COBIT®

MARCO REFERENCIAL

Abril de 1998
2da Edición

Emitido por el Comité Directivo de COBIT y
la *Information Systems Audit and Control Foundation*

Traducción al español por Gustavo A. Solís Montes, CISA

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.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Límite de Responsabilidad
La Information Systems Audit and Control Foundation y los patrocinadores de COBIT: Objetivos de Control para la Información y Tecnologías afines, han diseñado este producto principalmente como una fuente de instrucción para los profesionales dedicados a las actividades de control. La *Information Systems Audit and Control Foundation* y los patrocinadores no declaran que el uso de este producto asegurará un resultado exitoso. No deberá considerarse que este producto incluye todos los procedimientos o pruebas apropiados o que excluye otros procedimientos y pruebas que estén razonablemente dirigidos hacia la obtención de los mismos resultados. Para determinar la conveniencia de cualquier prueba o procedimiento específico, los expertos en control deberán aplicar su propio juicio profesional a las circunstancias de control especiales presentadas por cada entorno de sistemas en particular.

Acuerdo de Licencia *(disclosure)*

Information Systems Audit and Control Foundation
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org

ISBN 0-9629440-4-1 (Framework, English)

RECONOCIMIENTOS

PRINCIPALES PATROCINADORES DE LA CORPORACIÓN A NIVEL MUNDIAL

UNISYS
The Information Management Company

UNITECH SYSTEMS, Inc.
Information Integrity Specialists

MIS TRAINING INSTITUTE

Coopers &Lybrand

ZERGO

Information Systems Audit and Control Association

PATROCINADORES DE LOS ASOCIADOS DE LA CORPORACIÓN

Fellesdata a/s, Norway
NoviT a/s, Norway

PRINCIPALES CAPTÍULOS DE ISACA PATROCINADORES

Benelux
National Capital Area
New York Metropolitan
Norway
Toronto

CAPÍTULOS DE ISACA ASOCIADOS PATROCINADORES

Adelaide
Atlanta
Auckland
Austin
Bangkok
Brisbane
Canberra
Central Arkansas
Central Indiana
Central Maryland
Central New York
Denver
Detroit
Finland
Greater Hartford
Hawaii
Houston
Hudson Valley
Indonesia
London
Los Angeles
Middle Tennessee
Minnesota
New England
New Jersey
New Mexico
North Alabama
North Texas
Northeast Ohio
Northern United Kingdom
Philadelphia
Pittsburgh
Puget Sound
Research Triangle
Sacramento
San Diego
Santiago de Chile
Seoul
South Texas
St. Louis
Sweden
Tokyo
Tulsa
Victoria
Virginia
Wellington
Winnipeg

CONTRIBUCIONES INDIVIDUALES

Bill Bartgis
John Beveridge
William Bialkowski
Alllen Bragan
Maryanne S. Canant
Michael Donahue
John Lainhart
Teresa McCauley
Robert G. Parker
Daniel Ramos
Deepak Sarup
Lily Shue
Patrick Stachtchenko
Kevin Weston

RECONOCIMIENTOS

EL EQUIPO DEL PROYECTO

Erik Guldentops, S.W.I.F.T. S.C., Belgium
Eddy Schuermans, Coopers & Lybrand, Belgium
Thomas Lamm, ISACF, USA

COMITÉ QUE DIRIGE EL PROYECTO

Erik Guldentops, S.W.I.F.T. S.C., Belgium
John Beveridge, State Auditors' Office, Massachusetts, USA
Prof. Dr. Bart De Schutter, Vrije Universiteit Brussels, Chairman BRT Belgium
Gary Hardy, Arthur Andersen, United Kingdom
John Lainhart, Inspector General, U.S. House of Representatives, USA
Akira Matsuo, Chuo Audit Corporation, Japan
Eddy Schuermans, Coopers & Lybrand, Belgium
Paul Williams, Arthur Andersen, United Kingdom
Thomas Lamm, ISACF, USA

INVESTIGADORES

Vrije Universiteit Amsterdam, The Netherlands
Prof. M.E. Van Biene-Hershey
René Barlage, RB Consultants
California Polytechnic University, USA
Prof. Dan Manson, Lead Researcher

ANALISTAS EXPERTOS —EUROPA

Chris Bagot, NATO
René Barlage, RB Consultants
Prof. Dr. Henri Beker, Zergo, Ltd.
John Beveridge, ISACA Past President
Erik Guldentops, S.W.I.F.T. S.C.
Gary Hardy, Arthur Andersen
Eddy Schuermans, Coopers & Lybrand
Alan Stanley, European Security Forum
Danny Van Riel, Johnson & Johnson
Bram Vandenberg, Ernst & Young

ANALISTAS EXPERTOS —USA

Prof. Ulric J. Gelinas, Bentley College
John Hayes, Price Waterhouse LLP
Greg Hedges, Arthur Andersen & Co., S.C.
Dave Kent, Price Waterhouse LLP
Tom Kothe, Ernst & Young LLP
John Lainhart, Inspector General, U.S. House of Representatives, USA
Robert Roussey, University of Southern California

CALIDAD GARANTIZADA

Gary Austin, GAO
Chris Bagot, NATO
Rick Beatty, California Federal Bank
Peter De Koninck, Coopers & Lybrand
Balencia Dozier, Manufacturers Bank
Doris Gin, Arthur Andersen & Co., LLP
A.I. Heijkamp, Computercentrum VSB
Max Huijbers, Rijkscomputercentrum
Peter Maertens, NATO
Bill Pepper, Zergo, Ltd.
Mark Stanley, Santa Barbara Bank
Tjerk Terpstra, Inter Access
Mark Wheeler, Farmers Insurance
Carla Williams, Executive Consultants

AGRADECIMIENTO ESPECIAL a los miembros de la Mesa directiva de la Information Systems Audit and Control Association, y los Fideicomisarios de la Information Systems Audit and Control Foundation por su continuo y firme apoyo a la familia de productos de 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 criticalidad 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. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos *Mainframe*. 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 nueva tecnología***. Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados. COBIT ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona "prácticas sanas" a través de un Marco Referencial de dominios y procesos y presenta actividades en una estructura manejable y lógica. Las **prácticas sanas** de COBIT representan el consenso de los expertos (le ayudarán a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo que usted será juzgado si las cosas salen mal.

Las organizaciones deben cumplir con requerimientos de calidad, de reportes fiduciarios y de seguridad, tanto para su información, como para sus activos. La administración deberá obtener un balance adecuado en 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 expectativas, la administración deberá establecer un sistema adecuado de control interno. Por lo tanto, este sistema o marco referencial deberá existir para proporcionar soporte a los procesos de negocio y debe ser preciso en la forma en la que cada actividad individual de control satisface los requerimientos de información y puede impactar a los recursos de TI. El impacto en los recursos de TI es enfatizado en el Marco Referencial de COBIT conjuntamente a los requerimientos de información del negocio que deben ser alcanzados: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

La administración, mediante este *gobierno corporativo*[2], debe asegurar que la debida diligencia sea ejercitada por todos los individuos involucrados en la administración, empleo, diseño, desarrollo, mantenimiento u operación de sistemas de información.

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 a negocios es el tema principal de COBIT. Está diseñado no sólo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación[3] detallada para los propietarios de los pro-

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

[2] **Gobierno corporativo** (*corporate governance): Governance* es un término que representa *el* sis tema que establece la alta gerencia para asegurar el logro de los objetivos de una Organización.

[3] **Lista de verificación** (*check list)*

cesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y apoderamiento[4] de los dueños de procesos para que éstos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados. El Marco Referencial de COBIT proporciona herramientas al propietario de procesos de negocio que facilitan el cumplimiento de esta responsabilidad. El Marco Referencial 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.***

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 & organización, adquisición & implementación, entrega (de servicio) y monitoreo. Esta estructura cubre todos los aspectos de información y de la tecnología que la soporta. Dirigiendo 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. Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una directriz ó guía de auditoría o de aseguramiento que permite la revisión de los procesos de TI contra los 302 objetivos detallados de control recomendados por COBIT para proporcionar a la Gerencia la certeza de su cumplimiento y/o una recomendación para su mejora. COBIT contiene un *conjunto de herramientas de implementación* que proporciona lecciones aprendidas por empresas que rápida y exitosamente aplicaron COBIT en sus ambientes de trabajo. Incluye un Resumen Ejecutivo para el entendimiento y la sensibilización de la alta gerencia sobre los principios y conceptos fundamentales de COBIT. La guía de implementación cuenta con dos útiles herramientas (Diagnóstico de Sensibilización Gerencial[5] y Diagnóstico de Control en TI[6]) para proporcionar asistencia en el análisis del ambiente de control en una organización.

El Marco Referencial COBIT otorga especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el Marco Referencial proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con Tecnología de Información.

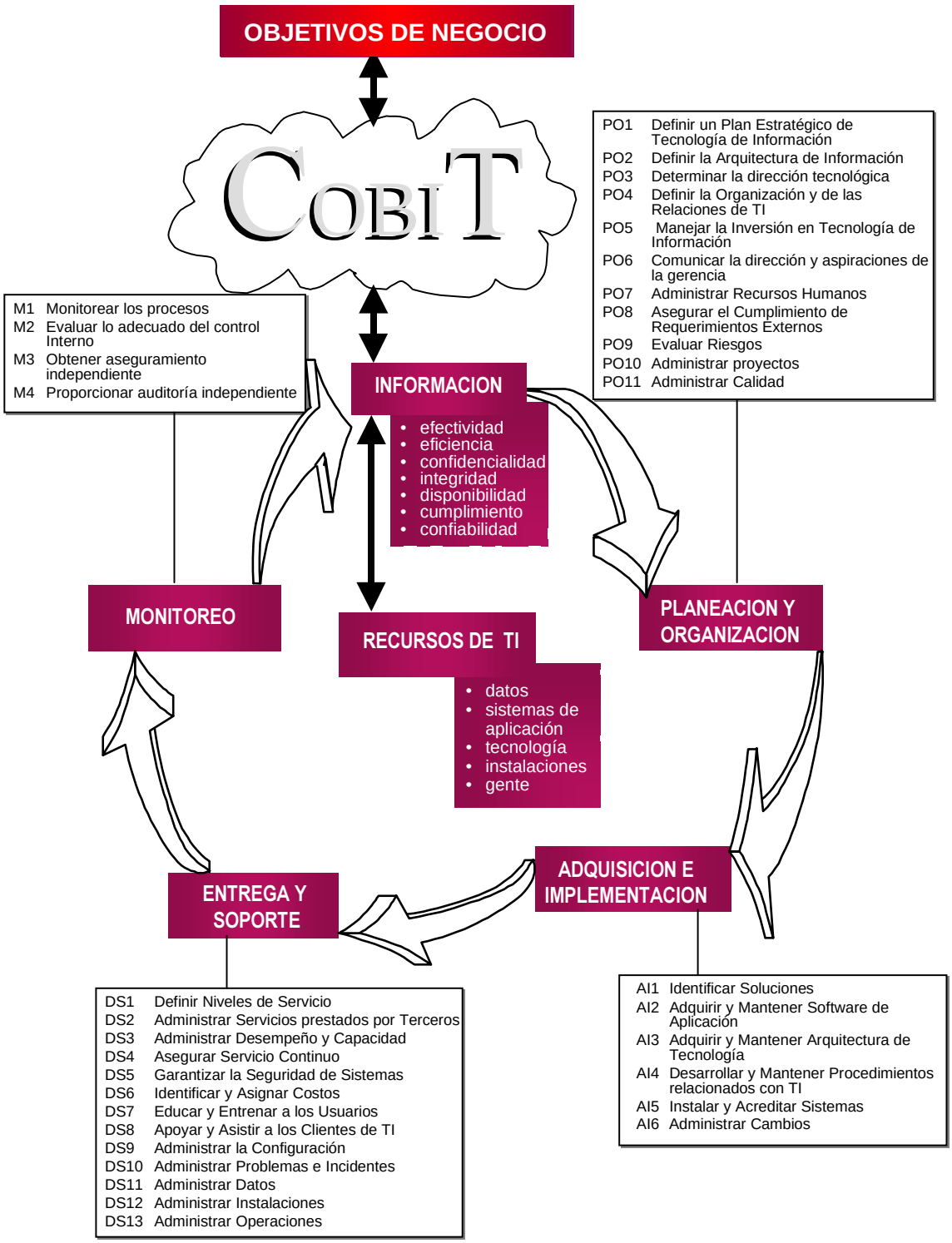
La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en TI para medir en forma comparativa[7] tanto su ambiente de TI existente, como su ambiente planeado.

COBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de organizaciones, a nivel mundial. El objetivo de COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

Por lo tanto, COBIT está orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas.

[4] **Apoderamiento** (*empowerment)*
[5] **Diagnóstico de Sensibilización Gerencial** *(management awareness diagnostic)*
[6] **Diagnóstico de Control en TI** (*IT control diagnostic)*
[7] **Medir en forma comparativa** *(benchmark)*

PROCESOS DE IT DE COBIT DEFINIDOS DENTRO DE LOS CUATRO DOMINOS



ANTECEDENTES

DESARROLLO DEL PRODUCTO COBIT

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). **– COBIT es *la* herramienta innovadora para el gobierno[8] deTI -.**

COBIT se fundamenta en los Objetivos de Control existentes de la *Information Systems Audit and Control Foundation* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en **sistemas de información en toda la empresa.** El término **"generalmente 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). Para propósitos del proyecto, **"buenas prácticas"** significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de *COBIT* ha traido como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

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

- ➔ **el desarrollo de un marco referencial para control en TI como fundamento para los objetivos de control en TI y como una guía para la investigación consistente en auditoría y control de TI;**
- ➔ **una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho; y**
- ➔ **una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en TI y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.) y**
- ➔ **una revisión crítica y actualización de las guías actuales para desarrollo de auditorías de sistemas de información**

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, IickIT, etc.;
Estándares Profesionales para control interno y auditoría: reporte COSO, GAO, IFAC, IIA, ISACA, estándares CPA, 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 y manufactura de TI.

(Ver Apéndice III Glosario de Términos para definiciones de siglas)

DEFINICIÓN DEL PRODUCTO COBIT

El desarrollo de COBIT ha resultado en la publicación de:

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

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

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

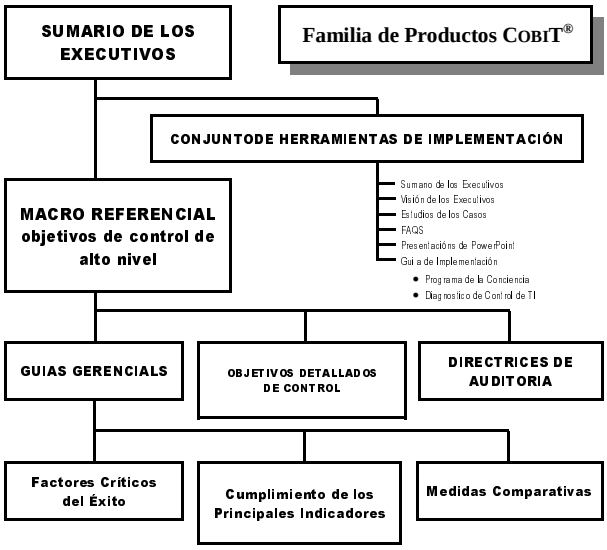
El Conjunto de Herramientas de Implementación incluye la *Síntesis Ejecutiva*, proporcionando a la alta gerencia conciencia y entendimiento de COBIT. También incluye una guía de implementación con dos útiles herramientas – Diagnóstico de la Conciencia de la Gerencia[9] y el Diagnóstico de Control de TI[10] - para proporcionar asistencia en el análisis del ambiente de control en TI de una organización. También se incluyen varios casos de estudio que detallan como organizaciones en todo el mundo han implementado COBIT exitosamente. Adicionalmente, se incluyen respuestas a las 25 preguntas mas frecuentes acerca de COBIT y varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.

EVOLUCIÓN DEL PRODUCTO COBIT

COBIT evolucionará a través de los años y será el fundamento de investigaciones futuras. Por lo tanto, se generará un familia de productos COBIT y al ocurrir esto, las tareas y actividades que sirven como la 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.

Una temprana adición significativa visualizada para la familia de productos COBIT, es el desarrollo de las Guías de Gerenciales que incluyen Factores Críticos de Exito, Indicadores Clave de Desempeño y Medidas Comparativas . Esta adición proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de COBIT. Los Factores Críticos de Exito identificarán los aspectos o acciones más importantes para la administración y poder así tomar dichas aciones o considerar los aspectos para lograr control sobre sus procesos de TI. Los Indicadores Clave de Desempeño proporcionarán medidas de éxito que permitan conocer a la gerencia si un proceso de TI esta alcanzando los requerimientos de negocio. La Medidas Comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: (1) determinar el nivel actual de madurez de la empresa; (2) determinar el nivel de madurez que desea lograr, como una función de sus riesgos y objetivos; y (3) proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de COBIT.

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



[9] **Diagnóstico de la Conciencia de la Gerencia** (*management awareness diagnostic*)
[10] **Diagnóstico de Control de TI** (*IT control diagnostic*)
[11] **Guías gerenciales** (*management guidelines*)
[12] **Medidas comparativas** (*benchmarks)*

EL MARCO REFERENCIAL DE **COBIT**

ESTABLECIENDO LA ESCENA

LA NECESIDAD DE CONTROL EN TECNOLOGIA DE INFORMACION

En años recientes, ha sido cada vez más evidente para los legisladores, usuarios y proveedores de servicios la necesidad de un Marco Referencial para la seguridad y el control de tecnología de información (TI). Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de 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 criticalidad 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[13]
- 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. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos *Mainframe.* ***Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología.*** Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados

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

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

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 frente a la Gerencia su opinión acerca de los controles internos. Sin contar con un marco referencial, ésta se convierte en una tarea demasiado complicada. Esto ha sido mostrado en varios estudios recientes acerca de la manera en la que los auditores evalúan situaciones complejas de seguridad y control en TI, estudios que fueron dados a conocer casi simultáneamente en diferentes partes del mundo. 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.

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

EL AMBIENTE DE NEGOCIOS: COMPETENCIA, CAMBIO & 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 tecnología de sistemas de información para mejorar su posición competitiva. La reingeniería en los negocios, las reestructuraciones, el *outsourcing*, 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 economía implica una dependencia creciente en la computación 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 los basados en hardware como los basados en software. Además, las características estructurales fundamentales de estos controles están evolucionando al mismo paso que las tecnologías de computación y las redes.

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 dentro de un marco contextual de cambios acelerados, 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.

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 y 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 (*Department of Trade and Industry*, 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 de negocio. El propósito de *COBIT* es el 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.

Un enfoque hacia los requerimientos de negocio en cuanto a controles para tecnología de información y la aplicación de nuevos modelos de control y estándares internacionales relacionados, hicieron evolucionar los Objetivos de Control y pasar de una herramienta de auditoría, a *COBIT*, que es una herramienta para la administración. **COBIT es, por lo tanto, *la* herramienta innovadora para el gobierno de TI que ayuda a la gerencia a comprender y administrar los riesgos asociados con TI.**

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 el 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 & AUDITORES

COBIT esta diseñado para ser utilizado por tres audiencias distintas:

ADMINISTRACION:

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 DE SISTEMAS DE INFORMACION:

Para dar soporte a las opiniones mostradas a la administración sobre los controles internos.

Además de responder a las necesidades de la audiencia inmediata de la Alta Gerencia, a los auditores y a los profesionales dedicados al control y seguridad, *COBIT* puede ser utilizado dentro de las empresas por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso, y por todos aquéllos responsables de TI en la empresa.

ORIENTACIÓN A OBJETIVOS DE NEGOCIO

Los Objetivos de Control muestran una relación clara y distintiva con los objetivos de 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. Se proporcionan 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 marco Referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 302 objetivos detallados de control. El Marco Referencial fue mostrado a la industria de TI y a los profesionales dedicados a la auditoría para abrir la posibilidad a revisiones, dudas y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

DEFINICIONES

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

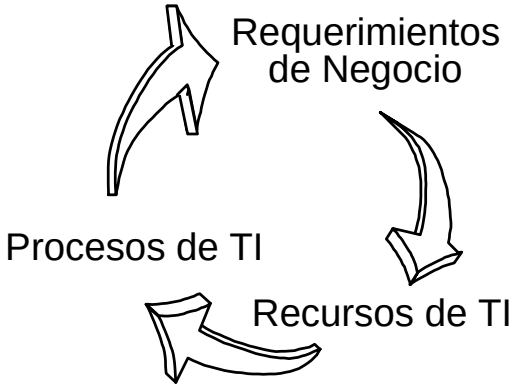
Objetivo de control en TI se define como

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

LOS PRINCIPIOS DEL MARCO REFERENCIAL

Existen dos clases distintas de modelos de control disponibles actualmente, 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 que 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 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 (de servicio)

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

Requerimientos de Seguridad
- Confidencialidad
- Integridad
- Disponibilidad

La Calidad ha sido considerada principalmente por su aspecto 'negativo' (no fallas, confiable, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo, atractivo, "ver y sentir[14]", 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 (de 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 es también considerado que queda cubierto por Eficiencia.

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

Con respecto a los aspectos de seguridad, CobiT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, fue descubierto 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.

[14] **Ver y Sentir** (*look and feel)*

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

A continuación se muestran las definiciones de trabajo de 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 — Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Aplicaciones — Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados

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

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

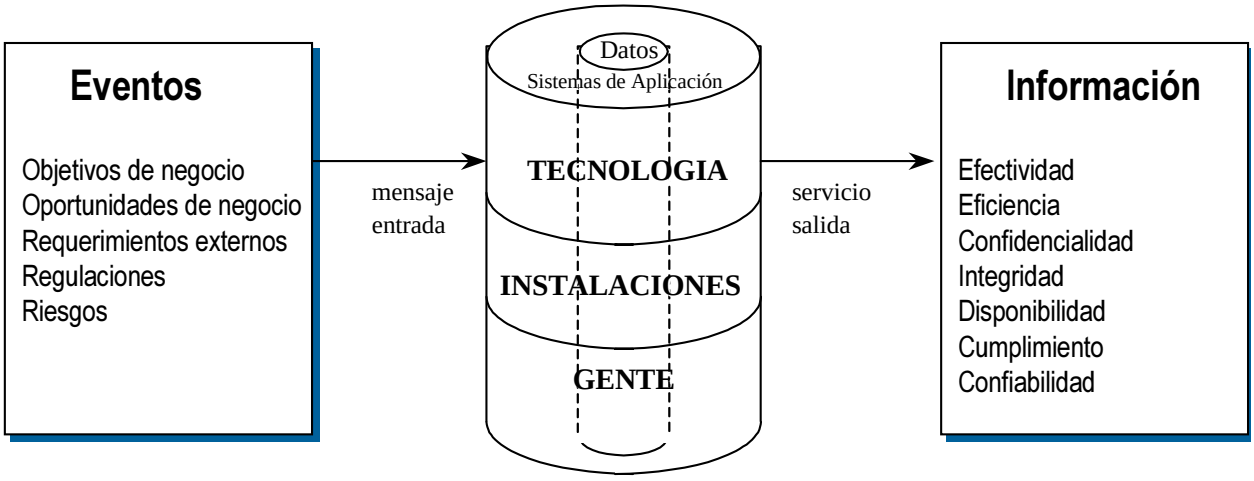
Personal — Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información

El dinero o capital no fue considerado como un recurso para la clasificación de objetivos de control para TI debido a que puede definirse como la inversión en cualquiera de los recursos mencionados anteriormente y podría causar confusión con los requerimientos de auditoría financiera.

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.

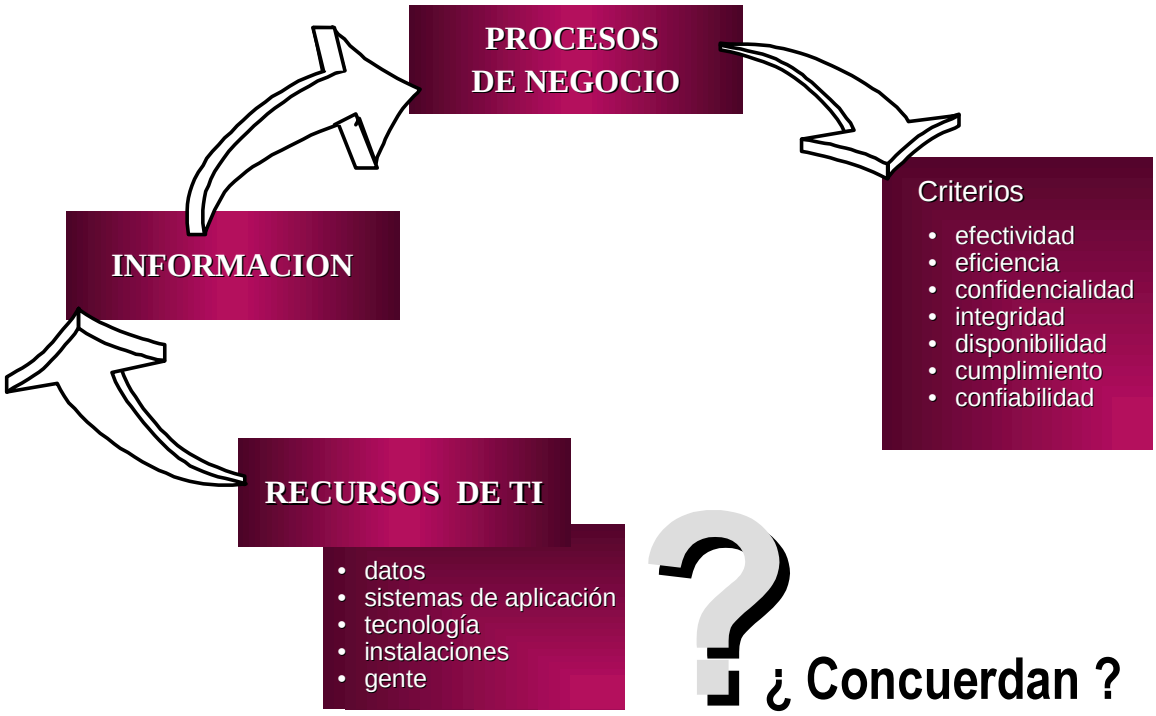
OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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



La información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos.

¿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.



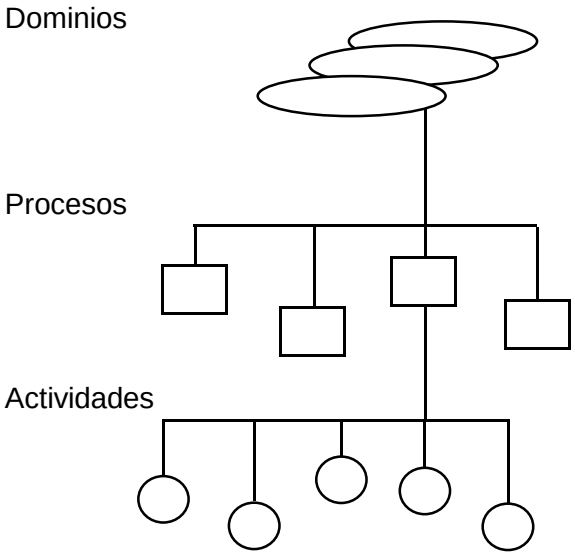
OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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

Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta típicamente con requerimientos de control diferentes a los de actividades discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control).

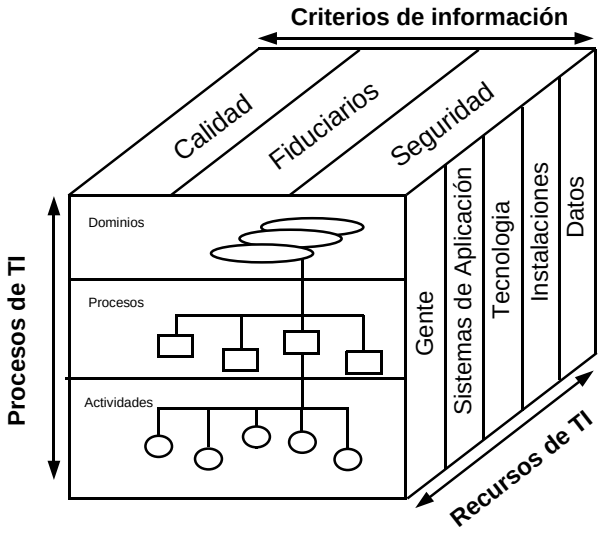
Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.



Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: (1) recursos de TI, (2) requerimientos de negocio para la información y (3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos). Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control.

Estos tres puntos estratégicos son descritos en el Cubo COBIT que se muestra a continuación:



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[15]" del auditor -. Por lo tanto, cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo.

[15] **Jerga** (*jargon)*

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Las definiciones para los dominios mencionados son las siguientes:

Planeación y organización

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Entrega y soporte

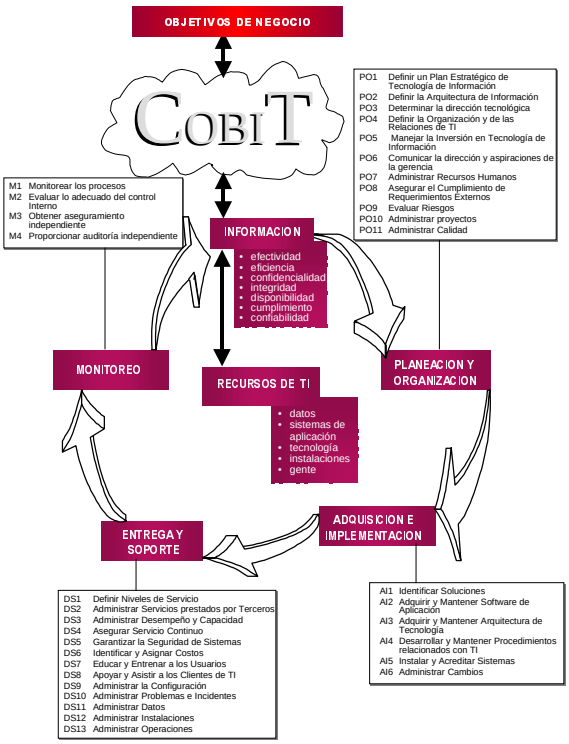
En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio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

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.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

El siguiente diagrama ilustra este concepto:



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

También debe ser tomado en cuenta que el criterio de efectividad de los procesos que planean o entregan soluciones a los requerimientos de negocio, cubrirán algunas veces los criterios de disponibilidad, integridad y confidencialidad. – en la práctica, se han convertido en requerimientos del negocio. Por ejemplo, el proceso de "identificar soluciones automatizadas" deberá ser efectivo en el cumplimiento de requerimientos de disponibilidad, integridad y confidencialidad.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación dentro del marco referencial *COBIT* basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente.

Primario es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

Secundario es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Blanco (vacío) podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Similarmente, todos las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de COBIT indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración (no por aquellos que simplemente toman parte en el proceso). Esta clasificación es hecha dentro el Marco Referencial de COBIT basado en el mismo proceso riguroso de información proporcionada por los investigadores, expertos y revisores, utilizando las definiciones estrictas indicadas previamente.

TABLA RESUMEN

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

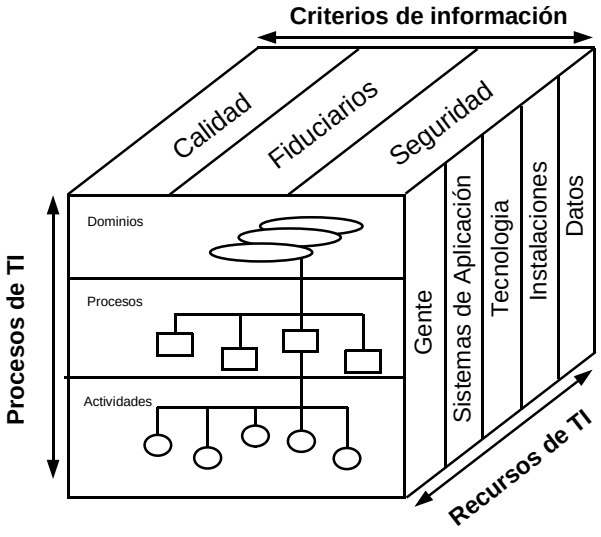
DOMINIO		PROCESO	Criterios de Información: efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	Recursos de TI: recursos	sistemas de aplicación	tecnología	instalaciones	datos
Planeación y Organización	PO1	Definir un plan estratégico de sistemas	P	S						☑	☑	☑	☑	☑
	PO2	Definir la arquitectura de información	P	S	S	S					☑			☑
	PO3	Determinar la dirección tecnológica	P	S								☑	☑	
	PO4	Definir la organización y sus relaciones	P	S						☑				
	PO5	Administrar las inversiones (en TI)	P	P					S	☑	☑	☑	☑	
	PO6	Comunicar la dirección y objetivos de la gerencia	P					S		☑				
	PO7	Administrar los recursos humanos	P	P						☑				
	PO8	Asegurar el apego a disposiciones externas	P					P	S	☑	☑			☑
	PO9	Evaluar riesgos	S	S	P	P	P	S	S	☑	☑	☑	☑	☑
	P010	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							☑	☑			
	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	Proporcionar auditoría independiente	P	P	S	S	S	S	S	☑	☑	☑	☑	☑

GUÍA PARA LA UTILIZACIÓN DEL MARCO REFERENCIAL Y LOS OBJETIVOS DE CONTROL COBIT

PERSPECTIVAS DIFERENTES; ENFOQUES DIFERENTES

El marco referencial conceptual puede ser enfocado desde tres puntos estratégicos:
1) recursos de TI, 2) requerimientos de negocio para la información y 3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos). Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control.

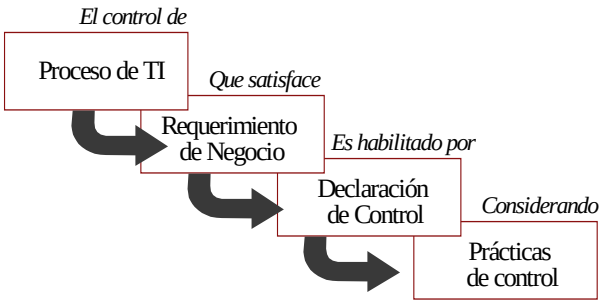


MARCO REFERENCIAL *COBIT*

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

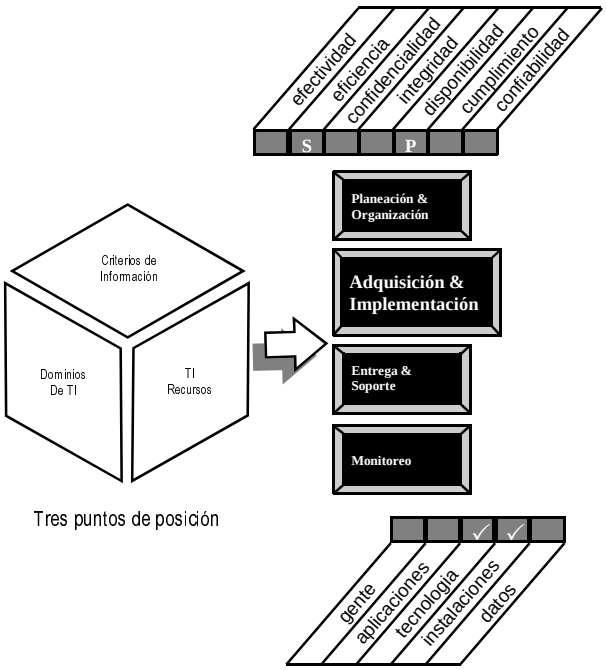
Los Objetivos de Control de TI han sido organizados por proceso/actividad, pero también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista estratégico como se explicó anteriormente, sino también para facilitar enfoques combinados o globales, 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 *COBIT* han sido definidos en una manera genérica, por ejemplo, sin depender de la plataforma técnica, aceptando el hecho de que algunos ambientes de tecnología especiales pueden requerir una cobertura separada para objetivos de control.



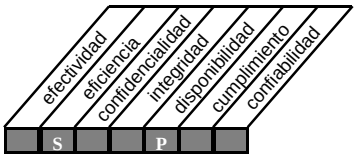
AYUDAS DE NAVEGACIÓN

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 referencial *COBIT* - procesos, recursos y criterios -

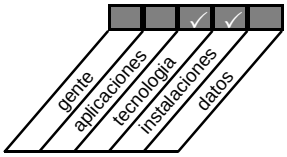


Los dominios son identificados ubicando la siguiente figura en la esquina superior derecha de cada página en la sección de Objetivos de Control, agrandando y haciendo más visible el dominio bajo revisión.

La clave para el criterio de información será proporcionado la esquina superior izquierda en la sección de Objetivos de Control mediante la siguiente "mini" matriz, la cual identificará cual criterio y en que 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 en la sección de Objetivos de Control identifica los recursos de TI que son administrados en forma específica por el proceso bajo consideración - no aquellos que simplemente toman parte en el proceso -. Por ejemplo, el proceso "administración de información" se concentra particularmente en la integridad y confiabilidad de los recursos de datos, mientras que disponibilidad y confidencialidad son primariamente proporcionadas por los procesos que administran los recursos que utilizan los datos (Ej. Aplicaciones y tecnología).

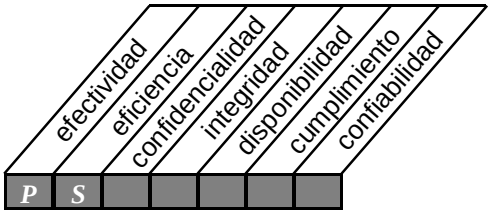


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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 de negocio de:

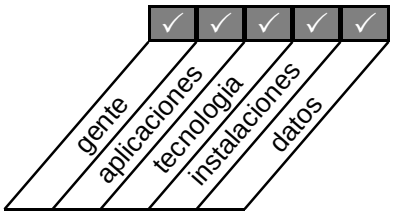
Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.

se hace posible a través de:

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:

- definición de objetivos de negocio y necesidades de TI
- inventario de soluciones tecnológicas e infraestructura actual
- servicios de vigilancia tecnológica
- cambios organizacionales
- estudios de factibilidad oportunos
- evaluación de sistemas existentes



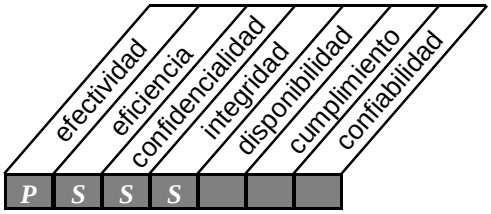
[16] **Vigilancia tecnológica** (*technology watch*)

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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:

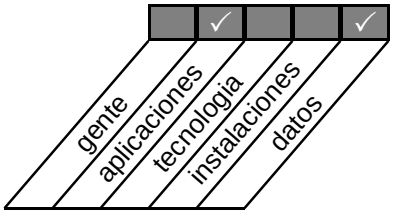
organizar de la mejor manera los sistemas de información

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:

- documentación
- diccionario de datos
- reglas de sintaxis de datos
- propiedad de la información y clasificación de severidad



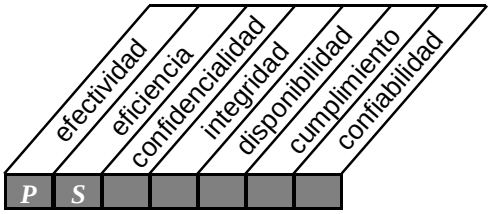
[17] **Severidad** (criticality)

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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:

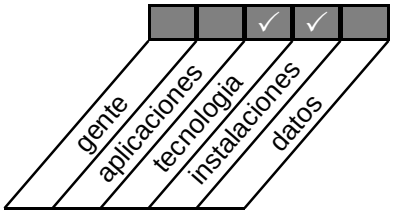
aprovechar la tecnología disponible o tecnología emergente

se hace posible a través de:

la creación y mantenimiento de un plan de infraestructura tecnológica

y toma en consideración:

- capacidad de adecuación y evolución de la infraestructura actual
- monitoreo de desarrollos tecnológicos
- contingencias
- planes de adquisición

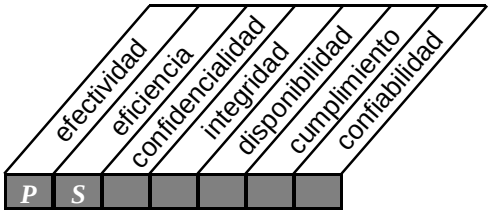


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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:

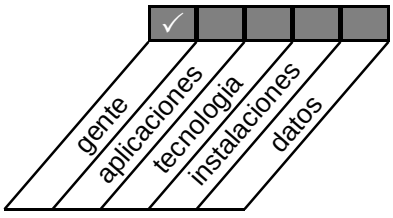
prestación de servicios de TI

se hace posible a través de:

una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas

y toma en consideración:

- comité de dirección
- responsabilidades a nivel consejo
- propiedad, custodia
- supervisión
- segregación de funciones
- roles y responsabilidades
- descripción de puestos
- niveles de asignación de personal
- personal clave

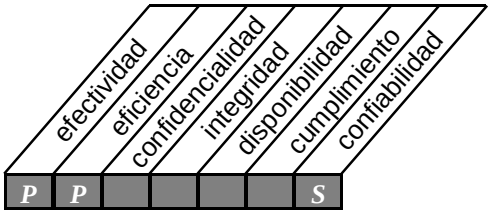


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO5



Control sobre el proceso de TI de:

Manejo de la inversión

que satisface los requerimientos de negocio de:

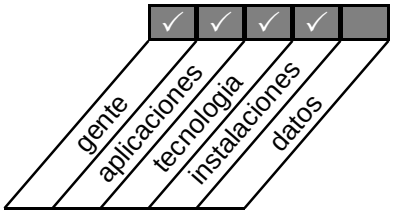
asegurar el financiamiento y el control de desembolsos de recursos financieros

se hace posible a través de:

presupuestos periódicos sobre inversiones y operación establecidos y aprobados por el negocio

y toma en consideración:

- alternativas de financiamiento
- control del gasto real
- justificación de costos
- justificación del beneficio

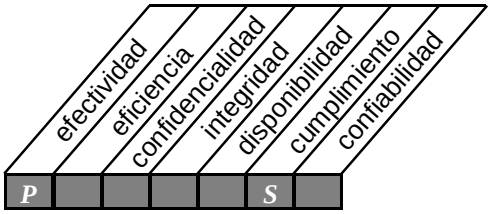


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO6



Control sobre el proceso de TI de:

comunicación de la dirección y aspiraciones de la gerencia

que satisface los requerimientos de negocio de:

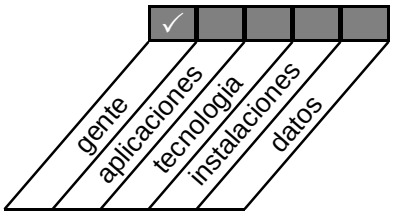
asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones

se hace posible a través de:

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

y toma en consideración:

- código de ética / conducta
- directrices tecnológicas
- cumplimiento
- compromiso con la calidad
- políticas de seguridad
- políticas de control interno

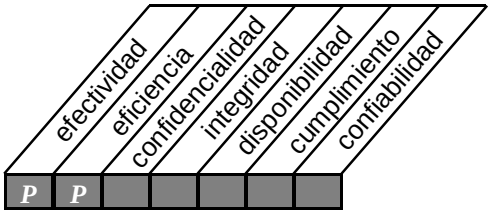


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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:

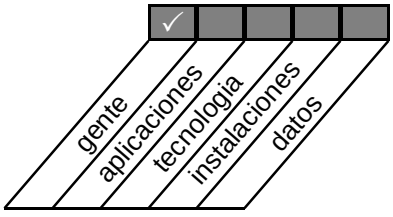
maximizar las contribuciones del personal a los procesos de TI

se hace posible a través de:

técnicas sólidas para administración de personal

y toma en consideración:

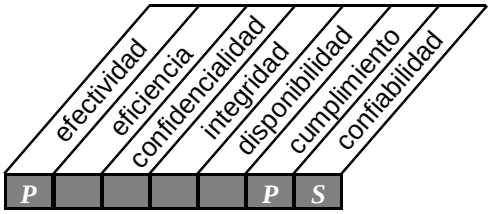
- reclutamiento y promoción
- requerimientos de calificaciones
- capacitación
- desarrollo de conciencia
- entrenamiento cruzado
- procedimientos de acreditación
- evaluación objetiva y medible del desempeño



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:

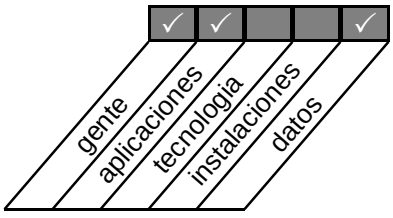
cumplir con obligaciones legales, regulatorias y contractuales

se hace posible a través de:

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

y toma en consideración:

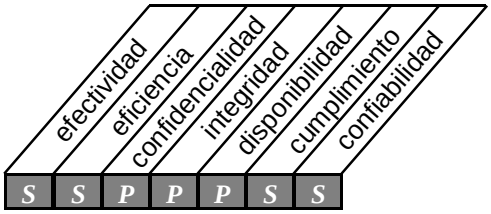
- leyes, regulaciones, contratos
- monitoreo de evoluciones legales y regulatorios
- revisiones regulares en cuanto a cambios
- búsqueda de asistencia legal y modificaciones
- seguridad y ergonomía
- privacidad
- propiedad intelectual
- flujo de datos



OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO9



Control sobre el proceso de TI de:

evaluación de riesgos

que satisface los requerimientos de negocio de:

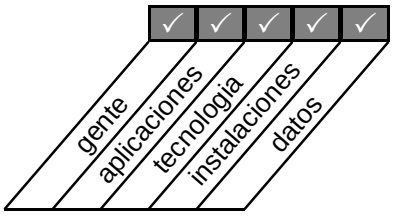
asegurar el logro de los objetivos de TI y responder a las amenazas a la provisión de servicios de TI

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, tomando medidas económicas para mitigar los riesgos

y toma en consideración:

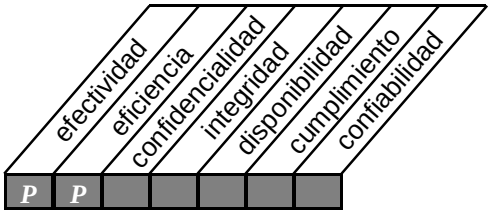
- diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.)
- alcance: global o de sistemas específicos
- actualización de evaluación de riegos
- metodología de evaluación de riesgos
- medición de riesgos cualitativos y/o cuantitativos
- plan de acción de riesgos



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:

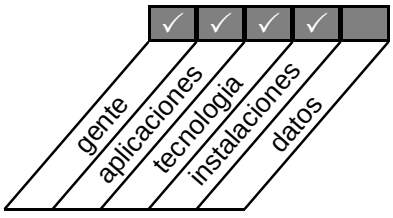
establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión

se hace posible a través de:

identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido

y toma en consideración:

- la propiedad de los proyectos
- el involucramiento de los usuarios
- la estructuración jerárquica de tareas y los puntos de revisión
- asignación de responsabilidades
- aprobación de fases y proyecto
- presupuestos de costos y horas hombre
- planes y metodología de aseguramiento de calidad

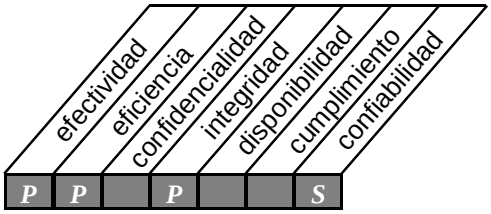


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO11



Control sobre el proceso de TI de:

Administración de calidad

que satisface los requerimientos de negocio de:

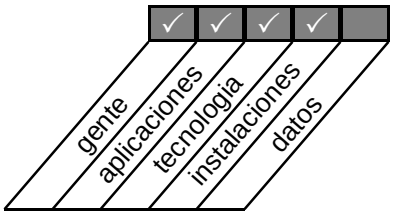
satisfacer los requerimientos del cliente

se hace posible a través de:

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

y toma en consideración:

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

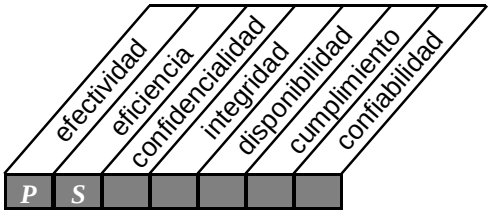


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICION E IMPLEMENTACION

AI1



Control sobre el proceso de TI de:

Identificación de soluciones

que satisface los requerimientos de negocio de:

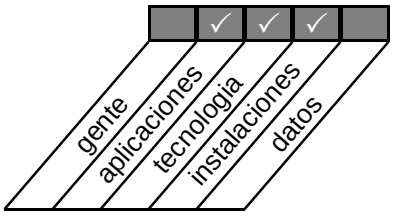
asegurar el mejor enfoque para cumplir con los requerimientos del usuario

se hace posible a través de:

un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios

y toma en consideración:

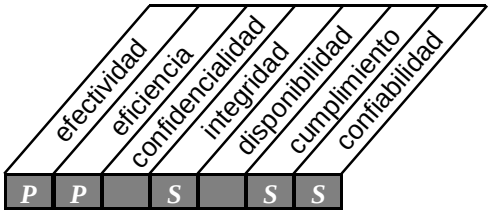
- definición de requerimientos de información
- estudios de factibilidad (de costo-beneficio, alternativas, etc)
- arquitectura de información
- seguridad con relación de costo-beneficio favorable
- pistas de auditoría
- contratación de terceros
- aceptación de instalaciones y tecnología



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICION E IMPLEMENTACION

AI2



Control sobre el proceso de TI de:

adquisición y mantenimiento de software de aplicación

que satisface los requerimientos de negocio de:

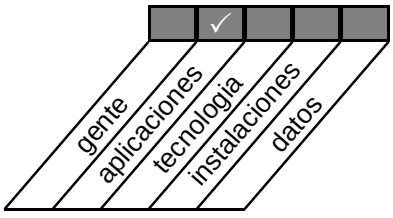
proporcionar funciones automatizadas que soporten efectivamente al negocio

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:

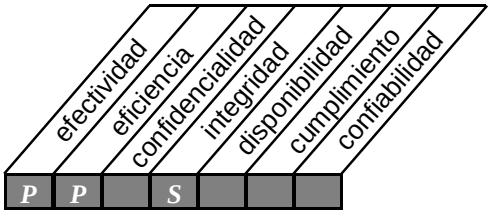
- requerimientos de usuarios
- requerimientos de archivo, entrada, proceso y salida
- interface usuario – máquina
- personalización de paquetes
- pruebas funcionales
- controles de aplicación y requerimientos funcionales
- documentación



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICION E IMPLEMENTACION

AI3



Control sobre el proceso de TI de:

adquisición y mantenimiento de arquitectura de software

que satisface los requerimientos de negocio de:

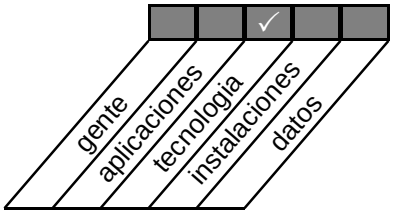
proporcionar las plataformas apropiadas para soportar aplicaciones de negocios

se hace posible a través de:

la evaluación del desempeño de hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema

y toma en consideración:

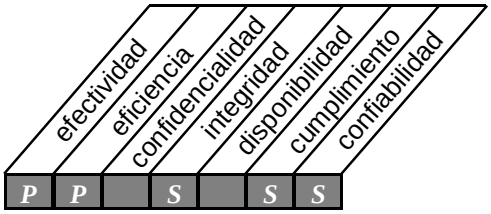
- evaluación de tecnología
- mantenimiento preventivo de hardware
- seguridad del software de sistema, instalación, mantenimiento y control sobre cambios



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICION E IMPLEMENTACION

AI4



Control sobre el proceso de TI de:

desarrollo y mantenimiento de procedimientos relacionados con tecnología de información

que satisface los requerimientos de negocio de:

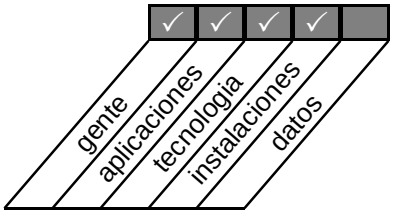
asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas

se hace posible a través de:

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

y toma en consideración:

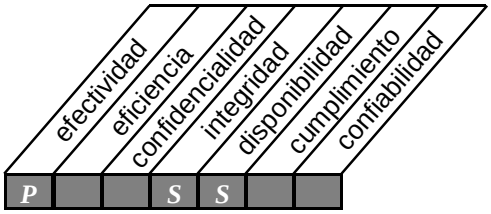
- procedimientos y controles de usuarios
- procedimientos y controles operacionales
- materiales de entrenamiento



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICION E IMPLEMENTACION

AI5



Control sobre el proceso de TI de:

instalación y acreditación de sistemas

que satisface los requerimientos de negocio de:

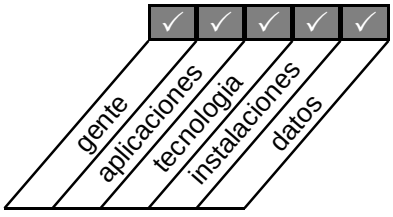
verificar y confirmar que la solución sea adecuada para el propósito deseado

se hace posible a través de:

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

y toma en consideración:

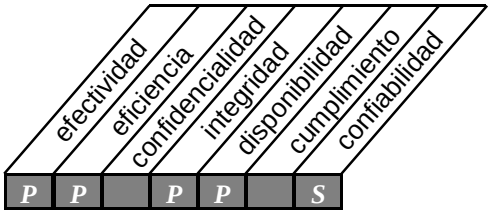
- capacitación
- conversión / carga de datos
- pruebas específicas
- acreditación
- revisiones post implementación



OBJETIVOS DE CONTROL DE ALTO NIVEL

ADQUISICION E IMPLEMENTACION

AI6



Control sobre el proceso de TI de:

administración de cambios

que satisface los requerimientos de negocio de:

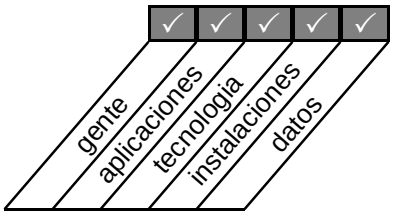
minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores

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:

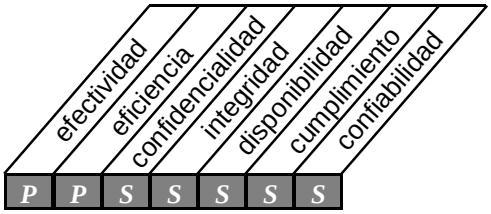
- identificación de cambios
- procedimientos de categorización, priorización y emergencia
- evaluación del impacto
- autorización de cambios
- manejo de liberación
- distribución de software



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS1



Control sobre el proceso de TI de:

Definición de niveles de servicio

que satisface los requerimientos de negocio de:

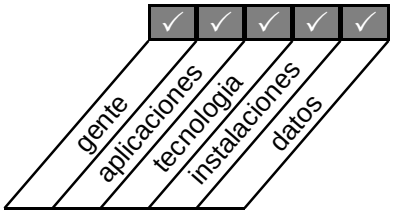
establecer una comprensión común del nivel de servicio requerido

se hace posible a través de:

el establecimiento de convenios 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:

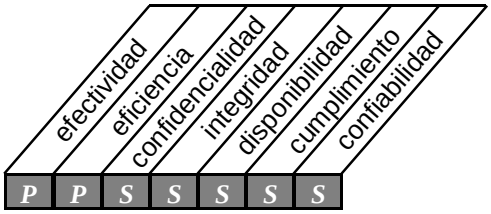
- convenios formales
- definición de responsabilidades
- tiempos y volúmenes de respuesta
- dependencias
- cargos
- garantías de integridad
- convenios de confidencialidad



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:

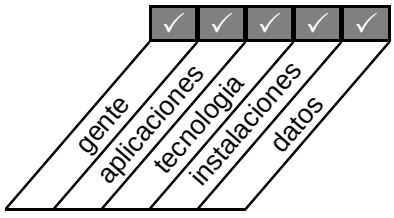
asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

se hace posible a través de:

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

y toma en consideración:

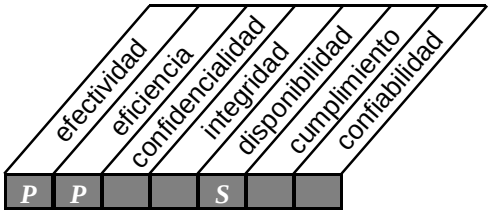
- acuerdos de servicio con terceras partes
- acuerdos de confidencialidad
- requerimientos legales regulatorios
- monitoreo de la entrega de servicio



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:

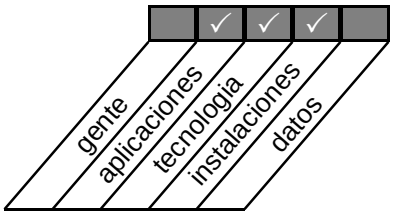
asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado

se hace posible a través de:

controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos

y toma en consideración:

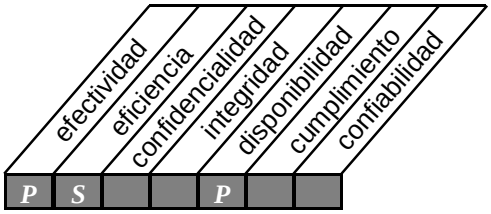
- requerimientos de disponibilidad y desempeño
- monitoreo y reporte
- herramientas de modelado
- administración de capacidad
- disponibilidad de recursos



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS4



Control sobre el proceso de TI de:

garantizar la seguridad de sistemas

que satisface los requerimientos de negocio de:

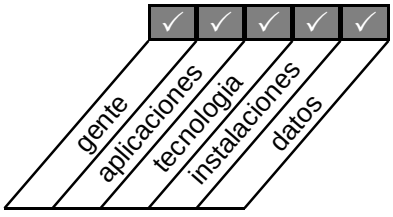
mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones

se hace posible a través de:

teniendo un plan de continuidad probado y funcional, que este alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio

y toma en consideración:

- clasificación de severidad
- plan documentado
- procedimientos alternativos
- respaldo y recuperación
- pruebas y entrenamiento sistemáticos y regulares

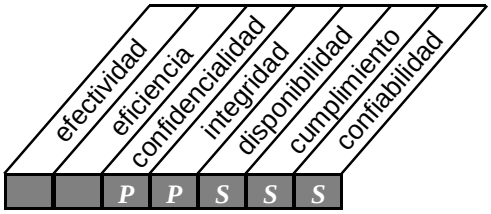


OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS5



Control sobre el proceso de TI de:

garantizar la seguridad de sistemas

que satisface los requerimientos de negocio de:

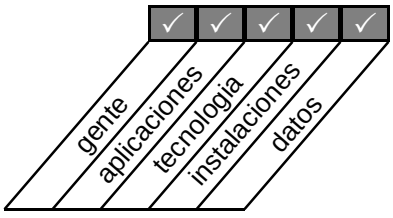
salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

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:

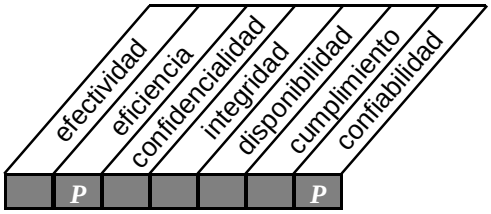
- autorización
- autenticación
- acceso
- perfiles e identificación de usuarios
- administración de llaves criptográficas
- manejo, reporte y seguimiento de incidentes
- Prevención y detección de virus
- *Firewalls*



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:

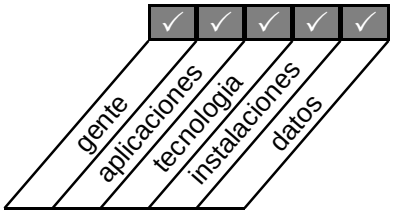
asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

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 toma en consideración:

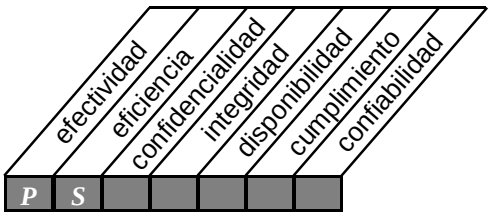
- recursos identificables y medibles
- procedimientos y políticas de cargo
- tarifas



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:

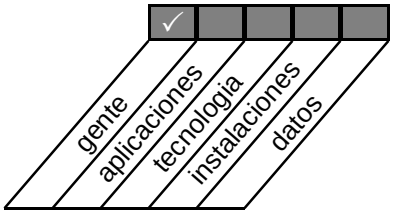
asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados

se hace posible a través de:

un plan completo de entrenamiento y desarrollo

y toma en consideración:

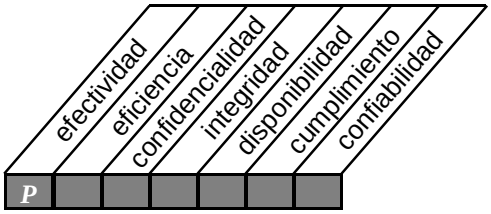
- curriculum de entrenamiento
- campañas de concientización
- técnicas de concientización



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:

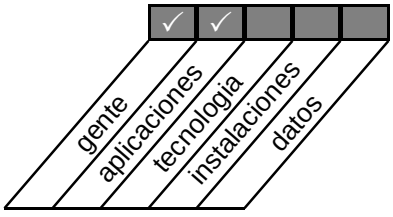
asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

se hace posible a través de:

un Buró de ayuda que proporcione soporte y asesoría de primera línea

y toma en consideración:

- consultas de usuarios y respuesta a problemas
- monitoreo de consultas y despacho
- análisis y reporte de tendencias

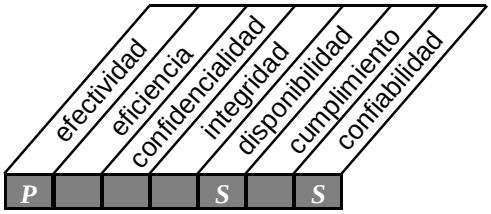


[18] **Buró de ayuda** (*help desk*)
[19] **Despacho** (*clearance*)

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:

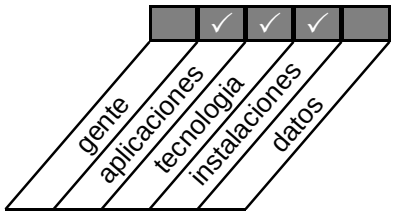
dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

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:

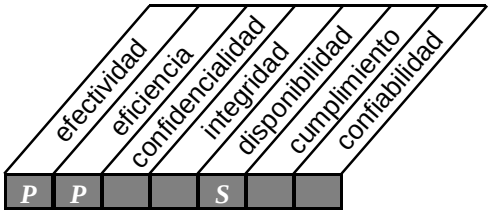
- registro de activos
- administración de cambios en la configuración
- chequeo de software no autorizado
- controles de almacenamiento de software



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:

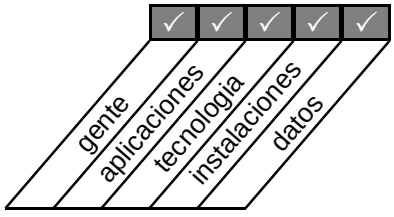
asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia

se hace posible a través de:

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

y toma en consideración:

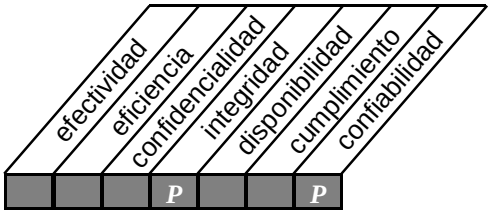
- suficientes pistas de auditoría de problemas y soluciones
- resolución oportuna de problemas reportados
- procedimientos de escalamiento
- reportes de incidentes



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:

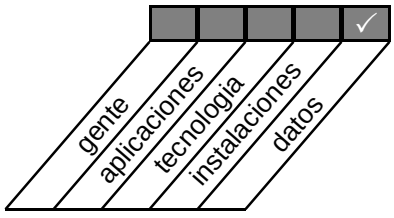
asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento

se hace posible a través de:

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

y toma en consideración:

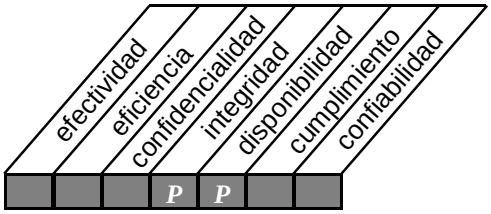
- diseño de formatos
- controles de documentos fuente
- controles de entrada
- controles de procesamiento
- controles de salida
- identificación, movimiento y administración de la librería de medios
- administración de almacenamiento y respaldo de medios
- autenticación e integridad



OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS12



Control sobre el proceso de TI de:

Administración de instalaciones

que satisface los requerimientos de negocio de:

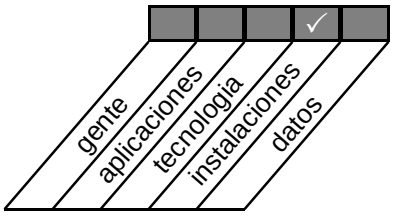
proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas

se hace posible a través de:

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

y toma en consideración:

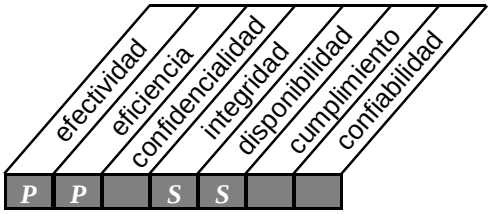
- acceso a instalaciones
- identificación del centro de cómputo
- seguridad física
- salud y seguridad del personal
- protección contra amenazas ambientales



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:

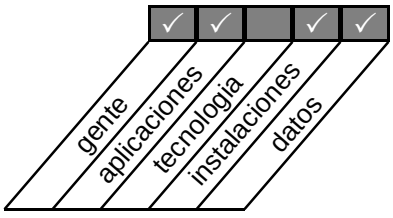
asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada

se hace posible a través de:

una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades

y toma en consideración:

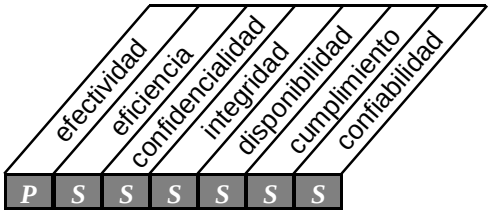
- manual de procedimiento de operaciones
- documentación de procedimientos de arranque
- administración de servicios de red
- calendarización de personal y cargas de trabajo
- proceso de cambio de turno
- registro de eventos de sistemas



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:

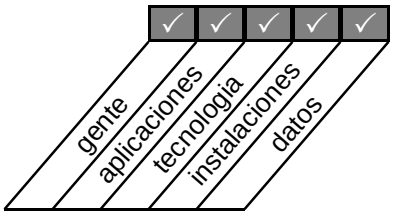
asegurar el logro de los objetivos establecidos para los procesos de TI

se hace posible a través de:

la definición por parte de la gerencia de reportes e indicadores de desempeño gerenciales, la implementación de sistemas de soporte así como la atención regular a los reportes emitidos

y toma en consideración:

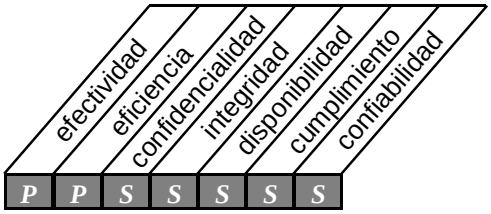
- indicadores clave de desempeño
- factores críticos de éxito
- evaluación de la satisfacción de clientes
- reportes gerenciales



OBJETIVOS DE CONTROL DE ALTO NIVEL

MONITOREO

M2



Control sobre el proceso de TI de:

Evaluar lo adecuado del control interno

que satisface los requerimientos de negocio de:

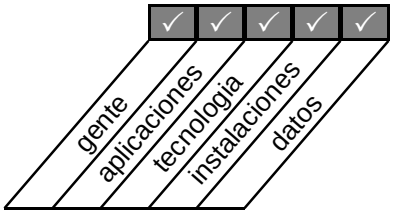
asegurar el logro de los objetivos de control interno establecidos para los procesos de TI

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:

- monitoreo permanente de control interno
- comparación con mejores prácticas
- reportes de errores y excepciones
- autoevaluaciones
- reportes gerenciales

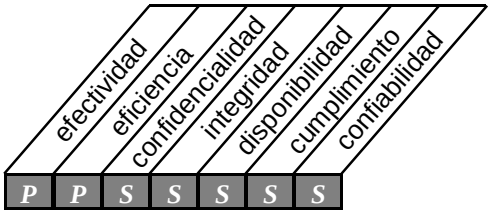


[20] **Comparación con mejores prácticas** (*benchmarks*)

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:

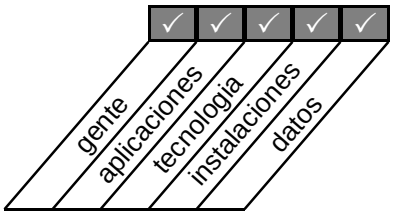
incrementar los niveles de confianza entre la organización, clientes y proveedores externos

se hace posible a través de:

revisiones de aseguramiento independientes llevadas al cabo en intervalos regulares

y toma en consideración:

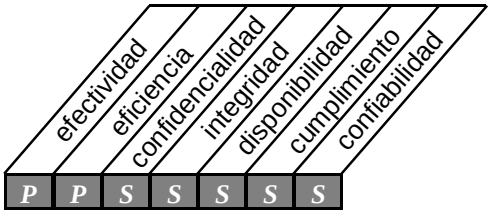
- certificaciones / acreditaciones independientes
- evaluaciones independientes de efectividad
- aseguramiento independiente sobre cumplimiento de requerimientos legales y regulatorios
- aseguramiento independiente de cumplimiento de compromisos contractuales
- revisiones a proveedores externos de servicios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

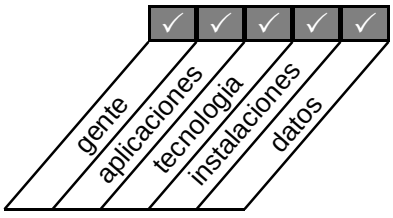
incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas

se hace posible a través de:

auditorías independientes desarrolladas en intervalos regulares

y toma en consideración:

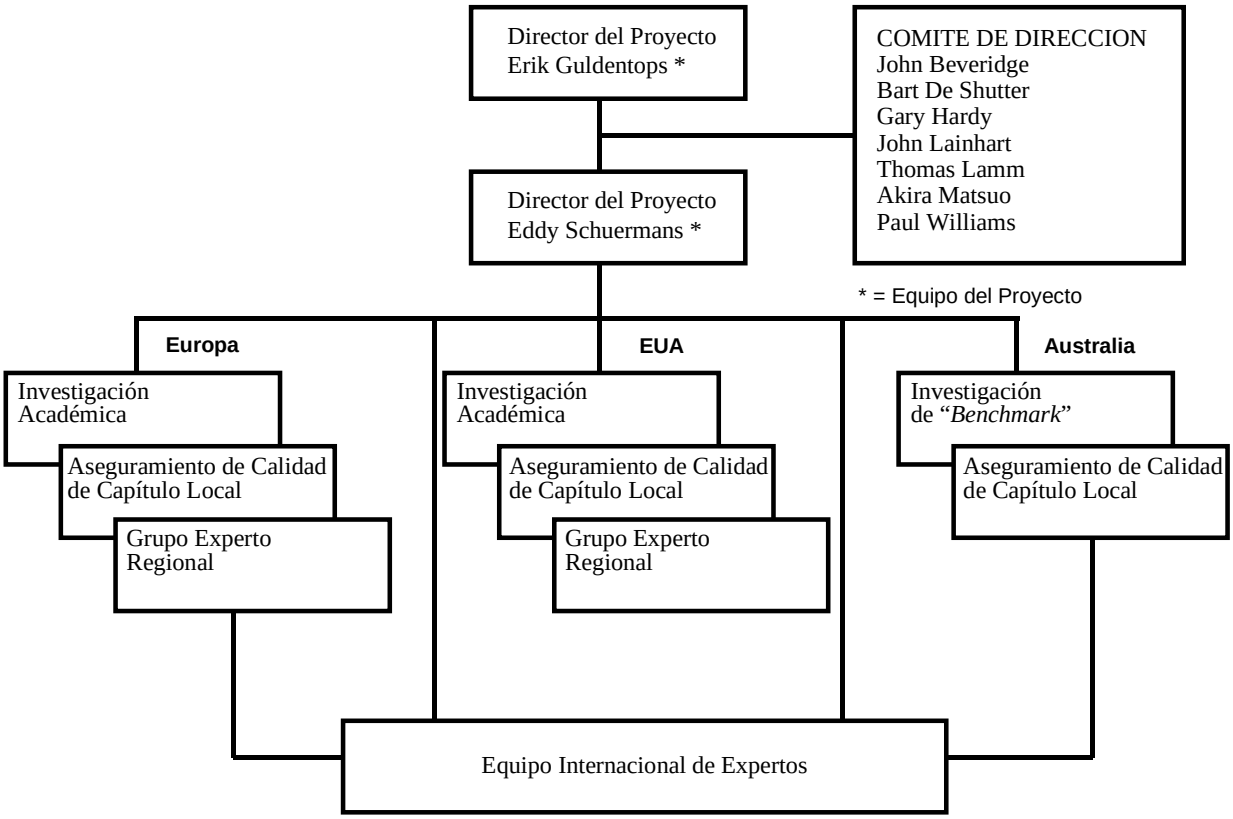
- independencia de auditoría
- involucramiento proactivo de auditoría
- ejecución de auditorías por parte de personal calificado
- aclaración de resultados y recomendaciones
- actividades de seguimiento



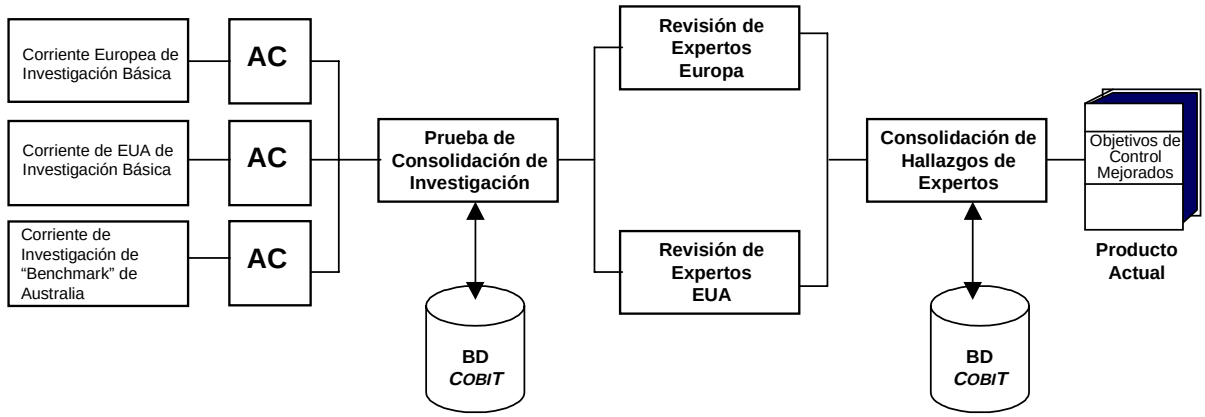
APÉNDICE I – DESCRIPCIÓN DEL PROYECTO COBIT

ORGANIZACION & RESPONSABILIDADES
El proyecto ha sido supervisado por un Comité de Dirección formado por representantes internacionales de la academia, industria, gobierno y la profesión de auditoría. La dirección global del proyecto fue proporcionada por el Consejo Directivo de ISACA. El Comité de Dirección de Proyectos intervino en el desarrollo del Marco Referencial ("Framework") *COBIT* y en la aplicación de los resultados de investigación.

Se establecieron grupos de trabajo internacionales con el propósito de asegurar la calidad y contar con una revisión experta de la investigación provisional y los elementos entregables del desarrollo del proyecto.



INVESTIGACION
La investigación 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 provistos de personal con representantes académicos y profesionales.
Después de la recolección y el análisis, los investigadores enfrentaron el reto de examinar cada campo, procesar con detenimiento y sugerir nuevos objetivos de control aplicables a cada proceso de tecnología de información particular. Se les atribuyó a los investigadores la responsabilidad de la compilación, revisión, evaluación e incorporación apropiadas de los estándares técnicos internacionales, códigos de conducta, estándares de calidad, estándares profesionales en las auditorías, prácticas y requerimientos industriales y requerimientos de industrias específicos, en cuanto a su relación con el marco de referencia y con objetivos de control individuales. Sus esfuerzos produjeron más de 300 objetivos de control nuevos y actualizados para poner a la consideración de los revisores de calidad y de los grupos expertos.

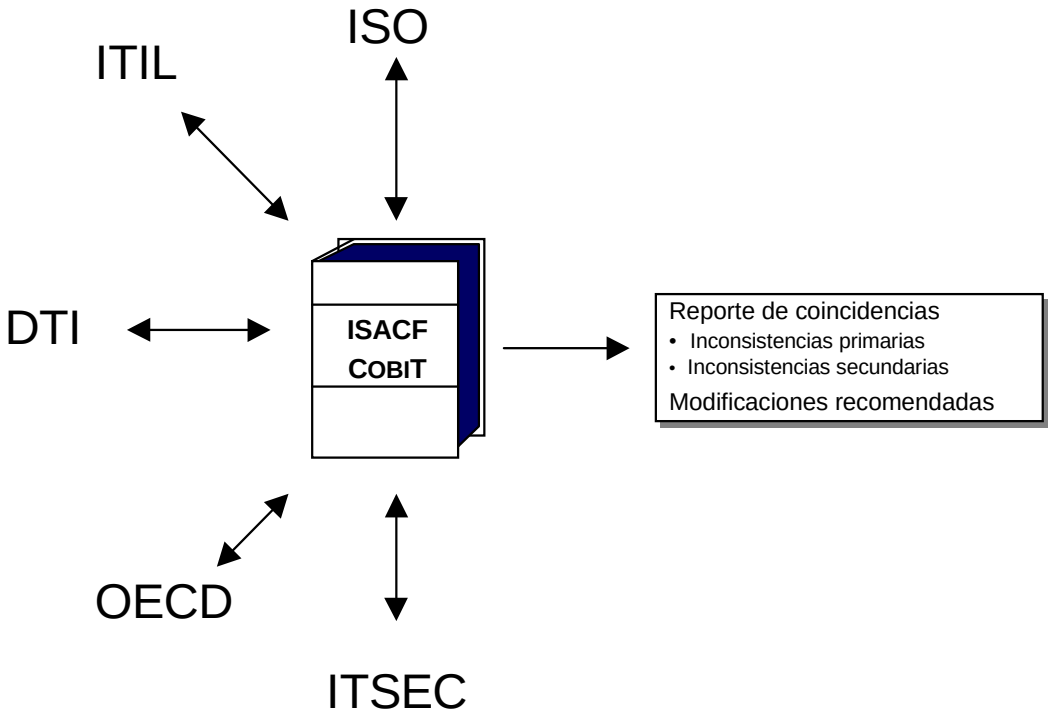


La consolidación de los resultados fue llevada a cabo primordialmente por el Equipo de Proyectos, compuesto por el Director de Proyectos, el Gerente de Proyectos y el Director de Investigaciones de ISACF.

ENFOQUE Y MATERIAL FUENTE

Siguiendo el desarrollo del marco referencial llevado a cabo por el Comité de Dirección, probado y actualizado por los Grupos Expertos, cada uno de los grupos de investigación llevó a cabo una comparación individual de los Objetivos de Control con cada uno de los documentos y estándares identificados. La intención no era llevar a cabo un análisis global de todo el material ni un "redesarrollo" de los Objetivos de Control desde el principio. Se trataba más bien de un proceso de comparación y actualización.

El resultado de esta investigación fue una lista de coincidencias primarias (en los Objetivos de Control, pero no en el material de comparación) y de coincidencias secundarias (en el material de comparación, pero no en los Objetivos de Control).



APENDICE II - 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.

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

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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.

APENDICE III - GLOSARIO DE TERMINOS ORIGINALES

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*)

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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 Control de TI Declaración del resultado deseado o propósito a ser alcanzado al implementar 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*)

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)