COBIT®

OBJETIVOS DE CONTROL

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.

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.

Traducido al español de COBIT 2da Edición: Objetivos de Control para la Información y Tecnologías afines por Gustavo A. Solís Montes, CISA con el permiso de la Information Systems Audit and Control Foundation (“ISACF”). Esta traducción no fue revisada por la ISACF, por lo tanto, no garantiza la fidelidad y/o exactitud de la misma. Si desea obtener mayor información sobre ISACF, visite su web site en www.isaca.org.

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

ISBN 0-9629440-5-X (Control Objectives, English)

RECONOCIMIENTOS

PRINCIPALES PATRIOCINADORES DE LA CORPORACIÓN A NIVEL MUNDRAL

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
Akira Matsuo
Teresa McCauley
Robert G. Parker
Daniel Ramos
Deepak Sarup
Lily Shue
Patrick Stachtchenko
Kevin Weston

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 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. Esta diseñado no solo para ser utilizado

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

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

por usuarios y auditores, sino que en forma más importante, esta diseñado para ser utilizado como una lista de verificación[3] detallada para los propietarios de los procesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y apoderamiento[4] de los dueños de procesos para que estos 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 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.

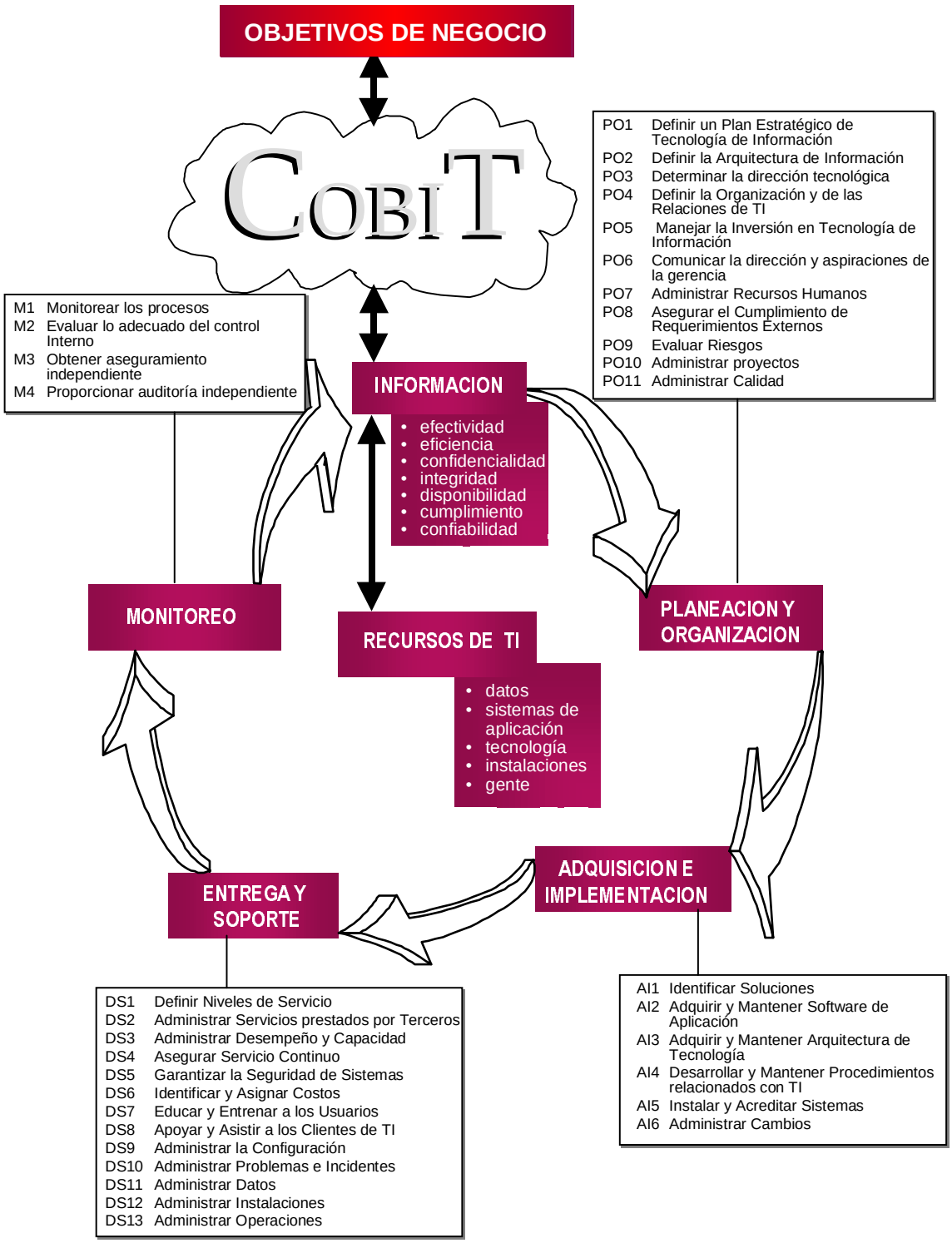
La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en TI para medir en forma comparativa[7] tanto su ambiente de TI existente, como su ambiente planeado.

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.

[3] **Lista de verificación** (*check list)*
[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] de TI -.**

COBIT se fundamenta en los Objetivos de Control existentes de la *Information Systems Audit and Control Foundation* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en **sistemas de información en toda la empresa.** El término **"generalmente 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 traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

Se determinó que las mejoras a los ***objetivos de control*** originales deberían 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, TickIT, 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 publicació 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);
- 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;

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

- ***Directrices de Auditoría,*** las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 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.

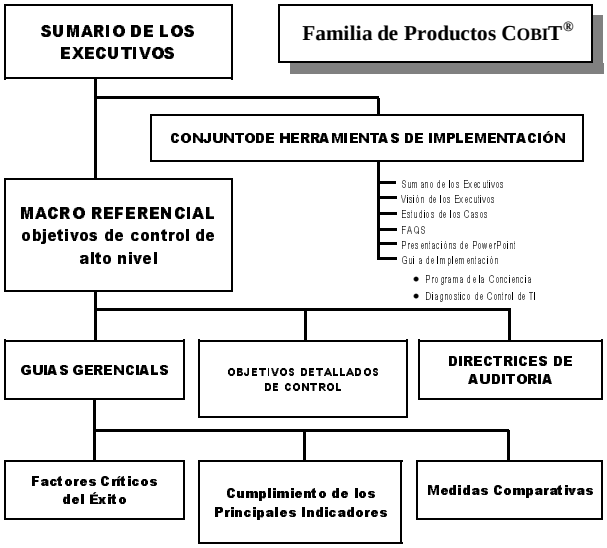
El Conjunto de Herramientas de Implementación incluye la *Síntesis Ejecutiva*, proporcionando a la alta gerencia conciencia y entendimiento de COBIT. También incluye una guía de implementación con dos útiles herramientas – Diagnóstico de la Conciencia de la Gerencia[9] y el Diagnóstico de Control de 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 cómo 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 una 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[11] que incluyen Factores Críticos de Exito, Indicadores Clave de Desempeño y Medidas Comparativas[12]. 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 acciones 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 posibles 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
- 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.

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 nego-

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

cios, 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 está 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

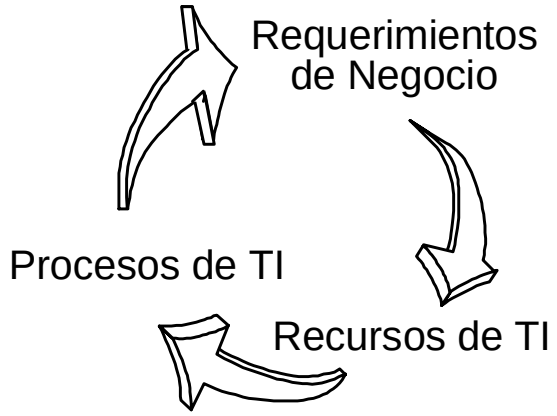
Objetivo de control en TI se define como

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 la 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 sólo 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

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

extrajeron siete categorías distintas, ciertamente superpuestas. 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.

Disponibildad 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.

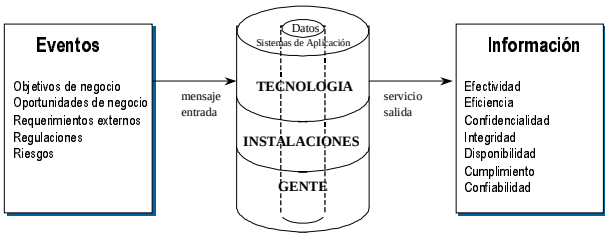
Instalaciones Recursos para alojar y dar soporte a los sistemas de información.

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.

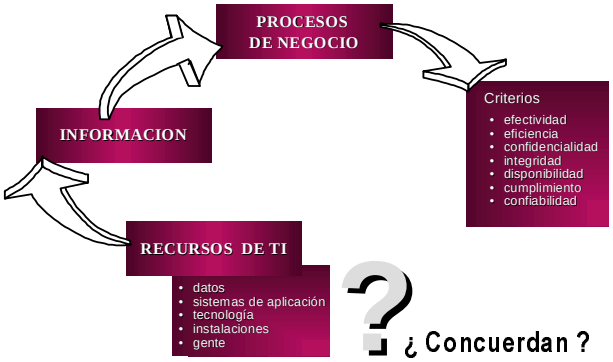
Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación:



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 con-

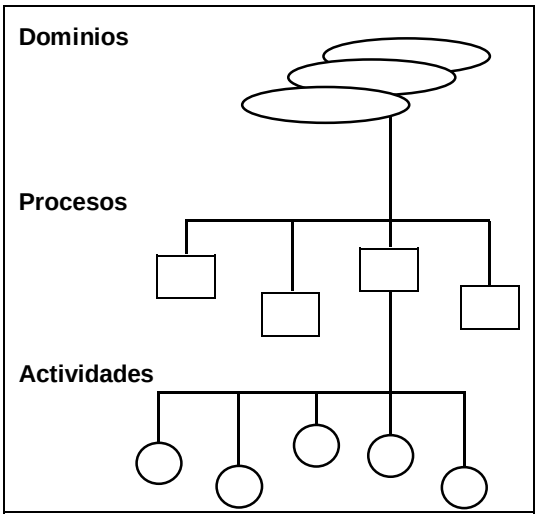
trol adecuadas para estos recursos.

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

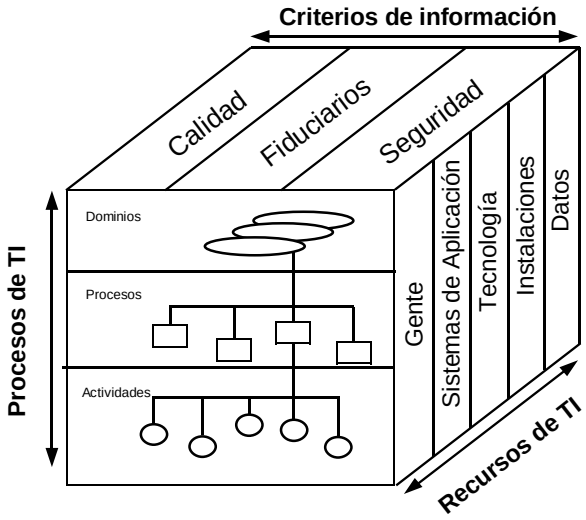


El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de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

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

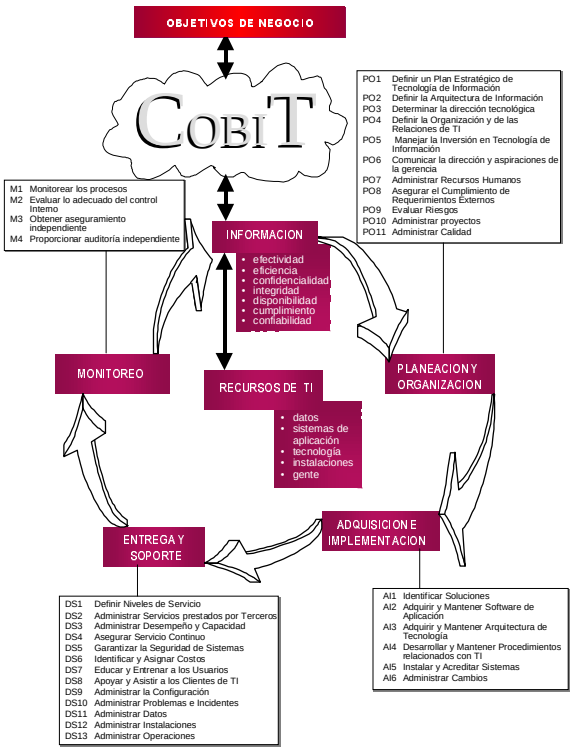
En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad.Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio incluye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

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

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.

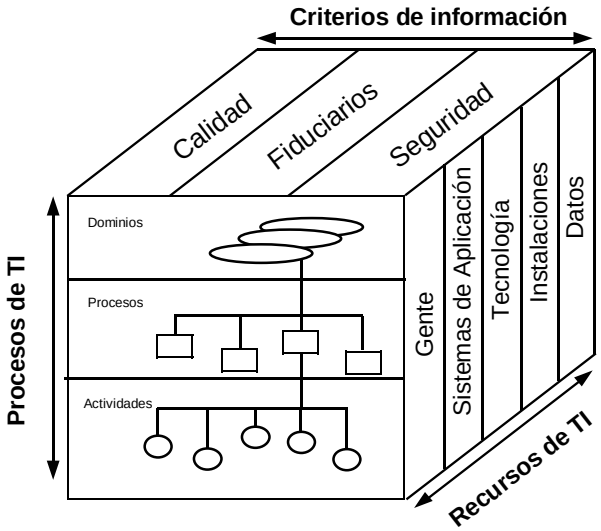
Similarmente, todas las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de COBIT indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración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

GÚIA 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.

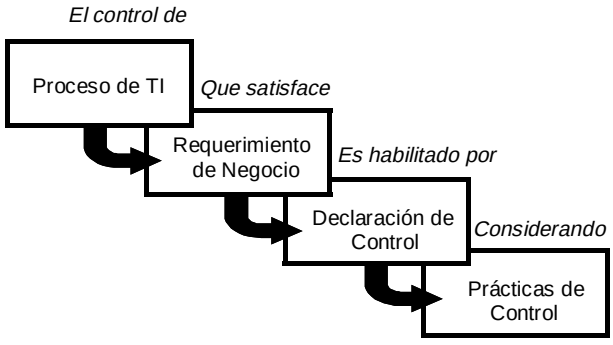


MARCO REFERENCIAL COBIT

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.

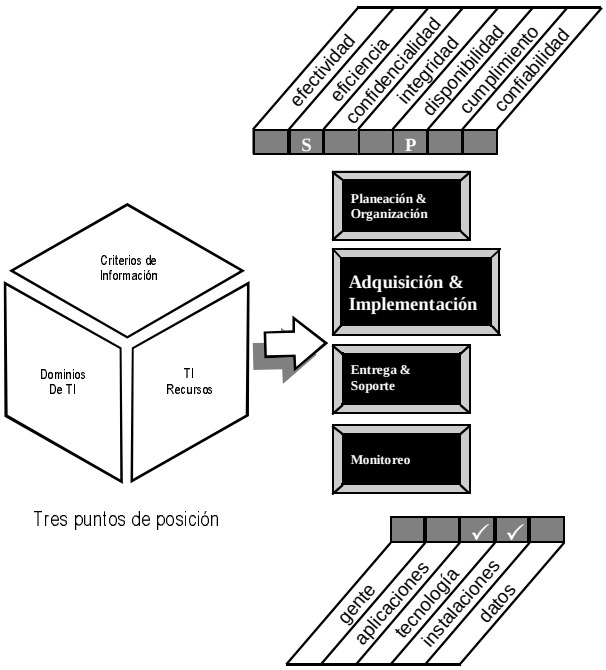
Los Objetivos de Control de TI han sido organizados por proceso/actividad, pero también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista estratégico como se explicó anteriormente, sino también para facilitar enfoques combinados o globales, 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.



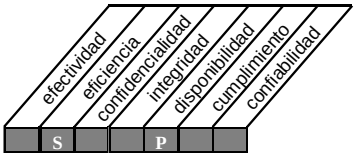
AYUDAS DE NAVEGACIÓN

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 -

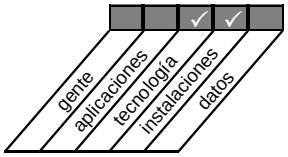


Los dominios son identificados ubicando la siguiente figura en la esquina superior derecha de cada página en la sección de Objetivos de Control, agrandando y haciendo más visible el dominio bajo revisión.

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 cuál criterio y en qué grado (primario o secundario) es aplicable a cada Objetivo de Control de TI de alto nivel.



Una segunda "mini" matriz en la esquina inferior derecha 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).



PRINCIPIOS DE LOS OBJETIVOS DE CONTROL

COBIT, como se presenta en la última versión de "Objetivos de Control", refleja el compromiso continuo de ISACF por mejorar y mantener el cuerpo común de conocimientos requeridos para apoyar la actividad de auditoría y control de sistemas de información. Así como el Marco de Referencia de COBIT (COBIT *Framework*) se encuentra enfocado a **controles de alto nivel** para cada proceso. El documento de Objetivos de Control se concentra en **objetivos detallados de control** específicos, asociados con cada uno de los procesos de TI. Para cada uno de los 34 procesos de TI del Marco de Referencia, existen de tres a 30 Objetivos de Control detallados. Los Objetivos de Control alinean el Marco de Referencia general con los Objetivos de Control detallados a partir de 36 fuentes primarias que comprenden los estándares internacionales de hecho y de derecho y las regulaciones relacionadas con TI. Este contiene la relación de los resultados o propósitos deseados que desean alcanzarse a través de la implementación de procedimientos de control específicos dentro de una actividad de TI y, de esta manera, proporciona una política clara y una "mejor práctica[16]" para el control de TI en toda la industria, a nivel mundial.

Los Objetivos de Control están dirigidos a la gerencia y al personal de los servicios de información, controles, funciones de auditoría y, lo más importante, a los propietarios de los procesos de negocios. Los Objetivos de Control proporcionan un documento de trabajo de escritorio para estas personas. Se presentan definiciones precisas y claras de un conjunto mínimo de controles para asegurar la eficacia, la eficiencia y la economía en la utilización de recursos. Para cada proceso, se identifican Objetivos de Control detallados como los controles mínimos que necesitan encontrarse establecidos - aquellos controles que cuya suficiencia será evaluada por el profesional en control. Existen 302 objetivos de control detallados que proporcionan una visión detallada sobre las relaciones dominio/proceso/objetivo de control.

Los Objetivos de Control permiten la traducción de los conceptos presentados en el Marco de Referencia en controles específicos aplicables para cada proceso de TI.

[16] **Mejor práctia** (*best practice*)

TABLA RESUMEN

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

DOMINIO		PROCESO	Criterios de Información							Recursos de TI				
			efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	recursos	sistemas de aplicacion	tecnologia	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	☑	☑	☑	☑	☑

RELACIONES DE OBJETIVOS DE CONTROL
DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

PLANEACIÓN Y ORGANIZACIÓN

1.0 Definición de un Plan Estratégico de Tecnología de Información
- 1.1 Tecnología de Información como parte del Plan de la Organización a corto y largo plazo
- 1.2 Plan a largo plazo de Tecnología de Información
- 1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura
- 1.4 Cambios al Plan a largo plazo de Tecnología de Información
- 1.5 Planeación a corto plazo para la función de Servicios de Información
- 1.6 Evaluación de sistemas existentes

2.0 Definición de la Arquitectura de Información
- 2.1 Modelo de la Arquitectura de Información
- 2.2 Diccionario de Datos y Reglas de sinta de datos de la corporación
- 2.3 Esquema de Clasificación de Datos
- 2.4 Niveles de Seguridad

3.0 Determinación de la dirección tecnológica
- 3.1 Planeación de la Infraestructura Tecnológica
- 3.2 Monitoreo de Tendencias y Regulaciones Futuras
- 3.3 Contingencias en la Infraestructura Tecnológica
- 3.4 Planes de Adquisición de Hardware y Software
- 3.5 Estándares de Tecnología

4.0 Definición de la Organización y de las Relaciones de TI
- 4.1 Comité de planeación o dirección de la función de servicios de información
- 4.2 Ubicación de los servicios de información en la organización
- 4.3 Revisión de Logros Organizacionales
- 4.4 Funciones y Responsabilidades
- 4.5 Responsabilidad del aseguramiento de calidad
- 4.6 Responsabilidad de la seguridad lógica y física
- 4.7 Propiedad y Custodia
- 4.8 Propiedad de Datos y Sistemas
- 4.9 Supervisión
- 4.10 Segregación de Funciones
- 4.11 Asignación de Personal para Tecnología de Información
- 4.12 Descripción de Puestos para el Personal de la Función de TI
- 4.13 Personal clave de TI
- 4.14 Procedimientos para personal por contrato
- 4.15 Relaciones

5.0 Manejo de la Inversión en Tecnología de Información
- 5.1 Presupuesto Operativo Anual para la Función de Servicio de información
- 5.2 Monitoreo de Costo - Beneficio
- 5.3 Justificación de Costo - Beneficio

6.0 Comunicación de la dirección y aspiraciones de la gerencia
- 6.1 Ambiente positivo de control de la información
- 6.2 Responsabilidad de la Gerencia en cuanto a Políticas
- 6.3 Comunicación de las Políticas de la Organización
- 6.4 Recursos para la implementación de Políticas
- 6.5 Mantenimiento de Políticas
- 6.6 Cumplimiento de Políticas, Procedimientos y Estándares
- 6.7 Compromiso con la Calidad
- 6.8 Política sobre el Marco de Referencia para la Seguridad y el Control Interno
- 6.9 Derechos de propiedad intelectual
- 6.10 Políticas Específicas
- 6.11 Comunicación de Conciencia de Seguridad en TI

7.0 Administración de Recursos Humanos
- 7.1 Reclutamiento y Promoción de Personal
- 7.2 Personal Calificado
- 7.3 Entrenamiento de Personal
- 7.4 Entrenamiento Cruzado o Respaldo de Personal

- 7.5 Procedimientos de Acreditación[17] de Personal
- 7.6 Evaluación de Desempeño de los Empleados
- 7.7 Cambios de Puesto y Despidos

8.0 Aseguramiento del Cumplimiento de Requerimientos Externos

- 8.1 Revisión de Requerimientos Externos
- 8.2 Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos
- 8.3 Cumplimiento de los Estándares de Seguridad y Ergonomía
- 8.4 Privacidad, Propiedad Intelectual y Flujo de Datos
- 8.5 Comercio Electrónico
- 8.6 Cumplimiento con Contratos de Seguros

9.0 Evaluación de Riesgos

- 9.1 Evaluación de Riesgos del Negocio
- 9.2 Enfoque de Evaluación de Riesgos
- 9.3 Identificación de Riesgos
- 9.4 Medición de Riesgos
- 9.5 Plan de Acción contra Riesgos
- 9.6 Aceptación de Riesgos

10.0 Administración de proyectos

- 10.1 Marco de Referencia para la Administración de Proyectos
- 10.2 Participación del Departamento Usuario en la Iniciación de Proyectos
- 10.3 Miembros y Responsabilidades del Equipo del Proyecto
- 10.4 Definición del Proyecto
- 10.5 Aprobación del Proyecto
- 10.6 Aprobación de las Fases del Proyecto
- 10.7 Plan Maestro del Proyecto
- 10.8 Plan de Aseguramiento de la Calidad de Sistemas
- 10.9 Planeación de Métodos de Aseguramiento
- 10.10 Administración Formal de Riesgos de Proyectos
- 10.11 Plan de Prueba
- 10.12 Plan de Entrenamiento
- 10.13 Plan de Revisión Post Implementación

11.0 Administración de Calidad

- 11.1 Plan General de Calidad
- 11.2 Enfoque de Aseguramiento de Calidad
- 11.3 Planeación del Aseguramiento de Calidad
- 11.4 Revisión de Aseguramiento de Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información
- 11.5 Metodología del Ciclo de Vida de Desarrollo de Sistemas
- 11.6 Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual
- 11.7 Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas
- 11.8 Coordinación y Comunicación
- 11.9 Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología
- 11.10 Relaciones con Terceras Partes como Implementadores
- 11.11 Estándares para la Documentación de Programas
- 11.12 Estándares para Pruebas de Programas
- 11.13 Estándares para Pruebas de Sistemas
- 11.14 Pruebas Piloto/En Paralelo
- 11.15 Documentación de las Pruebas del Sistema
- 11.16 Evaluación del Aseguramiento de la Cali dad sobre el Cumplimiento de Estándar de Desarrollo
- 11.17 Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información
- 11.18 Métricas de Calidad
- 11.19 Reportes de Revisiones de Aseguramiento de la Calidad

ADQUISICIÓN E IMPLEMENTACIÓN

1.0 Identificación de Soluciones

- 1.1 Definición de Requerimientos de Información
- 1.2 Formulación de Acciones Alternativas
- 1.3 Formulación de Estrategias de Adquisición.
- 1.4 Requerimientos de Servicios de Terceros
- 1.5 Estudio de Factibilidad Tecnológica
- 1.6 Estudio de Factibilidad Económica
- 1.7 Arquitectura de Información
- 1.8 Reporte de Análisis de Riesgos
- 1.9 Controles de Seguridad Económicos
- 1.10 Diseño de Pistas de Auditoría
- 1.11 Ergonomía
- 1.12 Selección de Software de Sistema

[17] **Acreditación** (*clearance*)

- 1.13 Control de Abastecimiento
- 1.14 Adquisición de Productos de Software
- 1.15 Mantenimiento de Software de Terceras Partes
- 1.16 Contratos de Programación de Aplicaciones
- 1.17 Aceptación de Instalaciones
- 1.18 Aceptación de Tecnología

2.0 Adquisición y Mantenimiento de Software de Aplicación
- 2.1 Métodos de Diseño
- 2.2 Cambios Significativos a Sistemas Actuales
- 2.3 Aprobación del Diseño
- 2.4 Definición y Documentación de Requerimientos de Archivos
- 2.5 Especificaciones de Programas
- 2.6 Diseño para la Recopilación de Datos Fuente
- 2.7 Definición y Documentación de Requerimientos de Entrada de Datos
- 2.8 Definición de Interfases
- 2.9 Interfases Usuario-Máquina
- 2.10 Definición y Documentación de Requerimientos de Procesamiento
- 2.11 Definición y Documentación de Requerimientos de Salida de Datos
- 2.12 Controlabilidad
- 2.13 Disponibilidad como Factor Clave de Diseño
- 2.14 Estipulación de Integridad de TI en programas de software de aplicaciones
- 2.15 Pruebas de Software de Aplicación
- 2.16 Materiales de Consulta y Soporte para Usuario
- 2.17 Reevaluación del Diseño del Sistema

3.0 Adquisición y Mantenimiento de Arquitectura de Tecnología
- 3.1 Evaluación de Nuevo Hardware y Software
- 3.2 Mantenimiento Preventivo para Hardware
- 3.3 Seguridad del Software del Sistema
- 3.4 Instalación del Software del Sistema
- 3.5 Mantenimiento del Software del Sistema
- 3.6 Controles para Cambios del Sofware del Sistema

4.0 Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información
- 4.1 Futuros Requerimientos y Niveles de Servicios Operacionales
- 4.2 Manual de Procedimientos para Usuario
- 4.3 Manual de Operación
- 4.4 Material de Entrenamiento

5.0 Instalación y Acreditación de Sistemas
- 5.1 Entrenamiento
- 5.2 Adecuación del Desempeño del Software de Aplicación
- 5.3 Conversión
- 5.4 Pruebas de Cambios
- 5.5 Criterios y Desempeño de Pruebas en Paralelo/Piloto
- 5.6 Prueba de Aceptación Final
- 5.7 Pruebas y Acreditación de Seguridad
- 5.8 Prueba Operacional
- 5.9 Promoción a Producción
- 5.10 Evaluación de la Satisfacción de los Requerimientos del Usuario
- 5.11 Revisión Gerencial Post - Implementación

6.0 Administración de Cambios
- 6.1 Inicio y Control de Requisiciones de Cambio
- 6.2 Evaluación del Impacto
- 6.3 Control de Cambios
- 6.4 Documentación y Procedimientos
- 6.5 Mantenimiento Autorizado
- 6.6 Política de Liberación de Software
- 6.7 Distribución de Software

ENTREGA DE SERVICIOS Y SOPORTE

1.0 Definición de Niveles de Servicio
- 1.1 Marco de Referencia para el Convenio de Nivel de Servicio
- 1.2 Aspectos sobre los Acuerdos de Nivel de Servicio
- 1.3 Procedimientos de Ejecución
- 1.4 Monitoreo y Reporte
- 1.5 Revisión de Convenios y Contratos de Nivel de Servicio
- 1.6 Elementos sujetos a Cargo
- 1.7 Programa de Mejoramiento del Servicio

2.0 Administración de Servicios prestados por Terceros
- 2.1 Interfases con Proveedores
- 2.2 Relaciones de Dueños
- 2.3 Contratos con Terceros
- 2.4 Calificaciones de terceros
- 2.5 Contratos con *Outsourcing*
- 2.6 Continuidad de Servicios

- 2.7 Relaciones de Seguridad
- 2.8 Monitoreo

3.0 Administración de Desempeño y Capacidad
- 3.1 Requerimientos de Disponibilidad y Desempeño
- 3.2 Plan de Disponibilidad
- 3.3 Monitoreo y Reporte
- 3.4 Herramientas de Modelado
- 3.5 Manejo de Desempeño Proactivo
- 3.6 Pronóstico de Carga de Trabajo
- 3.7 Administración de Capacidad de Recursos
- 3.8 Disponibilidad de Recursos
- 3.9 Calendarización de recursos

4.0 Aseguramiento de Servicio Continuo
- 4.1 Marco de Referencia de Continuidad de Tecnología de Información
- 4.2 Estrategia y Filosofía de Continuidad de Tecnología de Información
- 4.3 Contenido del Plan de Continuidad de Tecnología de Información
- 4.4 Minimización de requerimientos de Continuidad de Tecnología de Información
- 4.5 Mantenimiento del Plan de Continuidad de Tecnología de Información
- 4.6 Pruebas del Plan de Continuidad de Tecnología de Información
- 4.7 Capacitación sobre el Plan de Continuidad de Tecnología de Información
- 4.8 Distribución del Plan de Continuidad de Tecnología de Información
- 4.9 Procedimientos de Respaldo de Procesamiento para Departamentos Usuarios
- 4.10 Recursos críticos de Tecnología de Información
- 4.11 Centro de Cómputo y Hardware de respaldo
- 4.12 Procedimientos de Refinamiento del Plan de Continuidad de TI[18]

5.0 Garantizar la Seguridad de Sistemas
- 5.1 Administrar Medidas de Seguridad
- 5.2 Identificación, Autenticación y Acceso
- 5.3 Seguridad de Acceso a Datos en Línea
- 5.4 Administración de Cuentas de Usuario
- 5.5 Revisión Gerencial de Cuentas de Usuario
- 5.6 Control de Usuarios sobre Cuentas de Usuario
- 5.7 Vigilancia de Seguridad
- 5.8 Clasificación de Datos
- 5.9 Administración Centralizada de Identificación y Derechos de Acceso
- 5.10 Reportes de Violación y de Actividades de Seguridad
- 5.11 Manejo de Incidentes
- 5.12 Re-acreditación
- 5.13 Confianza en Contrapartes
- 5.14 Autorización de Transacciones
- 5.15 No Rechazo
- 5.16 Sendero Seguro
- 5.17 Protección de funciones de seguridad
- 5.18 Administración de Llave Criptográfica
- 5.19 Prevención, Detección y Corrección de Software "Malicioso"
- 5.20 Arquitecturas de *FireWalls* y conexión a redes públicas
- 5.21 Protección de Valores Electrónicos

6.0 Identificación y Asignación de Costos
- 6.1 Elementos Sujetos a Cargo
- 6.2 Procedimientos de Costeo
- 6.3 Procedimientos de Cargo y Facturación a Usuarios

7.0 Educación y Entrenamiento de Usuarios
- 7.1 Identificación de Necesidades de Entrenamiento
- 7.2 Organización de Entrenamiento
- 7.3 Entrenamiento sobre Principios y Conciencia de Seguridad

8.0 Apoyo y Asistencia a los Clientes de Tecnología de Información
- 8.1 Buró de Ayuda
- 8.2 Registro de Preguntas del Usuario
- 8.3 Escalamiento de Preguntas del Cliente
- 8.4 Monitoreo de Atención a Clientes
- 8.5 Análisis y Reporte de Tendencias

9.0 Administración de la Configuración
- 9.1 Registro de la Configuración
- 9.2 Base de la Configuración
- 9.3 Registro de Estatus
- 9.4 Control de la Configuración
- 9.5 Software no Autorizado
- 9.6 Almacenamiento de Software

[18] **Refinamiento del Plan de Continuidad de TI** (*wrap up*): procedimiento seguido para evaluar y actualizar el Plan

10.0 Administración de Problemas e Incidentes
- 10.1 Sistema de Administración de Problemas
- 10.2 Escalamiento de Problemas
- 10.3 Seguimiento de Problemas y Pistas de Auditoría

11.0 Administración de Datos
- 11.1 Procedimientos de Preparación de Datos
- 11.2 Procedimientos de Autorización de Documentos Fuente
- 11.3 Recopilación de Datos de Documentos Fuente
- 11.4 Manejo de Errores de Documentos Fuente
- 11.5 Retención de Documentos Fuente
- 11.6 Procedimientos de Autorización de Entrada de Datos
- 11.7 Chequeos de Exactitud, Suficiencia y Autorización
- 11.8 Manejo de Errores en la Entrada de Datos
- 11.9 Integridad de Procesamiento de Datos
- 11.10 Validación y Edición de Procesamiento de Datos
- 11.11 Manejo de Error en el Procesamiento de Datos
- 11.12 Manejo y Retención de Salida de Datos
- 11.13 Distribución de Salida de Datos
- 11.14 Balanceo y Conciliación de Datos de Salida
- 11.15 Revisión de Salida de Datos y Manejo de Errores
- 11.16 Provisiones de Seguridad para Reportes de Salida
- 11.17 Protección de Información Sensible durante transmisión y transporte
- 11.18 Protección de Información Crítica a ser Desechada
- 11.19 Administración de Almacenamiento
- 11.20 Períodos de Retención y Términos de Almacenamiento
- 11.21 Sistema de Administración de la Librería de Medios
- 11.22 Responsabilidades de la Administración de la Librería de Medios
- 11.23 Respaldo y Restauración
- 11.24 Funciones de Respaldo
- 11.25 Almacenamiento de Respaldo
- 11.26 Archivo
- 11.27 Protección de Mensajes Sensitivos
- 11.28 Autenticación e Integridad
- 11.29 Integridad de Transacciones Electrónicas
- 11.30 Integridad Continua de Datos Almacenados

12.0 Administración de Instalaciones
- 12.1 Seguridad Física
- 12.2 Discreción de las Instalaciones de Tecnología de Información
- 12.3 Escolta de Visitantes
- 12.4 Salud y Seguridad del Personal
- 12.5 Protección contra Factores Ambientales
- 12.6 Suministro Ininterrumpido de Energía

13.0 Administración de Operaciones
- 13.1 Manual de procedimientos de Operación e Instrucciones
- 13.2 Documentación del Proceso de Inicio y de Otras Operaciones
- 13.3 Calendarización de Trabajos
- 13.4 Salidas de la Calendarización de Trabajos Estándar
- 13.5 Continuidad de Procesamiento
- 13.6 Bitácoras de Operación
- 13.7 Operaciones Remotas

MONITOREO

1.0 Monitoreo del Proceso
- 1.1 Recolección de Datos de Monitoreo
- 1.2 Evaluación de Desempeño
- 1.3 Evaluación de la Satisfacción de Clientes
- 1.4 Reportes Gerenciales

2.0 Evaluar lo adecuado del Control Interno
- 2.1 Monitoreo de Control Interno
- 2.2 Operación oportuna del Control Interno
- 2.3 Reporte sobre el Nivel de Control Interno
- 2.4 Seguridad de operación y aseguramiento de Control Interno

3.0 Obtención de Aseguramiento Independiente
- 3.1 Certificación / Acreditación Independiente de Control y Seguridad de los servicios de TI
- 3.2 Certificación / Acreditación Independiente de Control y Seguridad de proveedores externos de servicios
- 3.3 Evaluación Independiente de la Efectividad de los Servicios de TI
- 3.4 Evaluación Independiente de la Efectividad de proveedores externos de servicios
- 3.5 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales
- 3.6 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulato-

rios y compromisos contractuales de proveedores externos de servicios
3.7 Competencia de la Función de Aseguramiento Independiente
3.8 Participación Proactiva de Auditoría

4.0 Proveer Auditoría Independiente
4.1 Estatutos de Auditoría
4.2 Independencia
4.3 Etica y Estándares Profesionales
4.4 Competencia
4.5 Planeación
4.6 Desempeño del Trabajo de Auditoría
4.7 Reporte
4.8 Actividades de Seguimiento

LOS OBJETIVOS DE CONTROL

En las páginas siguientes se individualizan objetivos de control detallados para cada uno de los 34 procesos dentro de una función de Tecnología de Información.

En la página de la izquierda se encuentra el Objetivo de Control de alto nivel duplicado del ***Marco de Referencia*** *para asegurar consistencia en todos los productos* COBIT *y para facilitar el entendimiento.*

El indicador de Dominio ("PO" para Planeación y Organización, "AI" para Adquisición e Implementación, "DS" para Entrega y Soporte y "M" para Monitoreo) se muestra en la esquina superior derecha. El proceso es entonces descrito. También se muestran los indicadores de importancia primaria y secundaria. Adicionalmente, se lista la información descriptiva del Marco de Referencia. Y los recursos de TI gastados son mostrados vía un diagrama.

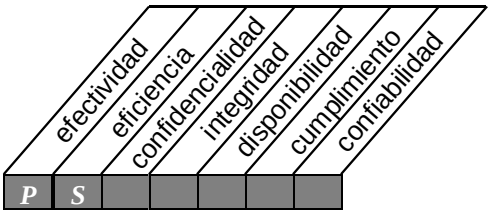
En la página de la derecha y en algunas ocasiones llevados hasta las siguientes páginas, se encuentran los objetivos de control detallados para cada proceso. Se muestra una descripción de dicho objetivo de control detallado. Para mantener el formato de lados izquierdo y derecho se requieren algunas páginas en blanco.

Se desarrollan objetivos de control detallados para cada uno de los 34 procesos.

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:

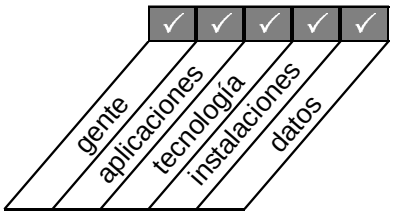
Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.

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[21]
- cambios organizacionales
- estudios de factibilidad oportunos
- evaluación de sistemas existentes



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

1. DEFINICIÓN DE UN PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN

1.1 Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.

OBJETIVO DE CONTROL

La alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas de la organización. A este respecto, la alta gerencia deberá asegurar que los problemas de tecnología de información, así como las oportunidades, sean evaluados adecuadamente y reflejados en los planes a largo y corto plazo de la organización.

1.2 Plan a largo plazo de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información será responsable de desarrollar regularmente planes a largo plazo de tecnología de información que apoyen el logro de la misión y las metas generales de la organización.

De la misma manera, la Gerencia deberá implementar un proceso de planeación a largo plazo, adoptar un enfoque estructurado y determinar la estructura para el plan.

1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá establecer y aplicar un enfoque estructurado al proceso de planeación a largo plazo. Esto deberá traer como resultado un plan de alta calidad que cubra las preguntas básicas de qué, quién y cuándo. Los aspectos que necesitan ser tomados en cuenta y ser cubiertos adecuadamente durante el proceso de planeación son el modelo de organización y sus cambios, la distribución geográfica, la evolución tecnológica, los costos, los requerimientos legales y regulatorios, requerimientos de terceras partes o del mercado, el horizonte de planeación, reingeniería de procesos del negocio, la asignación de personal, la designación de fuentes internas o externas, etc. El plan mismo deberá hacer referencia a otros planes tales como el plan de calidad de la organización y el plan de manejo de riesgos de información.

1.4 Cambios al Plan a largo plazo de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la tecnología de información.

1.5 Planeación a corto plazo para la Función de Servicios de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que el plan a largo plazo de tecnología de información sea traducido regularmente en planes a corto plazo de tecnología de información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de tecnología de información con una base consistente con el plan a largo plazo de tecnología de información. Los planes a corto plazo deberán ser reevaluados y modificados periódicamente según se considere necesario respondiendo a las condiciones de cambios en el negocio y en la tecnología de información. La realización oportuna de estudios de factibilidad deberá asegurar que la ejecución de los planes a corto plazo sea iniciada adecuadamente.

1.6 Evaluación de Sistemas Existentes

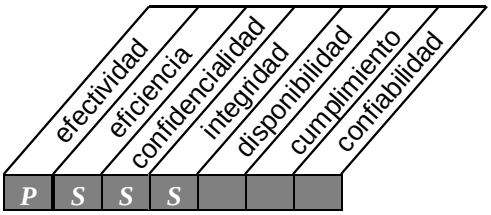
OBJETIVO DE CONTROL

En forma previa al desarrollo o modificación del Plan Estratégico de TI, la Gerencia de servicios de información debe evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

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:

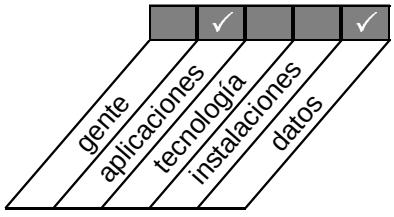
organizar de la mejor manera los sistemas de información

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[22]



[22] **Severidad** (criticality)

2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN

2.1 Modelo de la Arquitectura de Información

OBJETIVO DE CONTROL

La información deberá conservar consistencia con las necesidades y deberá ser identificada, capturada y comunicada en una forma y dentro de períodos de tiempo que permitan a los responsables llevar a cabo sus tareas eficiente y oportunamente. Asimismo, la función de sistemas de información deberá crear y actualizar regularmente un modelo de arquitectura de información, abarcando el modelo de datos corporativo y los sistemas de información asociados. El modelo de arquitectura de información deberá conservar consistencia con el plan a largo plazo de tecnología de información.

2.2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación

OBJETIVO DE CONTROL

La función de servicios de información deberá asegurar la creación y la continua actualización de un diccionario de datos corporativo que incorpore las reglas de sintaxis de datos de la organización.

2.3 Esquema de Clasificación de Datos

OBJETIVO DE CONTROL

Deberá establecerse un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información (por ejemplo, categorías de seguridad), así como a la asignación de propiedad. Las reglas de acceso para las clases deberán definirse apropiadamente.

2.4 Niveles de Seguridad

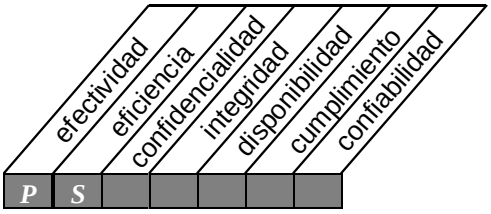
OBJETIVO DE CONTROL

La Gerencia deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de control apropiado (mínimo) para cada una de las clasificaciones.

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:

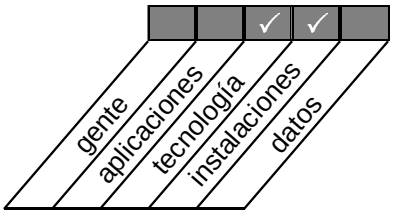
aprovechar la tecnología disponible o tecnología emergente

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



3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA

3.1 Planeación de la Infraestructura Tecnológica

OBJETIVO DE CONTROL

La función de servicios de información deberá crear y actualizar regularmente un plan de infraestructura tecnológica que concuerde con los planes a largo y corto plazo de tecnología de información. Dicho plan deberá abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

3.2 Monitoreo de Tendencias y Regulaciones Futuras

OBJETIVO DE CONTROL

La función de servicios de información deberá asegurar el continuo monitoreo de tendencias futuras y condiciones regulatorias, de tal manera que estos factores puedan ser tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

3.3 Contingencias en la Infraestructura Tecnológica

OBJETIVO DE CONTROL

El plan de infraestructura tecnológica deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia[23], capacidad de adecuación y evolución de la infraestructura).

3.4 Planes de Adquisición de Hardware y Software

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que los planes de adquisición de hardware y software sean establecidos y que reflejen las necesidades identificadas en el plan de infraestructura tecnológica.

3.5 Estándares de Tecnología

OBJETIVO DE CONTROL

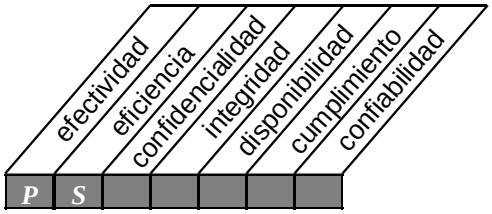
Tomando como base el plan de infraestructura tecnológica, la Gerencia deberá definir normas de tecnología con la finalidad de fomentar la estandarización.

[23] **Resistencia** (*resilience*): índice de resistencia al choque de un material

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:

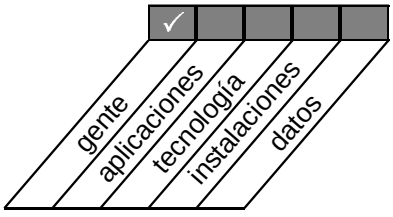
prestación de servicios de TI

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 de alta gerencia o del consejo
- propiedad, custodia
- supervisión
- segregación de funciones
- roles y responsabilidades
- descripción de puestos
- niveles de asignación de personal
- personal clave



4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE TI

4.1 Comité de planeación o dirección de la función de servicios de información

OBJETIVO DE CONTROL

La alta gerencia de la organización deberá designar un comité de planeación o dirección para vigilar la función de servicios de información y sus actividades. Entre los miembros del comité deberán encontrarse representantes de la alta gerencia, de la gerencia usuaria y de la función de servicios de información. El comité deberá reunirse regularmente y reportar a la alta gerencia.

4.2 Ubicación de los servicios de información en la organización

OBJETIVO DE CONTROL

Al ubicar la función de servicios de información en la estructura organizacional general, la alta gerencia deberá asegurar la existencia de autoridad, actitud crítica e independencia por parte del departamento usuario con un grado tal que sea posible garantizar soluciones de tecnología de información efectivas y progreso suficiente al implementarlas, así como establecer una relación de sociedad con la alta Gerencia para incrementar la capacidad de previsión, la comprensión y las habilidades para identificar y resolver problemas de tecnología de información.

4.3 Revisión de Logros Organizacionales

OBJETIVO DE CONTROL

Deberá establecerse un marco de referencia con el propósito de revisar que la estructura organizacional cumpla continuamente con los objetivos y se adapte a las cambiantes circunstancias.

4.4 Funciones y Responsabilidades

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todo el personal en la organización conozca sus funciones y responsabilidades en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad con respecto a la seguridad y al control interno. Consecuentemente, deberán organizarse y emprenderse campañas regulares para aumentar la conciencia y la disciplina.

4.5 Responsabilidad del aseguramiento de la calidad

OBJETIVO DE CONTROL

La Gerencia deberá asignar la responsabilidad de la ejecución de la función de aseguramiento de calidad a miembros del personal de la función de servicios de información y asegurar que existan sistemas de aseguramiento de calidad apropiados, controles y experiencia en comunicación dentro del grupo de aseguramiento de calidad de la función de servicios de información. La ubicación de la función dentro del área de servicios de información, las responsabilidades y el tamaño del grupo de aseguramiento de calidad deberán satisfacer los requerimientos de la empresa.

4.6 Responsabilidad de la Seguridad Lógica y Física

OBJETIVO DE CONTROL

La Gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un Gerente de seguridad de la información, quien reportará a la alta gerencia. Como mínimo, la responsabilidad de la Gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.

4.7 Propiedad y Custodia

OBJETIVO DE CONTROL

La Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

4.8 Propiedad de Datos y Sistemas

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todos los activos de información (sistemas y datos) cuenten con un propietario asignado que tome decisiones

sobre la clasificación y los derechos de acceso. Los propietarios del sistema normalmente delegarán la custodia diaria al grupo de liberación/ operación de sistemas y las responsabilidades de seguridad a un administrador de la seguridad. Los Propietarios, sin embargo, permanecerán como responsables del mantenimiento de medidas de seguridad apropiadas.

4.9 Supervisión

OBJETIVO DE CONTROL

La alta gerencia deberá implementar prácticas de supervisión adecuadas en la organización de servicios de información para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente, para evaluar si todo el personal cuenta con suficiente autoridad y recursos para llevar a cabo sus tareas y responsabilidades, y para revisar de manera general los indicadores clave de desempeño.

4.10 Segregación de Funciones

OBJETIVO DE CONTROL

La alta gerencia deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico. La Gerencia deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones:

- uso de sistemas de información;
- entrada de datos;
- operación de cómputo;
- administración de redes;
- administración de sistemas;
- desarrollo y mantenimiento de sistemas
- administración de cambios
- administración de seguridad; y
- auditoría de seguridad

4.11 Asignación de Personal para Tecnología de Información

OBJETIVO DE CONTROL

Las evaluaciones de los requerimientos de asignación de personal deberán llevarse a cabo regularmente para asegurar que la función de servicios de información cuente con un número suficiente de personal competente de tecnología de información. Los requerimientos de asignación de personal deberán ser evaluados por lo menos anualmente o al presentarse cambios mayores en el negocio, en el ambiente operacional o de tecnología de información. Deberá actuarse oportunamente tomando como base los resultados de las evaluaciones para asegurar una asignación de personal adecuada en el presente y en el futuro.

4.12 Descripción de Puestos para el Personal de la Función de Servicios de Información

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que las descripciones de los puestos para el personal de la función de servicios de información sean establecidos y actualizados regularmente. Estas descripciones de puestos deberán delinear claramente tanto la responsabilidad como la autoridad, incluir las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

4.13 Personal Clave de TI

OBJETIVO DE CONTROL

La Gerencia deberá definir e identificar al personal clave de tecnología de información.

4.14 Procedimientos para personal por contrato

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos relevantes para controlar las actividades de consultores y demás personal externo contratado por la función de servicios de información para asegurar la protección de los activos de información de la organización.

4.15 Relaciones

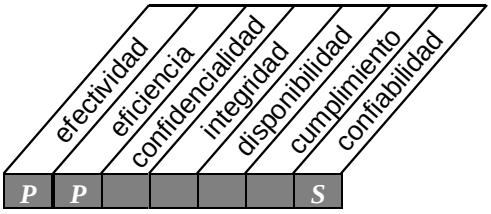
OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá llevar a cabo las acciones necesarias para establecer y mantener una coordinación, una comunicación y un enlace óptimos entre la función de servicios de información y demás elementos interesados dentro y fuera de la función de servicios de información (usuarios, proveedores, oficiales de seguridad, Gerentes).

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:

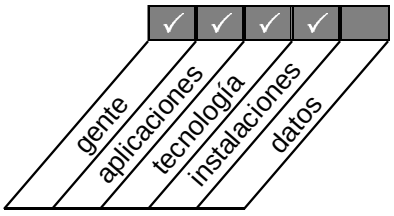
asegurar el financiamiento y el control de desembolsos de recursos financieros

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



5 MANEJO DE LA INVERSIÓN EN TECNOLOGÍA DE INFORMACIÓN

5.1 Presupuesto Operativo Anual para la Función de Servicios de Información

OBJETIVO DE CONTROL

La alta gerencia deberá implementar un proceso de definición de presupuestos para asegurar que un presupuesto operativo anual para la función de Servicios de Información sea establecido y aprobado en línea con los planes a largo y corto plazo de la organización, así como con los planes a largo y corto plazo de tecnología de información. Deberán investigarse alternativas de financiamiento.

5.2 Monitoreo de Costo - Beneficios

OBJETIVO DE CONTROL

La Gerencia deberá establecer un proceso de monitoreo de costos que compare los costos reales contra los presupuestados. Aun más, los posibles beneficios derivados de la actividad de tecnología de información deberán ser identificados y reportados. En cuanto al monitoreo de costos, la fuente de las cifras reales deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información. Por lo que toca a monitoreo de beneficios, se deberán definir indicadores de medición de desempeño de alto nivel y ser reportados y revisados regularmente para asegurar su adecuación.

5.3 Justificación de Costo - Beneficio

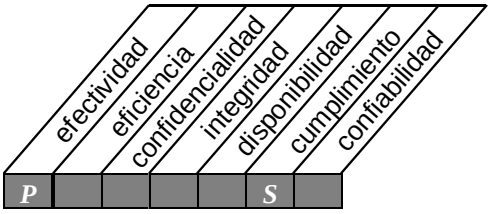
OBJETIVO DE CONTROL

Deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos y se encuentre en línea con la industria. Los beneficios derivados de las actividades de tecnología de información deberán ser analizados en forma similar.

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:

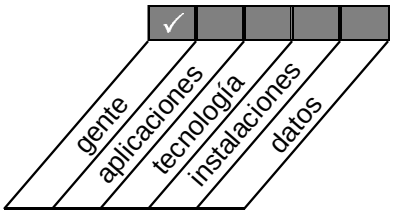
asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones

se hace posible a través de:

políticas establecidas y transmitidas a la comunidad de usuarios; además, se necesita estándares 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



6 COMUNICACIÓN DE LA DIRECCIÓN Y ASPIRACIONES DE LA GERENCIA

6.1 Ambiente Positivo de Control de la Información

OBJETIVO DE CONTROL

La Gerencia deberá crear un marco de referencia y un programa de previsión que fomente un ambiente de control positivo a través de toda la organización al aplicar elementos tales como: integridad, valores éticos, competencia del empleado, filosofía y estilo operativo de la Gerencia, responsabilidad, atención y dirección proporcionadas por el Consejo Directivo. Deberá ponerse especial atención a los aspectos relacionados con tecnología de información.

6.2 Responsabilidad de la Gerencia en cuanto a Políticas

OBJETIVO DE CONTROL

La Gerencia deberá asumir la responsabilidad completa de la formulación, el desarrollo, la documentación, la promulgación y el control de políticas que cubran metas y directrices generales. Deberán llevarse a cabo revisiones regulares de las políticas para asegurar su conveniencia. La complejidad de las políticas y los procedimientos escritos deberán estar siempre en proporción con el tamaño de la organización y el estilo gerencial.

6.3 Comunicación de las Políticas de la Organización

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que las políticas organizacionales sean comunicadas y comprendidas por todos los niveles de la organización.

6.4 Recursos para la implementación de Políticas

OBJETIVO DE CONTROL

Posterior a la comunicación, la Gerencia deberá destinar recursos para la implementación de sus políticas. La Gerencia deberá también monitorear la duración de la implementación de sus políticas.

6.5 Mantenimiento de Políticas

OBJETIVO DE CONTROL

Las políticas deberán ser ajustadas regularmente para adecuarse a las condiciones cambiantes. Las políticas deberán ser reevaluadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional o del negocio, para evaluar que sean convenientes y apropiadas y deberán ser modificadas en caso necesario. La Gerencia deberá proporcionar un marco de referencia y un proceso para las revisiones periódicas y la aprobación de estándares, políticas, directrices y procedimientos.

6.6 Cumplimiento de Políticas, Procedimientos y Estándares

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se establezcan procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.

6.7 Compromiso con la Calidad

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, así como políticas y objetivos que sean consistentes con la filosofía y las políticas de la corporación a este respecto. La filosofía de calidad, las políticas y los objetivos deberán ser comprendidos, implementados y mantenidos a todos los niveles de la función de servicios de información.

6.8 Política sobre el Marco de Referencia para la Seguridad y el Control Interno

OBJETIVO DE CONTROL

La Gerencia deberá asumir la responsabilidad total del desarrollo y mantenimiento de una política sobre el marco de referencia, que establezca el enfoque general de la organización en cuanto a seguridad y control interno. La política deberá cumplir con los objetivos generales del negocio y estar dirigida a la minimización de riesgos a través de medidas preventivas, identificación oportuna de irregularidades, limitación de pérdidas y recuperación oportuna. Estas medidas deberán basarse en análisis costo-beneficio y deberá prio-

rizarse. Además, la alta gerencia deberá asegurar que esta política de seguridad de alto nivel y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento con las políticas de seguridad y control interno.

6.9 Derechos de propiedad intelectual

OBJETIVO DE CONTROL

La gerencia deberá proveer e implementar una política por escrito sobre derechos de propiedad intelectual, que cubra el desarrollo de software, tanto interno como contratado a externos.

6.10 Políticas para Situaciones Específicas

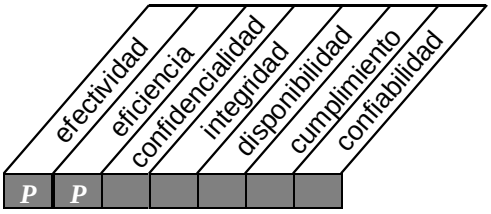
OBJETIVO DE CONTROL

Deberán ponerse en práctica medidas que aseguren el establecimiento de políticas para situaciones específicas con el fin de documentar las decisiones gerenciales con respecto al tratamiento de actividades, aplicaciones, sistemas o tecnologías particulares.

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:

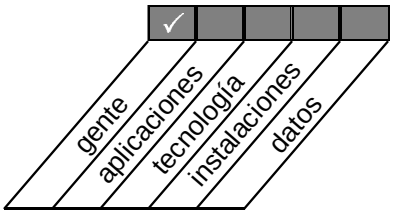
maximizar las contribuciones del personal a los procesos de TI

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



7 ADMINISTRACIÓN DE RECURSOS HUMANOS

7.1 Reclutamiento y Promoción de Personal

OBJETIVO DE CONTROL

La Gerencia deberá implementar y evaluar regularmente los procesos necesarios para asegurar que las prácticas de reclutamiento y promoción de personal tengan como base criterios objetivos y consideren factores como la educación, la experiencia y la responsabilidad. Estos procesos deberán estar en línea con las políticas y procedimientos generales de la organización a este respecto.

7.2 Personal Calificado

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá verificar regularmente que el personal que lleva a cabo tareas específicas esté calificado tomando como base una educación, entrenamiento y/o experiencia apropiados, según se requiera. La Gerencia deberá alentar al personal para que participe como miembro, en organizaciones profesionales.

7.3 Entrenamiento de Personal

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los empleados reciban orientación al ser contratados, así como entrenamiento y capacitación constantes con la finalidad de conservar los conocimientos, habilidades, destrezas y conciencia de seguridad al nivel requerido, para la ejecución efectiva de sus tareas. Los programas de educación y entrenamiento dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal deberán ser revisados regularmente.

7.4 Entrenamiento Cruzado o Respaldo de personal

OBJETIVO DE CONTROL

La Gerencia deberá proporcionar un entrenamiento "cruzado" o contar con suficiente personal de respaldo con la finalidad de solucionar posibles ausencias. El personal encargado de puestos delicados deberá tomar vacaciones ininterrumpidas con una duración suficiente como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

7.5 Procedimientos de Acreditación[24] de Personal

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que su personal se sujete a una revisión o acreditación de seguridad antes de ser contratado, transferido o promovido, dependiendo de lo delicado o sensible del puesto. Un empleado que no haya pasado por este procedimiento de revisión o acreditación al ser contratado por primera vez, no deberá ser colocado en un puesto delicado hasta que éste haya obtenido la acreditación de seguridad.

7.6 Evaluación de Desempeño de los Empleados

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso de evaluación de desempeño de los empleados y asegurar que dicha evaluación sea llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

7.7 Cambios de Puesto y Despidos

OBJETIVO DE CONTROL

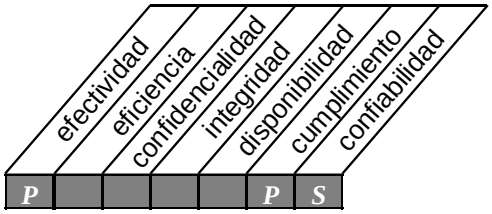
La Gerencia deberá asegurar que se tomen acciones oportunas y apropiadas con respecto a cambios de puesto y despidos, de tal manera que los controles internos y la seguridad no se vean perjudicados por estos eventos.

[24] **Acreditación** (*clearance*)

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:

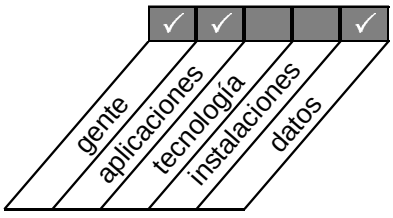
cumplir con obligaciones legales, regulatorias y contractuales

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



8 ASEGURAMIENTO DE CUMPLIMIENTO DE REQUERIMIENTOS EXTERNOS

8.1 Revisión de Requerimientos Externos

OBJETIVO DE CONTROL

La organización deberá establecer y mantener procedimientos para la revisión de requerimientos externos y para la coordinación de estas actividades. La investigación continua deberá determinar los requerimientos externos aplicables en la organización. Deberán revisarse los requerimientos legales, gubernamentales o cualquier otro requerimiento externo relacionado con las prácticas y controles de tecnología de información. La Gerencia deberá también evaluar el impacto de cualquier relación externa en las necesidades generales de información de la organización, incluyendo la determinación del grado al cual las estrategias de la función de servicios de información deben soportar o cumplir con los requerimientos de terceros.

8.2 Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos

OBJETIVO DE CONTROL

Las prácticas organizacionales deberán asegurar que se lleven a cabo oportunamente las acciones correctivas apropiadas para garantizar el cumplimiento de los requerimientos externos. Además, deberán establecerse y mantenerse procedimientos adecuados que aseguren el cumplimiento continuo. A este respecto la Gerencia deberá solicitar apoyo legal en caso necesario.

8.3 Cumplimiento de Seguridad y Ergonomía

OBJETIVO DE CONTROL

La Gerencia deberá asegurar el cumplimiento de los estándares ergonómicos y de seguridad en el ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

8.4 Privacidad, propiedad intelectual y flujos de datos y Flujo de Datos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar el cumplimiento de las regulaciones sobre privacidad o confidencialidad, propiedad intelectual, flujo de datos externos[25] y criptografía aplicables a las prácticas de tecnología de información de la organización.

8.5 Comercio Electrónico

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se establezcan contratos formales para determinar acuerdos entre socios comerciales sobre procesos de comunicación, así como sobre estándares de mensajes de transacción, seguridad y almacenamiento de datos. Cuando se realicen operaciones de intercambio en *Internet*, la gerencia deberá imponer adecuados controles para asegurar el cumplimiento de leyes locales y costumbres en un ámbito mundial.

8.6 Cumplimiento con los Contratos de Seguros

OBJETIVO DE CONTROL

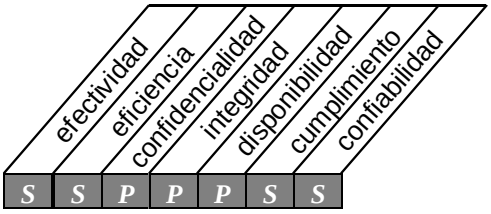
La Gerencia deberá asegurar la identificación y el continuo cumplimiento de los requerimientos de los contratos de seguros.

[25] **Externos** (*transborder*)

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:

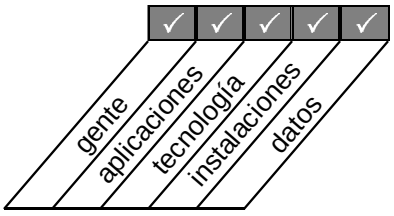
asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

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



9 EVALUACIÓN DE RIESGOS

9.1 Evaluación de Riesgos del Negocio

OBJETIVO DE CONTROL

La Gerencia deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos utilizando los resultados de auditorías, inspecciones e incidentes identificados.

9.2 Enfoque de Evaluación de Riesgos

OBJETIVO DE CONTROL

La Gerencia deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

9.3 Identificación de Riesgos

OBJETIVO DE CONTROL

La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.

9.4 Medición de Riesgos

OBJETIVO DE CONTROL

El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

9.5 Plan de Acción contra Riesgos

OBJETIVO DE CONTROL

El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

9.6 Aceptación de Riesgos

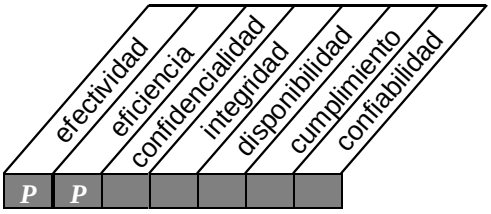
OBJETIVO DE CONTROL

El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

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:

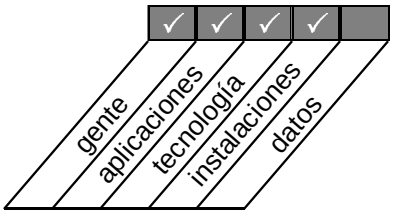
establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión

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



10 ADMINISTRACIÓN DE PROYECTOS

10.1 Marco de Referencia para la Administración de Proyectos

OBJETIVO DE CONTROL

La Gerencia deberá establecer un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

10.2 Participación del Departamento Usuario en la Iniciación de Proyectos

OBJETIVO DE CONTROL

El marco de referencia de la administración de proyectos de la organización deberá fomentar la participación del departamento usuario afectado en la definición y autorización de cualquier proyecto de desarrollo, implementación o modificación.

10.3 Miembros y Responsabilidades del Equipo del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá especificar las bases para asignar a los miembros del personal al proyecto y definir las responsabilidades y autoridades de los miembros del equipo del proyecto.

10.4 Definición del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá generar la creación de un estatuto claro por escrito que defina la naturaleza y el alcance de cada proyecto de implementación antes de que los trabajos del mismo sean iniciados.

10.5 Aprobación del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá asegurar que, para cada proyecto propuesto, la alta gerencia de la organización revise los reportes de los estudios de factibilidad relevantes como una base para fundamentar la decisión de proceder con el proyecto.

10.6 Aprobación de las Fases del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá disponer que los Gerentes designados para las funciones del usuario y de los servicios de información aprueben el trabajo realizado en cada fase del ciclo antes de iniciar los trabajos de la siguiente fase.

10.7 Plan Maestro del Proyecto

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, para cada proyecto aprobado, se cree un plan maestro adecuado que mantenga el control del proyecto a través de todo su desarrollo e incluya un método de monitoreo del tiempo y los costos incurridos durante su vida.

10.8 Plan de Aseguramiento de la Calidad de Sistemas

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la implementación de un sistema nuevo o modificado incluya la preparación de un plan de calidad que sea integrado posteriormente al plan maestro del proyecto y que sea formalmente revisado y acordado por todas las partes interesadas.

10.9 Planeación de Métodos de Aseguramiento

OBJETIVO DE CONTROL

Las tareas de aseguramiento deberán ser definidas durante la fase de planeación del marco de referencia de administración de proyectos. Las tareas de aseguramiento deberán apoyar la acreditación de sistemas nuevos o modificados y garantizar que los controles internos y los dispositivos de seguridad cumplan con los requerimientos necesarios.

10.10 Administración Formal de Riesgos de Proyectos

OBJETIVO DE CONTROL

La Gerencia deberá implementar un programa de administración formal de riesgos de proyectos para eliminar o minimizar los riesgos asociados con proyectos individuales (por ejemplo, identificación y control de áreas o eventos que tengan el potencial de causar cambios no deseados).

10.11 Plan de Prueba

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá requerir la creación de un plan de pruebas para cada proyecto de desarrollo, implementación y modificación.

10.12 Plan de Entrenamiento

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá requerir la creación de un plan de entrenamiento para cada proyecto de desarrollo, implementación y modificación.

10.13 Plan de Revisión Post - Implementación

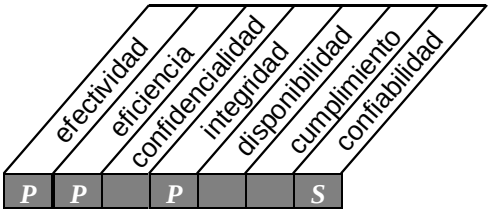
OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá disponer que, como parte integral de las actividades del equipo del proyecto, se desarrolle un plan de revisión post - implementación para cada sistema de información nuevo o modificado, con la finalidad de determinar si el proyecto ha generado los beneficios planeados.

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:

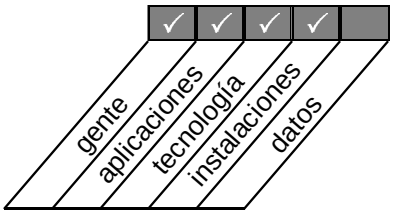
satisfacer los requerimientos del cliente

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



11 ADMINISTRACIÓN DE CALIDAD

11.1 Plan General de Calidad

OBJETIVO DE CONTROL

La alta gerencia deberá desarrollar y mantener regularmente un plan general de calidad basado en los planes organizacionales y de tecnología de información a largo plazo. El plan deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

11.2 Enfoque de Aseguramiento de Calidad

OBJETIVO DE CONTROL

La Gerencia deberá establecer un enfoque estándar con respecto al aseguramiento de calidad, que cubra tanto las actividades de aseguramiento de calidad generales como las específicas de un proyecto. El enfoque deberá determinar el (los) tipo(s) de actividades de aseguramiento de calidad (tales como revisiones, auditorías, inspecciones, etc.) que deben realizarse para alcanzar los objetivos del plan general de calidad. Asimismo deberá requerir una revisión específica de aseguramiento de calidad.

11.3 Planeación del Aseguramiento de Calidad

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso de planeación de aseguramiento de calidad para determinar el alcance y la duración de las actividades de aseguramiento de calidad.

11.4 Revisión del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que las responsabilidades asignadas al personal de aseguramiento de calidad incluyan una revisión del cumplimiento general de los estándares y procedimientos de la función de servicios de información.

11.5 Metodología del Ciclo de Vida de Desarrollo de Sistemas

OBJETIVO DE CONTROL

La alta gerencia de la organización deberá definir e implementar estándares de sistemas de información y adoptar una metodología del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información computarizados y tecnología afín. La metodología del ciclo de vida de desarrollo de sistemas elegida deberá ser la apropiada para los sistemas a ser desarrollados, adquiridos, implementados y mantenidos.

11.6 Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual

OBJETIVO DE CONTROL

En el caso de requerirse cambios mayores a la tecnología actual, la Gerencia deberá asegurar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas, como en el caso de adquisición de nueva tecnología.

11.7 Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas

OBJETIVO DE CONTROL

La alta gerencia deberá implementar una revisión periódica de su metodología del ciclo de vida de desarrollo de sistemas para asegurar que incluya técnicas y procedimientos actuales generalmente aceptados.

11.8 Coordinación y Comunicación

OBJETIVO DE CONTROL

La Gerencia deberá establecer un proceso para asegurar la coordinación y comunicación estrecha entre los clientes de la función de servicios de información y los implementadores de sistemas. Este proceso deberá ocasionar que los métodos estructurados que utilicen la metodología del ciclo de vida de desarrollo de sistemas aseguren la provisión de soluciones de tecnología de información de calidad que satisfagan las demandas de negocio. La Gerencia deberá promover una organización que se caracterice por la estrecha cooperación y comunicación a lo largo del ciclo de vida de desarrollo de sistemas.

11.9 Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología

OBJETIVO DE CONTROL

Deberá establecerse un marco de referencia general referente a la adquisición y mantenimiento de la infraestructura de tecnología. Los diferentes pasos que deben ser seguidos con respecto a la infraestructura de tecnología (tales como adquisición; programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y aplicación de correcciones) deberán estar regidos por y mantenerse en línea con el marco de referencia para la adquisición y mantenimiento de la infraestructura de tecnología.

11.10 Relaciones con Terceras Partes como Implementadores

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso para asegurar las buenas relaciones de trabajo con terceras partes como implementadores externos. Dicho proceso deberá disponer que el usuario y el implementador estén de acuerdo sobre los criterios de aceptación, el manejo de cambios, los problemas durante el desarrollo, las funciones de los usuarios, las instalaciones, las herramientas, el software, los estándares y los procedimientos.

11.11 Estándares para la Documentación de Programas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas deberá incorporar estándares para la documentación de programas que hayan sido impuestos y comunicados al personal interesado. La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema de información o de los proyectos de modificación coincida con estos estándares.

11.12 Estándares para Pruebas de Programas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar las unidades de software y los programas agregados[26], creados como parte de cada proyecto de desarrollo o modificación de sistemas de información.

11.13 Estándares para Pruebas de Sistemas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar el sistema total, como parte de cada proyecto de desarrollo o modificación de sistemas de información.

11.14 Pruebas Piloto/En Paralelo

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe definir las condiciones bajo las cuales deberán conducirse las pruebas piloto o en paralelo de sistemas nuevos y/o actuales.

11.15 Documentación de las Pruebas del Sistema

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe disponer, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información, que se conserve la documentación de los resultados de las pruebas del sistema.

11.16 Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo

OBJETIVO DE CONTROL

El enfoque de aseguramiento de calidad de la organización deberá requerir que una revisión post - implementación de un sistema de información operacional evalúe si el equipo encargado del proyecto, cumplió con las estipulaciones de la metodología del ciclo de vida de desarrollo de sistemas.

[26] **Agregados** (*aggredgated*)

11.17 Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información

OBJETIVO DE CONTROL

El enfoque de aseguramiento de calidad deberá incluir una revisión de hasta qué punto los sistemas particulares y las actividades de desarrollo de aplicaciones han alcanzado los objetivos de la función de servicios de información.

11.18 Métricas de calidad

OBJETIVO DE CONTROL

La gerencia deberá definir y utilizar métricas para medir los resultados de actividades, evaluando si las metas de calidad han sido alcanzadas.

11.19 Reportes de Revisiones de Aseguramiento de Calidad

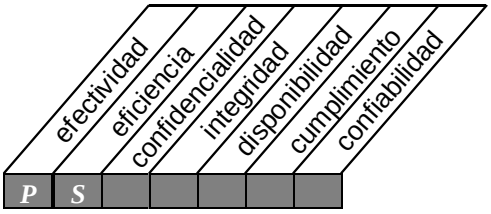
OBJETIVO DE CONTROL

Los reportes de revisiones de aseguramiento de calidad deberán ser preparados y enviados a la Gerencia de los departamentos usuarios y de la función de servicios de información.

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:

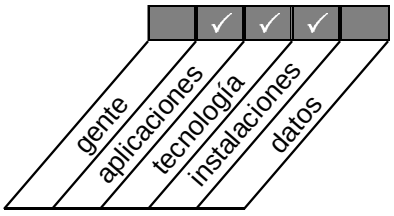
asegurar el mejor enfoque para cumplir con los requerimientos del usuario

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



1 IDENTIFICACIÓN DE SOLUCIONES

1.1 Definición de Requerimientos de Información

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los requerimientos del negocio ya satisfechos por el sistema actual y a ser satisfechos por el sistema nuevo propuesto o modificado (software, datos e infraestructura), estén claramente definidos antes de aprobar cualquier proyecto de desarrollo, implementación o modificación. La metodología del ciclo de vida de desarrollo de sistemas deberá exigir que los requerimientos de las soluciones funcionales y operacionales sean especificados, incluyendo desempeño, protección, confiabilidad, compatibilidad, seguridad y legislación.

1.2 Formulación de Acciones Alternativas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proveer el análisis de las acciones alternativas que deberán satisfacer los requerimientos del negocio, establecidos para un sistema nuevo o modificado.

1.3 Formulación de Estrategias de Adquisición

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un plan de estrategia de adquisición, definiendo si el software será "adquirido del mostrador[27]", desarrollados internamente, a través de contratación o mediante una combinación de estos.

1.4 Requerimientos de Servicios de Terceros

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular la evaluación de requerimientos y las especificaciones para una Solicitud de Propuesta[28] cuando se negocie con un proveedor de servicios externo.

1.5 Estudio de Factibilidad Tecnológica

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un examen de factibilidad tecnológica de cada alternativa con la finalidad de satisfacer los requerimientos de negocio establecidos para el desarrollo de un proyecto propuesto de cualquier sistema nuevo o modificado.

1.6 Estudio de Factibilidad Económica

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe generar, en cada proyecto de desarrollo, implementación y modificación de sistemas de información propuesto, el análisis de los costos y beneficios asociados con cada alternativa considerada para satisfacer los requerimientos del negocio establecidos.

1.7 Arquitectura de Información

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se tome en consideración el modelo de datos de la empresa al definir las soluciones y analizar la factibilidad de las mismas.

1.8 Reporte de Análisis de Riesgos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, en cada proyecto de desarrollo, implementación y modificación de sistemas de información propuesto, el análisis y la documentación de las amenazas a la seguridad, puntos de impacto y debilidad y protecciones factibles de seguridad y control interno, con la finalidad de reducir o eliminar el riesgo identificado. Esto deberá llevarse a cabo en línea con el marco de referencia general de evaluación de riesgos.

---

[27] **Del anaquel** (*off-the-shelf*): se dice de productos de software terminados que pueden adquirirse directamente de un proveedor o distribuidor.

[28] **Solicitud de propuesta** (*request for proposal, RFP*): invitación que se extiende a proveedores para que presenten una propuesta.

[29] **Económicos** (*cost-effective*)

1.9 Controles de Seguridad Económicos[29]

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los costos y beneficios de seguridad sean examinados cuidadosamente en términos monetarios y no monetarios, para garantizar que los costos de los controles no excedan a los beneficios. La decisión requerirá la firma de aprobación formal de la Gerencia.

1.10 Diseño de Pistas de Auditoría

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que existan mecanismos adecuados para pistas de auditoría o que dichos mecanismos puedan ser desarrollados para la solución identificada y seleccionada. Los mecanismos deberán proporcionar la capacidad de proteger datos sensitivos (ej. identificación de usuarios contra divulgación o mal uso)

1.11 Ergonomía

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los proyectos de desarrollo, implementación y cambios emprendidos por la función de servicios de información, tomen en consideración los aspectos ergonómicos asociados con la introducción de soluciones automatizadas.

1.12 Selección del Software del Sistema

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la función de servicios de información cumpla con un procedimiento estándar para identificar todos los programas de software potenciales que deberán satisfacer sus requerimientos operacionales.

1.13 Control de Abastecimiento

OBJETIVO DE CONTROL

La Gerencia deberá desarrollar e implementar un enfoque central de abastecimientos que describa un conjunto común de procedimientos y estándares a ser seguidos en la adquisición de hardware, software y servicios relacionados con la tecnología de información. Los productos deberán ser revisados y probados antes de su utilización y pago.

1.14 Adquisición de Productos de Software

OBJETIVO DE CONTROL

La adquisición de productos de software deberá seguir las políticas de adquisición de la organización.

1.15 Mantenimiento de Software de Terceras Partes

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, para el software con licencia adquirido a terceras partes, los proveedores cuenten con los procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de software. Deberá tomarse en consideración el soporte del producto en cualquier acuerdo de mantenimiento relacionado con el producto entregado.

1.16 Contratos de Programación de Aplicaciones

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los servicios de programación contratados estén justificados con una solicitud de servicios por escrito por parte de un miembro designado de la función de servicios de información. El contrato deberá estipular que el software, la documentación y otros elementos entregables[30] estén sujetos a pruebas y revisiones antes de ser aceptados. Además, deberá asegurar que los productos finales terminados por los servicios de programación contratados sean revisados y probados de acuerdo con los estándares definidos por el grupo de aseguramiento de calidad de la función de servicios de información y otras partes interesadas (como usuarios, administradores de proyecto, etc.) antes de pagar por el trabajo y aprobar el producto final. Las pruebas que deberán ser incluidas en las especificaciones del contrato deberán consistir en pruebas del sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de afinación y desempeño, pruebas de regresión, pruebas de aceptación del usuario y, finalmente, pruebas piloto del sistema total, con la finalidad de evitar fallas no esperadas del mismo.

[30] **Entregable** (*deliverable*): un producto formal que es entregado como parte final de un proceso de trabajo.

1.17 Aceptación de Instalaciones

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para las instalaciones a ser proporcionadas, el cual defina los procedimientos y criterios de aceptación. Además, deberán llevarse a cabo pruebas de aceptación para garantizar que el acomodo[31] y el medio cumplan con los requerimientos especificados en el contrato.

1.18 Aceptación de Tecnología

OBJETIVO DE CONTROL

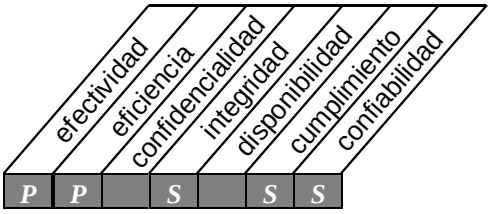
La Gerencia deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para la tecnología específica a ser proporcionada, el cual defina los procedimientos y criterios de aceptación. Además, las pruebas de aceptación establecidas en el plan, deberán incluir inspección, pruebas de funcionalidad y seguimiento de cargas de trabajo.

[31] **Acomodo** (*accommodation*)

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:

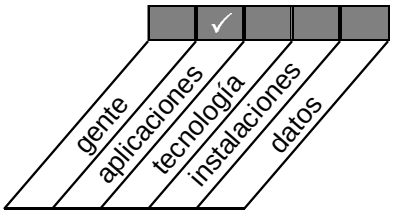
proporcionar funciones automatizadas que soporten efectivamente al negocio

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



2 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN

2.1 Métodos de Diseño

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que sean aplicados a técnicas y procedimientos apropiados, incluyendo una estrecha relación con los usuarios del sistema, en la creación de las especificaciones de diseño para cada nuevo proyecto de desarrollo de sistemas de información, y verificar las especificaciones del diseño contra los requerimientos del usuario.

2.2 Cambios Significativos a Sistemas Actuales

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, en caso de presentarse la necesidad de realizar modificaciones significativas a los sistemas actuales, se siga un proceso de desarrollo similar al utilizado en el desarrollo de sistemas nuevos.

2.3 Aprobación del Diseño

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización requerirá que las especificaciones de diseño para todos los proyectos de desarrollo y modificación de sistemas de información, sean revisados y aprobados por la Gerencia, por los departamentos usuarios afectados y por la alta gerencia de la organización, cuando esto sea pertinente.

2.4 Definición y Documentación de Requerimientos de Archivos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la aplicación de un procedimiento apropiado para la definición y documentación del formato de los archivos para cada proyecto de desarrollo y modificación de sistemas de información. Este procedimiento deberá garantizar el respeto a las reglas de diccionario de datos.

2.5 Especificaciones de Programas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la preparación de especificaciones detalladas por escrito, de los programas para cada proyecto de desarrollo o modificación de sistemas de información. Además, la metodología deberá garantizar que las especificaciones de los programas correspondan a las especificaciones del diseño del sistema.

2.6 Diseño para la Recopilación[32] de Datos Fuente

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la especificación de mecanismos adecuados, para la recopilación y entrada de datos para cada proyecto de desarrollo y modificación de sistemas de información.

2.7 Definición y Documentación de Requerimientos de Entrada de Datos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de entrada de datos para cada proyecto de desarrollo o modificación de sistemas de información.

2.8 Definición de Interfases

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que se especifiquen, diseñen y documenten apropiadamente todas las interfases internas y externas.

[32] **Recopilación** (*collection*): relevar, recabar o renuir información.

2.9 Interfase Usuario-Máquina

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar el desarrollo de una interfase entre el usuario y la máquina fácil de utilizar y que sea capaz de autodocumentarse (por medio de funciones de ayuda en línea).

2.10 Definición y Documentación de Requerimientos de Procesamiento

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de procesamiento para cada proyecto de desarrollo o modificación de sistemas de información.

2.11 Definición y Documentación de Requerimientos de Salida de Datos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de salida de datos para cada proyecto de desarrollo o modificación de sistemas de información

2.12 Controlabilidad

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se especifiquen mecanismos adecuados, para garantizar que se identifiquen los requerimientos de seguridad y control internos para cada proyecto de desarrollo o modificación de sistemas de información. La metodología deberá asegurar además que los sistemas de información estén diseñados para incluir controles de aplicación que garanticen que los datos de entrada y salida estén completos, así como su precisión, oportunidad[33] y autorización. Deberá llevarse a cabo una evaluación de sensibilidad durante el inicio del desarrollo o modificación del sistema. Los aspectos básicos de seguridad y control interno de un sistema a ser desarrollado o modificado deberán ser evaluados junto con el diseño conceptual del mismo, con el fin de integrar los conceptos de seguridad en el diseño tan pronto como sea posible.

2.13 Disponibilidad como Factor Clave de Diseño

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que la disponibilidad sea considerada en el proceso de diseño de nuevos o modificados sistemas de información en la fase más temprana posible. La disponibilidad debe ser analizada y, en caso necesario, incrementada a través de mejoras de mantenimiento y confiabilidad.

2.14 Consideraciones de Integridad de Tecnología para Software de Programas de Aplicación

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para asegurar, cuando esto aplique, que los programas de aplicación contengan estipulaciones que verifiquen rutinariamente las tareas realizadas por el software, para apoyar el aseguramiento de la integridad de los datos y el cual haga posible la restauración de la integridad a través de procedimientos de recuperación en reversa[34] u otros medios.

2.15 Pruebas de Software de Aplicación

OBJETIVO DE CONTROL

Deberán aplicarse pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga y estrés[35], de acuerdo con el plan de prueba del proyecto y con los estándares de pruebas establecidos antes de ser aprobado por el usuario. Se deberán aplicar adecuadas medidas de seguridad para prevenir divulgación de información sensitiva durante las pruebas.

[33] **Oportunidad** (*timeliness*)

[34] **En reversa** (*rollback*): estrategia de recuperación de bases de datos que se utiliza para restaurar un estado previo de los datas

[35] **Carga y estrés** (*load and stress*)

2.16 Materiales de Consulta y Soporte para Usuarios

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen manuales de referencia y soporte para usuarios adecuados (preferiblemente en formato electrónico) como parte de cada proyecto de desarrollo o modificación de sistemas de información

2.17 Reevaluación del Diseño del Sistema

OBJETIVO DE CONTROL

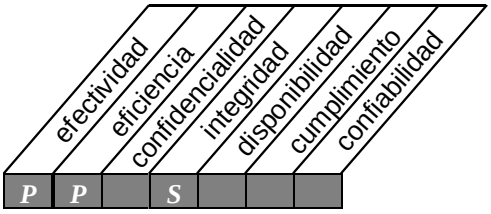
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que el diseño del sistema sea reevaluado siempre que ocurran discrepancias técnicas y/o lógicas durante el desarrollo o mantenimiento del sistema.

[33] **Oportunidad** (*timeliness*)
[34] **En reversa** (*rollback*): estrategia de recuperación de bases de datos que se utiliza para restaurar un estado previo de los datas
[35] **Carga y estrés** (*load and stress*)

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:

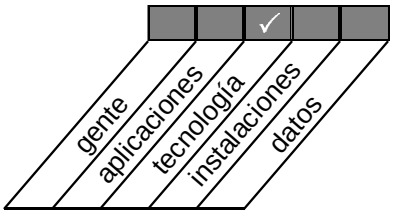
proporcionar las plataformas apropiadas para soportar aplicaciones de negocios

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



3 ADQUISICIÓN Y MANTENIMIENTO DE ARQUITECTURA DE TECNOLOGÍA

3.1 Evaluación de Nuevo Hardware y Software

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para evaluar el impacto de nuevo hardware y software sobre el rendimiento del sistema en general.

3.2 Mantenimiento Preventivo para Hardware

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá calendarizar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

3.3 Seguridad del Software del Sistema

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

3.4 Instalación del Software del Sistema

OBJETIVO DE CONTROL

Deberán implementarse procedimientos para asegurar que el software del sistema sea instalado de acuerdo al marco de referencia de adquisición y mantenimiento de infraestructura de tecnología. Las pruebas deberán ser llevadas a cabo antes de autorizarse su utilización en ambiente de producción.

3.5 Mantenimiento del Software del Sistema

OBJETIVO DE CONTROL

Deberán implementarse procedimientos para asegurar que el software del sistema sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

3.6 Controles para Cambios del Software del Sistema

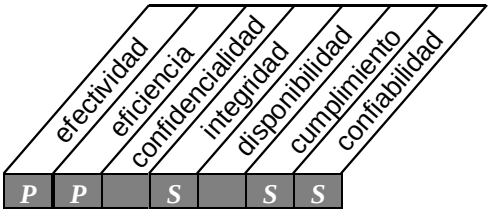
OBJETIVO DE CONTROL

Deberán implementarse procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la organización.

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:

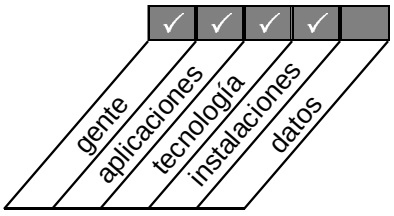
asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas

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



4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS RELACIONADOS CON TECNOLOGÍA DE INFORMACIÓN

4.1 Requerimientos Operacionales y Niveles de Servicios Futuros

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la definición oportuna de requerimientos operacionales y niveles de servicios futuros.

4.2 Manual de Procedimientos para Usuario

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen y actualicen manuales adecuados de procedimientos para los usuarios como parte de cada proyecto de desarrollo o modificación de sistemas de información.

4.3 Manual de Operaciones

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se prepare y se mantenga actualizado un manual de operaciones adecuado como parte de cada proyecto de desarrollo o modificación de sistemas de información.

4.4 Material de Entrenamiento

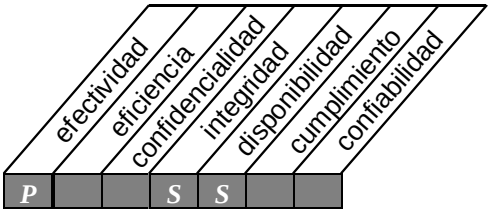
OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se desarrollen materiales de entrenamiento adecuados como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información. Estos materiales deberán enfocarse al uso del sistema en la práctica diaria.

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:

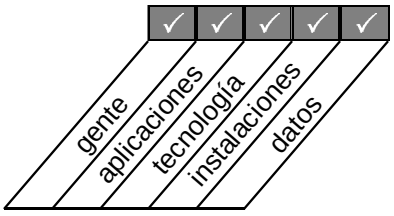
verificar y confirmar que la solución sea adecuada para el propósito deseado

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



5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS

5.1 Entrenamiento

OBJETIVO DE CONTROL

El personal de los departamentos usuarios afectados y el grupo de operaciones de la función de servicios de información deberán estar entrenados de acuerdo al plan de entrenamiento definido y los materiales relacionados, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información.

5.2 Adecuación[36] del Desempeño del Software de Aplicación

OBJETIVO DE CONTROL

La medición (optimización) del desempeño del software de aplicación deberá establecerse como una parte integral de la metodología del ciclo de vida de desarrollo de sistemas de la organización para predecir los recursos requeridos para operar software nuevo o significativamente modificado.

5.3 Conversión

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información, que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo de acuerdo con el plan preestablecido.

5.4 Pruebas de Cambios

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los cambios sean probados por un grupo de prueba independiente (distinto al de los desarrolladores) de acuerdo con la evaluación de impacto y recursos en un ambiente de prueba separado antes de comenzar su uso en el ambiente de operación regular. También deberán desarrollarse planes de respaldo externo[37]. Las pruebas de aceptación deberán llevarse a cabo en un ambiente representativo del ambiente operacional futuro (por ejemplo, condiciones similares de seguridad, controles internos, cargas de trabajo, etc.)

5.5 Criterios y Desempeño de Pruebas en Paralelo/Piloto

OBJETIVO DE CONTROL

Deben establecerse procedimientos para asegurar que las pruebas piloto o en paralelo sean llevadas a cabo de acuerdo con un plan preestablecido y que los criterios para la terminación del proceso de pruebas sean especificados con anterioridad.

5.6 Prueba de Aceptación Final

OBJETIVO DE CONTROL

Los procedimientos deberán asegurar, como parte de las pruebas de aceptación final o de aseguramiento de calidad de sistemas de información nuevos o modificados, una evaluación y aprobación formal de los resultados de las pruebas por parte de la Gerencia de los departamentos usuarios afectados y de la función de servicios de información. Las pruebas deben cubrir todos los componentes del sistema de información (software de aplicación, instalaciones, tecnología, procedimientos de usuarios).

5.7 Pruebas y Acreditación de Seguridad

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos para asegurar que la Gerencia de operaciones y la Gerencia usuaria aceptan formalmente los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

5.8 Prueba Operacional

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, antes de poner el sistema en operación, el usuario o custodio designado (la parte designada para correr el sistema en nombre del usuario), valide su operación como un producto completo, bajo condiciones similares a las del ambiente de aplicación y en la manera en la que el sistema será operado en un ambiente de producción.

---

[36] **Adecuación** (*sizing*): asignar la dimensión o tamaña adecuado.

[37] **Respaldo externo** (*back-out*)

5.9 Paso a Producción

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos formales para controlar la entrega[38] del sistema de desarrollo a pruebas y a operación. Los ambientes respectivos deberán separarse y protegerse apropiadamente.

5.10 Evaluación de la Satisfacción de los Requerimientos del Usuario

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se realice una revisión post - implementación de los requerimientos operacionales del sistema de información (por ejemplo, capacidad, desempeño de procesamiento[39] a través del sistema etc.) con el fin de evaluar si las necesidades del usuario están siendo satisfechas por el mismo.

5.11 Revisión Gerencial Post - Implementación

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que una revisión post - implementación del sistema de información operacional evalúe y reporte si el sistema proporcionó los beneficios esperados de la manera más económica.

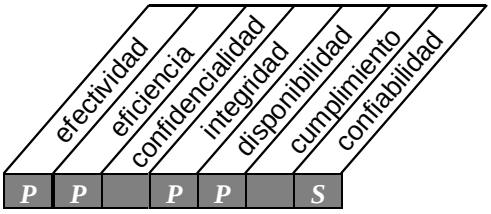
[38] **Entrega** (*handover*): traspaso del sistema de un ambiente de pruebas al ambiente de producción.

[39] **Desempeño de procesamiento** (*throughput*) capacidad de procesamiento de datos de un sistema de información.

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:

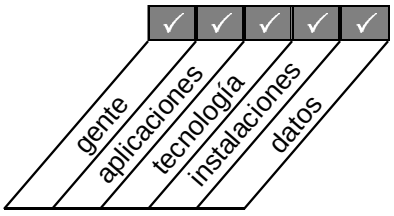
minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores

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



6 ADMINISTRACIÓN DE CAMBIOS

6.1 Inicio y Control de Requisiciones de Cambio

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todas las requisiciones de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios. Las solicitudes deberán categorizarse, priorizarse y establecerse procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estatus de su solicitud.

6.2 Evaluación del Impacto

OBJETIVO DE CONTROL

Deberá establecerse un procedimiento para asegurar que todas las requisiciones de cambio sean evaluadas en una forma estructurada en cuanto a todos los posibles impactos sobre el sistema operacional y su funcionalidad.

6.3 Control de Cambios

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración.

6.4 Documentación y Procedimientos

OBJETIVO DE CONTROL

El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

6.5 Mantenimiento Autorizado

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados.

6.6 Política de Liberación de Software

OBJETIVO DE CONTROL

La Gerencia deberá garantizar que la liberación de software esté regida por procedimientos formales asegurando aprobación, empaque[40], pruebas de regresión, entrega, etc.

6.7 Distribución de Software

OBJETIVO DE CONTROL

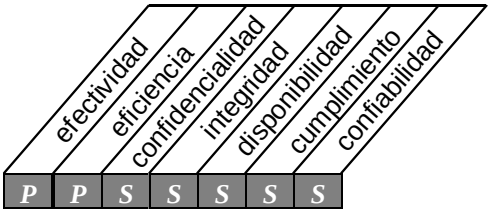
Deberán establecerse medidas de control específicas para asegurar la distribución del elemento de software correcto al lugar correcto, con integridad y de manera oportuna con pistas de auditoría adecuadas.

[40] **Empaque** (*packaging*)

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:

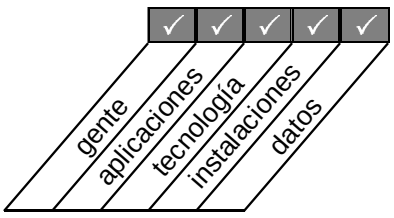
establecer una comprensión común del nivel de servicio requerido

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



1 DEFINICIÓN DE NIVELES DE SERVICIO

1.1 Marco de Referencia para el Convenio de Nivel de Servicio

OBJETIVO DE CONTROL

La alta gerencia deberá establecer un marco de referencia en donde presente la definición de los convenios sobre niveles formales de servicio y determine el contenido mínimo: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia/Recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio. Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos. El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y la cantidad de servicios ofrecida y los usuarios deberán ajustar los servicios solicitados a los límites acordados.

1.2 Aspectos sobre los Convenios de Nivel de Servicio

OBJETIVO DE CONTROL

Deberá lograrse un acuerdo explícito sobre los aspectos que el convenio de nivel de servicios deberá tener. El convenio de nivel de servicio deberá cubrir por lo menos los siguientes aspectos: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados a los usuarios, plan de contingencia/ Recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambios

1.3 Procedimientos de Desempeño

OBJETIVO DE CONTROL

Deberán definirse procedimientos que aseguren que la manera y responsabilidades sobre las relaciones que rigen el desempeño (por ejemplo, convenios de confidencialidad) entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

1.4 Monitoreo y Reporte

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá designar a un Gerente de nivel de servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

1.5 Revisión de Convenios y Contratos de Nivel de Servicio

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de servicios como terceras partes.

1.6 Elementos sujetos a Cargo

OBJETIVO DE CONTROL

Deberán incluirse provisiones para elementos sujetos a cargo en los acuerdos de niveles de servicio para hacer posible comparaciones y decisiones de niveles de servicio contra su costo.

1.7 Programa de Mejoramiento del Servicio

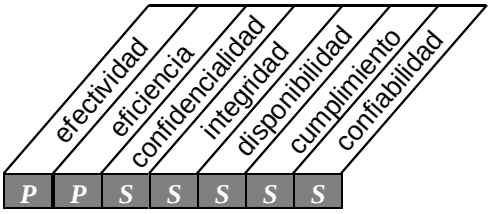
OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso para asegurar que los usuarios y los Gerentes de nivel de servicio concuerden regularmente en un programa de mejoramiento del servicio con el fin de dar seguimiento a mejoras al nivel de servicio cuyo costo esté justificado.

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:

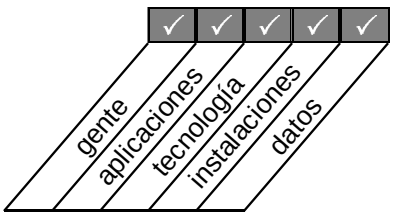
asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

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



2 ADMINISTRACIÓN DE SERVICIOS PRESTADOS POR TERCEROS[41]

2.1 Interfases con Proveedores

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todos los servicios prestados por terceros sean propiamente identificados y que las interfaces técnicas y organizacionales con los proveedores sean documentadas.

2.2 Relaciones de Dueños[42]

Objetivos de Control

La Gerencia de la organización del cliente deberá designar un dueño que sea responsable de asegurar la calidad de las relaciones con terceros.

2.3 Contratos con Terceros

OBJETIVO DE CONTROL

La gerencia debe definir procedimientos específicos para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con un proveedor.

2.4 Calificación de Terceros

OBJETIVO DE CONTROL

La gerencia debe asegurar en forma previa a su selección, que los terceros potenciales cuentan con las calificaciones adecuadas a través de una evaluación de su capacidad para proporcionar los servicios requeridos[43].

2.5 Contratos con Fuentes Externas[44]

OBJETIVO DE CONTROL

Deberán definirse procedimientos organizacionales específicos para asegurar que el contrato entre la organización y el proveedor de la administración de instalaciones esté basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

2.6 Continuidad de Servicios

OBJETIVO DE CONTROL

Con respecto al aseguramiento de la continuidad de los servicios, la gerencia deberá considerar el riesgo de negocios relacionado con la participación de terceros en términos de incertidumbre legal y con el concepto de interés sobre la continuidad[45] y negociar contratos en depósito[46].

2.7 Relaciones de Seguridad

OBJETIVO DE CONTROL

Con respecto a las relaciones con los proveedores de servicios como terceras partes, la Gerencia deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de no - revelación) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en línea con los requerimientos legales y regulatorios, incluyendo obligaciones.

2.8 Monitoreo

OBJETIVO DE CONTROL

La Gerencia deberá establecer un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

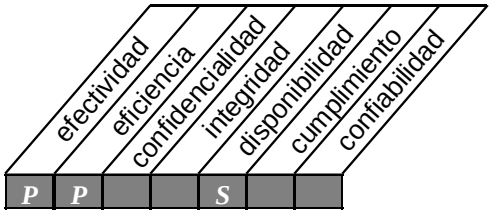
---

41 **Terceros** (*third party*)
42 **Dueños** (*owners*)
43 **Capacidad de proporcionar el servicio** (*due dilligence)*
44 ***Fuentes* externas** (outsourcers)
45 **Concepto de interés sobre la continuidad** (*going concern concept*)
46 **Contrato en depósito** (*scrow contract*) contratos que se celebran para garantizar la continuidad del servicio aun cuando el proveedor no pueda proporcionarlo.

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:

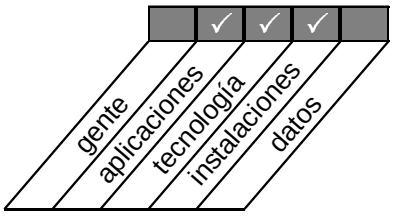
asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado

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



3 ADMINISTRACIÓN DE DESEMPEÑO Y CAPACIDAD

3.1 Requerimientos de Disponibilidad y Desempeño

OBJETIVO DE CONTROL

El proceso de administración deberá asegurar que las necesidades de negocio con respecto a disponibilidad y desempeño de los servicios de información sean identificados y convertidas en requerimientos y términos de disponibilidad.

3.2 Plan de Disponibilidad

OBJETIVO DE CONTROL

La Gerencia deberá asegurar el establecimiento de un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.

3.3 Monitoreo y Reporte

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso que asegure que el desempeño de los recursos de tecnología de información sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

3.4 Herramientas de Modelado

OBJETIVO DE CONTROL

La gerencia deberá asegurar que se utilicen las herramientas de modelado apropiadas para producir un modelo del sistema actual, calibrado y ajustado según la carga de trabajo real y que sea preciso dentro de los niveles de carga recomendados. Las herramientas de modelado deberán utilizarse para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad. Deberán llevarse a cabo investigaciones técnicas profundas sobre el hardware de los sistemas y deberán incluirse pronósticos acerca de futuras tecnologías.

3.5 Manejo Proactivo del Desempeño

OBJETIVO DE CONTROL

El proceso de administración del desempeño deberá incluir la capacidad de pronóstico para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado del impacto y magnitud del daño.

3.6 Pronóstico de Carga de Trabajo

OBJETIVO DE CONTROL

Deberán establecerse controles para asegurar que se preparen pronósticos de carga de trabajo con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad[47].

3.7 Administración de Capacidad de Recursos

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá establecer un proceso de planeación para la revisión del desempeño y capacidad del hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas, prescritas en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

3.8 Disponibilidad de Recursos

OBJETIVO DE CONTROL

La gerencia deberá prevenir que se pierda la disponibilidad de los recursos, mediante la implementación de mecanismos de tolerancia de fallas, mecanismos de asignación equitativa de recursos y la definición de prioridades de tareas.

3.9 Calendarización de Recursos

OBJETIVO DE CONTROL

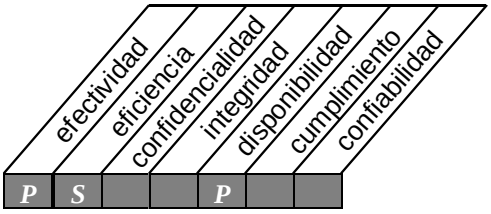
La Gerencia deberá asegurar la adquisición oportuna de la capacidad requerida, tomando en cuenta aspectos como resistencia, contingencia, cargas de trabajo y planes de almacenamiento.

[47] **Plan de capacidad** (*capacity planning*)

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:

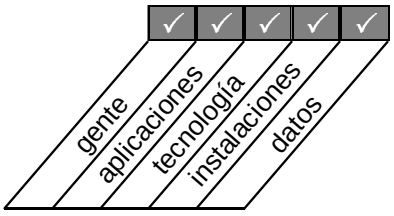
mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones

se hace posible a través de:

teniendo un plan de continuidad probado y funcional, que esté 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



4 ASEGURAR LA CONTINUIDAD DEL SERVICIO

4.1 Marco de Referencia de Continuidad de Tecnología de información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá crear un marco de referencia de continuidad que defina los roles, responsabilidades, el enfoque basado en riesgo /la metodología a seguir y las reglas y la estructura para documentar el plan, así como los procedimientos de aprobación.

4.2 Estrategia y Filosofía de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia deberá garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa para asegurar consistencia. Aún más, el plan de continuidad de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.

4.3 Contenido del Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se desarrolle un plan escrito conteniendo lo siguiente:

- Guías sobre la utilización del Plan de Continuidad;
- Procedimientos de emergencia para asegurar la integridad de todo el personal afectado;
- Procedimientos de respuesta definidos para regresar al negocio al estado en que se encontraba antes del incidente o desastre;
- Procedimientos para salvaguardar y reconstruir las instalaciones;
- Procedimientos de coordinación con las autoridades públicas;
- Procedimientos de comunicación con los interesados: empleados, clientes clave, proveedores críticos, accionistas y gerencia; y
- Información crítica sobre grupos de continuidad, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.

4.4 Minimización de requerimientos de Continuidad de Tecnología de Información.

OBJETIVO DE CONTROL

La Gerencia de servicios de información deberá establecer procedimientos y guías para minimizar los requerimientos de continuidad con respecto a personal, instalaciones, hardware, software, equipo, formatos, consumibles y mobiliario.

4.5 Mantenimiento Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de servicios de información deberá proveer procedimientos de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja requerimientos de negocio actuales.

Esto requiere de procedimientos de mantenimiento del plan de continuidad alineados con el cambio, la administración y los procedimientos de recursos humanos.

4.6 Pruebas del Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

Para contar con un Plan efectivo de Continuidad, la gerencia necesita evaluar su adecuación de manera regular; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.

4.7 Capacitación sobre el Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La metodología de Continuidad para desastres deberá asegurar que todas las partes interesadas reciban sesiones de entrenamiento regulares con respecto a los procedimientos a ser seguidos en caso de un incidente o un desastre.

4.8 Distribución del Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

Debido a la naturaleza sensitiva de la información del plan de continuidad, dicha información deberá ser distribuida solo a personal autorizado y mantenerse bajo adecuadas medidas de seguridad para evitar su divulgación. Consecuentemente, algunas secciones del plan deberán ser distribuidas solo a las personas cuyas actividades hagan necesario conocer dicha información.

4.9 Procedimientos de respaldo de procesamiento para Departamentos usuarios

OBJETIVO DE CONTROL

La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.

4.10 Recursos Críticos de Tecnología de Información

OBJETIVO DE CONTROL

El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre.

4.11 Centro de cómputo[48] y Hardware de Respaldo

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la metodología de continuidad incorpora la identificación de alternativas relativas al centro de cómputo y al hardware de respaldo, así como una selección alternativa final. En caso de aplicar, deberá establecerse un contrato formal para este tipo de servicios.

4.12 Procedimiento de refinamiento del Plan de Continuidad

OBJETIVO DE CONTROL

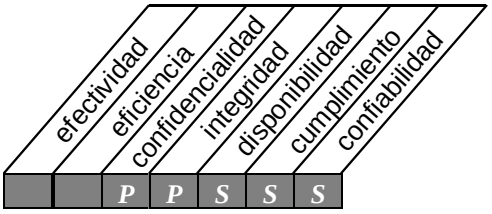
Dada una exitosa reanudación de la función de servicios de información después de un desastre, la gerencia de servicios de información deberá establecer procedimientos para evaluar lo adecuado del plan y actualizarlo de acuerdo con los resultados de dicha evaluación.

[48] **Centro de cómputo** (*site*)

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:

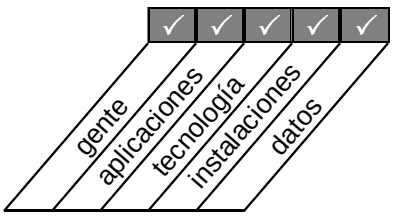
salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

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*



5 GARANTIZAR LA SEGURIDAD DE SISTEMAS

5.1 Administrar Medidas de Seguridad

OBJETIVO DE CONTROL

La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye:

- traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología;
- implementar el plan de seguridad de tecnología de información;
- actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología;
- evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información;
- monitorear la implementación del plan de seguridad de tecnología de información; y
- alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos

5.2 Identificación, Autenticación y Acceso

OBJETIVO DE CONTROL

El acceso lógico y el uso de los recursos de TI deberá restringirse a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas de marcado[49] y otros puertos de entrada del sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá minimizar la necesidad de firmas de entrada[50] múltiples a ser utilizadas por usuarios autorizados. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).

5.3 Seguridad de Acceso a Datos en Línea

OBJETIVO DE CONTROL

En un ambiente de tecnología de información en línea, la Gerencia de la función de servicios de información deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

5.4 Administración de Cuentas de Usuario

OBJETIVO DE CONTROL

La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

5.5 Revisión Gerencial de Cuentas de Usuario

OBJETIVO DE CONTROL

La Gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

5.6 Control de Usuarios sobre Cuentas de Usuario

OBJETIVO DE CONTROL

Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

5.7 Vigilancia de Seguridad

OBJETIVO DE CONTROL

La administración de seguridad de la función de servicios de información debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

[49] **Marcado** (*dial up*)
[50] **Firmas de entrada** (*sign-on*)

5.8 Clasificación deDatos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran "no protección" deberán contar con una decisión formal que les asigne dicha clasificación.

5.9 Clasificación de Datos

OBJETIVO DE CONTROL

Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

5.10 Reportes de Violación y de Actividades de Seguridad

OBJETIVO DE CONTROL

La administración de la función de servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo[51] (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

5.11 Manejo de Incidentes

OBJETIVO DE CONTROL

La Gerencia deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

5.12 Reacreditación

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se lleve a cabo periódicamente una reacreditación de seguridad por ejemplo, a través de equipos de personal técnico *"tigre"*[52] con el fin de conservar al día el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.

5.13 Confianza en Contrapartes

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que se instrumenten prácticas de control para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas. Esto puede lograrse mediante el intercambio confiable de passwords, dispositivos de seguridad[53] o llaves criptográficas.

5.14 Autorización de transacciones

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que, en donde sea apropiado, sean instrumentados controles para proporcionar autenticidad de transacciones. Esto requiere el empleo de técnicas criptográficas para "firmar" y verificar tran-

[51] **Registro de recursos de cómputo** (*accountability*)

[53] **Equipo "tigre"** (*Tiger team*): es un grupo de personal técico al cual se le asignan trabajos de verificación de seguridad en una instalación. Estos trabajos consisten tipicamente en actuar en forma incógnita y tratar de violar las medidas de seguridad establecidas para probar la inefectividad de las mismas e identificar las áreas vulnerables que requiren atención.

sacciones.

5.15 No negación

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes y que se instrumenten controles para proporcionar no negación (*non repudiation*) de origen o destino, prueba de envío (*proof of submission*), y recibo de transacciones. Esto puede ser implementado a través de firmas digitales, registro de tiempos y terceros confiables.

5.16 Sendero Seguro

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (*trusted paths*). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

5.17 Protección de funciones de seguridad

OBJETIVO DE CONTROL

Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

5.18 Administración de Llaves Criptográficas

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas contra modificaciones y divulgación no autorizada. Si una llave se encuentra comprometida (en riesgo), la gerencia deberá asegurarse de que esta información se hace llegar a todas las partes interesadas a través de un listado de revocación de certificados o mecanismos similares.

5.19 Prevención, Detección y Corrección de Software "Malicioso"

OBJETIVO DE CONTROL

Con respecto al software malicioso, tal como los virus computacionales o *Caballos de Troya*, la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

5.20 Arquitectura de *Fire Walls* y conexión a redes públicas

OBJETIVO DE CONTROL

Si existe conexión con Internet u otras redes públicas en la organización. Se deberá contar con sistemas *Fire Wall* adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.

5.21 Protección de Valores Electrónicos

OBJETIVO DE CONTROL

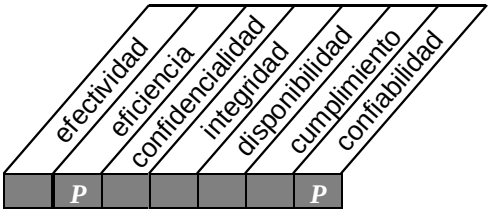
La Gerencia debe proteger consistentemente la integridad de todas las tarjetas o dispositivos físicos similares, que son utilizados para autenticación o almacenamiento de información financiera u otra información sensitiva, tomando en consideración las instalaciones relacionadas, dispositivos, empleados y métodos de validación utilizados.

[53] **Dispositivos** (*tokens*)

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:

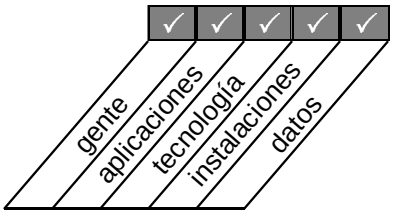
asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

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



6 IDENTIFICACIÓN Y ASIGNACIÓN DE COSTOS

6.1 Elementos Sujetos a Cargo[54]

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los usuarios. Los usuarios deberán ser capaces de controlar el uso de los servicios de información y de los niveles de facturación asociados.

6.2 Procedimientos de Costeo

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir e implementar procedimientos de costeo para proporcionar información gerencial acerca del costo de prestar servicios de información, asegurando al mismo tiempo la economía. Las variaciones entre los costos pronosticados y los reales deberán ser analizadas adecuadamente y reportados, con el fin de facilitar el monitoreo de los mismos. Además, la alta gerencia deberá evaluar periódicamente los resultados de los procedimientos de contabilidad de costos de la función de servicios de información, a la luz de los otros sistemas de medición financiera de la organización.

6.3 Procedimientos de Cargo[54] y Facturación a Usuarios

OBJETIVO DE CONTROL

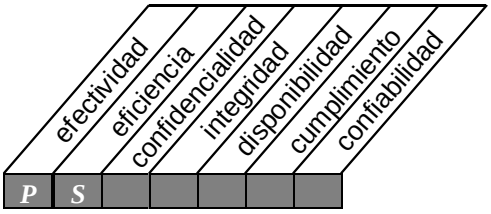
La Gerencia de la función de servicios de información deberá definir y utilizar procedimientos de cargo y facturación. Esta deberá mantener procedimientos de cargo y facturación que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades. El monto cargado deberá reflejar los costos asociados con la prestación de servicios.

[54] **Cargo** (*charge back*)

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:

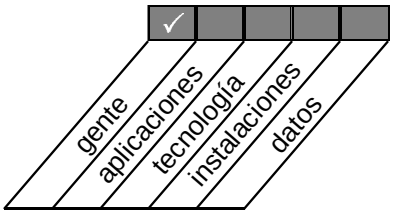
asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados

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



7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS

7.1 Identificación de Necesidades de Entrenamiento

OBJETIVO DE CONTROL

En línea con el plan a largo plazo, la Gerencia deberá establecer y mantener procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información. Deberá establecerse un curriculum de entrenamiento para cada grupo de empleados.

7.2 Organización del Entrenamiento

OBJETIVO DE CONTROL

Tomando como base las necesidades identificadas, la Gerencia deberá definir los grupos objetivo, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento. Asimismo, deberán investigarse las alternativas de entrenamiento (Localidad interna o externa, entrenadores internos o externos, etc.).

7.3 Entrenamiento sobre Principios y Conciencia de Seguridad

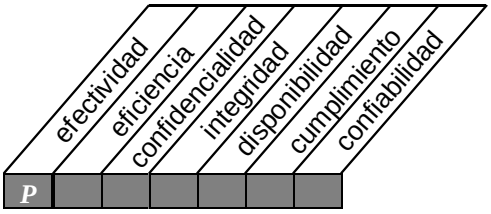
OBJETIVO DE CONTROL

Todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas. La alta gerencia deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de la función de servicios de información, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.

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:

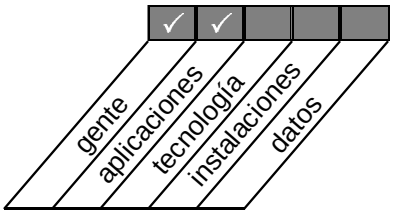
asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

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



[55] **Buró de ayuda** (*help desk*)
[56] **Despacho** (*clearance*)

8 APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN

8.1 Buró de Ayuda

OBJETIVO DE CONTROL

Deberá establecerse un soporte para usuarios dentro de una función de buró de ayuda. Las personas responsables de llevar a cabo esta función deberán interactuar estrechamente con el personal de manejo de problemas.

8.2 Registro de Preguntas del Usuario

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que todas las preguntas de los clientes sean registradas adecuadamente por el buró de ayuda.

8.3 Escalamiento de Preguntas del Cliente

OBJETIVO DE CONTROL

Los procedimientos del buró de ayuda deberán asegurar que las preguntas de los clientes que no puedan ser resueltas inmediatamente sean reasignadas apropiadamente dentro de la función de servicios de información hasta el nivel adecuado para atenderlas.

8.4 Monitoreo de Atención a Clientes

OBJETIVO DE CONTROL

La Gerencia deberá establecer procedimientos para monitorear oportunamente la atención a las preguntas de los clientes. Las preguntas que permanezcan pendientes por largo tiempo deberán ser investigadas y atendidas.

8.5 Análisis y Reporte de Tendencias

OBJETIVO DE CONTROL

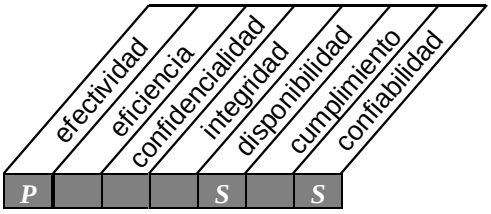
Deberán establecerse procedimientos que aseguren el reporte adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias. Los reportes deberán ser analizados y sus resultados deberán ser atendidos adecuadamente.

[55] **Buró de ayuda** (*help desk*)

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:

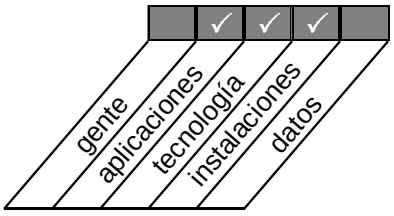
dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

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



9 ADMINISTRACIÓN DE LA CONFIGURACIÓN

9.1 Registro de la Configuración

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo). El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

9.2 Configuración Base

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurarse de que exista una configuración base de elementos como punto de verificación al cual regresar después de las modificaciones.

9.3 Registro de Estatus

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que los registros de configuración reflejen el estatus real de todos los elementos de la configuración incluyendo la historia de los cambios.

9.4 Control de la Configuración

OBJETIVO DE CONTROL

Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de la función de servicios de información sean revisadas periódicamente.

9.5 Software no Autorizado

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización.

9.6 Almacenamiento de Software

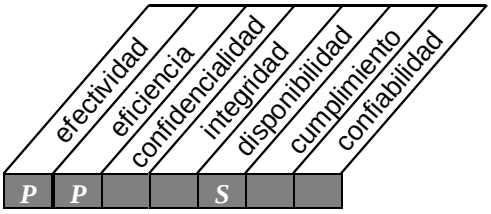
OBJETIVO DE CONTROL

Deberá definirse un área de almacenamiento de archivos (biblioteca) para todos los elementos de software válidos en las fases apropiadas del ciclo de vida de desarrollo de sistemas. Estas áreas deberán estar separadas unas de otras y de las áreas de almacenamiento de archivos de desarrollo, pruebas y producción.

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:

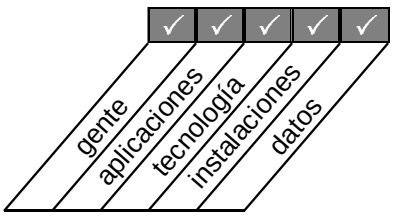
asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia

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



10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES

10.1 Sistema de Administración de Problemas

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir e implementar un sistema de administración de problemas para asegurar que todos los eventos operacionales que no formen parte de la operación estándar (incidentes, problemas y errores) sean registrados, analizados y resueltos oportunamente. Deberán emitirse reportes de incidentes en el caso de problemas significativos.

10.2 Escalamiento de Problemas

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos de escalamiento de problemas para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el procedimiento de escalamiento para la activación del plan de continuidad de tecnología de información.

10.3 Seguimiento de Problemas y Pistas de Auditoría

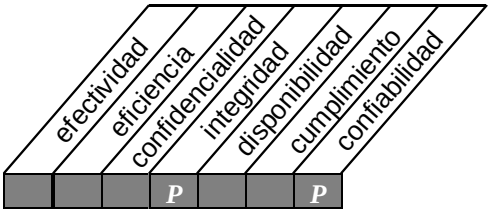
OBJETIVO DE CONTROL

El sistema de administración de problemas deberá proporcionar elementos adecuados para pistas de auditoría que permitan el seguimiento de las causas a partir de un incidente (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

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:

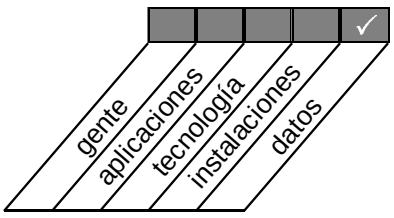
asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento

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



11 ADMINISTRACIÓN DE DATOS

11.1 Procedimientos de Preparación de Datos

OBJETIVO DE CONTROL

La Gerencia deberá establecer procedimientos de preparación de datos a ser seguidos por los departamentos usuarios. En este contexto, el diseño de formas de entrada de datos deberá ayudar a minimizar los errores y las omisiones. Durante la creación de los datos, los procedimientos de manejo de errores deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

11.2 Procedimientos de Autorización de Documentos Fuente

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los documentos fuente sean preparados apropiadamente por personal autorizado que actúa dentro de su autoridad, y que se establezca una separación de funciones adecuada con respecto al origen y aprobación de documentos fuente.

11.3 Recopilación de Datos de Documentos Fuente

OBJETIVO DE CONTROL

Los procedimientos de la organización deberán asegurar que todos los documentos fuente autorizados estén completos, sean precisos, registrados apropiadamente y transmitidos oportunamente para la entrada de datos.

11.4 Manejo de errores de documentos fuente

OBJETIVO DE CONTROL

Los procedimientos de manejo de errores durante la creación de datos deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

11.5 Retención de Documentos Fuente

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que la organización pueda retener o reproducir los documentos fuente originales durante un período de tiempo razonable para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requerimientos legales.

11.6 Procedimientos de Autorización de Entrada de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos apropiados para asegurar que la entrada de datos sea llevada a cabo únicamente por personal autorizado.

11.7 Chequeos de Exactitud, Suficiencia y Autorización

OBJETIVO DE CONTROL

Los datos sobre transacciones, capturados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.

11.8 Manejo de Errores en la Entrada de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.

11.9 Integridad de Procesamiento de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de actualización adecuados como totales de control "corrida a corrida" y controles de actualización de archivos maestros.

11.10 Validación y Edición de Procesamiento de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible. Cuando se utilicen sistemas de Inteligencia Artificial, dichos sistemas serán ubica-

dos en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son aprobadas.

11.11 Manejo de Errores en el Procesamiento de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos de manejo de errores en el procesamiento de datos que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.

11.12 Manejo y Retención de Datos de Salida

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para el manejo y la retención de datos de salida de sus programas de aplicación de tecnología de información. En caso de que instrumentos negociables (ej. tarjetas de valor[58]) sean los receptores de la salida, se deberá poner cuidado especial en prevenir usos inadecuados.

11.13 Distribución de Datos de Salida

OBJETIVO DE CONTROL

La organización deberá establecer y comunicar procedimientos escritos para la distribución de datos de salida de tecnología de información.

11.14 Balanceo y Conciliación de Datos de Salida

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para asegurar que los datos de salida sean balanceados rutinariamente con los totales de control relevantes. Deberán existir pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de los datos con problema.

11.15 Revisión de Datos de Salida y Manejo de Errores

OBJETIVO DE CONTROL

La Gerencia de la organización deberá establecer procedimientos para asegurar que la precisión de los reportes de los datos de salida sea revisada por el proveedor y por los usuarios relevantes. Asimismo, deberán establecerse procedimientos para controlar los errores contenidos en los datos de salida.

11.16 Provisiones de Seguridad para Reportes de Salida

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para garantizar que la seguridad de los reportes de datos de salida sea mantenida para todos aquellos reportes que estén por distribuirse, así como para todos aquéllos que ya hayan sido distribuidos a los usuarios.

11.17 Protección de Información Sensible durante transmisión y transporte

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

11.18 Protección de Información Crítica a Ser Desechada

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos deberán garantizar que ninguna información marcada como “borrada” o “desechada”, pueda ser accedida por personas internas o externas a la organización.

11.19 Administración de Almacenamiento

OBJETIVO DE CONTROL

Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y las políticas de seguridad.

[58] **Tarjetas de valor** (*valor cards*): tarjetas que pueden almacenar valor, talcomo los “monederos electrónicos”.

11.20 Períodos de Retención y Términos de Almacenamiento

OBJETIVO DE CONTROL

Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de entrada y de salida), así como los datos (claves, certificados) utilizados para su encriptamiento y autenticación.

11.21 Sistema de Administración de la Librería de Medios

OBJETIVO DE CONTROL

La función de servicios de información deberá establecer procedimientos para asegurar que el contenido de su librería de medios sea inventariado sistemáticamente, que cualquier discrepancia revelada por un inventario físico sea solucionada oportunamente y que se lleven a cabo las medidas necesarias para mantener la integridad de los medios magnéticos almacenados en la librería.

11.22 Responsabilidades de la Administración de la Librería de Medios

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá establecer procedimientos de administración para proteger el contenido de la librería de medios. Deberán definirse estándares para la identificación externa de medios magnéticos y el control de su movimiento y almacenamiento físico para soportar su seguimiento y registro. Las responsabilidades sobre el manejo de la librerías de medios (cintas magnéticas, cartuchos, discos y diskettes) deberán ser asignadas a miembros específicos del personal de servicios de información.

11.23 Respaldo y Restauración

OBJETIVO DE CONTROL

La Gerencia deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

11.24 Funciones de Respaldo

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

11.25 Almacenamiento de Respaldos

OBJETIVO DE CONTROL

Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

11.26 Archivo

OBJETIVO DE CONTROL

La Gerencia deberá implementar una política y procedimientos para asegurar que el archivo cumple con requerimientos legales y de negocio y que se encuentra debidamente protegido y registrado adecuadamente.

11.27 Protección de Mensajes Sensitivos

OBJETIVO DE CONTROL

Con respecto a la transmisión de datos a través de Internet u otra red pública, la Gerencia deberá definir e implementar procedimientos y protocolos para ser utilizados para el aseguramiento de la integridad, confidencialidad y "no negación" de mensajes sensitivos.

11.28 Autenticación e Integridad

OBJETIVO DE CONTROL

Previamente a que alguna acción crítica sea tomada sobre información originada fuera de la Organización que se reciba vía teléfono, correo de voz, documentos (en papel), fax o correo electrónico, se deberá verificar adecuadamente la autenticidad e integridad de dicha información.

11.29 Integridad de Transacciones Electrónicas

OBJETIVO DE CONTROL

Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, la Gerencia deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, asegurando la integridad y autenticidad de:

- *atomicidad* (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan)
- *consistencia* (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial);
- *aislamiento* (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y
- *durabilidad* (los efectos de una transacción son permanentes después que concluye su proceso[59], los cambios que origina deben sobrevivir fallas de sistema)

11.30 Integridad Continua de Datos Almacenados

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la integridad y lo adecuado de los datos mantenidos en archivos y otros medios (ej. tarjetas electrónicas) se verifique periódicamente. Atención específica deberá darse a dispositivos[60] de valor, archivos de referencia[61] y archivos que contengan información privada.

[59] **Concluye su proceso** (*commits*): se dice de una transacción que actualiza los datos que maneja al concluir su proceso.

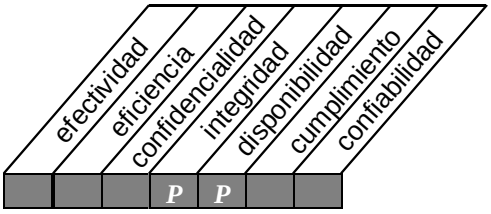
[60] **Dispositivos** (*tokens*)

[61] **Archivos de referencia** (*reference files*)

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:

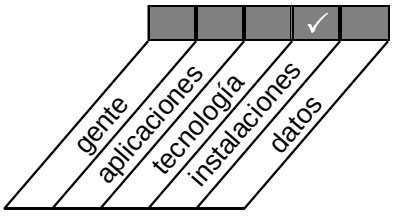
proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas

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



12 ADMINISTRACIÓN DE INSTALACIONES

12.1 Seguridad Física

OBJETIVO DE CONTROL

Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.

12.2 Discreción[62] de las Instalaciones de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones relacionadas con sus operaciones de tecnología de información sea limitada.

12.3 Escolta de Visitantes

OBJETIVO DE CONTROL

Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

12.4 Salud y Seguridad del Personal

OBJETIVO DE CONTROL

Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones internacionales, nacionales, regionales, estatales y locales.

12.5 Protección contra Factores Ambientales

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

12.6 Suministro Ininterrumpido de Energía

OBJETIVO DE CONTROL

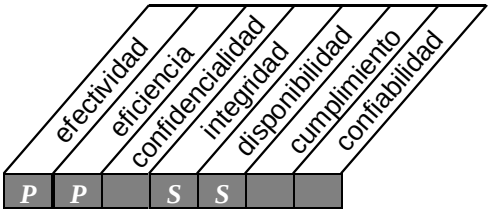
La Gerencia deberá evaluar regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de tecnología de información, con el fin de asegurarse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.

[62] **Discreción** (*low profile*)

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:

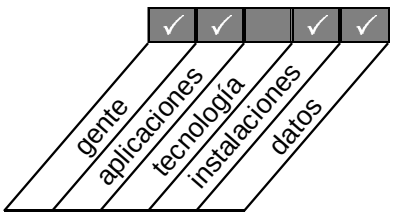
asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada

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



13 ADMINISTRACIÓN DE OPERACIONES

13.1 Manual de procedimientos de Operación e Instrucciones

OBJETIVO DE CONTROL

La función de servicios de información deberá establecer y documentar procedimientos estándar para las operaciones de tecnología de información (incluyendo operaciones de red). Todas las soluciones y plataformas de tecnología de información establecidas deberán ser operadas utilizando estos procedimientos, los cuales deberán ser revisados periódicamente para asegurar su efectividad y cumplimiento.

13.2 Documentación del Proceso de Inicio y de Otras Operaciones

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que el personal de operaciones esté adecuadamente familiarizado y se sienta seguro con las tareas del proceso de inicio y con otras operaciones al tenerlas documentadas y al ser éstas probadas y ajustadas periódicamente según se requiera.

13.3 Calendarización de Trabajos[63]

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que la calendarización continua de trabajos, procesos y tareas sea organizada en la secuencia más eficiente, maximizando el proceso y la utilización, con el fin de alcanzar los objetivos establecidos en los convenios de nivel de servicio. Las caledarizaciones iniciales así como los cambios a estas caledarizaciones deberán ser autorizados apropiadamente.

13.4 Salidas[64] de la Calendarización de Trabajos Estándar

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para identificar, investigar y aprobar las salidas de calendarización de trabajos estándar.

13.5 Continuidad de Procesamiento

OBJETIVO DE CONTROL

Los procedimientos deberán requerir continuidad de procesamiento durante los cambios de turno de operadores mediante la existencia de un paso o entrega formal de actividades, actualizaciones y reportes de estatus sobre las responsabilidades actuales.

13.6 Bitácoras de Operación

OBJETIVO DE CONTROL

Los controles de la Gerencia deberán garantizar que se esté almacenando suficiente información cronológica en bitácoras de operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que lo rodean y soportan.

13.7 Operaciones Remotas

OBJETIVO DE CONTROL

Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la(s) instalación(es) remota(s) sean identificadas e implementadas.

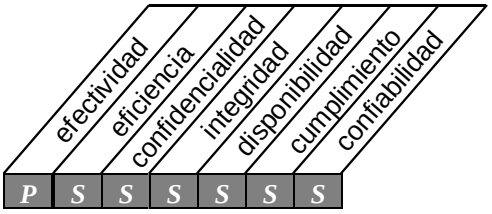
---

[63] **Trabajos** (*jobs*)
[64] **Salidas** (*departures*)

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:

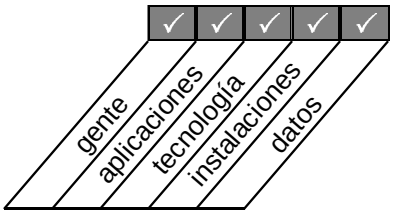
asegurar el logro de los objetivos establecidos para los procesos de TI

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



1 MONITOREO DEL PROCESO

1.1 Recolección de Datos de Monitoreo

OBJETIVO DE CONTROL

Para los procesos de tecnología de información y de control interno, la Gerencia deberá asegurar que se definan indicadores de desempeño relevantes (ej. comparaciones externas) tanto para actividades internas como las proporcionadas por terceros y que se recolecten datos para la creación de reportes relevantes de desempeño y reportes de excepción relacionados con estos indicadores.

1.2 Evaluación de Desempeño

OBJETIVO DE CONTROL

Los servicios a ser proporcionados por la función de servicios de información deberán ser medidos (indicadores clave de desempeño y/o factores críticos de éxito) y comparados con los niveles objetivo. Las evaluaciones a la función de servicios de información deberán ser desarrolladas en forma continua.

1.3 Evaluación de la satisfacción de Clientes

OBJETIVO DE CONTROL

A intervalos regulares, la Gerencia deberá efectuar mediciones de la satisfacción de los clientes con respecto a los servicios proporcionados por la función de servicios de información, con la intención de identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento.

1.4 Reportes Gerenciales

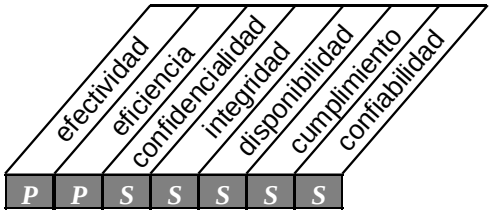
OBJETIVO DE CONTROL

Deberán proporcionarse reportes gerenciales para ser revisados por la alta gerencia en cuanto al avance de la organización hacia las metas identificadas. Con base en la revisión, la Gerencia deberá iniciar y controlar las acciones pertinentes.

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:

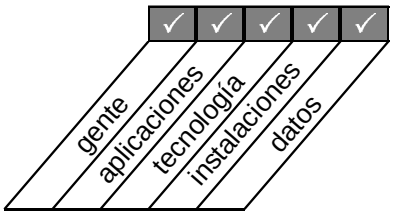
asegurar el logro de los objetivos de control interno establecidos para los procesos de TI

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



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

2 EVALUAR LO ADECUADO DEL CONTROL INTERNO

2.1 Monitoreo de Control Interno

OBJETIVO DE CONTROL

La Gerencia deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

2.2 Operación Oportuna de Controles Internos

OBJETIVO DE CONTROL

La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la Gerencia.

2.3 Reporte sobre el Nivel de Control Interno

OBJETIVO DE CONTROL

La Gerencia deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

2.4 Seguridad de Operación y Aseguramiento de Control Interno

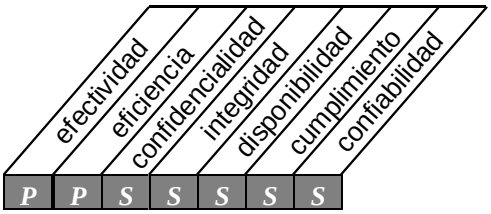
OBJETIVO DE CONTROL

La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos a través de una "autoauditoría" o de una auditoría independiente para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

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:

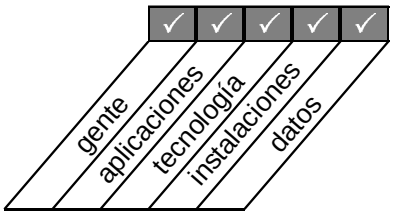
incrementar los niveles de confianza entre la organización, clientes y proveedores externos

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



3 OBTENCIÓN DE ASEGURAMIENTO INDEPENDIENTE

3.1 Certificación / Acreditación Independiente de Control y Seguridad de los servicios de TI

OBJETIVO DE CONTROL

La Gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos y obtener re-certificaciones o re-acreditaciones de estas actividades en forma una cíclica rutinaria después de haber hecho la implementación.

3.2 Certificación / Acreditación Independiente de Control y Seguridad de proveedores externos de servicios

OBJETIVO DE CONTROL

La Gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de utilizar proveedores de servicios de tecnología de información y obtener re-certificaciones o re-acreditaciones de estas actividades en forma cíclica rutinaria.

3.3 Evaluación Independiente de la Efectividad de los Servicios de TI

OBJETIVO DE CONTROL

La Gerencia deberá obtener una evaluación independiente sobre la efectividad de los servicios de tecnología de información en forma cíclica rutinaria.

3.4 Evaluación Independiente de la Efectividad de proveedores externos de servicios

OBJETIVO DE CONTROL

La Gerencia deberá obtener una evaluación independiente sobre la efectividad de los proveedores de servicios de tecnología de información en forma cíclica rutinaria.

3.5 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales

OBJETIVO DE CONTROL

La Gerencia deberá obtener un aseguramiento independiente sobre el cumplimiento de la función de servicios de tecnología de información con respecto a requerimientos regulatorios y compromisos contractuales en forma cíclica rutinaria.

3.6 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales de proveedores externos de servicios

OBJETIVO DE CONTROL

La Gerencia deberá obtener un aseguramiento independiente sobre el cumplimiento de proveedores externos de servicios de tecnología de información con respecto a requerimientos regulatorios y compromisos contractuales en forma cíclica rutinaria.

3.7 Competencia de la Función de Aseguramiento Independiente

OBJETIVO DE CONTROL

La Gerencia deberá asegurarse de que la función de aseguramiento independiente posee competencia técnica, habilidades y conocimiento necesario para desempeñar dicha función en una forma efectiva, eficiente y económica.

3.8 Participación Proactiva de Auditoría

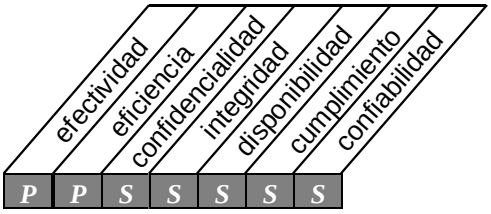
OBJETIVO DE CONTROL

La Gerencia de Tecnología de Información deberá buscar la participación de auditoría en una forma proactiva, antes de finalizar soluciones de servicio de tecnología de información.

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:

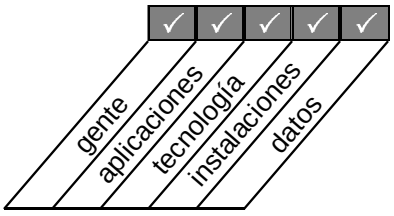
incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas

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



4 PROVEER AUDITORÍA INDEPENDIENTE

4.1 Estatutos[66] de Auditoría

OBJETIVO DE CONTROL

La alta gerencia de la organización deberá establecer los estatutos para la función de auditoría. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoría. Asimismo este documento deberá ser revisado periódicamente para asegurar que se mantengan la independencia, autoridad y responsabilidad de la función de auditoría.

4.2 Independencia

OBJETIVO DE CONTROL

El auditor deberá ser independiente del auditado tanto en actitud como en apariencia (real y percibida). Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa. De esta manera, la función de auditoría deberá ser suficientemente independiente del área auditada para concluir una auditoría en forma objetiva.

4.3 Etica y Estándares Profesionales

OBJETIVO DE CONTROL

La función de auditoría deberá asegurar el cumplimiento de los códigos aplicables de ética profesional (ej. Código de Etica de la *Information Systems Audit and Control Association*) y estándares de auditoría (ej. Estándares de la *Information Systems Audit and Control Association*) en todo lo que lleve a cabo. El debido cuidado profesional deberá observarse en todos los aspectos del trabajo de auditoría, incluyendo el respeto de estándares aplicables sobre auditoría y tecnología de información.

4.4 Competencia

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los auditores responsables de las revisiones de las actividades de la función de servicios de información de la organización, sean técnicamente competentes y cuentan en forma general con las habilidades y conocimientos (ej. dominios de CISA[68]) necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica. La Gerencia deberá asegurar que el personal asignado[68] a tareas de auditoría de sistemas de información, mantiene su nivel de competencia técnica mediante un programa adecuado de educación profesional continua.

4.5 Planeación

OBJETIVO DE CONTROL

La alta gerencia deberá establecer un plan de auditoría para garantizar que se obtenga un aseguramiento regular e independiente con respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno, así como de la habilidad de la Gerencia para controlar las actividades de la función de servicios de información. Dentro de este plan la Gerencia deberá determinar las prioridades relacionadas con la obtención de aseguramiento independiente. Los auditores deberán planear el trabajo de auditoría para alcanzar los objetivos de auditoría y cumplir con los estándares profesionales correspondientes.

4.6 Ejecución del Trabajo de Auditoría

OBJETIVO DE CONTROL

Las auditorías deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoría están siendo alcanzados y que los estándares profesionales de auditoría que sean aplicables están siendo observados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil para alcanzar los objetivos de auditoría de forma efectiva. Los hallazgos y conclusiones de auditoría deben estar soportadas por un análisis apropiado y una correcta interpretación de esta evidencia.

---

[66] **Estatutos** (*charter*)

[67] **CISA**: es un acrónimo para el titulo de *Certified Information Systems Auditor* (auditor certificado de sistemas de información).

[68] **Personal asignado** (*staff*)

4.7 Reporte

OBJETIVO DE CONTROL

La función de auditoría de la organización deberá proporcionar un reporte en un formato adecuado, para todo el personal interesado una vez concluida su revisión. El reporte de auditoría deberá mostrar los objetivos de la auditoría, el período de cobertura y la naturaleza y extensión de trabajo de auditoría realizado. El reporte deberá identificar a la Organización, los destinatarios del informe y cualquier restricción en su circulación. El reporte de auditoría deberá también mostrar los hallazgos, conclusiones y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo, así como cualquier salvedad o comentario que el auditor tenga con respecto a la auditoría.

4.8 Actividades de Seguimiento

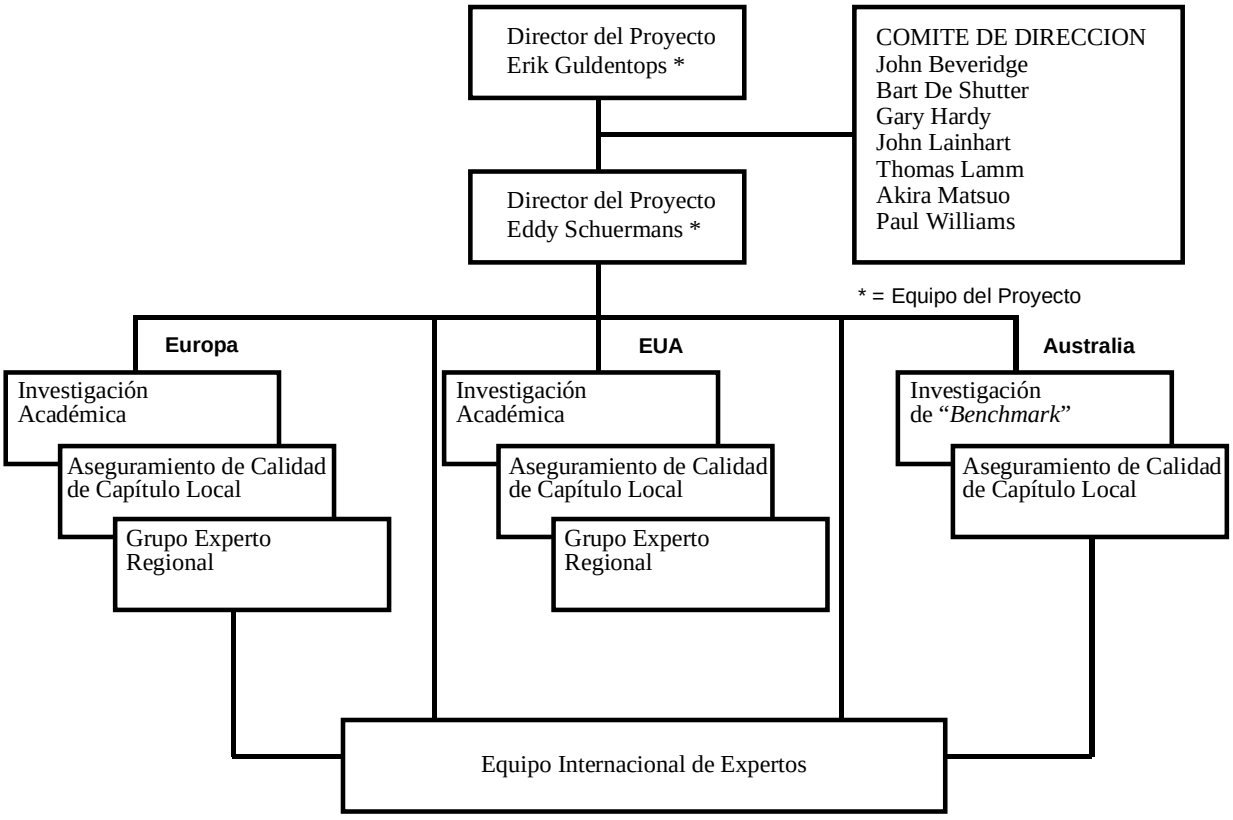
OBJETIVO DE CONTROL

La resolución acerca de los comentarios sobre la auditoría depende de la Gerencia. Los auditores deberán solicitar y evaluar información pertinente sobre hallazgos, conclusiones y recomendaciones previos para determinar si las acciones apropiadas han sido implementadas de manera oportuna.

APÉNDICE I – DESCRIPCIÓN DEL PROYECTO COBIT

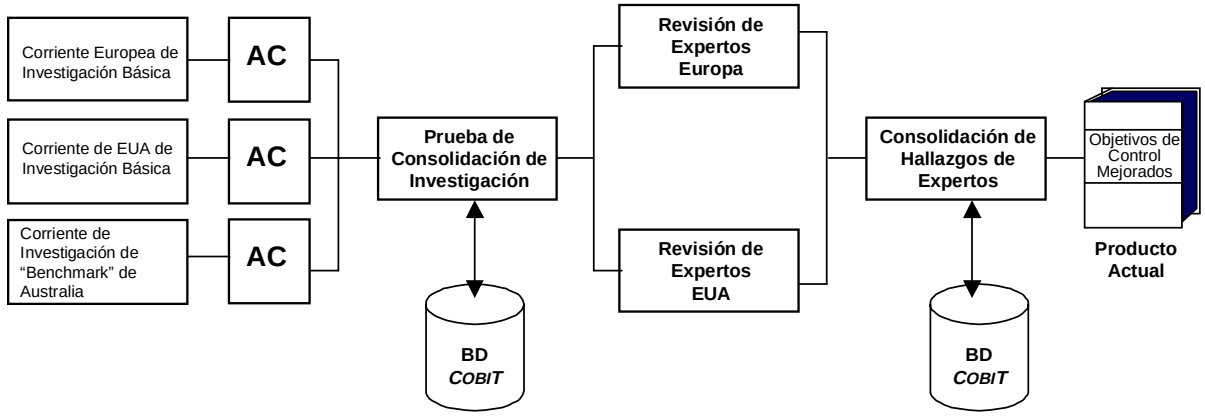
ORGANIZACION & RESPONSABILIDADES
El proyecto ha sido supervisado por un Comité de Dirección formado por representantes internacionales de la academia, industria, gobierno y la profesión de auditoría. La dirección global del proyecto fue proporcionada por el Consejo Directivo de ISACA. El Comité de Dirección 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.

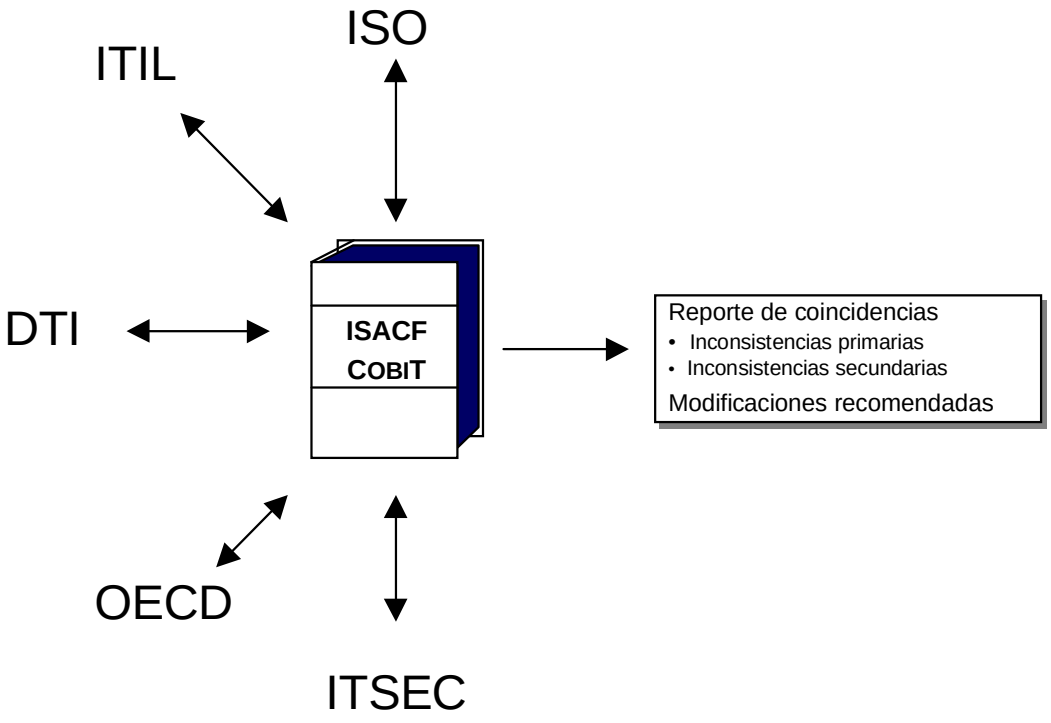


La consolidación de los resultados fue llevada a cabo primordialmente por el Equipo de Proyectos, compuesto por el Director de Proyectos, el Gerente de Proyectos y el Director de Investigaciones de ISACF.

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).



APÉNDICE 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.

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.

APÉNDICE 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*)

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)