GOVERNANCE INSTITUTE®

COBIT®

MARCO REFERENCIAL

3a Edición

Emitido por el Comité Directivo de COBIT y

El IT Governance Institute MR

La Misión de COBIT:

Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

ARGENTINA
ARUBA
AUSTRALIA
AUSTRIA
BAHAMAS
BAHRAIN
BANGLEDESH
BARBADOS
BÉLGICA
BERMUDA
BOLIVIA
BOSTSWANA
BRASIL
BRUENI
CANADÁ
CHILE
CHINA
COLOMBIA
COSTA RICA
CROATA
CURAZAO
CYPRUS
REPÚBLICA CHECA
DINAMARCA
REPÚBLICA DOMINICANA
ECUADOR
EGIPTO
ESTONIA
ISLAS FAEROE
FINLANDIA
FRANCIA
ALEMANIA
GHANA
GRECIA
GUAM
GUATEMALA
HONDURAS
HONG KONG
HUNGRÍA
ISLANDIA
INDIA
INDONESIA
IRLANDA
ISRAEL
ITALIA
IVORY COAST
JAMAICA
JAPÓN
JORDÁN
KENYA
COREA
KUWAIT
LATVIA
LEBANON

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

Una sola Fuente Internacional para los Controles de la Tecnología de Información

Information Systems Audit and Control Association es una organización global líder de profesionales que representa a individuos en más de 100 países y comprende todos los niveles de la tecnología de información —Dirección ejecutiva, gerencia media y practicantes. La Asociación está únicamente posesionada para cubrir el papel de generador central que armoniza los estándares de las prácticas de control de TI a nivel mundial. Sus alianzas estratégicas con otros grupos dentro del ámbito profesional financiero, contable, de auditoría y de TI aseguran a los dueños del proceso del negocio un nivel sin paralelo de integración y compromiso.

Programas y Servicios de la Asociación

Los Programas y Servicios de la Asociación han ganado prestigio al establecer los niveles más altos de excelencia en certificación, estándares, educación profesional y publicidad técnica.

- *su programa de certificación (el Auditor de Sistemas de Información Certificado) es la única designación global en toda la comunidad de control y auditoría de la TI.*
- *sus actividades estándar establecen la base de calidad mediante la cual otras actividades de control y auditoría de TI se miden.*
- *su programa de educación profesional ofrece conferencias técnicas y administrativas en cinco continentes, así como seminarios en todo el mundo para ayudar a los profesionistas de todas partes a recibir educación continúa de alta calidad.*
- *su área de publicidad técnica proporciona materiales de desarrollo profesional y referencias con el fin de aumentar su distinguida selección de programas y servicios.*

La Information Systems Audit and Control Association se creó en 1969 para cubrir las necesidades únicas, diversas y de alta tecnología en el naciente campo de la TI. En una industria donde el progreso se mide en nanosegundos, ISACA se ha movido ágil y velozmente para satisfacer las necesidades de la comunidad de negocios internacionales y de la profesión de controles de la TI.

Para más Información

Para recibir información adicional, puede llamar al (+1.847.253.1545), enviar un e-mail a (research@isaca.org) o visitar los siguentes sitios web:

www.itgovernance.org
www.isaca.org

LIECHTENSTEIN
LITUANIA
LUXEMBURGO
MALASIA
MALTA
MALAWI
MÉXICO
PAÍSES BAJOS
NUEVA GUINEA
NUEVA ZELANDA
NIGERIA
NORUEGA
OMÁN
PAKISTÁN
PANAMÁ
PERÚ
FILIPINAS
POLONIA
PORTUGAL
QATAR
RUSIA
SAIPAN
ARABIA SAUDITA
ESCOCIA
SEYCHELLES
SINGAPUR
REP. ESLOVACA
ESLOVENIA
SUDÁFRICA
ESPAÑA
SRI LANKA
ST. KITTS
ST. LUCIA
SUECIA
SUIZA
SIRIA
TAIWAN
TANZANIA
TASMANIA
TAILANDIA
TRINIDAD & TOBAGO
TURQUÍA
UGANDA
EMIRATOS ARAB UNIDOS
REINO UNIDO
ESTADOS UNIDOS
URUGUAY
VENEZUELA
VIETNAM
GALES
YEMEN
ZAMBIA
ZIMBABWE

MARCO REFERENCIAL

Information Systems Audit and Control Foundation
IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA.
Teléfono: 1+847.253.1525
Fax: 1+847.253.1443
E-mail: *research@isaca.org*
Web sites: *www.isaca.org*
www.itgi.org

ISBN 1-893209-98-9 (*Marco Referencial*, Español)
ISBN 1-933284-02-1 (Paquete completo de los 6 libros y CD)

Impreso en los Estados Unidos de América

Límite de Responsabilidad

La Information Systems Audit and Control Association—ISACA- y el IT Governance Institute –ITGI- (los propietarios) han creado esta publicación titulada COBIT: *Objetivos de Control para la Información y las Tecnologías Relacionadas (el "trabajo")* principalmente como un recurso educativo para los profesionales dedicados a las actividades de control. Los Propietarios declaran que no responden o garantizan que el uso que se le de al "Trabajo" asegurará un resultado exitoso. No deberá considerarse que el "Trabajo" incluye toda la información, los procedimientos o las pruebas apropiadas o excluye otra información, procedimientos y pruebas que estén razonablemente dirigidas a la obtención de los mismos resultados. Para determinar la conveniencia de cualquier información, procedimiento o prueba específica, los expertos en control deberán aplicar su propio juicio profesional a las circunstancias específicas presentadas por los sistemas o por el ambiente de tecnología de información en particular.

Esta edición de COBIT fue traducida al idioma español por Gustavo Adolfo Solís Montes, Lucio Augusto Molina Focazzio, Johann Tello Meryk y Rocío Torres Suárez, (los "traductores"). Los traductores asumen la responsabilidad exclusiva por la actualización y por la fidelidad de la traducción. La Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI) declaran que no responden por la actualización, totalidad, o por la calidad de la traducción. En ningún evento ISACA/ITGI será responsable ante un individuo u organización por los daños causados en relación con la edición del lenguaje, cualquier actualización, modificación, localización o traducción.

RECONOCIMIENTOS

Agradecimientos Especiales a los Capítulos de ISACA del área de la Capital Nacional y al de Boston por su contribución a los *Objetivos de Control* de COBIT

Agradecimientos Especiales a los miembros de la Mesa Directiva de la Information Systems Audit and Control Association y a los Fideicomisarios de la Information Systems Audit and Control Foundation, encabezados por el Presidente Internacional Paul Williams, por su contínuo y firme apoyo al COBIT

RESUMEN EJECUTIVO

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) Relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información[1]
- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos mas valiosos de la empresa. Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la Gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI. Por lo tanto, la Administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega; al tiempo que demanda que esto se realice a un costo más bajo**.**

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

Hay numerosos cambios en TI y en su ambiente de operación que enfatiza la necesidad de un mejor manejo relacionado con los riesgos de TI. La dependencia en la información electrónica y en los sistemas de TI son esenciales para soportar los procesos críticos del negocio. Adicionalmente, el ambiente regulatorio demanda control estricto sobre la información. Esto a su vez conduce a un incremento de los desastres en los sistemas de información y al incremento del fraude electrónico. La Administración de los riesgos relacionados con TI está siendo entendido como un aspecto clave en el gobierno o dirección empresarial.

Dentro del Gobierno Empresarial, el Gobierno / Gobernabilidad de TI[2] se está volviendo mas y mas importante y está definido como una estructura de relaciones y procesos para dirigir y controlar a la empresa con el fin que ésta pueda cumplir sus metas dando valor agregado mientras balancea sus riesgos versus el retorno sobre TI y sus procesos. El Gobierno de TI es parte integral del éxito de la Gerencia de la Empresa al asegurar mejoras medibles, eficientes y efectivas de los procesos relacionados de la empresa. El Gobierno de TI provee las estructuras que unen los procesos de TI, los recursos de TI y la información con las estrategias y los objetivos de la empresa. Además, el Gobierno de TI integra e institucionaliza buenas (o mejores) prácticas de planeación y organización, adquisición e implementación, entrega de servicios y soporte y monitorea el desempeño de TI para asegurar que la información de la empresa y las tecnologías relacionadas soportan sus objetivos del negocio. El Gobierno de TI conduce a la empresa a tomar total ventaja de su información logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva

GOBIERNO DE TI

Una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la empresa y añadir valor mientras se balancean los riesgos versus el retorno sobre TI y sus procesos.

Las organizaciones deben cumplir con requerimientos de calidad, fiduciarios y de seguridad, tanto para su información, como para sus activos. La Administración deberá además optimizar el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus

[1] **Guerra de información** *(information warfare)*

[2] **Gobierno de TI** (IT Governance) *Governance* es un término que representa *el* sistema de control o administración que establece la alta gerencia para asegurar el logro de los objetivos de una Organización.

objetivos, la Administración debe entender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

Los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), ahora en esta tercera edición, ayuda a satisfacer las múltiples necesidades de la Administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. Provee buenas prácticas a través de un dominio y el marco referencial de los procesos y presenta actividades en una estructura manejable y lógica. Las "Buenas prácticas" de COBIT reúne el consenso de expertos - quienes ayudarán a optimizar la inversión de la información y proporcionarán un mecanismo de medición que permitirá juzgar cuando las actividades van por el camino equivocado.

La Administración debe asegurar que los sistemas de control interno o el marco referencial están funcionando y soportan los procesos del negocio y debe tener claridad sobre la forma como cada actividad individual de control satisface los requerimientos de información e impacta los recursos de TI. El impacto sobre los recursos de TI son resaltados en el M*arco de Referencia* de COBIT junto con los requerimientos del negocio que deben ser alcanzados: eficiencia, efectividad, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

La administración, mediante este gobierno corporativo, debe asegurar que todos los individuos involucrados en la administración, uso, diseño, desarrollo, mantenimiento u operación de sistemas de información actúen con la debida diligencia.

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI.

La orientación al negocio es el tema principal de COBIT. Está diseñado no solo para ser utilizado por usuarios y auditores, sino que, lo más importante, esta diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible. A medida que ascendemos, las prácticas de negocio requieren de una mayor delegación y empoderamiento[3] de los dueños de los procesos para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En particular, esto incluye el proporcionar controles adecuados.

El *Marco de Referencia* de COBIT proporciona, al propietario de procesos de negocio, herramientas que facilitan el cumplimiento de esta responsabilidad. El *Marco de Referencia* comienza con una premisa simple y práctica:

Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos de TI agrupados en forma natural.

El *Marco de Referencia* continúa con un conjunto de 34 *Objetivos de Control* de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios: Planeación y Organización, Adquisición e Implementación, Entrega de servicios y Soporte y Monitoreo. Esta estructura cubre todos los aspectos de información y de tecnología que la soporta. Administrando adecuadamente estos 34 Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información.

El *Marco de Referencia* de COBIT provee además una guía o lista de verificación para el Gobierno de TI. El Gobierno de TI proporciona las estructuras que encadenan los procesos de TI, los recursos de TI y la información con los objetivos y las estrategias de la empresa. El Gobierno de TI integra de una forma óptima el desempeño de la Planeación y Organización, la Adquisición e Implementación, la Entrega de Servicios y Soporte y el Monitoreo. El Gobierno de TI facilita que la empresa obtenga total ventaja de su información y así mismo maximiza sus beneficios, capitalizando sus oportunidades y obteniendo ventaja competitiva

Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una *Guía o directriz de Auditoría* o de aseguramiento que permite la revisión de los procesos de TI contra los 318 objetivos detallados de control recomendados por COBIT para proporcionar a la Gerencia la certeza de su cumplimiento y/o sugerencias para su mejoramiento.

[3] **Empoderamiento** (*empowerment)*

Las Guías o Directrices Gerenciales de COBIT, desarrolladas recientemente, ayudan a la Gerencia a cumplir de una forma mas efectiva con las necesidades y requerimientos del Gobierno de TI. Las Directrices son acciones genéricas orientadas a proveer a la Administración la dirección para mantener bajo control la información de la empresa y sus procesos relacionados, para monitorear el logro de las metas organizacionales, para monitorear el desempeño de cada proceso de TI y para llevar a cabo un benchmarking de los logros organizacionales.

Específicamente COBIT provee **Modelos de Madurez** para el control sobre los procesos de TI de tal forma que la Administración puede ubicarse en el punto donde la organización está hoy, donde está en relación con los "mejores de su clase" en su industria y con los estándares internacionales y así mismo determinar a donde quiere llegar; **Factores Críticos de Éxito (Critical Success Factors)**, que definen o determina cuales son las mas importantes directrices que deben ser consideradas por la Administración para lograr control sobre y dentro de los procesos de TI. **Indicadores Claves del logro / Objetivos o de Resultados (Key Goal Indicators)** los cuales definen los mecanismos de medición que indicarán a la Gerencia—después del hecho– si un proceso de TI ha satisfecho los requerimientos del negocio; y los **Indicadores Clave de desempeño (Key Performance Indicators)** los cuales son indicadores primarios que definen la medida para conocer qué tan bien se está ejecutando el proceso de TI frente o comparado contra el objetivo que se busca.

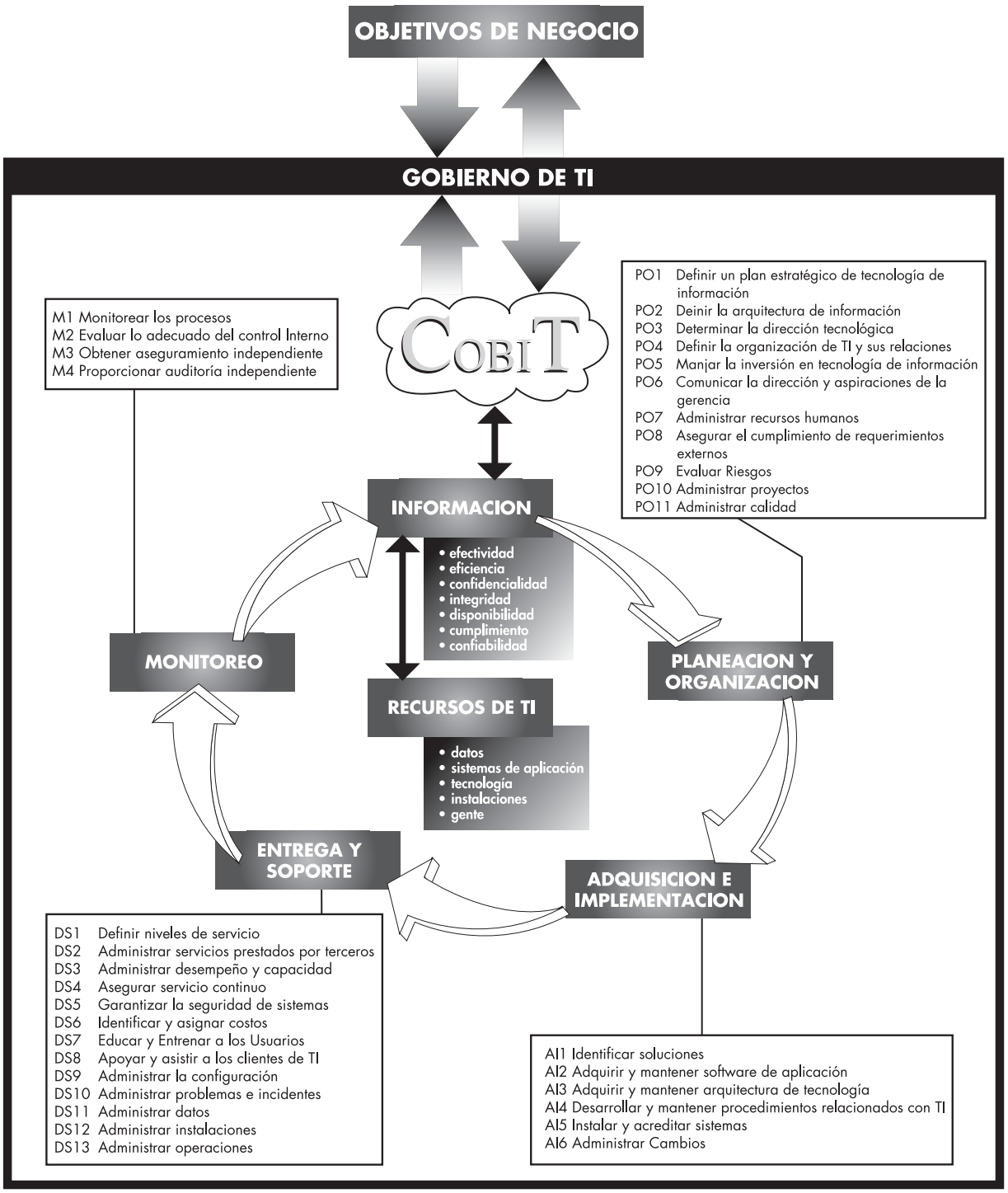
Las *Directrices Gerenciales* de COBIT son genéricas y son acciones orientadas al propósito de responder los siguientes tipos de preguntas gerenciales: ¿Qué tan lejos debemos ir y se justifica el costo respecto al beneficio obtenido? ¿Cuáles son los indicadores de buen desempeño? ¿Cuáles son los factores críticos de éxito? ¿Cuáles son los riesgos de no lograr nuestros objetivos? ¿Qué hacen otros? ¿Cómo nos podemos medir y comparar?

COBIT contiene adicionalmente un *Conjunto de Herramientas de Implementación* que proporciona lecciones aprendidas por empresas que rápida y exitosamente aplicaron COBIT en sus ambientes de trabajo. Incluye dos herramientas particularmente útiles - Diagnóstico de Sensibilización Gerencial (Management Awareness Diagnostic) y Diagnóstico de Control en TI (IT Control Diagnostic) - para proporcionar asistencia en el análisis del ambiente de control de TI en una organización.

En los próximos años las Directivas de las Organizaciones necesitarán demostrar que están logrando incrementar sus niveles de seguridad y control. COBIT es una herramienta que ayuda a los Directivos a colocar un puente entre los requerimientos de control, los aspectos técnicos y los riesgos del negocio y adicionalmente informa a los accionistas o dueños de la empresa el nivel de control alcanzado. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de las organizaciones, a nivel mundial.

Por lo tanto, COBIT está diseñado para ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas.

PROCESOS DE TI DEFINIDOS DENTRO DE LOS CUATRO DOMINIOS DE COBIT



EL MARCO REFERENCIAL DE COBIT

LA NECESIDAD DE CONTROL EN TECNOLOGIA DE INFORMACION

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 un efectiva dirección y controles adecuados.

LA ADMINISTRACION (MANAGEMENT) 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.

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.

EL AMBIENTE DE NEGOCIOS: COMPETENCIA, CAMBIO Y COSTOS

La competencia global es ya un hecho. Las organizaciones se reestructuran con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en TI para mejorar su posición competitiva. La reingeniería en los negocios, las reestructuraciones o right-sizing, el *outsourcing*, el empoderamiento, las organizaciones horizontales y el procesamiento distribuido son cambios que impactan la manera en la que operan tanto los negocios como las entidades gubernamentales. Estos cambios han tenido y continuarán teniendo, profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo.

La especial atención prestada a la obtención de ventajas competitivas y a la eficiencia en costos implica una dependencia creciente en la tecnología como el componente más importante en la estrategia de la mayoría de las organizaciones. La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en las computadoras y en las redes, tanto para las basadas en hardware como las basadas en software. Además, las características estructurales fundamentales de estos controles están evolucionando al mismo paso que las tecnologías de computación y las redes.

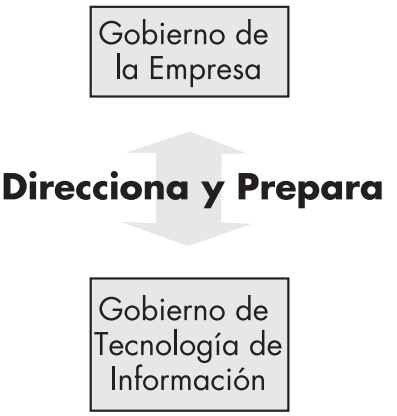
Dentro del marco referencial de cambios acelerados, si los administradores, los especialistas en sistemas de información y los auditores desean en realidad ser capaces de cumplir con sus tareas en forma efectiva , deberán aumentar y mejorar sus habilidades tan rápidamente como lo demandan la tecnología y el ambiente. Debemos comprender la tecnología de controles involucrada y su naturaleza cambiante si deseamos emitir y ejercer juicios razonables y prudentes al evaluar las prácticas de control que se encuentran en los negocios típicos o en las organizaciones gubernamentales.

APARICION DEL GOBIERNO DE LA EMPRESA Y DEL GOBIERNO DE TI

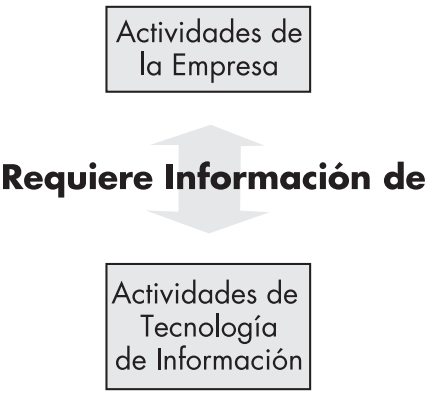
Para lograr el éxito en esta economía de información, el Gobierno de la empresa y el Gobierno de TI no pueden ser consideradas separadamente y en distintas disciplinas. El gobierno efectivo de la empresa enfoca el conocimiento y la experiencia en forma individual y grupal, donde puede ser mas productivo, monitoreado y medido el desempeño así como provisto el aseguramiento para aspectos críticos. TI, por mucho tiempo considerada aislada dentro del logro de los objetivos de la empresa debe ahora ser considerada como una parte integral de la estrategia.

El Gobierno de TI provee la estructura que une los procesos de TI, los recursos de TI y las estrategias y objetivos de la empresa. El Gobierno de TI integra e institucionaliza de una manera óptima la planeación y organización, la adquisición e implementación, la entrega de servicios y soporte y el monitoreo del desempeño de TI. El Gobierno de TI es integral para el éxito del Gobierno de la Empresa asegurando una eficiente y efectiva medición para mejorar los procesos de la empresa. El Gobierno de TI le permite a la empresa tomar ventaja total de su información, al maximizar sus beneficios, capitalizar sus oportunidades y ganar ventaja competitiva.

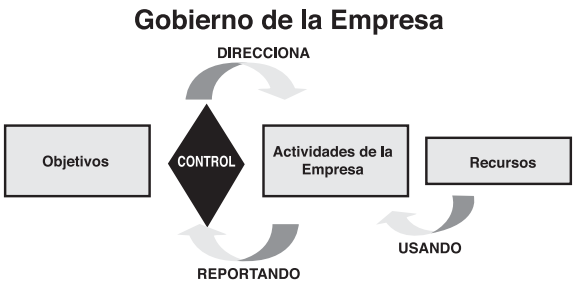
Observando en el contexto a la empresa y los procesos del Gobierno de TI con mayor detalle, el gobierno de la empresa, el sistema por el cual las entidades son dirigidas y controladas direcciona y analiza el Gobierno de TI. Al mismo tiempo, TI debería proveer insumos críticos y constituirse en un componente importante de los planes estratégicos. De hecho TI puede influenciar las oportunidades estratégicas de la empresa.



Las actividades de la empresa requieren información de las actividades de TI con el fin de satisfacer los objetivos del negocio. Organizaciones exitosas aseguran la interdependencia entre su plan estratégico y sus actividades de TI. TI debe estar alineado y debe permitir a la empresa tomar ventaja total de su información para maximizar sus beneficios, capitalizar oportunidades y ganar ventaja competitiva.



Las empresas son gobernadas por buenas (o mejores) prácticas generalmente aceptadas para asegurar que la empresa cumpla sus metas asegurando que lo anterior esté garantizado por ciertos controles. Desde estos objetivos fluye la dirección de la organización, la cual dicta ciertas actividades a la empresa usando sus propios recursos. Los resultados de las actividades de la empresa son medidos y reportados proporcionando insumos para el mantenimiento y revisión constante de los controles, comenzando el ciclo de nuevo.



También TI es gobernado por buenas (o mejores) prácticas para asegurar que la información de la empresa y sus tecnologías relacionadas apoyan sus objetivos del negocio, estos recursos son utilizados responsablemente y sus riesgos son manejados apropiadamente. Estas prácticas conforman una base para la dirección de las actividades de TI las cuales pueden ser enmarcadas en la Planeación y Organización, Adquisición e Implementación, Entrega de Servicios y Soporte y Monitoreo para los propósitos duales como son el manejo de riesgo (para obtener seguridad, confiabilidad y cumplimiento) y la obtención de beneficios (incrementando la efectividad y eficiencia). Los reportes son enfocados sobre los resultados de las actividades de TI, los cuales son medidos contra diferentes prácticas y controles y el ciclo comienza otra vez.

Para asegurar que la Gerencia alcance los objetivos de negocios, ésta debe dirigir y administrar las actividades de TI para alcanzar un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para cumplir esto, la Gerencia necesita identificar las actividades mas importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando que tan bien se están desarrollando los procesos de TI. Aun mas, necesita tener la habilidad de avaluar el nivel de madurez de la organización contra las mejores practicas industriales y los modelos internacionales. **Para soportar estas necesidades la Gerencia necesita las *Directrices Gerenciales* de COBIT en las cuales se han identificado Factores Críticos de Exito específicos, Indicadores Claves por Objetivo e Indicadores Clave de Desempeño y un Modelo de Madurez asociado al Gobierno de TI, como se puede apreciar en el Apédice I.**

RESPUESTA A LAS NECESIDADES

En vista de estos continuos cambios, el desarrollo de este Marco Referencial de objetivos de control para TI, conjuntamente con una investigación continua aplicada a controles de TI basada en este marco referencial, constituyen el fundamento para el progreso efectivo en el campo de los controles de sistemas de información.

Por otro lado, hemos sido testigos del desarrollo y publicación de modelos de control generales de negocios como COSO [*Committee of Sponsoring Organisations of the Treadway Commisssion Internal Control-Integrated Framework*, 1992] en los EUA, *Cadbury* en el Reino Unido, *CoCo* en Canadá y *King* en Sudáfrica. Por otro lado, existe un número importante de modelos de control más enfocados al nivel de tecnología de información. Algunos buenos ejemplos de esta última categoría son el *Security Code of Conduct* del DTI (*Departamento de Industria y Comercio*, Reino Unido) y el *Security Handbook* de NIST (*National Institute of Standards and Technology*, EUA). Sin embargo, estos modelos de control con orientación específica no proporcionan un modelo de control completo y utilizable sobre tecnología de información como soporte para los procesos del negocio. El propósito de *COBIT* es cubrir este vacío proporcionando una base que esté estrechamente ligada a los objetivos de negocio, al mismo tiempo que se enfoca a la tecnología de información.

(El documento que más se acerca al COBIT es una publicación reciente de *AICPA/CICA Systrust ™ Principios y Criterios para la Confiabilidad de los Sistemas*. SysTrust es una autoridad que realiza publicaciones para el Comité Ejecutivo de Servicios de Aseguramiento de los Estados Unidos y para el Comité de Desarrollo de Servicios de Calidad de Canadá, basado en parte en los *Objetivos de Control* de COBIT . SysTrust está diseñado para incrementar el confort de la Administración, los clientes y los socios de negocios con los sistemas que soportan un negocio o una actividad en particular. Los servicios de SysTrust incluyen al contador público proporcionándole un servicio de aseguramiento en el cual él o ella evalúa y prueba si el sistema es confiable cuando lo mide contra cuatro principios esenciales: Disponibilidad, seguridad, integridad y mantenimiento.

Un enfoque hacia los requerimientos del negocio en cuanto a controles para tecnología de información y la aplicación de modelos de control emergentes y estándares internacionales relacionados incluyen los *Objetivos de Control* originales de la Information Systems Audit and Control Foundation como una herramienta usada por el Auditor y la Administración**.** Adicionalmente, el desarrollo de las *Directrices Gerenciales* de TI ha llevado al COBIT al siguiente nivel proporcionando a la Administración Indicadores Clave de Logros (KGIs— Key Goal Indicators), Indicadores Claves de Desempeño (KPIs— Key Performance Indicators), Factores Críticos de Éxito (CSFs—Critical Success Factors) y un Modelo de Madurez con el cual puede analizar el ambiente de TI y considerar opciones para la implementación y mejoramiento de los controles sobre la información de la organización y sus tecnologías relacionadas.

Por lo tanto, el objetivo principal del proyecto *COBIT* es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. (Esto concuerda con la perspectiva COSO, que constituye el primer y mejor marco referencial para la administración en cuanto a controles internos.) Posteriormente, los objetivos de control fueron desarrollados a partir de la perspectiva de los objetivos de auditoría (certificación de información financiera, certificación de medidas de control interno, eficiencia y efectividad, etc.)

AUDIENCIA: ADMINISTRACION, USUARIOS Y AUDITORES

COBIT está diseñado para ser utilizado por tres audiencias distintas:

ADMINISTRACION/ GERENCIA (Management):

Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

USUARIOS:

Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

AUDITORES:

Para soportar su opinión y/o proporcionar consejos a la Administración sobre los controles internos.

ORIENTACIÓN A OBJETIVOS DE NEGOCIO

El COBIT está alineado con los Objetivos del Negocio. Los Objetivos de Control muestran una relación clara y distintiva con los objetivos del negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoría. Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Adicionalmente, se establecen consideraciones y guías para definir e implementar el Objetivo de Control de TI.

La clasificación de los dominios a los que se aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los requerimientos de negocio para la información en ese dominio, así como los recursos de TI que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el M*arco de Referencia de* COBIT. El *Marco de Referencia* toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 318 objetivos de control detallados. El *Marco de Referencia* fue presentado a la industria de TI y a los profesionales dedicados a la auditoría para abrir la posibilidad a revisiones, cambios y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

DEFINICIONES GENERALES

Para propósitos de este proyecto, se proporcionan las siguientes definiciones. La definición de "Control" está adaptada del reporte *COSO [Committee of Sponsoring Organisations of the Treadway Commission. Internal Control-Integrated Framework*, 1992 y la definición para "Objetivo de Control de TI" ha sido adaptada del reporte SAC (*Systems Auditability and Control Report, The Institute of Internal Auditors Research Foundation*, 1991 y 1994).

Control se define como

Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos

Objetivo de control de TI se define como

Una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

Gobierno de TI se define como

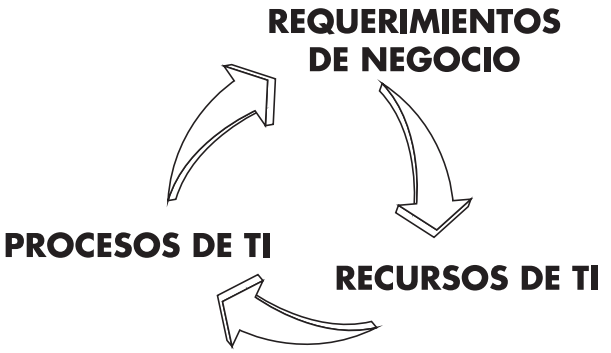
Una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el retorno sobre TI y sus procesos.

LOS PRINCIPIOS DEL MARCO REFERENCIAL

Existen dos clases distintas de modelos de control actualmente disponibles, aquéllos de la clase del "modelo de control de negocios" (por ejemplo COSO) y los "modelos más enfocados a TI" (por ejemplo, DTI). *COBIT* intenta cubrir la brecha que existe entre los dos. Debido a esto, COBIT se posiciona como una herramienta más completa para la Administración y para operar a un nivel superior a los estándares de tecnología para la administración de sistemas de información.. **Por lo tanto, COBIT es el modelo para el gobierno de TI!**

El concepto fundamental del *Marco Referencial de* 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.

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



Requerimientos de Calidad
- Calidad
- Costo
- Entrega o Distribución (de servicio)

Requerimientos Fiduciarios (COSO)
- Efectividad y eficiencia de las operaciones
- Confiabilidad de la información
- Cumplimiento de las leyes y regulaciones

Requerimientos de Seguridad
- Confidencialidad
- Integridad
- Disponibilidad

La Calidad ha sido considerada principalmente por su aspecto 'negativo' (ausencia de fallas, confiabilidad, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos, pero menos tangibles, de la calidad (estilo, atractivo, "ver y sentir", desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la Calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega o distribución del servicio, de la Calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el Costo también es considerado, siendo cubierto por la Eficiencia.

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

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

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas. A continuación se muestran las definiciones utilizadas por COBIT:

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

Eficiencia Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

Confidencialidad Se refiere a la protección de información sensible contra divulgación no autorizada.

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

Disponibilidad Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento 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.

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

Los recursos de TI identificados en COBIT pueden explicarse/definirse como se muestra a continuación:

Datos Son objetos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

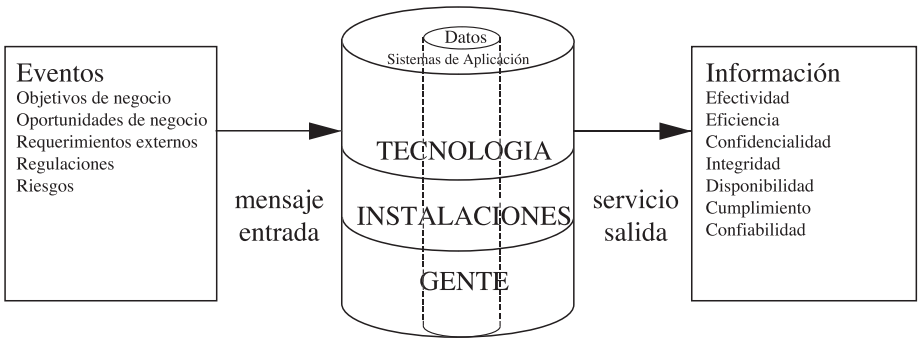
Sistemas de Aplicación Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Tecnología La tecnología cubre hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Instalaciones Recursos para alojar y dar soporte a los sistemas de información.

Personal Habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

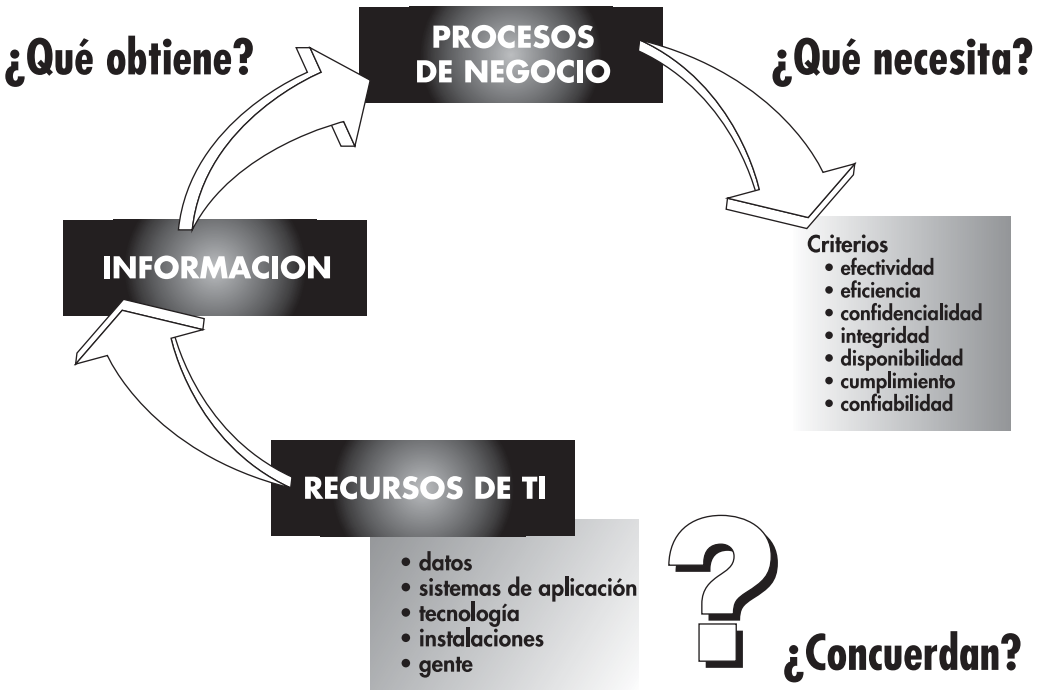
Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación:



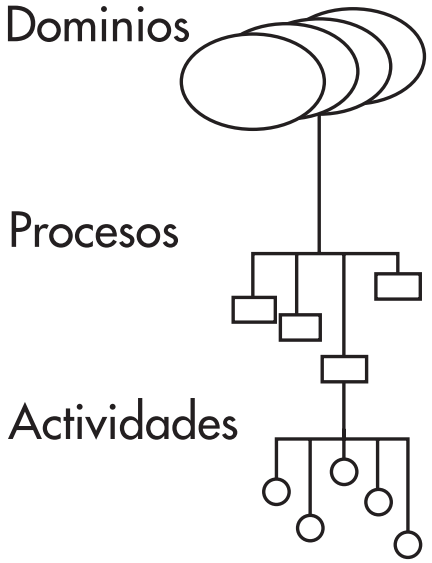
El dinero o capital no se tuvo en cuenta como un recurso para la clasificación de objetivos de control para TI debido a que puede considerarse como la inversión en cualquiera de los recursos mencionados anteriormente. Es importante hacer notar también que el *Marco Referencial* no menciona, en forma específica para todos los casos, la documentación de todos los aspectos "materiales" importantes relacionados con un proceso de TI particular. 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 futuros de controles de compensación en cualquier área específica en revisión.

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.

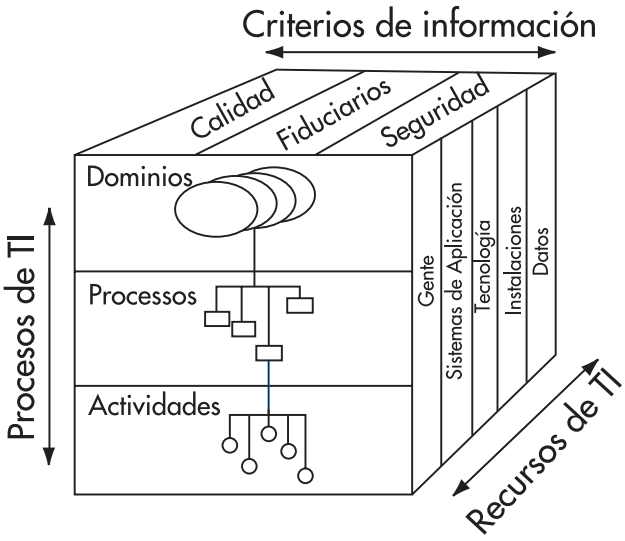
¿Cómo pueden entonces las empresas estar satisfechas respecto a que la información obtenida presente las características que necesitan? Es aquí donde se requiere de un sano marco referencial de Objetivos de Control para TI. El diagrama mostrado a continuación ilustra este concepto.



El *Marco de Referencia de COBIT* 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. 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. Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control). En el nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es denominado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.



Por lo tanto, el *Marco de Referencia* conceptual puede ser enfocado desde tres puntos estratégicos: (1) Criterios de información, (2) recursos de TI y (3) procesos de TI. Estos tres puntos estratégicos son descritos en el Cubo COBIT que se muestra a continuación:



Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización –y no la "jerga[4]" o terminología del auditor -. Por lo tanto, cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo.

Las definiciones para los dominios mencionados son las siguientes:

Planeación y organización

Este dominio cubre las estrategias 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, deberá establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro

[4] **Jerga** (*jargon*)

del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes, para asegurar que el ciclo de vida es contínuo para esos sistemas

Entrega y soporte

En este dominio se hace referencia a la entrega o distribución de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la continuidad de las operaciones así como aspectos sobre entrenamiento. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio incluye el procesamiento de los datos el cual es ejecutado por los sistemas de aplicación, frecuentemente clasificados como controles de aplicación.*

Monitoreo

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Este dominio también advierte a la Administración sobre la necesidad de asegurar procesos de control independientes, los cuales son provistos por auditorías internas y externas u obtenidas de fuentes alternativas.

Es importante tener en cuenta que estos procesos de TI pueden ser aplicados en diferentes niveles de la organización. Por ejemplo, algunos de los procesos serán aplicados al nivel de la empresa, otros al nivel de la función de TI, otros al nivel del propietario de los procesos del negocio, etc.

Debe notarse además, que el criterio de efectividad en los procesos que planean o distribuyen soluciones para los requerimientos del negocio cubrirá algunas veces los criterios de disponibilidad, integridad y confidencialidad— en la práctica, éstos se han convertido en requerimientos del negocio. Por ejemplo, el proceso de "identificar soluciones" tiene que ser efectivo en proveer requerimientos de disponibilidad, integridad y Confidencialidad.

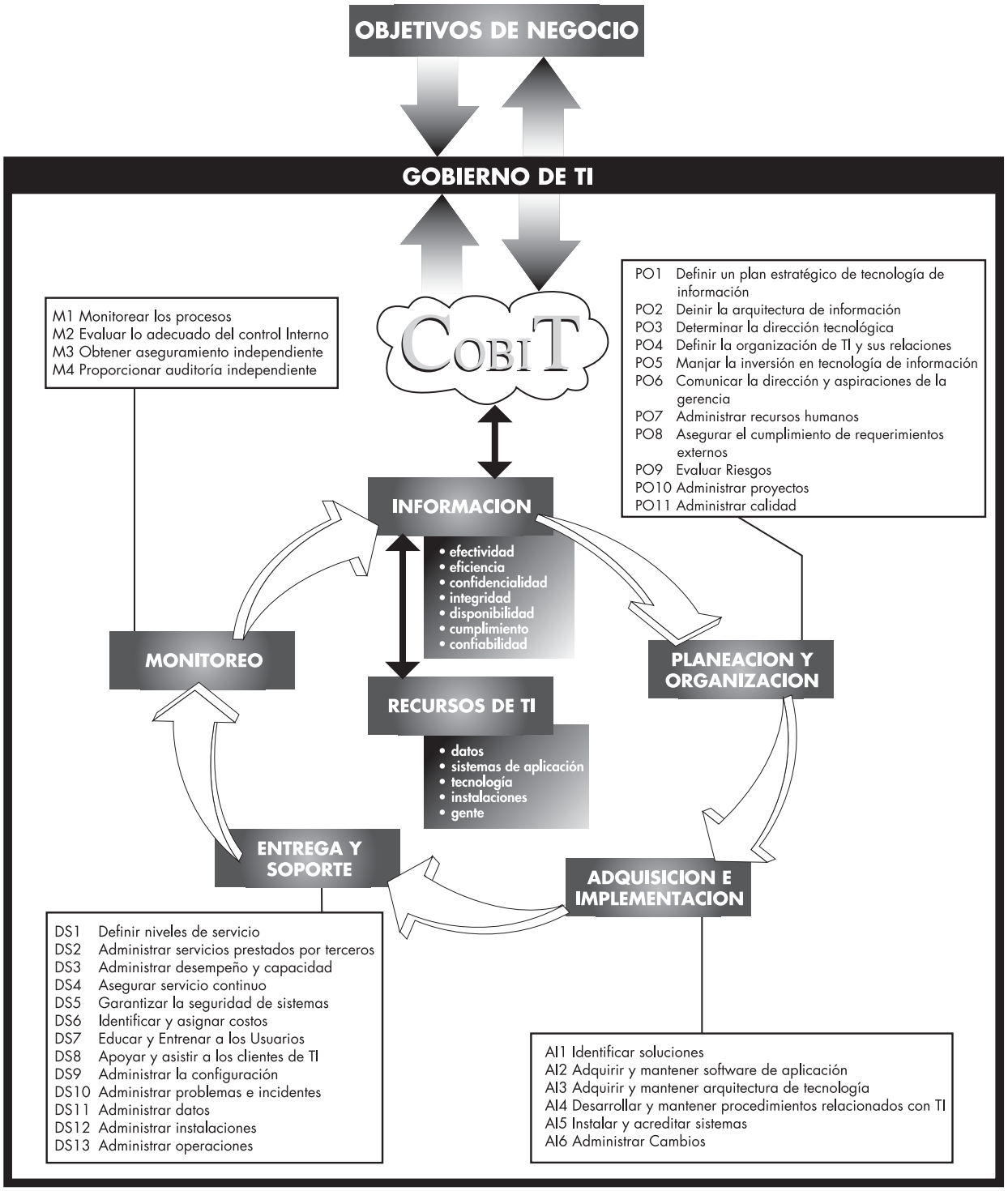
Es claro que todas las medidas de control no necesariamente satisfarán los diferentes requerimientos del negocio para la información en el mismo grado.

- **Primario** es el grado en el cual se definen objetivos de control que impactan directamente los criterios de información considerados
- **Secundario** es el grado en el cual se definen objetivos de control que solo satisfacen una extensión pequeña o satisfacen indirectamente al criterio de información considerado.
- **En blanco** podría ser aplicable. Sin embargo los requerimientos son satisfechos de una forma mas apropiada por otro criterio en este proceso y/o en otro proceso.

En forma similar, todas las medidas de control no necesariamente impactarán a los diferentes recursos de TI en el mismo grado. Por consiguiente, el *Marco de Referencia* de COBIT indica específicamente la aplicabilidad de los recursos de TI que son específicamente administrados por el proceso bajo consideración (no solamente los que toman parte en el proceso) . Esta clasificación se realiza con el *Marco de Referencia* de COBIT, basado sobre un riguroso proceso de recolección de ideas proporcionadas por investigadores, expertos y revisores, usando estrictas definiciones previamente indicadas.

En resumen, con el fin de proveer la información que la organización necesita para lograr sus objetivos, el Gobierno de TI debe ser entrenado por la organización para asegurar que los recursos de TI serán administrados por una colección de procesos de TI agrupados naturalmente. El siguiente diagrama ilustra este concepto.

PROCESOS DE TI DE COBIT DEFINIDOS EN LOS CUATRO DOMINIOS



HISTORIA Y ANTECEDENTES DE COBIT

La tercera edición de COBIT es la mas reciente versión de los Objetivos de Control para la información y sus tecnologías relacionadas, que fue liberado primero por la *Information Systems Audit and Control Foundation* (ISACF) en 1996. La 2da edición que refleja un incremento en el número de documentos fuente, una revisión en el alto nivel y objetivos de control detallados y la adición del *Conjunto de herramientas de Implementación* fue publicado en 1998. La 3a edición marca el ingreso de un nuevo editor para COBIT: El Instituto de Gobierno[5] de TI (IT Governance Institute).

El Instituto de Gobierno de TI fue formado por la Information Systems Audit and Control Association (ISACA) y su Fundación asociada en 1998 para avanzar en el entendimiento y la adopción de principios de gobierno de TI. Con la adición de las Directrices Gerenciales en la 3a edición de COBIT y su expansión y mayor cubrimiento sobre el Gobierno de TI, el Instituto de Gobierno de TI adquirió un rol de liderazgo en el desarrollo de la publicación.

COBIT se basó originalmente en los *Objetivos de Control* de la ISACF y ha sido mejorado con las actuales y emergentes estándares internacionales a nivel técnico, profesional, regulatorio y específicos de la industria. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en **sistemas de información de toda la empresa.** El término **"generalmente aplicables y aceptados"** es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés).

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.

Sin excluir ningún otro estándar aceptado en el campo del control de sistemas de información que pudiera emitirse durante la investigación, las fuentes han sido identificadas inicialmente como:

Estándares Técnicos de ISO, EDIFACT, etc.
Códigos de Conducta emitidos por el *Council of Europe*, OECD, ISACA, etc.;
Criterios de Calificación para sistemas y procesos de TI: ITSEC, ISO9000, SPICE, TickIT, Common Criteria, etc.;
Estándares Profesionales para control interno y auditoría: reporte COSO, IFAC, IIA, ISACA, GAO, PCIE, CICA, AICPA, etc.;
Prácticas y requerimientos de la Industria de foros industriales (ESF, 14) y plataformas patrocinadas por el gobierno (IBAG, NIST, DTI); y
Nuevos requerimientos específicos de la industria de la banca, Comercio Electrónico y manufactura de TI.

(Ver Apéndice II, Descripción del Proyecto COBIT; Apéndice III Material de Referencia Primaria de COBIT y Apéndice IV, Glosario de Términos)

[5] **Gobierno** (*governance):* sistema que establece la alta gerencia para asegurar el logro de los objetivos de una Organización.

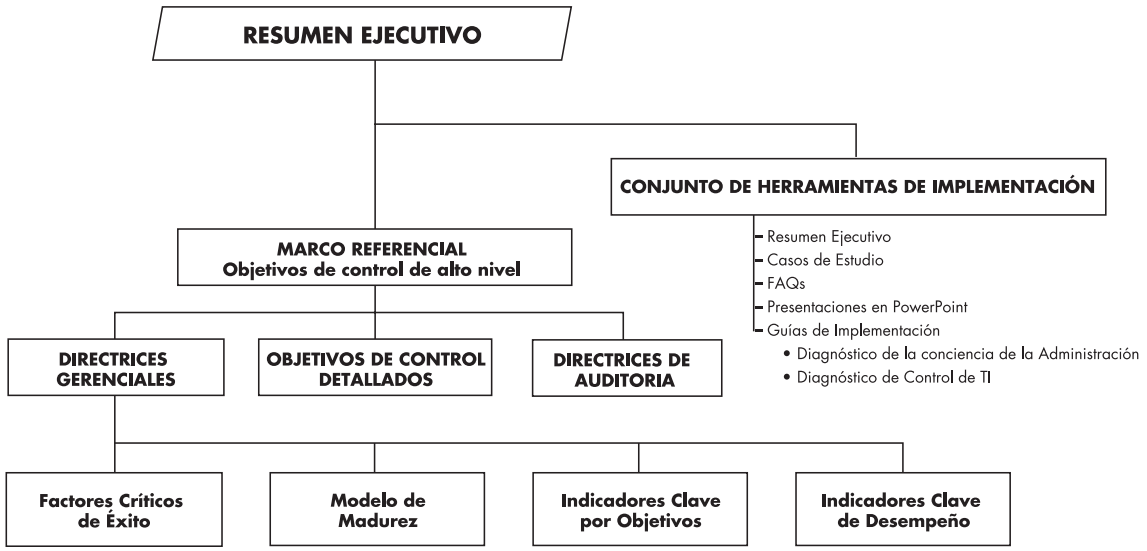
HISTORIA Y ANTECEDENTES DE COBIT

EVOLUCIÓN DEL PRODUCTO COBIT

COBIT evolucionará a través de los años y será el fundamento de investigaciones futuras. Por lo tanto, se generará una familia de productos COBIT y al ocurrir esto, las tareas y actividades que sirven como estructura para organizar los Objetivos de Control de TI, serán refinadas posteriormente. También será revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria.

La investigación y las publicaciones han sido posibles gracias al fundamental apoyo de PricewaterhouseCoopers y las donaciones de los capítulos de ISACA y de miembros de todo el mundo. La European Security Forum (ESF) amablemente llevó a cabo la recolección de material disponible para el proyecto. La Gartner Group además participó en el desarrollo y realizó la revisión de aseguramiento de calidad de las *Directrices Gerenciales.*

PRODUCTOS DE LA FAMILIA COBIT



OBJETIVOS DE CONTROL
TABLA RESUMEN

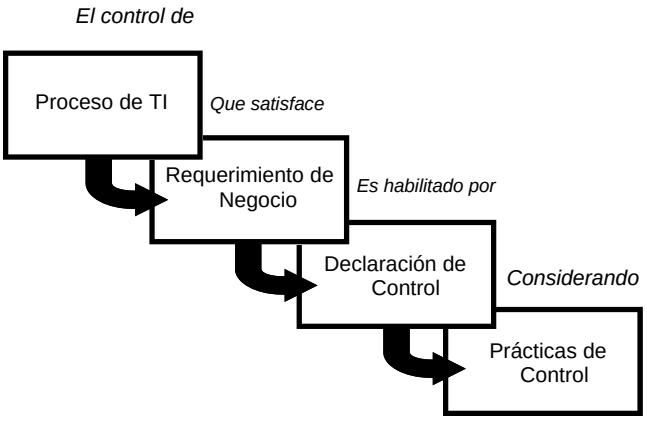
La siguiente tabla proporciona una indicación, por proceso y dominio de TI, de cuáles criterios de información son impactados por los objetivos de alto nivel, así como una indicación de cuáles recursos de TI son aplicables.

DOMINIO		PROCESO	Criterios de Información							Recursos de TI				
			efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	recursos	sistemas de aplicación	tecnología	instalaciones	datos
Planeación y Organización	PO1	Definir un plan estratégico de sistemas	P	S						✔	✔	✔	✔	✔
	PO2	Definir la arquitectura de información	P	S	S	S					✔			✔
	PO3	Deteminar la dirección tecnológica	P	S								✔	✔	
	PO4	Definir la organización de TI y sus relaciones	P	S						✔				
	PO5	Administrar las inversiones (en TI)	P	P					S	✔	✔	✔	✔	
	PO6	Comunicar los objetivos y aspiraciones de la gerencia	P					S		✔				
	PO7	Administrar los recursos humanos	P	P						✔				
	PO8	Asegurar el cumplimiento de requerimientos externos	P					P	S	✔	✔			✔
	PO9	Evaluar riegos	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Administrar proyectos	P	P						✔	✔	✔	✔	
	PO11	Administrar calidad	P	P		P			S	✔	✔	✔	✔	
Adquisición e Implementación	AI1	Identificar soluciones de automatización	P	S							✔	✔	✔	
	AI2	Adquirir y mantener software de aplicación	P	P		S		S	S		✔			
	AI3	Adquirir y mantener la arquitectura tecnológica	P	P		S						✔		
	AI4	Desarrollar y mantener procedimientos	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Instalar y acreditar sistemas de información	P			S	S			✔	✔	✔	✔	✔
	AI6	Administrar cambios	P	P		P	P		S	✔	✔	✔	✔	✔
Entrega de Servicios y Soporte	DS1	Definir niveles de servicio	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Administrar servicios de terceros	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Administrar desempeño y capacidad	P	P			S				✔	✔	✔	
	DS4	Asegurar continuidad de servicio	P	S			P			✔	✔	✔	✔	✔
	DS5	Garantizar la seguridad de sistemas			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identificar y asignar costos		P					P	✔	✔	✔	✔	✔
	DS7	Educar y capacitar a usuarios	P	S						✔				
	DS8	Apoyar y orientar a clientes	P	P						✔	✔			
	DS9	Administrar la configuración	P				S		S		✔	✔	✔	
	DS10	Administrar problemas e incidentes	P	P			S			✔	✔	✔	✔	✔
	DS11	Administrar la información				P			P					✔
	DS12	Administrar las instalaciones				P	P						✔	
	DS13	Administrar la operación	P	P		S	S			✔	✔		✔	✔
Monitoreo	M1	Monitorear el proceso	P	S	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Evaluar lo adecuado del control interno	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M4	Proprocionar auditoría independiente	P	P	S	S	S	S	S	✔	✔	✔	✔	✔

PRINCIPIOS DE LOS OBJETIVOS DE CONTROL

COBIT, tal como aparece en esta última versión de los *Objetivos de Control* refleja los compromisos de ISACA para engrandecer y mantener el cuerpo común del conocimiento requerido para soportar la profesión de auditoría y control de los sistemas de información

El *Marco de Referencia* de *COBIT* ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de TI particular, cuyo logro es posible a través del establecimiento de controles, para el cual deben considerarse controles potenciales aplicables.



Los *Objetivos de Control* de TI han sido organizados por proceso/actividad y también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista estratégico como se explicó anteriormente, sino también para facilitar enfoques combinados o globales, tales como instalación/implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de TI por un proceso.

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

Mientras que el *Marco de Referencia* de COBIT enfoca **controles a alto nivel** para cada proceso, los *Objetivos de Control* se enfocan sobre objetivos de control detallados y específicos asociados a cada proceso de TI. Por cada uno de los 34 procesos de TI del marco referencial, hay desde tres hasta 30 objetivos de control detallados, para un total de 318.

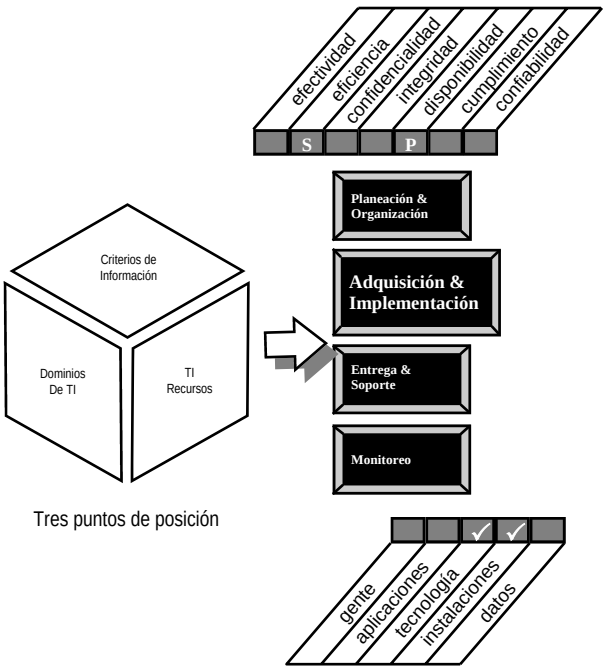
Los *Objetivos de Control* se alinean para cubrir todo el Marco referencial con objetivos de control detallados con base en 41 fuentes primarias que comprenden estándares y regulaciones internacionales de TI, *de facto* y *de jure*. Contiene sentencias de los resultados deseados o propósitos a ser alcanzados mediante la implementación de procedimientos de control específicos en una actividad de TI, de esta manera provee políticas claras y buenas prácticas para los controles de TI a través de la industria, alrededor del mundo.

Los *Objetivos de Control* están dirigidos a la Administración y al staff de TI, a las funciones de control y auditoría — y lo mas importante, a los propietarios de los procesos del negocio. Los Objetivos de Control proporcionan un trabajo, que es un *documento* de escritorio para esos individuos. Se identifican definiciones precisas y claras para un mínimo conjunto de controles con el fin de asegurar la efectividad, eficiencia y economía de la utilización de los recursos. Objetivos de control detallados son identificados para cada proceso, como los controles mínimos necesarios . Esos controles serán analizados por los profesionales de control para verificar su suficiencia.

Los *Objetivos de Control* permiten el traslado de los conceptos presentados en el *Marco de Referencia* hacia controles específicos aplicables a cada proceso de TI.

AYUDAS DE NAVEGACIÓN

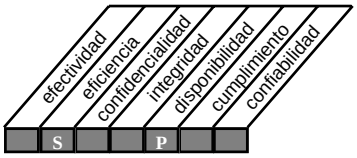
La sección de los Objetivos de Control contienen objetivos de control detallados para cada uno de los 34 procesos de TI. A la izquierda de cada página, se presenta el objetivo de control de alto nivel. El indicador del dominio ("PO" para Planeación y Organización, "AI" para Adquisición e Implementación, "DS" para Entrega de Servicios y Soporte y "M" para Monitoreo se presentan a la izquierda y arriba de cada página. El criterio de información aplicable y el recurso de TI utilizado son mostrados en matrices pequeñas como se describe a continuación. Iniciando en la derecha de la página están las descripciones de los objetivos de control detallados para cada proceso de TI.



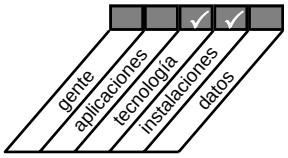
Para facilitar el empleo eficiente de los objetivos de control como soporte a los diferentes puntos de vista, se proporcionan algunas ayudas de navegación como parte de la presentación de los objetivos de control de alto nivel. Se proporciona una ayuda de navegación para cada una de las tres dimensiones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

Los dominios son identificados por este ícono en la ESQUINA SUPERIOR DERECHA de cada página, en la sección de Objetivos de Control, agrandando y haciendo más visible el dominio bajo revisión.

La clave para el criterio de información se presentará en la ESQUINA SUPERIOR IZQUIERDA, en la sección de Objetivos de Control mediante la siguiente "mini" matriz, la cual identificará cuál criterio y en qué grado (primario o secundario) es aplicable a cada Objetivo de Control de TI de alto nivel.



Una segunda "mini" matriz en la ESQUINA INFERIOR DERECHA de la sección de Objetivos de Control identifica los recursos de TI que son administrados en forma específica por el proceso bajo consideración - no solo aquellos que simplemente toman parte en el proceso -. Por ejemplo, el proceso "administración de datos" se concentra particularmente en la integridad y confiabilidad de los recursos de datos.

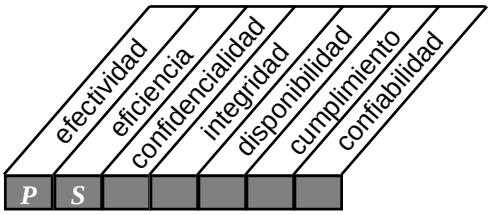


OBJETIVOS DE CONTROL DE ALTO NIVEL

OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO1



Control sobre el proceso de TI de:

Definición de un plan Estratégico de Tecnología de Información

que satisface los requerimientos del negocio de:

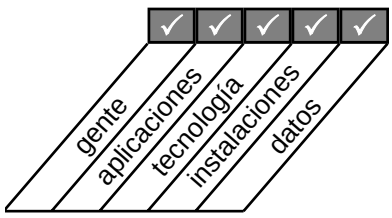
Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos del negocio para TI, así como para asegurar sus logros futuros.

se hace posible a través de:

un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo. Los planes a largo plazo deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo:

y toma en consideración:

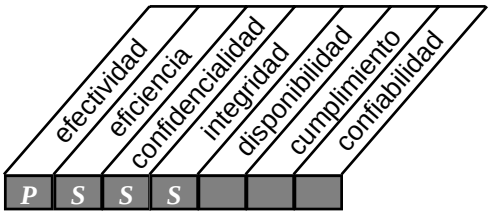
- Estrategia del negocio de la empresa
- definición de cómo TI soporta los objetivos de negocio
- inventario de soluciones tecnológicas e infraestructura actual
- Monitoreo del mercado de tecnología
- Estudios de factibilidad oportunos y chequeos con la realidad
- Análisis de los sistemas existentes
- Posición de la empresa sobre riesgos, en el proceso de compra (time-on-market), calidad
- Necesidades de la Administración senior en el proceso de compra, soportado en revisión crítica



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO2



Control sobre el proceso de TI de:

Definición de la Arquitectura de Información

que satisface los requerimientos de negocio de:

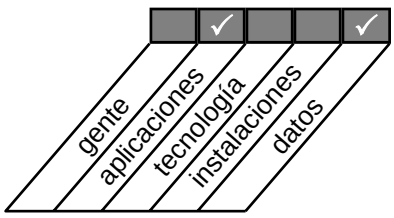
organizar de la mejor manera los sistemas de información

se hace posible a través de:

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

y toma en consideración:

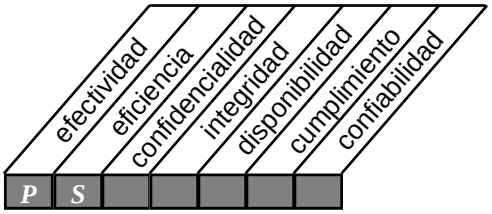
- Repositorio automatizado de datos y diccionario
- reglas de sintaxis de datos
- propiedad de la información y clasificación con base en criticidad /seguridad
- un modelo de información que represente el negocio
- Normas de arquitectura de información de la empresa



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO3



Control sobre el proceso de TI de:

determinación de la dirección tecnológica

que satisface los requerimientos de negocio de:

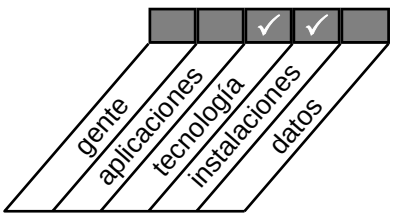
aprovechar la tecnología disponible y las que van apareciendo en el mercado para impulsar y posibilitar la estrategia del negocio.

se hace posible a través de:

la creación y mantenimiento de un plan de infraestructura tecnológica que establece y administra expectativas claras y realistas de lo que puede brindar la tecnología en términos de productos, servicios y mecanismos de entrega

y toma en consideración:

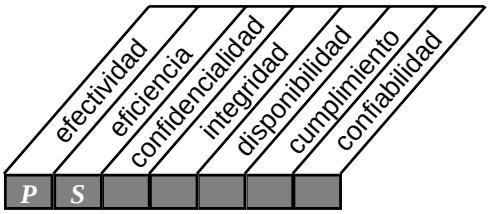
- capacidad de la infraestructura actual
- monitoreo de desarrollos tecnológicos por la vía de fuentes confiables
- realización de prueba de conceptos
- riesgos, restricciones y oportunidades
- planes de adquisición
- estrategia de migración y planes de desarrollo futuro (roadmaps)
- relaciones con los vendedores
- reevaluación independiente de la tecnología
- Cambios de precio /desempeño de hardware y de software



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO4



Control sobre el proceso de TI de:

definición de la organización y de las relaciones de TI

que satisface los requerimientos de negocio de:

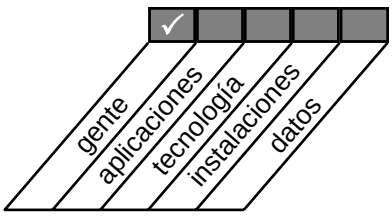
prestación de los servicios correctos de TI

se hace posible a través de:

una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, acordes con el negocio y que facilita la estrategia y provee una dirección efectiva y un control adecuado.

y toma en consideración:

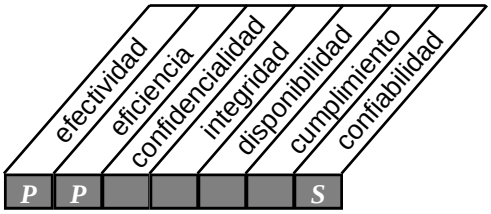
- responsabilidades del nivel directivo sobre TI
- dirección de la gerencia y supervisión de TI
- Alineación de TI con el negocio
- participación de TI en los procesos clave de decisión
- flexibilidad organizacional
- roles y responsabilidades claras
- equilibrio entre supervisión y delegación de autoridad (empoderamiento)
- descripciones de puestos de trabajo
- Niveles de asignación de personal y personal clave
- Ubicación organizacional de las funciones de seguridad, calidad y control interno
- Segregación de funciones



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO5



Control sobre el proceso de TI de:

Manejo o administración de la inversión de TI

que satisface los requerimientos de negocio de:

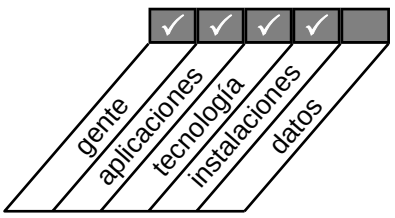
asegurar el financiamiento y el control de desembolsos de recursos financieros

se hace posible a través de:

Inversión periódica y presupuestos operacionales establecidos y aprobados por el negocio

y toma en consideración:

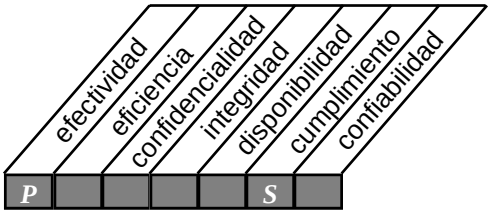
- alternativas de financiamiento
- Claros responsables del presupuesto
- Control sobre los gastos actuales
- justificación de costos y concientización sobre el costo total de la propiedad
- justificación del beneficio y contabilización de todos los beneficios obtenidos
- Ciclo de vida del software de aplicación y de la tecnología
- Alineación con las estrategias del negocio de la empresa
- Análisis de impacto



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO6



Control sobre el proceso de TI de:

comunicación de los objetivos y aspiraciones de la gerencia

que satisface los requerimientos de negocio de:

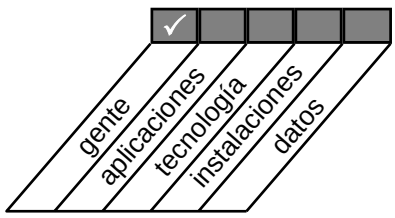
asegurar que el usuario sea conciente y comprenda dichas aspiraciones

se hace posible a través de:

políticas establecidas y transmitidas a la comunidad de usuarios; además, se necesitan estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables

y toma en consideración:

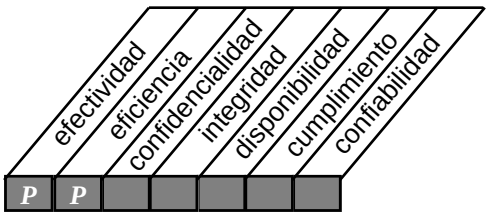
- Misión claramente articulada
- Directivas tecnológicas vinculadas con aspiraciones de negocios
- Código de ética / conducta
- Compromiso con la calidad
- Políticas de seguridad y control interno
- Practicas de seguridad y control interno
- Ejemplos de liderazgo
- Programación continua de comunicaciones
- Proveer guías y verificar su cumplimiento



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO7



Control sobre el proceso de TI de:

administración de recursos humanos

que satisface los requerimientos de negocio de:

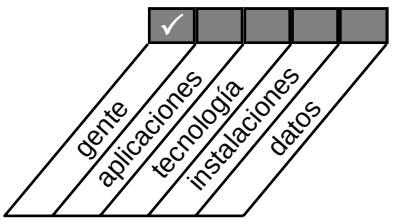
Adquirir y mantener una fuerza de trabajo motivada y competente y maximizar las contribuciones del personal a los procesos de TI

se hace posible a través de:

prácticas de administración de personal, sensatas, justas y transparentes para reclutar, alinear, pensionar, compensar, entrenar, promover y despedir

y toma en consideración:

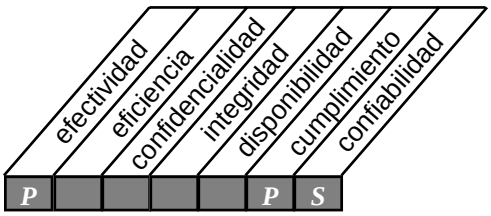
- reclutamiento y promoción
- Entrenamiento y requerimientos de calificaciones
- desarrollo de conciencia
- entrenamiento cruzado y rotación de puestos
- Procedimientos para contratación, veto y despidos
- evaluación objetiva y medible del desempeño
- responsabilidades sobre los cambios técnicos y de mercado
- Balance apropiado de recursos internos y externos
- Plan de sucesión para posiciones clave



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO8



Control sobre el proceso de TI de:

aseguramiento del cumplimiento de requerimientos externos

que satisface los requerimientos de negocio de:

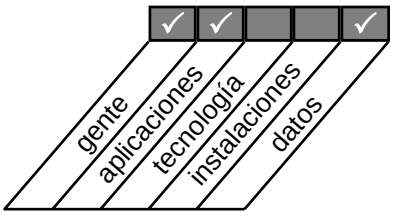
cumplir con obligaciones legales, regulatorias y contractuales

se hace posible a través de:

la identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, y realizando las medidas apropiadas para cumplir con ellos

y toma en consideración:

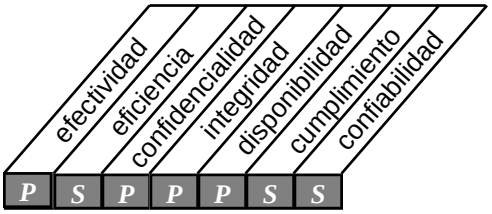
- leyes, regulaciones y contratos
- monitoreo de desarrollos legales y regulatorios
- Monitoreo regular sobre cumplimiento
- seguridad y ergonomía
- privacidad
- propiedad intelectual



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO9



Control sobre el proceso de TI de:

análisis de riesgos

que satisface los requerimientos de negocio de:

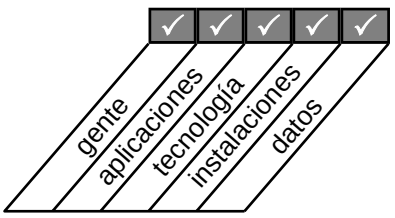
Soportar las decisiones de la gerencia a través del logro de los objetivos de TI y responder a las amenazas reduciendo su complejidad e incrementando objetivamente e identificando factores importantes de decisión.

se hace posible a través de:

la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, involucrando funciones multidisciplinarias y tomando medidas costo-efectivas para mitigar los riesgos

y toma en consideración:

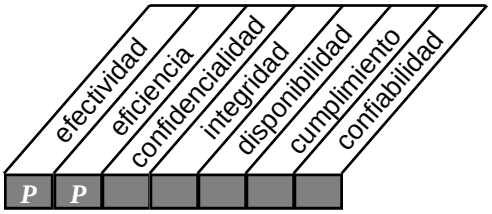
- Administración de riesgos de la propiedad y del registro de las operaciones
- diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.)
- Definir y comunicar un perfil tolerable de riesgos
- Análisis de las causas y sesiones de tormenta de ideas sobre riesgos
- Medición cuantitativa y/o cualitativa de los riesgos
- metodología de análisis de riesgos
- Plan de acción contra los riesgos
- Volver a realiza análisis oportunos



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO10



Control sobre el proceso de TI de:

administración de proyectos

que satisface los requerimientos de negocio de:

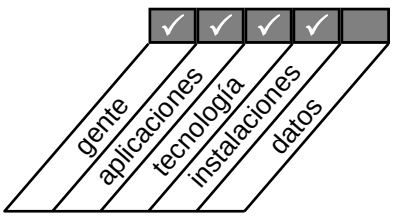
establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión

se hace posible a través de:

La organización identificando y priorizando proyectos en línea con el plan operacional y la adopción y aplicación de técnicas de administración de proyectos para cada proyecto emprendido

y toma en consideración:

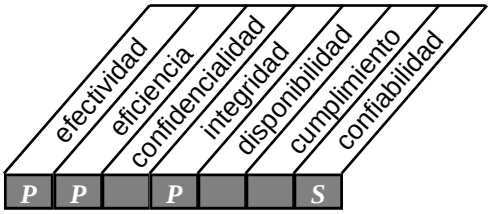
- El patrocinio que la gerencia de negocios debe dar a los proyectos
- Administración de programas
- Capacidad para el manejo de proyectos
- Involucramiento del usuario
- División de tareas, definición de puntos de control y aprobación de fases
- Distribución de responsabilidades
- Rastreo riguroso de puntos de control y entregables
- Costos y presupuestos de mano de obra, balance de recursos internos y externos
- Planes y métodos de aseguramiento de calidad
- Programa y análisis de riesgos del proyecto
- Transición de desarrollo a operación



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO11



Control sobre el proceso de TI de:

Administración de la calidad

que satisface los requerimientos de negocio de:

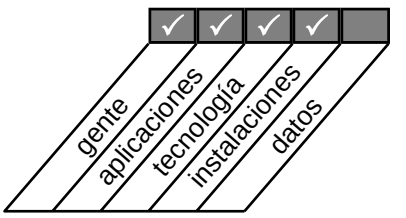
satisfacer los requerimientos del cliente de TI

se hace posible a través de:

la planeación, implementación y mantenimiento de estándares de administración de calidad y sistemas provistos para las distintas fases de desarrollo, claros entregables y responsabilidades explícitas

y toma en consideración:

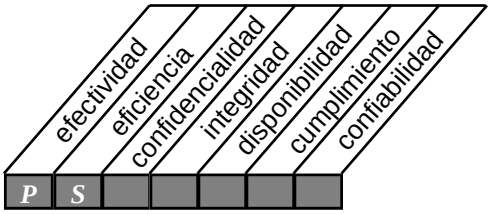
- Establecimiento de una cultura de calidad
- Planes de calidad
- responsabilidades de aseguramiento de la calidad
- Practicas de control de calidad
- metodología del ciclo de vida de desarrollo de sistemas
- pruebas y documentación de sistemas y programas
- revisiones y reporte de aseguramiento de calidad
- Entrenamiento e involucramiento del usuario final y del personal de aseguramiento de calidad
- Desarrollo de una base de conocimiento de aseguramiento de calidad
- Benchmarking contra las normas de la industria



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICIÓN E IMPLEMENTACIÓN

AI1



Control sobre el proceso de TI de:

Identificación de soluciones automatizadas

que satisface los requerimientos de negocio de:

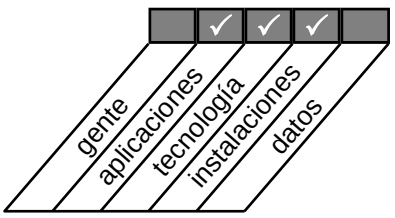
asegurar un efectivo y eficiente enfoque para satisfacer los requerimientos del usuario

se hace posible a través de:

Una objetiva y clara identificación y análisis de oportunidades alternativas comparadas contra los requerimientos de los usuarios

y toma en consideración:

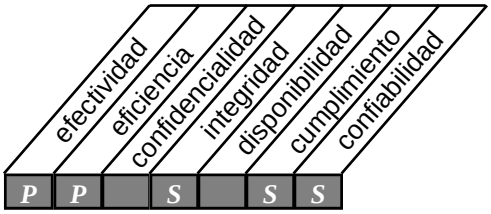
- Conocimientos de soluciones disponibles en el mercado
- Metodologías de Adquisición e implementación
- Involucramiento del usuario en el proceso de compra
- Alineamiento con las estrategias de la empresa y de TI
- definición de requerimientos de información
- estudios de factibilidad (de costo-beneficio, alternativas, etc)
- Requerimientos de funcionalidad, operatividad, aceptación y sostenimiento
- Cumplimiento con la arquitectura de información
- Costo—efectividad de la seguridad y los controles
- Responsabilidades de los proveedores



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICIÓN E IMPLEMENTACIÓN

AI2



Control sobre el proceso de TI de:

adquisición y mantenimiento del software de aplicación

que satisface los requerimientos de negocio de:

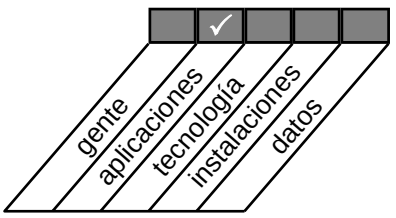
proporcionar funciones automatizadas que soporten efectivamente los procesos del negocio

se hace posible a través de:

la definición de declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros

y toma en consideración:

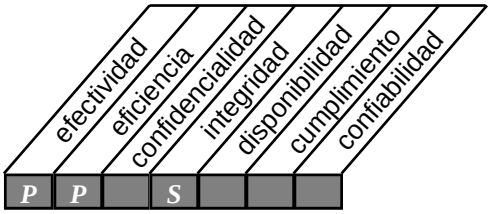
- pruebas funcionales y de aceptación
- controles de aplicación y requerimientos de seguridad
- Requerimientos de documentación
- Ciclo de vida del software de aplicación
- Arquitectura en la información empresarial
- Metodología para el ciclo de vida de desarrollo del sistema
- Interfase usuario-maquina
- Personalización de paquetes



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICIÓN E IMPLEMENTACIÓN

AI3



Control sobre el proceso de TI de:

adquisición y mantenimiento de la infraestructura tecnológica

que satisface los requerimientos de negocio de:

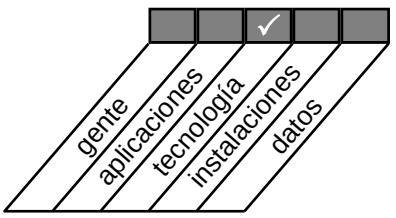
proporcionar las plataformas apropiadas para soportar las aplicaciones de negocios

se hace posible a través de:

la juiciosa adquisición de hardware y software, estandarización del software, análisis del rendimiento del hardware y de software y la administración consistente del sistema

y toma en consideración:

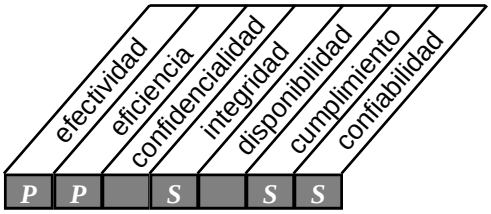
- Cumplimiento con las direcciones y estándares de la infraestructura tecnológica
- evaluación de tecnología
- Instalación, mantenimiento y control de cambios
- Actualización, conversión y planes de migración
- Uso de infraestructuras y/o recursos internos y externos
- Responsabilidades y relaciones del proveedor
- Administración de cambios
- Costo total de propiedad
- Seguridad del software del sistema



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICIÓN E IMPLEMENTACIÓN

AI4



Control sobre el proceso de TI de:

Desarrollo y mantenimiento de Procedimientos

que satisface los requerimientos de negocio de:

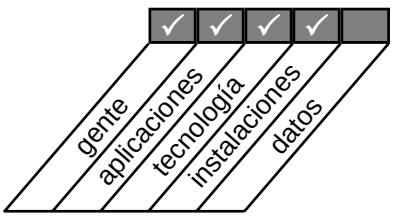
asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas

se hace posible a través de:

un enfoque estructurado del desarrollo de manuales de procedimientos para las operaciones y para los usuarios, requerimientos de servicio y material de entrenamiento

y toma en consideración:

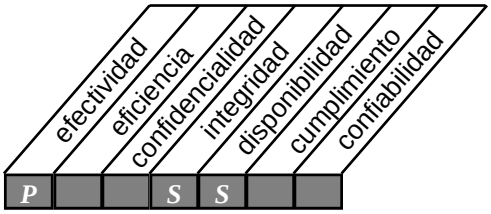
- Rediseño de los procesos de negocios
- Tratamiento de procedimientos como cualquier otra tecnología disponible
- Desarrollo a tiempo
- procedimientos y controles de usuarios
- procedimientos y controles operacionales
- materiales de entrenamiento
- Administración de cambios



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICIÓN E IMPLEMENTACIÓN

AI5



Control sobre el proceso de TI de:

instalación y acreditación de sistemas

que satisface los requerimientos de negocio de:

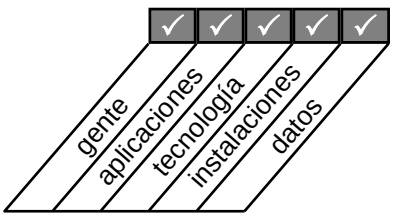
verificar y confirmar que la solución sea adecuada para el propósito deseado

se hace posible a través de:

la realización de una migración de instalación, conversión y plan de aceptación adecuadamente formalizados

y toma en consideración:

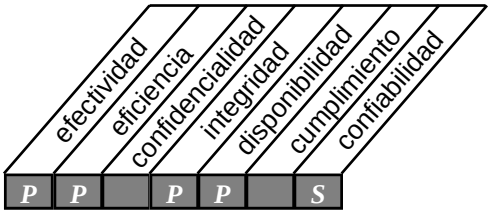
- Entrenamiento del usuario y personal de operaciones de TI
- Conversión de datos
- Una prueba ambiental reflejando al ambiente real
- Acreditación
- revisiones post implementación y retroalimentación
- Participación del usuario final en las pruebas
- Planes continuos de mejoramiento de calidad
- Requerimientos de continuidad del negocio
- Medición de capacidad y desempeño a través del sistema
- Acuerdos y criterios de aceptación



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICIÓN E IMPLEMENTACIÓN

AI6



Control sobre el proceso de TI de:

administración de cambios

que satisface los requerimientos de negocio de:

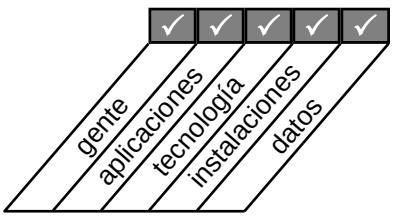
minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores

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:

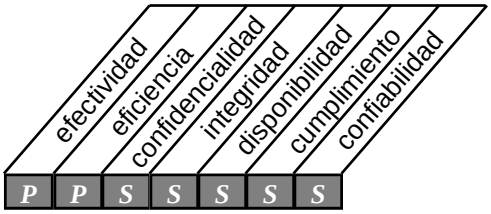
- identificación de cambios
- procedimientos de categorización, priorización y emergencia
- Análisis de impacto
- autorización de cambios
- Administración de la liberación del cambio
- distribución de software
- Uso de herramientas automatizadas
- Administración de la configuración
- Rediseño del proceso del negocio



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS1



Control sobre el proceso de TI de:

Definición y administración de niveles de servicio

que satisface los requerimientos de negocio de:

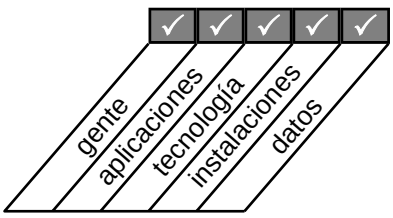
establecer un entendimiento común del nivel de servicio requerido

se hace posible a través de:

el establecimiento de acuerdos de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio

y toma en consideración:

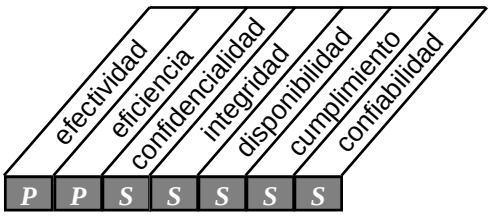
- Acuerdos o convenios formales
- definición de responsabilidades
- tiempos y volúmenes de respuesta
- cargos
- garantías de integridad
- Acuerdos de confidencialidad
- Criterio de satisfacción del cliente
- Análisis costo-beneficio de los niveles de servicio requerido
- Monitoreo y reporte



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS2



Control sobre el proceso de TI de:

administración de servicios prestados por terceros

que satisface los requerimientos de negocio de:

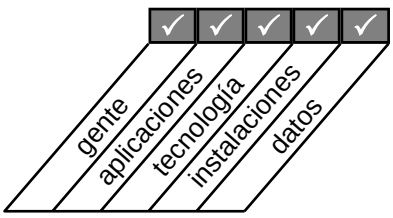
asegurar que los roles y responsabilidades de las terceras partes estén claramente definidas y que cumplan y continúen satisfaciendo los requerimientos

se hace posible a través de:

medidas de control dirigidas a la revisión y monitoreo de acuerdos/contratos y procedimientos existentes, en cuanto a su efectividad y cumplimiento, con respecto a las políticas de la organización

y toma en consideración:

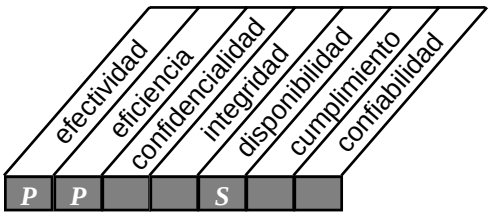
- Acuerdos de servicio con terceras partes
- Administración de contrato
- Acuerdos de confidencialidad
- Requerimientos legales y regulatorios
- Monitoreo y reporte de la entrega de servicio
- Análisis de riesgos de la empresa y de TI
- Ejecución de recompensas y sanciones
- Contabilidad organizacional interna y externa
- Análisis de costos y variaciones en los niveles de servicio



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS3



Control sobre el proceso de TI de:

administración de desempeño y capacidad

que satisface los requerimientos de negocio de:

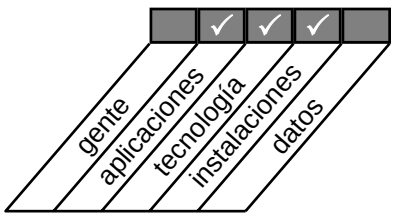
asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado

se hace posible a través de:

Recolección de datos, análisis y reporte del rendimiento de los recursos, aplicación de mediciones y demanda de cargas de trabajo

y toma en consideración:

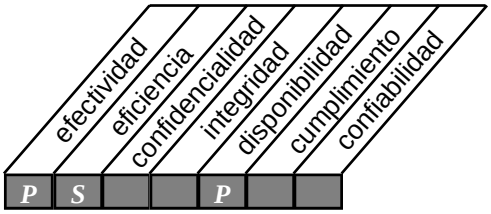
- requerimientos de disponibilidad y desempeño
- monitoreo y reporte automatizado
- herramientas de modelado
- administración de capacidad
- disponibilidad de recursos
- Cambios en precio-rendimiento del hardware y software



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS4



Control sobre el proceso de TI de:

asegurar el servicio continuo

que satisface los requerimientos de negocio de:

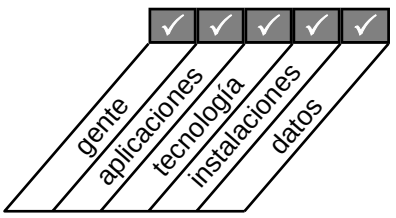
Asegurar que los servicios de TI estén disponibles cuando se requieran y asegurar el impacto mínimo en el negocio en el evento que se presente una interrupción mayor

se hace posible a través de:

tener un plan de continuidad de TI probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio

y toma en consideración:

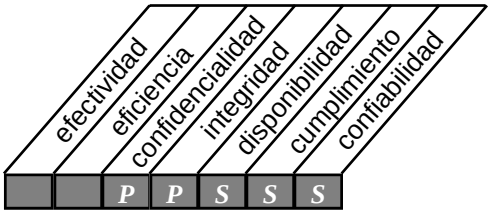
- clasificación de criticidad (severidad)
- Procedimientos alternativos
- respaldo y recuperación
- pruebas y entrenamiento sistemáticos y regulares
- Monitoreo y procesos de escalamiento
- Responsabilidades organizacionales internas y externas
- Activación de la continuidad del negocio, vuelta atrás (fallback) y plan de reactivación
- Actividades de administración de riesgos
- Análisis de puntos únicos de falla
- Administración de problemas



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS5



Control sobre el proceso de TI de:

garantizar la seguridad de los sistemas

que satisface los requerimientos de negocio de:

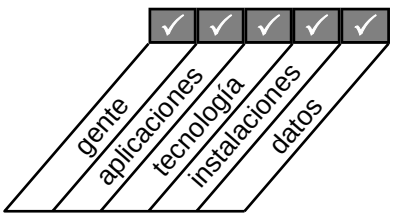
salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida

se hace posible a través de:

controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados

y toma en consideración:

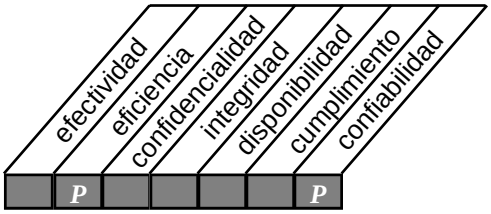
- Requerimientos de privacidad y confidencialidad
- Autorización, autenticación y control de acceso
- identificación de usuarios y perfiles de autorización
- Necesidad de saber y necesidad de tener (need-to-know and need-to-have)
- administración de llaves criptográficas
- manejo, reporte y seguimiento de incidentes
- Prevención y detección de virus
- *Firewalls*
- Administración centralizada de seguridad
- Entrenamiento a los usuarios
- Herramientas para monitoreo del cumplimiento, pruebas de intrusión y reportes



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS6



Control sobre el proceso de TI de:

identificación y asignación de costos

que satisface los requerimientos de negocio de:

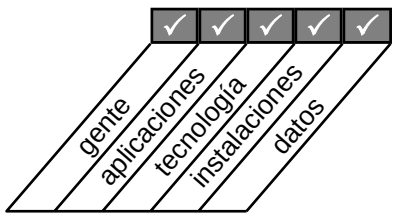
asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

se hace posible a través de:

un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y al apropiado servicio ofrecido

y toma en consideración:

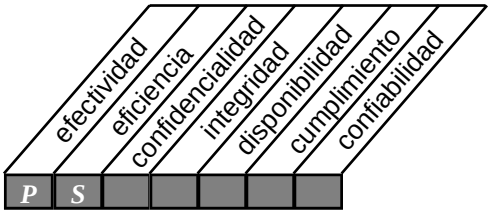
- Recursos identificables y medibles
- Procedimientos y políticas de cargo
- Tarifas de cargo y procesos de reversión de cargos.
- Conexión a acuerdo de niveles de servicio
- Reporte automatizado
- Verificación de comprensión de beneficios
- Benchmarking externo



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS7



Control sobre el proceso de TI de:

educación y entrenamiento de usuarios

que satisface los requerimientos de negocio de:

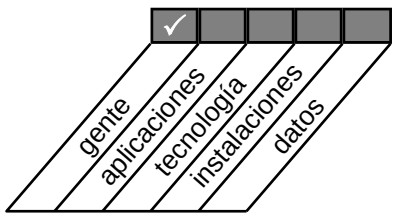
asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y sean conscientes de los riesgos y responsabilidades involucrados

se hace posible a través de:

un plan completo de entrenamiento y desarrollo

y toma en consideración:

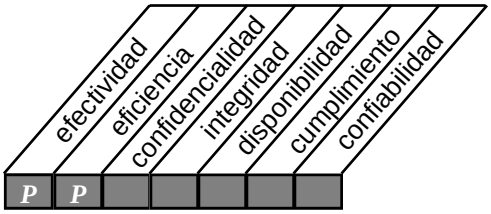
- Plan de entrenamiento
- Inventario de habilidades
- Campañas de concientización
- Técnicas de concientización
- Uso de nuevas tecnologías y métodos de entrenamiento
- Productividad del personal
- Desarrollo de una base de conocimientos



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS8



Control sobre el proceso de TI de:

Apoyo y asistencia a los clientes de TI

que satisface los requerimientos de negocio de:

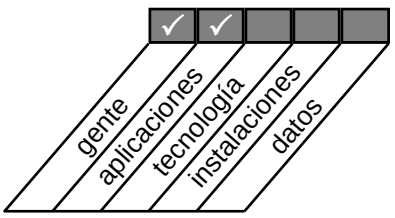
asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

se hace posible a través de:

un help desk, o mesa de control y ayuda, que proporcione soporte y asesoría de primera línea

y toma en consideración:

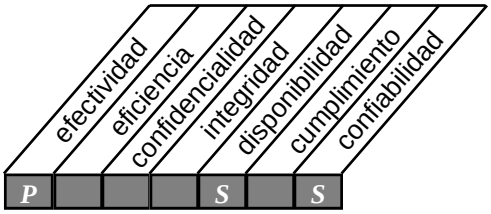
- consultas de los clientes y respuesta a problemas
- monitoreo de consultas y respuestas
- análisis y reporte de tendencias
- Desarrollo de una base de conocimientos
- Análisis de las causas
- Escalamiento y seguimiento de problemas



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS9



Control sobre el proceso de TI de:

Administración de la configuración

que satisface los requerimientos de negocio de:

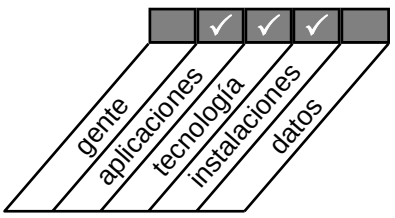
dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para la sana administración del cambio

se hace posible a través de:

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:

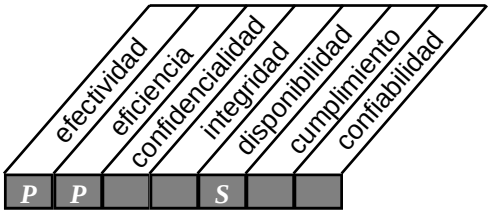
- registro de activos
- administración de cambios en la configuración
- chequeo de software no autorizado
- controles de almacenamiento de software
- Integración e interrelación de hardware y software
- Uso de herramientas automatizadas



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS10



Control sobre el proceso de TI de:

administración de problemas e incidentes

que satisface los requerimientos de negocio de:

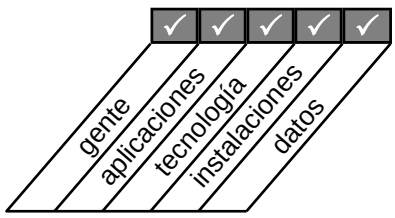
asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia

se hace posible a través de:

un sistema de administración de problemas que registre y dé seguimiento a todos los incidentes

y toma en consideración:

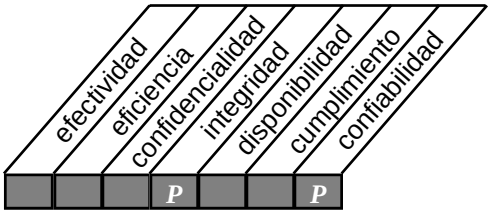
- pistas de auditoría de problemas y soluciones
- resolución oportuna de problemas reportados
- procedimientos de escalamiento
- reportes de incidentes
- accesibilidad a la información de la configuración
- responsabilidades del proveedor
- coordinación con la administración de cambios



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS11



Control sobre el proceso de TI de:

Administración de datos

que satisface los requerimientos de negocio de:

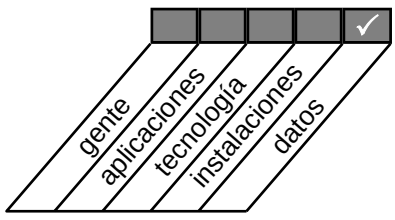
asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento

se hace posible a través de:

una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI

y toma en consideración:

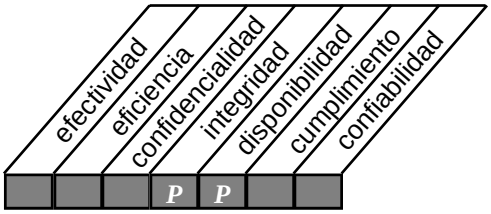
- diseño de formatos
- controles sobre documentos fuente
- controles de entrada, procesamiento y salida
- identificación, movimiento y administración de la librería de medios
- Recuperación y almacenamiento de datos
- autenticación e integridad
- propiedad de datos
- políticas de administración de datos
- modelos de datos y estándares de representación de datos
- integración y consistencia en todas las plataformas
- requisitos legales y regulatorios



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS12



Control sobre el proceso de TI de:

Administración de instalaciones (sitios donde se procesa información)

que satisface los requerimientos de negocio de:

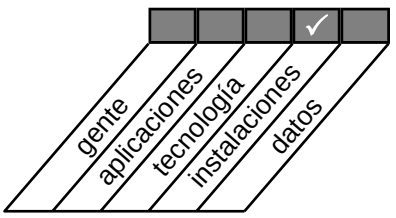
proporcionar un ambiente físico conveniente que proteja los equipos y al personal de TI contra peligros naturales o fallas humanas

se hace posible a través de:

la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su adecuado funcionamiento

y toma en consideración:

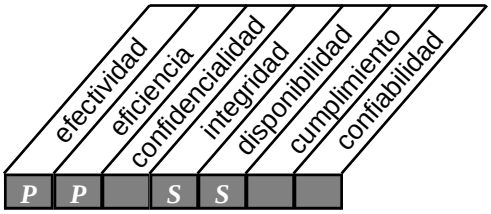
- acceso a instalaciones
- identificación del sitio (instalación)
- seguridad física
- Políticas de inspección y escalamiento
- Plan de continuidad de negocios y administración de crisis
- salud y seguridad del personal
- Políticas de mantenimiento preventivo
- protección contra amenazas ambientales
- Monitoreo automatizado



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS13



Control sobre el proceso de TI de:

administración de operaciones

que satisface los requerimientos de negocio de:

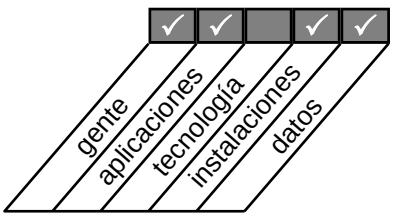
asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada

se hace posible a través de:

una programación o planeación de las actividades que sea registrada y diligenciada con base en el cumplimiento de todas las actividades

y toma en consideración:

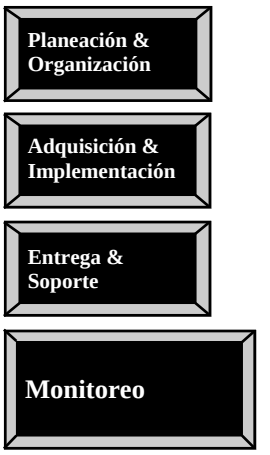
- manual de procedimiento de operaciones
- documentación para el inicio de procesos
- administración de servicios de red
- Programación del personal y cargas de trabajo
- proceso de cambio de turno
- registro de eventos del sistema
- Coordinación con las áreas de administración de cambios, disponibilidad y manejo continuo de negocios
- Mantenimiento preventivo
- Acuerdos de niveles de servicio
- Operaciones automatizadas
- Registro, rastreo y escalamiento de incidentes

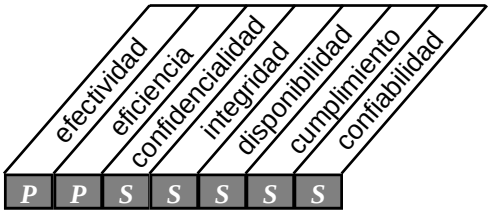


OBJETIVOS DE CONTROL DE ALTO NIVEL

MONITOREO

M1





Control sobre el proceso de TI de:

monitoreo del proceso

que satisface los requerimientos de negocio de:

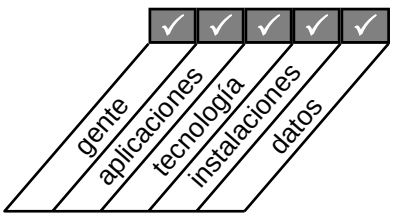
asegurar el logro de los objetivos establecidos para los procesos de TI

se hace posible a través de:

la definición de indicadores de desempeño gerenciales, el reporte oportuno y sistemático del desempeño y la oportuna acción sobre las desviaciones

y toma en consideración:

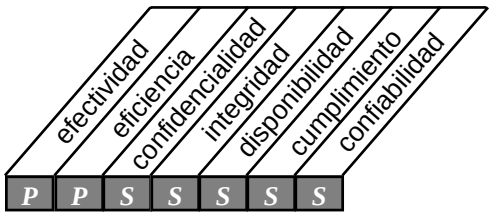
- Tarjetas de decisión (scorecards) con indicadores de desempeño y medición de resultados
- evaluación de la satisfacción de clientes
- reportes gerenciales
- Base de conocimientos del desempeño histórico
- Benchmarking externo



OBJETIVOS DE CONTROL DE ALTO NIVEL

MONITOREO

M2



Control sobre el proceso de TI:

Evaluar lo adecuado del control interno

que satisface los requerimientos de negocio de:

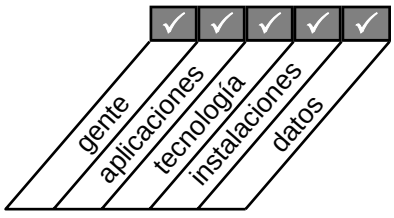
asegurar el logro de los objetivos de control interno establecidos para los procesos de TI

se hace posible a través de:

el compromiso de la Gerencia de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular

y toma en consideración:

- Responsabilidades para el control interno
- Monitoreo del control interno en proceso
- benchmarks[6]
- reportes de errores y excepciones
- auto evaluaciones
- reportes gerenciales
- Cumplimiento con los requerimientos legales y regulatorios

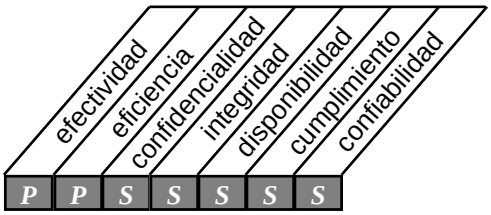


[6] **Comparación con mejores prácticas** (*benchmarks*)

OBJETIVOS DE CONTROL DE ALTO NIVEL

MONITOREO

M3



Control sobre el proceso de TI de:

obtención de aseguramiento independiente

que satisface los requerimientos de negocio de:

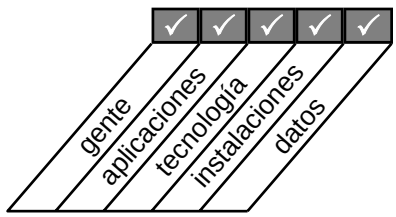
incrementar los niveles de confianza entre la organización, clientes y proveedores externos

se hace posible a través de:

revisiones de aseguramiento independientes llevadas a cabo en intervalos regulares

y toma en consideración:

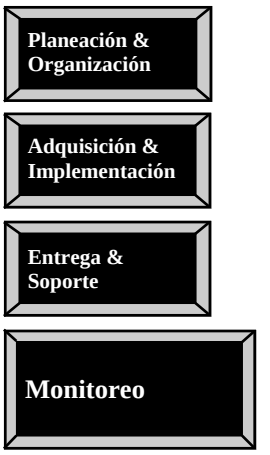
- certificaciones / acreditaciones independientes
- evaluaciones independientes de efectividad
- aseguramiento independiente sobre cumplimiento de requerimientos legales y regulatorios
- aseguramiento independiente del cumplimiento de compromisos contractuales
- revisiones y benchmarking a proveedores externos de servicios
- Revisión por personal calificado del aseguramiento de desempeño
- involucramiento proactivo de la auditoría

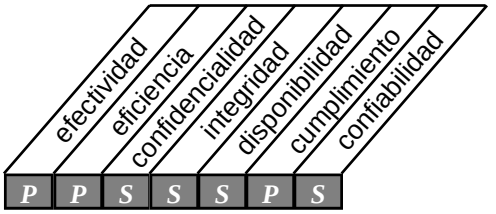


OBJETIVOS DE CONTROL DE ALTO NIVEL

MONITOREO

M4





Control sobre el proceso de TI de:

proveer auditoría independiente

que satisface los requerimientos de negocio de:

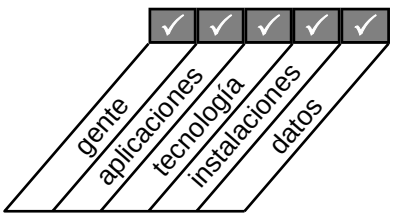
incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas

se hace posible a través de:

auditorías independientes desarrolladas a intervalos regulares

y toma en consideración:

- independencia de auditoría
- involucramiento proactivo de la auditoría
- ejecución de auditorías por parte de personal calificado
- aclaración de resultados y recomendaciones
- actividades de seguimiento
- Evaluación del impacto de las recomendaciones de la auditoria (costos, beneficios, y riesgos)



PAGINA INTENCIONALMENTE EN BLANCO

APENDICES

PAGINA INTENCIONALMENTE EN BLANCO

APÉNDICE I – DIRECTRICES GERENCIALES DE GOBIERNO/GOBERNABILIDAD DE TI

Las siguientes Directrices Gerenciales y el Modelo de Madurez identifican los Factores Críticos de Éxito (Critical Success Factors — CSFs), los Indicadires Claves de objetivos/resultados (Key Goal Indicators—KGIs), Indicadores Claves de Desempeño (Key Performance Indicators—KPIs) para la **Gobernabilidad de TI**. Primero, la Gobernabilidad de TI se define articulando las necesidades del negocio. A continuación, los criterios de información relacionados con la Gobernabilidad de TI son identificados. Las necesidades del negocio son medidas por los Indicadores Claves de Resultados - KGIs - y organizados por sentencias de control apoyado por todos los recursos de TI. El resultado de las sentencias de control organizadas son medidas por los Indicadores Clave de desempeño - KPIs los cuales consideran los Factores críticos de Éxito - CSFs.

El modelo de madurez se utiliza para evaluar el nivel de la organización para cumplir con lo establecido por la Gobernabilidad de TI—desde el mas bajo nivel donde no existe, pasando por un estado inicial /adhoc, ascendiendo a otro repetible pero intuitivo, luego a otro con procesos definidos, a otro administrado y medido y llegando al nivel optimista que es el mas alto nivel. Para llegar al nivel de madurez optimista para la Gobernabilidad de TI, una organización debe estar al menos en el nivel optimizado del dominio de Monitoreo y al menos estar en el nivel de medir y administrar los demás dominios.

(Ver las *Directrices Gerenciales* de COBIT para una completa discusión del uso de esas herramientas)

APÉNDICE I - DIRECTRICES GERENCIALES DE LGOBIERNO/GOBERNABILIDAD DE TI

Gobierno sobre la tecnología de información y los procesos con las metas del negocio para añadir valor, mientras se balancean los riesgos y el retorno

Asegurar la entrega de información al Negocio el cual establece los **Criterios de Información** requeridos y es medido por **Indicadores Clave de Resultados/Logros**

Se hace posible a través de *la creación y mantenimiento de un sistema de procesos y controles apropiados para el negocio, el cual dirige y monitorea el valor del negocio proporcionado por TI*

Considera **Factores Críticos de Éxito** que tiene en cuenta todos los **Recursos de TI** y es medido por **Indicadores Clave de Desempeño**

Factores Críticos de Éxito - CSFs

- Las actividades del gobierno de TI son integradas dentro del proceso de gobierno de la empresa y las conductas de liderazgo
- El gobierno de TI se enfoca en los objetivos y metas de la empresa, en las iniciativas estratégicas y el uso de tecnología para mejorar el negocio, con base en la disponibilidad de recursos y capacidades suficientes para soportar las demandas del negocio.
- Las actividades del Gobierno de TI están definidas sobre propósitos claros, documentados e implementados, basados en las necesidades de la empresa y con responsabilidades concretas.
- Las prácticas gerenciales son implementadas para incrementar la eficiencia y el uso óptimo de los recursos así como incrementar la efectividad de los procesos de TI.
- Se establecen prácticas organizacionales para: evitar descuidos; una cultura/ ambiente de control; análisis de riesgos como práctica estándar; grado de adherencia a estándares establecidos; monitoreo y seguimiento a los riesgos y a las deficiencias de control.
- Se definen prácticas de control para evitar el incumplimiento o mal uso de controles internos.
- Hay integración e interoperabilidad transparente de los procesos de TI mas complejos como podrían ser: problemas, cambios y administración de la configuración.
- Se establece un comité de auditoría para designar y supervisar un auditor independiente enfocado sobre TI cuando dirige la ejecución de planes de auditoría y revisa los resultados de las auditorías y revisiones de terceros.

Criterios de Información	Recursos de TI
Efectividad	Personas
Eficiencia	Aplicaciones
Confidencialidad	Tecnología
Integridad	Instalaciones
Disponibilidad	Datos
Cumplimiento	
Confiabilidad	

Indicadores Clave de Resultados / Logros — KGIs

- Incrementar el desempeño y la administración de costos
- Mejorar el retorno de la inversión sobre las mayores inversiones de TI
- Mejorar el tiempo de comercialización
- Incrementar la calidad, la innovación y la administración de riesgos
- Procesos del negocio apropiadamente integrados y estandartizados
- Búsqueda de nuevos clientes y satisfacer los existentes
- Disponibilidad de apropiado ancho de banda, poder de cómputo y mecanismos para la entrega de servicios de TI
- Satisfacer los requerimientos y las expectativas de los clientes de los procesos con base en un presupuesto y a tiempo
- Cumplir con las leyes, regulaciones, estándares de la industria y compromisos contractuales.
- Transparencia en los riesgos asumidos y cumplimiento con el acuerdo del perfil de riesgo organizacional.
- Comparaciones mediante Benchmarking sobre el nivel de madurez de TI
- Creación de nuevos canales de distribución y entrega de servicios

I - DIRECTRICES GERENCIALES DEL GOBIERNO DE TI

Indicadores Clave de Desempeño - KPIs

- Mejorar los procesos de costo-eficiencia de TI (costos versus entregables o servicios)
- Incrementare el número de planes de acción de TI para las iniciativas de mejoramiento de procesos
- Incrementar la utilización de la infraestructura de TI
- Incrementar la satisfacción de los socios y accionistas (encuestas y número de reclamaciones).
- Incrementar la productividad de los funcionarios de TI (número de entregables) y su moral (encuesta)
- Incrementar la disponibilidad de conocimiento e información para administrar la empresa.
- Incrementar las relaciones entre el gobierno de la empresa y el gobierno de TI
- Incrementar el desempeño mediante mediciones utilizando tarjetas de medición (Balanced Scorecards).

Modelo de Madurez del Gobierno de TI

El Gobierno sobre la tecnología de información es un proceso que tiene como finalidad proveer valor agregado al negocio mientras balancea riesgos versus retorno.

0 **No existe.** Hay una completa falta de cualquier proceso de gobierno de TI identificable. La organización no ha reconocido aun que hay aspectos que deben ser identificados y resaltados y no hay comunicación al respecto.

1 **Inicial / Ad Hoc[7].** Hay evidencia de que la organización ha reconocido que existen aspectos del gobierno de TI que deben ser considerados. Hay, sin embargo, procesos no estandarizados, pero en su lugar, hay procedimientos ad hoc aplicados sobre un caso individual o sobre bases de caso a caso[8]. El enfoque Gerencial es caótico y hay una esporádica e inconsistente comunicación sobre aspectos y enfoques que deban ser considerados. Puede haber algún reconocimiento para utilizar el valor de TI en el desempeño orientado al resultado de los procesos relacionados de la empresa. No hay procesos de análisis estándar. El monitoreo de TI está implementado en una forma reactiva a incidentes que han causado algunas pérdidas o apuros a la organización.

2 **Repetible pero Intuitiva.** Hay una conciencia global sobre los aspectos del gobierno de TI. Las actividades del gobierno de TI y los indicadores de desempeño están en desarrollo, incluyendo la planeación de TI y los procesos de entrega y monitoreo. Como parte de los esfuerzos, las actividades del gobierno de TI están formalmente establecidas dentro del proceso de administración del cambio con el involucramiento activo de la alta gerencia. Procesos seleccionados de TI son identificados para mejorar y/o controlar el núcleo de los procesos de la empresa, son efectivamente planeados y monitoreados como si fueran inversiones y son derivados en el contexto de un marco de referencia de la arquitectura de TI. La gerencia ha identificado los métodos y técnicas básicos de análisis y medición del gobierno de TI, sin embargo, el proceso no ha sido adoptado a través la organización. No hay entrenamiento y comunicación sobre los estándares de gobernabilidad y las responsabilidades son dejadas a los individuos. Los individuos direccionan los procesos de gobernabilidad como si no fueran procesos y proyectos de TI. Las herramientas de gobernabilidad son limitadas, escogidas e implementadas para lograr métricas de gobernabilidad pero puede que no se usen en toda su capacidad debido a la falta de experiencia en su funcionalidad.

3 **Procesos Definidos.** La necesidad de actuar con respecto al gobierno de TI es entendida y aceptada. Se desarrolla un grupo básico de indicadores de Gobierno de TI, donde el encadenamiento entre medidas de ingresos y controladores de desempeño es definido, documentado e integrado dentro de la planeación operacional y estratégica .
Los procedimientos han sido estandarizados, documentados e implementados. La Gerencia ha comunicado los procedimientos estandarizados y se establece un entrenamiento informal. Los

[7] **Ad Hoc:** porque sí, por costumbre
[8] **case-by-case basis**: Bases de caso a caso

empresa. Aunque medidos, los procedimientos no son sofisticados pero son la formalización de prácticas existentes. Las herramientas están estandarizadas, utilizando técnicas disponibles y modernas. La idea de utilizar tarjetas de medición que balancean el negocio y TI son adoptadas por la organización. Esto, sin embargo, deja que el individuo, de acuerdo con su entrenamiento, siga y aplique los estándares. El análisis de causa efecto es ocasionalmente aplicado. La mayoría de los procesos son monitoreados sobre métricas (bases), pero cualquier desviación, debido a que generalmente se basa en las iniciativas de los individuos, probablemente no serían detectadas por la Gerencia. De todas maneras, el registro total del desempeño de los procesos claves es realizado y la gerencia es recompensada basada en mediciones clave de desempeño.

4 **Administrado y Medible**. Hay un completo entendimiento de los aspectos de Gobierno de TI a todos los niveles de la organización, soportado por un entrenamiento formal. Hay un claro entendimiento de quien es el cliente y sus responsabilidades están definidas y monitoreadas a través de acuerdos de nivel de servicio. Las responsabilidades son claras y el proceso de "propiedad" está establecido. Los procesos de TI están alineados con el negocio y con la estrategia de TI. El mejoramiento de los procesos de TI está basado primariamente sobre un entendimiento cuantitativo y por ello es posible monitorear y medir el cumplimiento con procesos y con métrica de procesos. Todos los responsables o propietarios de los procesos son advertidos sobre los riesgos, la importancia de TI y las oportunidades que TI puede ofrecer. La Gerencia ha definido una tolerancia bajo la cual los procesos deben operar. Se toman acciones en la mayoría, pero no en todos los casos, donde parece que los procesos no están operando efectiva o eficientemente**.** Los procesos se mejoran ocasionalmente y se refuerzan las mejores prácticas internas. Se estandariza el uso de análisis causa-efectos. Hay un limitado, primario y táctico uso de la tecnología, basado en técnicas de madurez y reforzado con herramientas estándar. Hay involucramiento de todos los expertos internos requeridos. El gobierno de TI involucra los procesos a todo lo ancho de la empresa. Las actividades del gobierno de TI están llegando a integrarse con los procesos de gobierno de la empresa.

5 **Optimizado.** En esta fase hay un entendimiento avanzado y hacia futuro de los aspectos y soluciones del gobierno de TI. El entrenamiento y las comunicaciones son soportadas por conceptos y técnicas de vanguardia. Los procesos han sido refinados a un nivel de mejores prácticas externas basadas sobre resultados de mejoramiento contínuo y modelos de madurez con otras organizaciones. La implementación de esas políticas han permitido a la organización, a la gente y a los procesos que se adapten rápidamente y por completo a los requerimientos de gobierno de TI. Todos los problemas y desviaciones son analizados de raíz y con base en ese análisis se identifican e inician acciones eficientes y oportunas. La Tecnología de Información es utilizada de una manera extensiva y optimizada para automatizar el flujo de trabajo y proporcionar herramientas para mejorar la calidad y la efectividad. Los riesgos y el retorno de los procesos de TI son definidos, balanceados y comunicados a través de toda la empresa. Se aprovechan expertos externos y se utilizan benchmarks como guías. El monitoreo y el auto-análisis de riesgos y las comunicaciones acerca de las expectativas del gobierno influencian la organización y hay un óptimo uso de la tecnología para soportar la medición, el análisis, las comunicaciones y el entrenamiento. El gobierno de la empresa y el gobierno de TI están estratégicamente conectados empujando a los recursos humanos y financieros a incrementar la ventaja competitiva de la empresa.

APÉNDICE II – DESCRIPCIÓN DEL PROYECTO COBIT

El proyecto continua siendo supervisado por un Comité de Dirección formado por representantes internacionales de la academia, industria, gobierno y la profesión de auditoría. El Comité de Dirección del Proyecto intervino en el desarrollo del *Marco Referencial* ("Framework") *COBIT* y en la aplicación de los resultados de la investigación. Se establecieron grupos de trabajo internacionales con el propósito de asegurar la calidad y contar con una revisión experta de la investigación y los elementos entregables del desarrollo del proyecto. El IT Governance Institute proporcionó toda la dirección del proyecto.

INVESTIGACION Y ENFOQUE PARA EL DESARROLLO INICIAL

Empezando con el *Marco Referencial de COBIT*, definido en la primera edición, la aplicación de estándares y directrices internacionales y la investigación dentro de mejores prácticas ha permitido el desarrollo de los *Objetivos de Control*. Las *Guías o Directrices de Auditoría* fueron desarrolladas a continuación para analizar si esos objetivos de control son apropiadamente implementados.

La investigación de la primera y segunda edición incluyó la recolección y el análisis de fuentes identificadas y fue llevada a cabo por equipos de investigación en Europa (Free University of Amsterdam), Estados Unidos (California Polytechnic University) y Australia (University of New South Wales). Los equipos de investigación fueron encargados de la compilación, revisión, análisis y apropiada incorporación de estándares técnicos internacionales, códigos de conducta, estándares de calidad, estándares profesionales en prácticas y requerimientos de la auditoría y de la industria, en cuanto a su relación con el *Marco de* Referencia y con los *Objetivos de Control* individuales. Después de la colección y análisis los investigadores fueron encargados de examinar cada dominio y cada proceso en profundidad y sugerir nuevos o modificados objetivos de control aplicables a los procesos particulares de TI. La Consolidación de los resultados fue llevada a cabo por el Comité de Dirección de COBIT y por el Director de Investigaciones de ISACF.

INVESTIGACION Y ENFOQUE PARA LA 3a EDICION

El proyecto de la 3a edición de COBIT consistió en desarrollar las *Directrices Gerenciales* y actualizar la 2a Edición de COBIT basado en nuevas y revisadas referencias internacionales.
Adicionalmente, el *Marco de Referencia* de COBIT fue revisado y mejorado para soportar el incremento de controles gerenciales, introducir gerencia de desempeño y también desarrollar el Gobierno de TI. Con el fin de proporcionarle a la gerencia una aplicación del *Marco de Referencia* para que pueda analizar y efectuar cambios para la implementación de controles y el mejoramiento sobre la información y las tecnologías relacionadas, así como medir el desempeño, las Directrices Gerenciales incluyen Modelos de Madurez, Factores Críticos de Éxito, Indicadores Clave de Logros/resultados e Indicadores Clave de Desempeño relacionados con los *Objetivos de Control*.

Las Directrices Gerenciales fueron desarrolladas para ser utilizadas por un grupo de 40 expertos de todo el mundo, pertenecientes a la industria, la academia, el gobierno y profesionales en control y seguridad de TI. Esos expertos participaron en talleres de trabajo guiados por facilitadores profesionales que utilizaron guías definidas por el Comité de Dirección del Proyecto COBIT. Los talleres fueron fuertemente apoyados por el Gartner Group y PricewaterhouseCoopers, quienes no solo proporcionaron liderazgo de pensamiento sino que también enviaron varios de sus expertos en control, gerencia del desempeño y seguridad de la información. Los resultados de los talleres generaron los borradores de los Modelos de Madurez, los Factores Críticos de Éxito, los Indicadores Clave de Logros y los Indicadores Clave de Desempeño para cada uno de los 34 objetivos de control de alto nivel. El aseguramiento de calidad de los entregables iniciales fue dirigido por el Comité de Dirección del Proyecto y el resultado de este trabajo fue colocado a disposición en la Web site de ISACA. El documento de las *Directrices Gerenciales* fue finalmente preparado para ofrecer un nuevo grupo de herramientas orientadas a la gerencia, mientras que ofrecía integración y consistencia con el *Marco de Referencia* de COBIT.

La actualización de los *Objetivos de Control*, basada en nuevos y revisados estándares internacionales fue conducida por miembros de los Capítulos de ISACA, bajo la coordinación de los miembros del Comité de Dirección de COBIT. La intención no fue llevar a cabo un análisis global de todo el material o volver a desarrollar los *Objetivo de Control*, sino generar un proceso de actualización incremental.

El resultado del desarrollo de las *Directrices Gerenciales* fue utilizado para revisar el *Marco de Referencia* de COBIT, especialmente en lo que tiene que ver con las consideraciones, objetivos y sentencias que configuran los objetivos de control de alto nivel.

APÉNDICE III - MATERIAL DE REFERENCIA PRIMARIA

Nota del traductor: Debido a que el contenido de este apéndice se compone principalmente de nombres propios de instituciones y publicaciones, dichos nombres han sido respetados manteniéndolos en inglés.

COSO: Committee of Sponsoring Organisations of the Treadway Commission. Internal Control - Integrated Framework. 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.

OECD Guidelines: Organisation for Economic Co-operation and Development. Guidelines for the Security of Information, Paris, 1992.

DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. A Code of Practice for Information Security Management, London, 1993, 1995.

ISO 9000-3: International Organisation for Standardisation. Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software, Switzerland, 1991.

An Introduction to Computer Security: The NIST Handbook: National Institute of Standards and Technology, U.S. Department of Commerce. Washington, DC, 1995.

ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and Telecommunications Agency (CCTA), London, 1989.

IBAG Framework: Draft Framework from the Infosec Business Advisory Group to SOGIS (Senior Officials Group on Information Security, advising the European Commission) Brussels, Belgium, 1994.

NSW Premiers Office Statements of Best Practices and Planning Information Management and Techniques: Statements of Best Practice #1 through #6. premier's Department New South Wales, Government of New South Wales, Australia, 1990 through 1994.

Memorandum Dutch Central Bank: Memorandum on the Reliability and Continuity of Electronic Data Processing in Banking. De Nederlandsche Bank, Reprint from Quarterly Bulletin #3, Netherlands, 1998.

EDPAF Monograph #7, EDI: An Audit Approach: Jamison, Rodger. EDI: An Audit Approach, Monograph Series #7, Information Systems Audit and Control Foundation, Inc., Rolling Meadows, IL, April 1994.

PCIE (president's Council on Integrity and Efficiency) Model Framework: A Model Framework for Management Over Automated Information Systems. Prepared jointly by the president's Council on Management Improvement and the president's Council on Integrity and Efficiency, Washington, DC, 1987.

Japan Information Systems Auditing Standards: Information System Auditing Standard of Japan. Provided by the Chuo Audit Corporation, Tokyo, August 1994.

CONTROL OBJECTIVES: Controls in an Information Systems Environment: **Control Guidelines and Audit Procedures:** EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Fourth Edition, Rolling Meadows, IL, 1992.

CISA Job Analysis: Information Systems Audit and Control Association Certification Board. "Certified Information Systems Auditor Job Analysis Study", Rolling Meadows, IL, 1994.

CICA Computer Control Guidelines: Canadian Institute of Chartered Accountants, Toronto, 1986.

IFAC International Guidelines for Managing Security of Information and Communications: International Federation of Accountants, New York, NY, 1997.

IFAC International Guidelines on Information Technology Management - Managing Information Technology Planning for Business Impact (Draft): International Federation of Accountants, New York, NY, 1998.

Standards for Internal Control in the U.S. Federal Government: U.S. General Accounting Office, Washington, DC, 1983.

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: NBS Special Publication 500-153: National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

Government Auditing Standards: U. S. General Accounting Office, Washington, DC, 1994.

Denmark Generally Accepted IT Management Practices: The Institute of State Authorized Accountants, Denmark, 1994.

SPICE: Software Process Improvement and Capability Determination. A standard on software process improvement, British Standards Institution, London, 1995.

DRI International, Professional Practices for Business Continuity Planners: Disaster Recovery Institute International. Guideline for Business Continuity Planners, St. Louis, MO, 1997.

IIA, SAC Systems Audibility and Control: Institute of Internal Auditors Research Foundation, Systems Audibility and Control Report, Alamonte Springs, FL, 1991, 1994.

IIA, Professional Practices Pamphlet 97-1, Electronic Commerce: Institute of Internal Auditors Research Foundation, Alamonte Springs, FL, 1997.

E & Y Technical Reference Series: Ernst & Young, SAP R/3 Audit Guide, Cleveland, OH, 1996.

C & L Audit Guide SAP R/3: Coopers & Lybrand, SAP R/3: Its Use, Control and Audit, New York, NY, 1997.

ISO IEC JTC1/SC27 Information Technology - Security: International Organisation for Standardisation (ISO) Technical Committee on Information Technology Security, Switzerland, 1998.

ISO IEC JTC1/SC7 Software Engineering: International Organisation for Standardisation (ISO) Technical Committee on Software Process Assessment. An Assessment Model and Guidance Indicator, Switzerland, 1992.

ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services: International Organisation for Standardisation (ISO) Technical Committee on Banking and Financial Services, Draft, Switzerland, 1997.

CCEB 96/011, Common Criteria for Information Technology Security Evaluation: Common Criteria Implementation Board, Alignment and comparison of existing European, US and Canadian IT Security Criteria, Draft, Washington, DC, 1997.

Recommended Practice for EDI: EDIFACT (EDI for Administration Commerce and Trade), Paris, 1987.

TickIT: Guide to Software Quality Management System Construction and Certification. British Department of Trade and Industry (DTI), London, 1994

ESF Baseline Control - Communications: European Security Forum, London. Communications Network Security, September 1991; Baseline Controls for Local Area Networks, September, 1994.

ESF Baseline Control - Microcomputers: European Security Forum, London. Baseline Controls Microcomputers Attached to Network, June 1990.

Computerized Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

Guide for Developing Security Plans for Information Technology: NIST Special Publication 800-18, National Institute for Standards and Technology, US Department of Commerce, Washington, DC 1998

Financial Information Systems Control Audit Manual (FISCAM): US General Accounting Office, Washington, DC, 1999.

BS7799-Information Security Management: British Standards Institute, London, 1999.

CICA Information Technology Control Guidelines, 3er Edition: Canadian Institute of Chartered Accountants, Toronto, 1998

ISO/IEC TR 1335-n Guidelines for the Management of IT Security, (GMITS) Parts 1-5: International Organisation for Standardisation, Switzerland, 1998.

AICPA/CICA Systrust™ Principles and Criteria for Systems Reliability, Version 1.0: American Institute of Certified Public Accountants, New York, and Canadian Institute of Chartered Accountants, Toronto, 1999.

APÉNDICE IV—GLOSARIO 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*)

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).*

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 Foundation)*

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.

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*)

Objetivo de imple**Control** Una sentencia o declaración del resultado deseado o propósito a ser alcanzado mediante la mentación de procedimientos de control en una actividad particular de TI

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*)

SPICE Mejoramiento del Proceso de Software y Determinación de la Capacidad (*Software Process Improvement and Capability Determination*) - un estándar pare el mejoramiento del proceso de software

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*)