. La mesa siguiente cataloga los objetivos de control nivel altos para la Supervisión del dominio. [C6]

5.2.5 Subdominios.

Los subdominios son los primeros Objetivos de Control de CoBIT y se constituyen en los macroprocesos definidos como el conjunto de buenas prácticas, una evaluación a este nivel se denomina evaluación al primer nivel. Estos subdominios o procesos están distribuidos entre los 4 dominios y se listan tal y como sigue:

En el primer dominio se encuentran:

Definir un plan estratégico de sistemas, Definir la arquitectura de información, Determinar la dirección tecnológica, Definir la organización y sus relaciones, Administrar las inversiones, Comunicar la dirección y objetivos de la gerencia, Administrar los recursos humanos, Asegurar el apego a disposiciones externas, Evaluar riesgos, Administrar proyectos, Administrar calidad.

En el segundo dominio se encuentran:

Identificar soluciones de automatización, Adquirir y mantener software de aplicación, Adquirir y mantener la arquitectura tecnológica, Desarrollar y mantener procedimientos, Instalar y acreditar sistemas de información, Administrar cambios

En el tercer dominio se encuentran:

Definir niveles de servicio, Administrar servicios de terceros, Administrar desempeño y capacidad, Asegurar continuidad de servicio, Garantizar la seguridad de sistemas, Identificar y asignar costos, Educar y capacitar a usuarios, Apoyar y orientar a clientes, Administrar la configuración, Administrar problemas e incidentes, Administrar la información, Administrar las instalaciones, Administrar la operación

En el cuarto dominio se encuentran:

Monitorear el proceso, Evaluar lo adecuado del control interno, Obtener aseguramiento independiente, Proporcionar auditoria independiente [C13]

Conclusiones.

El impacto creciente de la tecnología en los procesos de negocio y el advenimiento de las operatorias de las organizaciones por medio de Internet, ocasionarán grandes cambios que modificarán radicalmente las pautas de los controles que se deberán establecer en estas nuevas realidades. La productividad y supervivencia futura de una organización dependerá cada vez en mayor grado, del funcionamiento ininterrumpido de los sistemas de tecnología informática, transformando a todo el entorno como un proceso crítico adicional. Todas las empresas, incluidas aquellas que ignoran las nuevas tecnologías, sentirán el impacto de estos nuevos escenarios de riesgo. Por ello la importancia de contar con marco de referencia metodológico que agilice todo el proceso de la Auditoría de Sistemas de Información.

Durante el transcurso de esta investigación, se encontró información sobre las aplicaciones del sistema CoBIT, pero algunas de estas tienen interés sobre todo en las grandes empresas, industrias ya sean nacionales e internacionales; la tecnología ha crecido a pasos agigantados, pero algo que les falta a los grandes investigadores es dar a conocer la tecnología de este tipo de sistemas, debido a que es necesario tener conocimientos en los diferentes sistemas que se aplican para obtener mejoras en los estándares internacionales, técnicos, profesionales, regulativos y específicos para las industrias.

Es importante también tener en consideración el buscar otras aplicaciones, ya que el potencial es demasiado grande, y de ello depende las buenas practicas de seguridad y control en tecnología de la información, existen objetivos que controlan la tecnología que se debe desarrollar en una empresa para determinar el buen funcionamiento, la organización, el monitoreo y la entrega

Muchas organizaciones en la actualidad reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados. Es portal razón que se estudio una herramienta de control que beneficie a todos los procesos dentro de la entidad en la búsqueda de la eficiente y eficaz de la misma para un mayor grado de desempeño y crecimiento institucional.

Este tipo de sistemas proporciona el desarrollo de un estándar generalmente aceptado y aplicable a las buenas prácticas de seguridad y control en TIC. Ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona “prácticas sanas” a través de un Marco Referencial de dominios y procesos y presenta actividades en una estructura manejable y lógica.

Las prácticas sanas de COBIT representan el consenso de los expertos que tiene una premisa simple y práctica: con el fin de proporcionar la información que la

organización necesita para alcanzar sus objetivos, señala que los recursos de TIC deben ser administrados por un conjunto de procesos de TIC agrupados en forma natural. Está diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como un Check List detallado para los responsables de cada proceso. Proporciona herramientas al responsable de los procesos que facilitan el cumplimiento de esta tarea .es, por lo tanto, la herramienta innovadora para el manejo de TIC que ayuda a la gerencia a comprender y administrar los riesgos asociados con TIC.

Entender y aplicar la TI no como un simple apoyo para la empresa sino como una función organizacional vital, es una necesidad y un reto para los profesionales de la computación y lo es aún más, dado que en el país donde vivimos el perfil profesional no está capacitado para hacer frente a dicha labor. Se encuentra desatendido curricularmente, tal desatención genera perjuicios para las organizaciones, pues sumidas en mayor o menor grado en el fenómeno del despilfarro computacional, no encuentran personas que atiendan efectivamente dicha problemática. Esto no quiere decir que en general la calidad de los profesionales en computación sea deficiente, sino que en la formación universitaria no se desarrollan competencias administrativas informáticas (a nivel organizacional más no técnico) que ataquen este fenómeno para contribuir a solucionar la problemática atacándola de raíz: El desarrollo de competencias profesionales en ATI. No obstante, se ha de reconocer que la tarea no resulta sencilla, puesto que la computación nacional, como profesión, nunca ha tenido las riendas de un direccionamiento propio de la TI. Por tal razón, queda aún mucho

por hacer tanto académica como empresarialmente, siendo un buen punto de partida la transformación curricular en las universidades para la aplicación de modelos como CoBIT en las empresas.

Glosario.

AICPA:

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

ASL:

Application Services Library (Biblioteca de servicios de aplicativos).

CCEB:

Criterios comunes para seguridad en tecnología de información. (*Common Criteria for*)

CCTA:

Central Computer and Telecommunications Agency. Central de computadoras y telecomunicaciones de agencia.

CICA:

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

CISA:

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

CMM:

Modelo de Capacidad y Madurez.

COBIT:

Objetivos de Control para la información y Tecnologías relacionadas (en inglés: Control Objectives for Information and related Technology)

Control de TI:

Procedimientos de control en una actividad particular de TI.

Control:

Políticas, procedimientos, prácticas y estructuras organizacionales, diseñados para proporcionar una seguridad razonable de que los objetivos del negocio serán alcanzados y que eventos no deseados serán prevenidos o detectados y corregidos.

COSO:

Comité de Organizaciones Patrocinadoras de la Comisión de Intercambio. "Tradeway" (*Committee of Sponsoring Organisations of the Tradeway Commission*). *Data Interchange for Administration, Commerce and Trade*)

DRI:

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

DSDM:

Método de desarrollo de sistemas dinámicos (*Dynamic Systems Development Method*).

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

EDIFACT:

Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria (*Electronic*)

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. (*for IT Security Matters to the European Commission*)

GAAP:

Principios Contables Generalmente Aceptados.

GAO:

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

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 Information Technology Security*)

INFOSEC:

Comité Consultivo para la Comisión Europea en Materia de Seguridad TI.
(*Advisory Committee*)

ISACA:

La Asociación para la Auditoría y Control de Sistemas de Información, (en inglés: 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*) (con oficinas en Génova, Suiza)

ISO9000:

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

ISPL:

Information Services Procurement Library (Biblioteca de adquisición de servicios de información).

ITGI:

Instituto de Administración de las Tecnologías de la Información (en inglés: IT Governance Institute).

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. (*the United Kingdom*)

Ticket:

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

Bibliografía

- B1. “Diccionario Educativo Inicial Larousse”. (2003). Editorial Ultra S.A. de C.V. México.
- B2. “Diccionario Enciclopédico océano uno color” (1996). MCMXCVI Océano, S.A. de Barcelona (España).

Cibergrafía.

- C1. Objetivos de control para la información y tecnologías relacionadas.
<http://www.monografias.com>
Fecha de consulta: Noviembre 2007.
- C2. En consiste cobit
<http://www.monografias.com/trabajos38/cobit/cobit2.shtml#rese>
Fecha de consulta: Noviembre del2008
- C3. COBIT–Objetivos de Control para la Información Pública y Tecnologías Relacionadas <http://www.comip.mendoza.gov.ar/cobit>. Gobierno de Mendoza–Com.I.P.doc.
Fecha de consulta: Noviembre del 2007
- C4. ISACA. COBIT. “Control objectives IT Weber, Ron; “EDP Auditing: Conceptual Foundations and Practice”. Ed. McGraw Hill. 1998.
<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=5623&TEMPLATE=/ContentManagement/ContentDisplay.cfm>
Fecha de consulta: Noviembre del 2007
- C5. Instrumento de puesta
práctica<http://www.coit.es/publicac/publbit/bit128/bitcd1/hm/herramientas/Auditoria.htm> Fecha de consulta: Febrero 2008
- C6. COBIT (objetivos de control para tecnología de información y tecnologías Relacionadas). <http://www.unap.cl/~setcheve/cobit/CobIT-106.htm> Fecha De consulta: Abril 2008
- C7 Gran parte de COBIT está disponible como descarga complementaria en <http://www.isaca.org/cobit> . Puede adquirir copias impresas en ISACA Bookstore (<http://www.isaca.org/bookstore>) por 190 dólares. También Existe una emisión Web complementaria detallada de COBIT 4.0 Disponible en <https://www.livemeeting.com/cc/isaca/view>. Fecha de Consulta: Abril 2008
- C8. Para qué sirve COBIT familia de producto Como se aplica o como se usa Reseña histórica COBIT y otras normas
<http://www.monografias.com/trabajos38/cobit/cobit.shtml>
Fecha de consulta: Abril 2008

-
- C9. Red de Abastecimiento, En qué consiste COBIT 4.0 Documentos Técnicos
Red de Abastecimiento – Dirección Postal: Casilla 52983, Correo Central,
Santiago, Chile Correo: redaba@terra.cl
Sitio Web: www.redaba.cl
<http://reddeabastecimiento.org/COBIT%204.pdf>
Fecha de consulta: Febrero2008
- C10. Decreto n°.: 1806/99–Resolución n°.: 54–Gobierno de Mendoza–Com.I.P.
COBIT–Objetivos de Control para la Información Pública y Tecnologías
Relacionadas. Fuente: www.isaca.org
<http://www.comip.mendoza.gov.ar/cobit.doc>
Consulta: Marzo 2008
- C11. Nueva Versión COBIT, Mejora de Procesos
(www.itgi.org.)
Consulta: Marzo 2008
- C12. Universidad de Palermo, Facultad de Ciencia y Tecnología, Auditoria y
seguridad de Sistema Cobit la Auditoria por Objetivos de Control
http://www.tecnobank.com.ar/magazine/19/nota_15.html
<http://www.cpcipc.org/razonestado/seguridad.htm>
<http://www.isaca.org>
Consulta: Marzo 2008
- C13. Soluciones de negocios para futuras generaciones antecedentes.
www.newtech.co.cr
Consulta: Marzo 2008
- C 14 Cobit – Resumen UNSa. Coordinación Informática Secretaría de
Cooperación Técnica.
<http://bo.unsa.edu.ar/sct/gestion/docs/tic/cobit.html>
Consulta: Marzo 20