

COBIT®

DIRECTRICES DE AUDITORIA

Abril de 1998
2da Edición

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

La Misión de COBIT:

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

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

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

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

Information Systems Audit and Control Association es una organización global líder de profesionales que representa a individuos en más de 100 países y comprende de todos los niveles de la tecnología de información ¾ Dirección ejecutiva, media gerencia y practicantes. La Asociación está únicamente posesionada para cubrir el papel de generador central que armoniza los estándares de las prácticas de control de la TI a nivel mundial. Sus alianzas estratégicas con otros grupos dentro del ámbito profesional financiero, contable, de auditoría y de la TI aseguran un nivel sin paralelo de integración y compromiso a los dueños del proceso de negocio.

Programas y Servicios de la Asociación

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

- *su programa de certificación (el Auditor de Sistemas de Información Certificado) es la única designación global en toda la comunidad de control y auditoría de la TI.*
- *las actividades estándares establecen la base de calidad mediante la cual otras actividades de control y auditoría de la TI se miden.*

- *su programa de educación profesional ofrece conferencias técnicas y administrativas en cinco continentes, así como seminarios en todo el mundo para ayudar a los profesionistas de todo el mundo a recibir educación continua de alta calidad.*
- *su área de publicidad técnica proporciona materiales de desarrollo profesional y referencias con el fin de aumentar su distinguida selección de programas y servicios.*

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

Para más Información

Para recibir información adicional, puede llamar al (+1.847.253.1545), enviar un e-mail a (research@isaca.org) o visitar nuestra página (www.isaca.org).

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

CONTENIDO

Reconocimientos	4-5
Resumen Ejecutivo	7-8
Antecedentes	9-10
El Marco Referencial de COBIT	
Estableciendo la escena.....	11-13
Los Principios del Marco Referencial.....	14-18
Guía para la utilización del Marco Referencial y Objetivos de Control.....	19-20
Tabla Resumen	21
Introducción a los Lineamientos de Auditoría	
Lineamiento General de Auditoría	28
Lineamientos de Auditoría	33
Planeación y Organización.....	35-86
Adquisición e Implementación.....	87-118
Entrega de Servicios y Soporte.....	119-188
Monitoreo.....	189-204
Apéndice I	
Lista de Dominios, Procesos y Objetivos de Control.....	205-209
Apéndice II	
Material de Referencia Primaria.....	210-211
Apéndice III	
Glosario de Términos.....	212
Apéndice IV	
Proceso de Auditoría.....	213-216
Apéndice V	
Cumplimiento del Año 2000.....	217-219
Índice	220-222

Límite de Responsabilidad

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

Acuerdo de Licencia (disclosure)

Copyright 1996, 1998 de la *Information Systems Audit and Control Foundation (ISACF)*. La reproducción para fines comerciales no está permitida sin el previo consentimiento por escrito de la ISACF. Se otorga permiso para reproducir el Resumen Ejecutivo, el Marco Referencial y los Objetivos de Control para uso interno no comercial, incluyendo almacenamiento en medios de recuperación de datos y transmisión en cualquier medio, incluyendo electrónico, mecánico, grabado u otro medio. Todas las copias del Resumen Ejecutivo, el Marco Referencial y los Objetivos de Control deben incluir el siguiente reconocimiento y leyenda de derechos de autor:

Copyright 1996, 1998 *Information Systems Audit and Control Foundation, reimpreso con la autorización de la Information Systems Audit and Control Foundation*. Ningún otro derecho o permiso relacionado con esta obra es otorgado.

Las Directrices de Auditoría y el conjunto de herramientas de implementación no pueden ser reproducidos, almacenados en un sistema de recuperación de datos o transmitido en ninguna forma ni por ningún medio – electrónico, mecánico, fotocopiado, grabado u otro medio– sin la previa autorización por escrito de la ISACF.

Excepto por lo indicado, no se otorga ningún otro derecho o permiso relacionado con esta obra.

Traducido al español de COBIT 2^{da} 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: +1.847.253.1545

Fax: +1.847.253.1443

E-mail: research@isaca.org

Website: www.isaca.org

ISBN 0-9629440-6-8 (Audit Guidelines, English)

RECONOCIMIENTOS

PRINCIPALES PATROCINADORES DE LA CORPORACIÓN A NIVEL MUNDIAL



UNITECH SYSTEMS, Inc.
Information Integrity Specialists



**Coopers
& Lybrand**



PATROCINADORES DE LOS ASOCIADOS DE LA CORPORACIÓN

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

PRINCIPALES CAPÍTULOS DE ISACA PATROCINADORES

Benelux
National Capital Area
New York Metropolitan
Norway
Toronto

CAPÍTULOS DE ISACA ASOCIADOS PATROCINADORES

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

CONTRIBUCIONES INDIVIDUALES

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

RECONOCIMIENTOS

EL EQUIPO DEL PROYECTO

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

COMITÉ QUE DIRIGE EL PROYECTO

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

INVESTIGADORES

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

ANALISTAS EXPERTOS —EUROPA

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

ANALISTAS EXPERTOS —USA

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

CALIDAD GARANTIZADA

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

AGRADECIMIENTO ESPECIAL a los miembros de la Mesa directiva de la Information Systems Audit and Control Association, y los Fideicomisarios de la Information Systems Audit and Control Foundation por su continuo y firme apoyo a la familia de productos de COBIT

RESUMEN EJECUTIVO

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

- la creciente dependencia en información y en los sistemas que proporcionan dicha información
- la creciente vulnerabilidad y un amplio espectro de amenazas, tales como las “ciber amenazas” y la guerra de información
- 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*, 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 por usuarios y auditores, sino que en forma más importante, esta diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y apoderamiento 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 y Diagnóstico de Control en TI) 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 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 esta 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.

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.

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

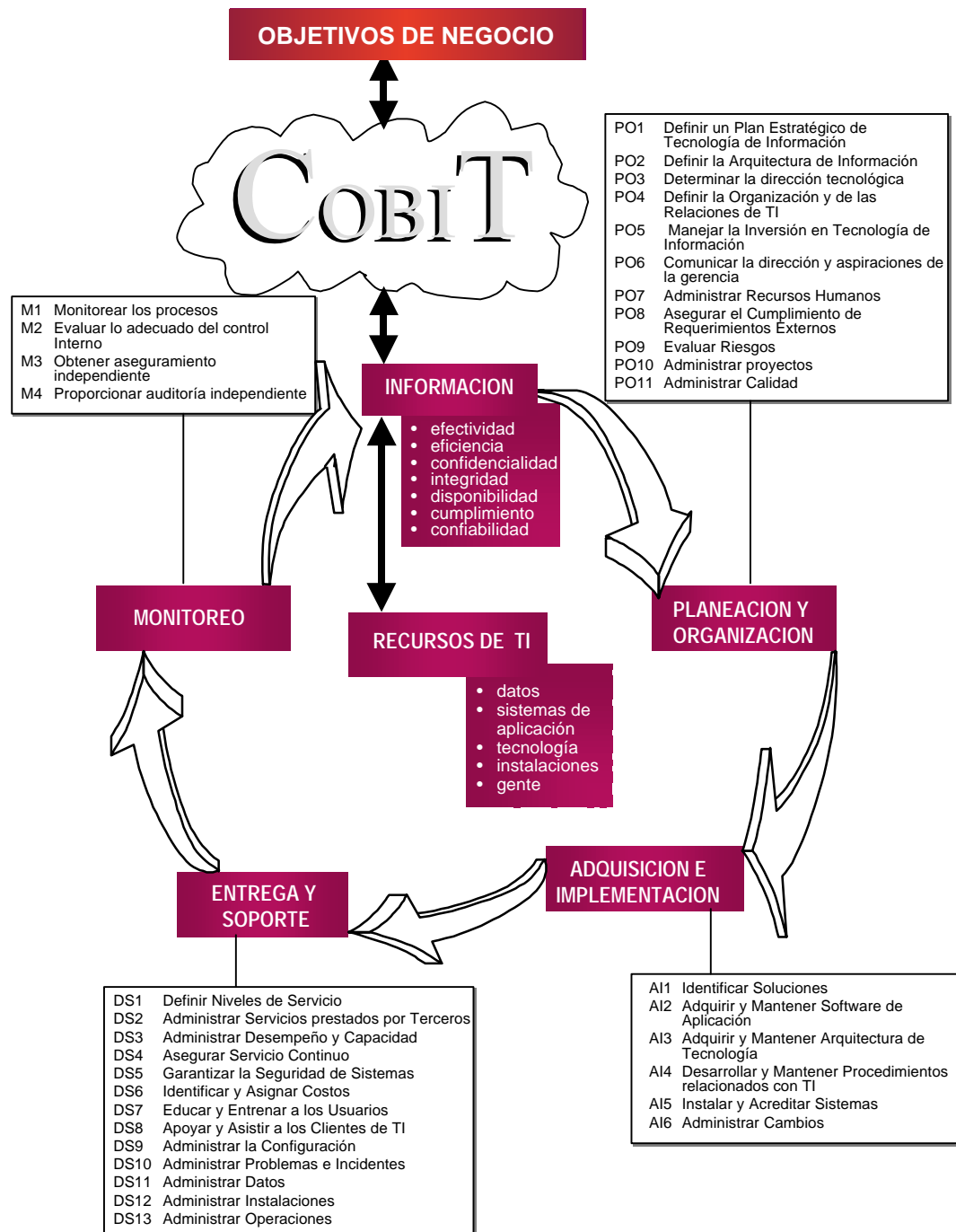
⁴ **Apoderamiento (empowerment)**

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 DOMINIOS



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 gobierno⁸ 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 publicación de:

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

ANTECEDENTES, *continúa*

- **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 Gerencia⁹ y el Diagnóstico de Control de TI¹⁰ – 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.

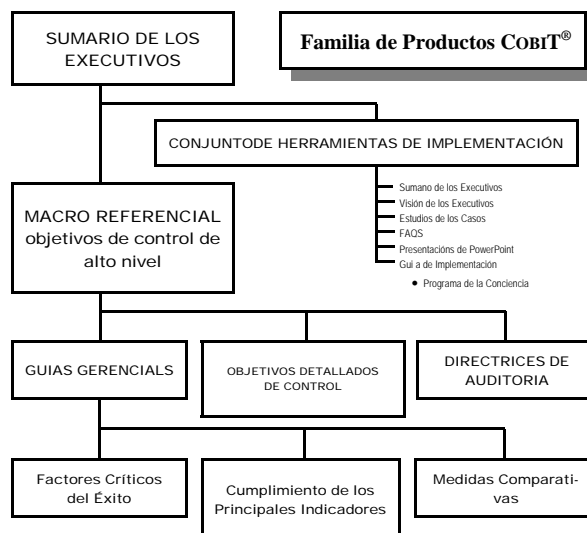
EVOLUCIÓN DEL PRODUCTO COBIT

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 Gerenciales¹¹ que incluyen Factores Críticos de Éxito, Indicadores Clave de Desempeño y Medidas Comparativas¹². 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 Éxito 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 TECNOLOGÍA DE INFORMACIÓN

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 “ciberspacio” 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 cuan-

to 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 negocios, las reestructuraciones, el *outsourcing*, las organizaciones horizontales y el procesamiento distribuido son cambios que impactan la manera en la que operan tanto los negocios como las entidades gubernamentales. Estos cambios han tenido y continuarán teniendo, profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo.

La especial atención prestada a la obtención de ventajas competitivas y a la economía implica una dependencia creciente en la computación como el componente más importante en la estrategia de la mayoría de las organizaciones. La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en

¹³ Guerra de información (*information warfare*)

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 Commission 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.

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

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

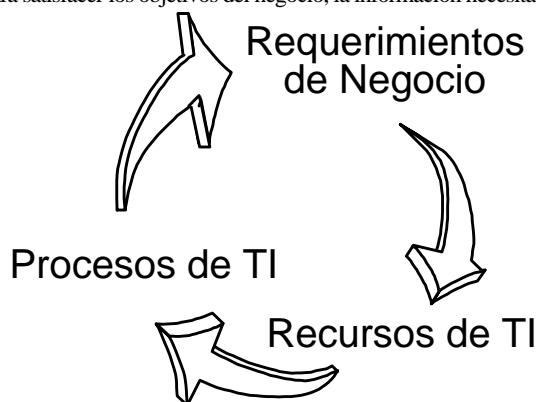
Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos

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 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.

¹⁴ **Ver y Sentir** (*look and feel*)

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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

Cumplimiento Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

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

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

Datos Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

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

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

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

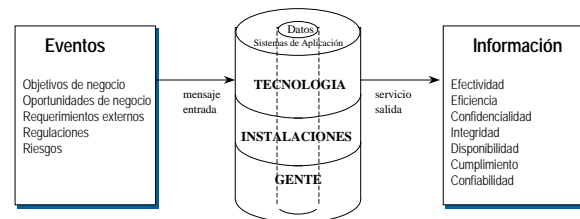
Personal Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

El dinero o capital no fue considerado como un recurso para la clasificación de objetivos de control para TI debido a que puede

definirse como la inversión en cualquiera de los recursos mencionados anteriormente y podría causar confusión con los requerimientos de auditoría financiera.

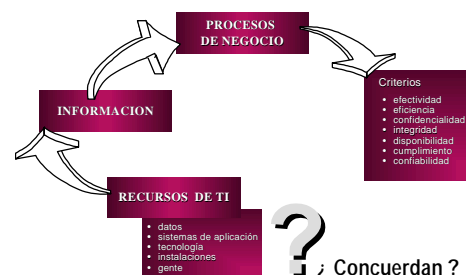
El Marco referencial no menciona, en forma específica para todos los casos, la documentación de todos los aspectos “materiales” importantes relacionados con un proceso de TI particular. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión.

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



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

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

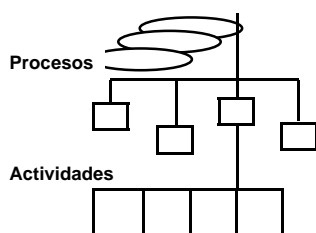


El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de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

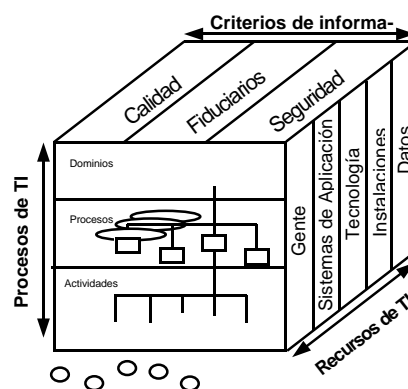
Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad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

Dominios



Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: (1) recursos de TI, (2) requerimientos de negocio para la información y (3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente. Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos).

Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control. Estos tres puntos estratégicos son descritos en el Cubo COBIT que se muestra a continuación:



Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización –y no la “jerga”¹⁵ del auditor -. Por lo tanto, cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo.

¹⁵ Jerga (jargon)

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Las definiciones para los dominios mencionados son las siguientes:

Planeación y organización

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

Adquisición e implementación

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

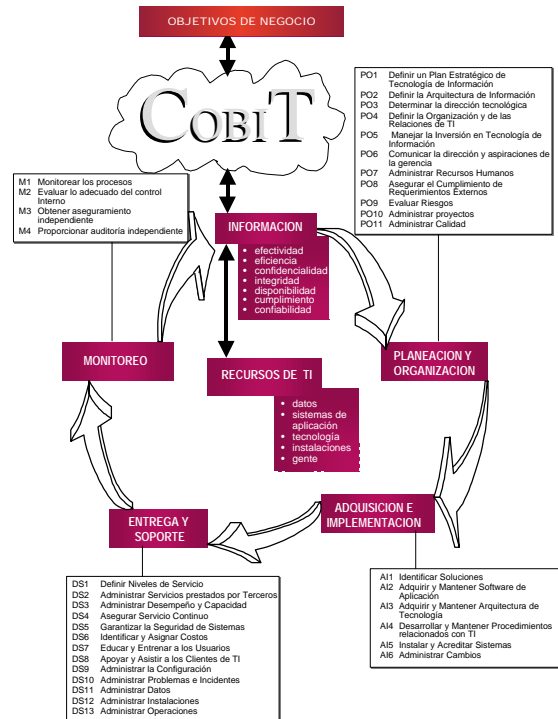
Entrega y soporte

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

Monitoreo

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

El siguiente diagrama ilustra este concepto:



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.

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

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

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

Primario

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

Secundario

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

Blanco (vacío)

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

Similarmente, 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.

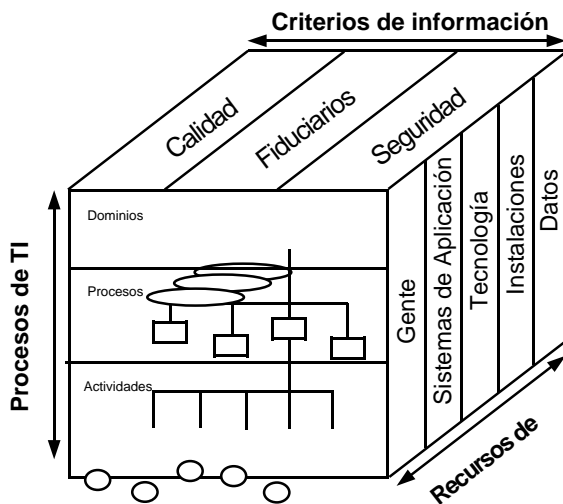
GUÍA PARA LA UTILIZACIÓN DEL MARCO REFERENCIAL Y LOS OBJETIVOS DE CONTROL COBIT

PERSPECTIVAS DIFERENTES; ENFOQUES DIFERENTES

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

1) recursos de TI, 2) requerimientos de negocio para la información y 3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

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

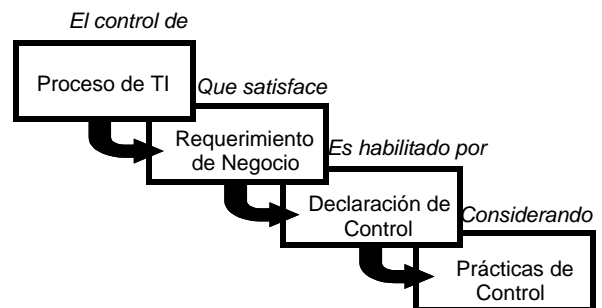


MARCO REFERENCIAL COBIT

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

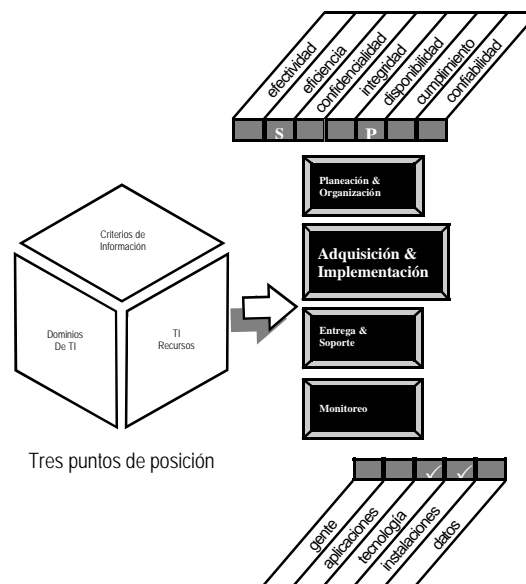
Los Objetivos de Control de TI han sido organizados por proceso/actividad, pero también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista estratégico como se explicó anteriormente, sino también para facilitar enfoques combinados o globales,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

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



AYUDAS DE NAVEGACIÓN

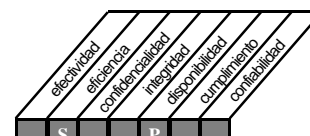
Para facilitar el empleo eficiente de los objetivos de control como soporte a los diferentes puntos de vista, se proporcionan algunas ayudas de navegación como parte de la presentación de los objetivos de control de alto nivel. Se proporciona una ayuda de navegación para cada una de las tres dimensiones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



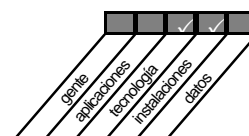
Los dominios son identificados ubicando la siguiente figura en la esquina superior derecha de cada página en la sección de Objetivos de Control, agrandando y haciendo más visible el dominio bajo revisión.



La clave para el criterio de información será proporcionado la esquina superior izquierda en la sección de Objetivos de Control mediante la siguiente “mini” matriz, la cual identificará 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).



OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

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				
									eficiencia	seguridad	confidencialidad	disponibilidad	cumplimiento
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				
	PO10	Administrar proyectos	P	P									
	PO11	Administrar calidad	P	P		P							
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	Educación y capacitación 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				

INTRODUCCIÓN A LAS DIRECTRICES DE AUDITORÍA

COBIT LAS DIRECTRICES DE AUDITORÍA

Las *Directrices de Auditoría* ofrecen una herramienta complementaria para la fácil aplicación del *Marco Referencial* y los *Objetivos de Control* COBIT dentro de las actividades de auditoría y evaluación. El propósito de las *Directrices de Auditoría* es contar con una estructura sencilla para auditar y evaluar controles, con base en prácticas de auditoría generalmente aceptadas y compatibles con el esquema global COBIT.

Los objetivos y prácticas individuales varían considerablemente de organización a organización y existen muchos tipos de practicantes dedicados a actividades relacionadas con la auditoría; por ejemplo auditores externos, auditores internos, evaluadores, revisores de calidad, y asesores técnicos. Por estas razones, las *Directrices de Auditoría* tienen una estructura genérica y de alto nivel.

Los auditores deben cumplir con algunos requerimientos generales para proporcionar a los directivos y a los poseedores de los procesos de negocios, seguridad y asesoría respecto a los controles en una organización: ofrecer una seguridad razonable de que se está cumpliendo con los objetivos de control correspondientes; identificar dónde se encuentran las debilidades significativas en dichos controles; justificar los riesgos que pueden estar asociados con tales debilidades, y finalmente, aconsejar a estos ejecutivos sobre las medidas correctivas que deben adoptarse. COBIT ofrece políticas claras y prácticas eficaces en materia de seguridad y control de información, así como tecnología asociada. Por tanto, las *Directrices de Auditoría* firmemente basados en los *Objetivos de Control*, toman la opinión del auditor a partir de la conclusión de auditoría, replazándola con criterios normativos (36 normas y las mejores prácticas (?) tomadas de normas privadas y públicas aceptadas a nivel mundial).

Estas *Directrices de Auditoría* proporcionan orientaciones para preparar planes de auditoría que se integran al *Marco COBIT* y a los *Objetivos de Control* detallados. Deben ser usados conjuntamente con estos dos últimos, y a partir de ahí pueden desarrollarse programas específicos de auditoría. Sin embargo, las *Directrices* no son exhaustivos ni definitivos. No pueden incluir todo ni ser aplicables a todo, así que deberán ajustarse a condiciones específicas. No obstante, hay cuatro cosas que las *Directrices* no son:

2. Las *Directrices de Auditoría* no pretenden ser una herramienta para crear el plan y cobertura general de auditoría

que considera una amplia gama de factores, incluyendo debilidades anteriores, riesgo a la organización, incidentes conocidos, nuevos acontecimientos, y selección de estrategias. Aun cuando el *Marco* y los *Objetivos de Control* ofrecen algunas orientaciones, los alcances de las *Directrices* no incluyen una guía precisa para actividades específicas.

2. Las *Directrices de Auditoría* no están diseñados como instrumento para enseñar las bases de la auditoría, aun cuando incorporen los elementos normalmente aceptados de la auditoría general y de TI.
3. Las *Directrices de Auditoría* no pretenden explicar en detalle la forma en que pueden utilizarse las herramientas computarizadas para apoyar y automatizar los procesos de auditoría IT, en materia de planeación, evaluación, análisis y documentación (que incluyen las Técnicas de Auditoría Asistidas por Computadora, pero no se limitan a ellas). Existe un enorme potencial para usar la tecnología de información dirigida a aumentar la eficiencia y efectividad de las auditorías, pero una orientación en este sentido, tampoco está dentro de los alcances de las *Directrices*.
4. Los *Las Directrices de Auditoría* no son exhaustivos ni definitivos, pero se desarrollarán conjuntamente con COBIT y sus *Objetivos de Control* detallados.

Las *Directrices de Auditoría COBIT* permiten al auditor cotejar los procesos específicos de TI con los *Objetivos de Control* COBIT recomendados para auxiliar a los directivos a identificar en qué casos los controles son suficientes, o para asesorarlos respecto a los procesos que requieren ser mejorados.

Desde el punto de vista de los directivos, los propietarios de los procesos harán las preguntas: ¿Estoy haciendo lo correcto?, y si no es así: ¿Qué puedo hacer para corregirlo? El *Marco* y las *Directrices de Auditoría COBIT* ayudarán a responder a estas preguntas. El enfoque ofrece una perspectiva “reactiva”, mientras que los auditores necesitan también apoyar a la directiva de una manera “proactiva”. El *Marco* y las *Directrices de Auditoría* pueden aplicarse igualmente en forma proactiva en las primeras etapas de los procesos y el desarrollo de proyectos, al responder a la pregunta: “¿What do I need so it will not need to be fixed?” (¿Qué es lo que necesito para no tener que ajustarlo después?

ESTRUCTURA GENERAL DE LAS DIRECTRICES DE AUDITORÍA

El modelo más común para evaluar el control es el modelo de auditoría. Otro enfoque que se está adoptando cada vez más es el modelo de análisis de riesgos, que se cubrirá hacia el final de esta introducción. Todos aquellos involucrados en la evaluación del control pueden inclinarse por cualquiera de los dos modelos.

Los objetivos de la auditoría son:

- Proporcionar administración con aseguramiento razonable de que se están cubriendo los objetivos de control,
- En donde existan debilidades de control significativas, justificar los riesgos resultantes, y
- Aconsejar a la administración sobre acciones correctivas

La estructura generalmente aceptada del proceso de auditoría es:

- Identificación y documentación
- Evaluación
- Pruebas de cumplimiento
- Pruebas justificantes

El proceso de TI, por lo tanto, se audita mediante:

- **La obtención** de un entendimiento de los riesgos relacionados con los requerimientos del negocio, y de las medidas relevantes de control
- **La evaluación** de la conveniencia de los controles establecidos
 - **La valoración** del cumplimiento por medio de probar si los controles establecidos están funcionando como se espera, de manera consistente y continua
 - **La justificación** del riesgo de que los objetivos de control no se estén cumpliendo mediante el uso de técnicas analíticas y/o consultando fuentes alternativas.

Con el objetivo de brindar asistencia a la administración en la forma de asesoría de aseguramiento, hemos desarrollado esta estructura dentro de un marco referencial fundamentado en los requerimientos del COBIT:

- Presentación en un enfoque de niveles
- Orientación hacia los objetivos del negocio

- Manejado en función del proceso
- Enfocado sobre
 - Los recursos que necesitan administrarse
 - Los criterios de información que se requieren

En el nivel más alto, este enfoque general de auditoría está apoyado por:

- El *marco referencial* de COBIT, particularmente el resumen con la clasificación de procesos de TI, los criterios de información aplicables y los recursos de TI (vea la página 21)
- Los requerimientos para el proceso de auditoría mismo (vea la sección Requerimientos del Proceso de Auditoría en la página 26)
- Los requerimientos genéricos para la auditoría de procesos de TI (vea la sección *Directrices de Auditoría* Genéricos de TI, página 27)
- Los principios generales de control (vea la sección Observaciones del Proceso de Control, página 27)

El segundo nivel está compuesto por las Directrices detalladas de auditoría para cada uno de los procesos de TI como se muestra en la sección principal de esta publicación.

Las Directrices han sido presentados en una plantilla estándar que sigue la estructura general de Obtención, Evaluación, Valoración y Justificación. Esta plantilla ha sido aplicada a las Directrices *de Auditoría* Genéricos de TI, así como también a las Directrices *de Auditoría* Detallados.

En el tercer y último nivel, el auditor puede complementar las Directrices *de Auditoría* para cubrir las condiciones locales, conduciendo la fase de planeación de auditoría con puntos de atención de auditoría que influyen sobre los objetivos detallados de control mediante:

- Criterios específicos del sector
- Estándares de la industria
- Elementos específicos de la plataforma
- Técnicas detalladas de control empleadas

De importancia para este nivel está el hecho de que los objetivos de control no son necesariamente aplicables siempre y en cualquier lugar. Por lo tanto se sugiere que se realice una evaluación de riesgos de alto nivel para determinar sobre qué objetivos se necesita enfocarse específicamente y cuáles pueden ignorarse.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Todos estos elementos se ofrecen para apoyar la planeación y la realización de las auditorías de TI, y para una mejor aplicación integrada de los lineamientos detallados de auditoría. Los lineamientos no son exhaustivos y no son aplicables universalmente.

El nivel de información de apoyo (lineamientos genéricos, requerimientos del proceso de auditoría y observaciones de control) ayudará a los auditores a desarrollar el programa de auditoría que necesitan.

ESTRUCTURA DETALLADA PARA LA APLICACIÓN DE LAS DIRECTRICES DE AUDITORÍA	
Nivel 1 Enfoque general de auditoría de TI	<ul style="list-style-type: none"> ➤ Marco Referencial de COBIT ➤ Requerimientos del Proceso de Auditoría ➤ Observaciones de Control ➤ Directriz General de Auditoría
Nivel 2 Directrices del proceso de auditoría	<ul style="list-style-type: none"> ➤ Directrices de Auditoría detallados
Nivel 3 Puntos de atención de auditoría para complementar los objetivos detallados de control	<ul style="list-style-type: none"> ➤ Condiciones Locales <ul style="list-style-type: none"> • Criterios específicos del sector • Estándares de la industria • Elementos específicos de la plataforma • Técnicas detalladas de control utilizadas

REQUERIMIENTOS DEL PROCESO DE AUDITORÍA

Una vez definido qué vamos a auditar y sobre qué vamos a proporcionar aseguramiento, tenemos que determinar el enfoque o estrategia más apropiado para llevar a cabo el trabajo de auditoría. Primero tenemos que *determinar el alcance correcto de nuestra auditoría*. Para lograrlo, necesitamos investigar, analizar y definir:

- Los procesos del negocio involucrados;
- Las plataformas y los sistemas de información que están apoyando el proceso del negocio, así como la interconectividad con otras plataformas o sistemas;
- Los papeles y responsabilidades definidas de TI, incluyendo qué ha sido realizado por fuentes internas y externas; y
- Los riesgos asociados del negocio y las decisiones estratégicas.

El siguiente paso es *identificar los requerimientos de información* que tienen una relevancia particular con respecto a los procesos del negocio. Luego necesitaremos *identificar los riesgos inherentes de TI, así como el nivel general de control* que puede asociarse con el proceso del negocio. Para lograrlo, identificamos:

- Los cambios recientes en el ambiente del negocio que tienen impacto sobre TI;
- Los cambios recientes al ambiente de TI, nuevos desarrollos, etc.;
- Los incidentes recientes relevantes para los controles y el ambiente del negocio;
- Los controles de monitoreo de TI aplicados por la administración;
- Los reportes recientes de auditoría y/o certificación; y
- Los resultados recientes de autoevaluaciones.

Basándonos en la información obtenida, ahora podemos seleccionar los procesos relevantes de COBIT, así como también los recursos que aplican a los mismos. Esto pudiera requerir que ciertos procesos de COBIT necesiten auditarse varias veces, cada vez para una plataforma o sistema distinto.

La persona deberá determinar una estrategia de auditoría basándose en el plan detallado de auditoría que deberá elab-

orarse con más profundidad, por ejemplo, si uno busca un enfoque basado en controles o un enfoque sustantivo.

Finalmente, necesitan considerarse todos los pasos, tareas y puntos de decisión para llevar a cabo la auditoría. Un ejemplo de un proceso genérico de auditoría (con pasos, tareas y puntos de decisión), que sigue la plantilla estándar, se proporciona en el Apéndice IV.

REQUERIMIENTOS DEL PROCESO DE AUDITORÍA	
• Definir el alcance de la auditoría	<ul style="list-style-type: none"> ⇒ procesos del negocio involucrados ⇒ plataformas, sistemas y su interconectividad, que apoyan el procesos ⇒ papels, responsabilidades y estructura organizacional
• Identificar los requerimientos de información relevantes para el proceso del negocio	<ul style="list-style-type: none"> ⇒ revelancia para el proceso del negocio
• Identificar los riesgos inherentes de TI y el nivel general de control	<ul style="list-style-type: none"> ⇒ cambios recientes e incidentes en el ambiente del negocio y de la tecnología ⇒ resultados de auditorías, autoevaluaciones, y certificación ⇒ controles de monitores aplicados por la administración
• Seleccionar procesos y plataformas para auditar	<ul style="list-style-type: none"> ⇒ procesos ⇒ recursos
• Fijar una estrategia de auditoría	<ul style="list-style-type: none"> ⇒ Controles de riesgo x ⇒ Pasos y tareas ⇒ Puntos de decisión

DIRECTRIZ GENERAL DE AUDITORÍA DE TI

La plantilla en la página 28 presenta los requerimientos genéricos para auditar procesos de TI para brindar el primer nivel de lineamientos de auditoría, generalmente aplicables a todos los procesos. Está primordialmente orientado hacia la comprensión del proceso y la determinación de la propiedad y deberá ser el fundamento y el marco referencial para todos los lineamientos detallados de auditoría.

Esta misma plantilla luego se aplica a los 34 procesos que se identifican en el *Marco Referencial de COBIT*.

OBSERVACIONES DEL PROCESO DE CONTROL

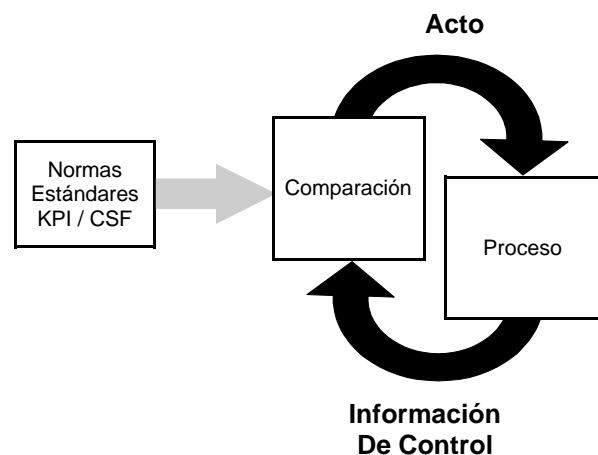
Los principios generales de control también pueden proporcionar una guía adicional sobre cómo complementar las *Directrices de Auditoría*. Estos principios están primordialmente enfocados sobre el proceso y las responsabilidades del control, los estándares de control y los flujos de la información de control.

El control, desde el punto de vista de la administración, se define como el determinar qué se está logrando; esto es, evaluar el desempeño y si es necesario aplicar medidas correctivas para que el desempeño tome lugar de acuerdo con lo planeado.

El proceso de control consiste de cuatro pasos. Primero, se especifica un estándar de desempeño deseado para un proceso. Segundo, existe un medio de saber qué está sucediendo en el proceso, por ejemplo, el proceso proporciona información de control a una unidad de control. Tercero, la unidad de control compara la información con el estándar. Cuarto, si lo que realmente está sucediendo no cumple con el estándar, la unidad de control dirige aquella acción correctiva a tomar, en forma de información para el proceso. A partir de este modelo, las siguientes observaciones de control pueden resultar relevantes para la auditoría:

1. Para que este modelo funcione, la *responsabilidad* por el proceso del negocio (o en este caso, de la TI) debe ser claro y la responsabilidad no debe ser ambigua. Si no es así, la información de control no fluirá y no podrá tomarse acción correctiva.
2. Los *estándares* pueden ser de una amplia variedad, desde planes y estrategias de alto nivel hasta indicadores clave de desempeño (KPI - Key Performance Indicators) y factores críticos de éxito (CSF - Critical Success Factors). Los estándares claramente documentados, mantenidos y comunicados son necesarios para un buen proceso de control. La responsabilidad clara por la custodia de dichos estándares también es un requerimiento para un buen control.
3. El *proceso de control* tiene los mismos requerimientos: bien documentado en cuanto a cómo funciona y con responsabilidades claras. Un aspecto importante es la clara definición de lo que constituye una desviación, esto es, cuáles son los límites de desviación.
4. La oportunidad, integridad y conveniencia de la *información de control*, así como también otra información, son básicas para el buen funcionamiento de un sistema de control y es algo que el auditor debe tratar.

Tanto la información de control como la información de acción correctiva tendrán requerimientos como *evidencia*, con el fin de establecer la *responsabilidad* después del evento.



DIRECTRIZ GENERAL DE AUDITORÍA

OBTENCIÓN DE UN ENTENDIMIENTO

Los pasos de auditoría a realizar para documentar las actividades subyacentes a los objetivos de control, así como también identificar las medidas/procedimientos de control establecidas.

Entrevistar al personal administrativo y de staff indicado para lograr la comprensión de:

- Los requerimientos del negocio y los riesgos asociados
- La estructura organizacional
- Los papeles y responsabilidades
- Las medidas de control establecidas
- La actividad de reporte a la administración (estatus, desempeño, acciones)

Documentar los recursos de TI relacionados con el proceso que se ven especialmente afectados por el proceso bajo revisión. Confirmar el entendimiento del proceso bajo revisión, los Indicadores Clave de Desempeño (KPI) del proceso, las implicaciones de control, por ejemplo, mediante una revisión paso a paso del proceso.

EVALUACIÓN DE LOS CONTROLES

Los pasos de auditoría a realizar en la evaluación de la eficacia de las medidas de control establecidas o el grado en el que se logra el objetivo de control. Básicamente, decidir qué se va a probar, si se va a probar y cómo se va a probar.

Evaluar la conveniencia de las medidas de control para el proceso bajo revisión mediante la consideración de los criterios identificados y las prácticas estándares de la industria, los Factores Críticos de Éxito (CSF) de las medidas de control y la aplicación del juicio profesional de auditor.

- Existen procesos documentados
- Existen resultados apropiados
- La responsabilidad y es clara y eficaz
- Existen controles compensatorios, en donde es necesario

Concluir el grado en el que se cumple el objetivo de control.

VALORACIÓN DEL CUMPLIMIENTO

Los pasos de auditoría a realizar para asegurar que las medidas de control establecidas estén funcionando como es debido, de manera consistente y continua, y concluir sobre la conveniencia de ambiente de control.

Obtener evidencia directa o indirecta de puntos/períodos seleccionados para asegurarse que se ha cumplido con los procedimientos durante el período de revisión, utilizando evidencia tanto directa como indirecta.

Realizar una revisión limitada de la suficiencia de los resultados del proceso.

Determinar el nivel de pruebas justificantes y trabajo adicional necesarios para asegurar que el proceso de TI es adecuado.

JUSTIFICAR EL RIESGO

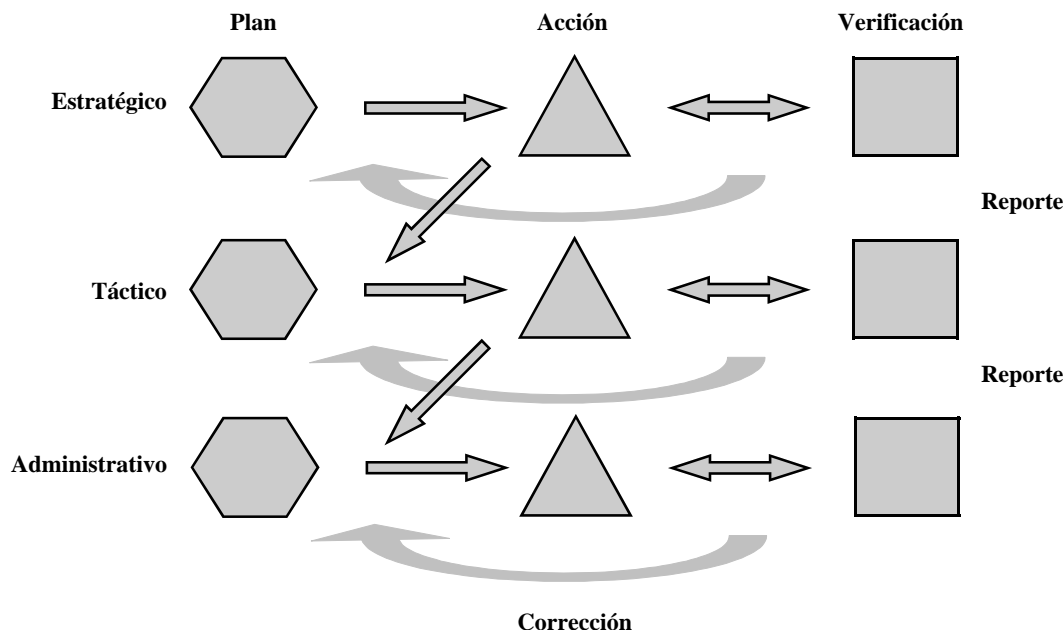
Los pasos de auditoría a realizar para justificar el riesgo de que no se cumpla el objetivo de control mediante el uso de técnicas analíticas y/o consultas a fuentes alternativas. El objetivo es respaldar la opinión e “impresionar” a la administración para que tome acción. Los auditores tienen que ser creativos para encontrar y presentar esta información que con frecuencia es susceptible y confidencial.

Documentar las debilidades del control y las amenazas y vulnerabilidades resultantes.

Identificar y documentar el impacto real y potencial; por ejemplo, mediante el análisis de causa-raíz.

Brindar información comparativa; por ejemplo, mediante puntos de referencia.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES



Los controles también operan en diferentes niveles dentro del ciclo tradicional de Planear-Hacer-Verificar-Corregir con el que la administración se siente cómoda. Este modelo ilustra:

- La secuencia lógica de planear-hacer-verificar y corregir el plan si es necesario;
- Cómo sucede esto a nivel estratégico, táctico y administrativo;
- Las diversas relaciones laterales y horizontales
 - El “hacer” estratégico da como resultado planeación táctica; el “hacer” táctico da como resultado planeación administrativa;
 - Las actividades de “verificar” y “hacer” co-operan e influyen continuamente una con otra; y
 - La actividad administrativa de “verificar” reporta a “verificar” táctico, quien a su vez reporta a “verificar” estratégico.

Cuando se evalúan mecanismos de control, los revisores deberán estar conscientes de que estos controles operan en estos diferentes niveles y de que tienen relaciones intrínsecas. La orientación hacia el proceso de COBIT proporciona algunas indicaciones acerca de los diferentes procesos de control, niveles e interrelaciones, pero la implantación o valoración real de los sistemas de control requiere tomar en cuenta esta compleja dimensión adicional.

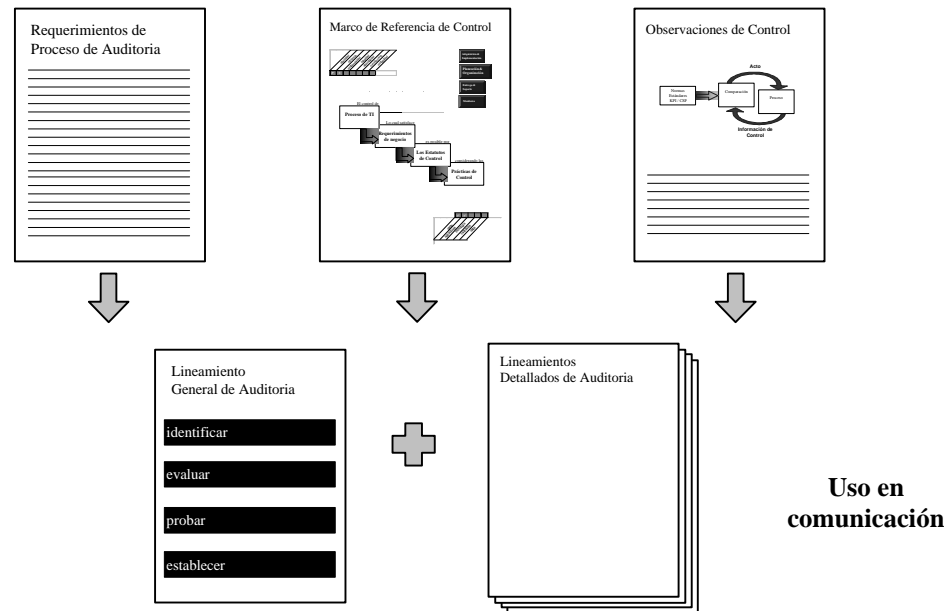
RESUMEN

En breve, las Directrices *de Auditoría* detallados siempre pueden complementarse tomando en cuenta el Lineamiento Genérico y el proceso bajo revisión, y obteniendo tareas de auditoría adicionales para lograr el objetivo de auditoría. El desarrollo del programa de auditoría en sí puede beneficiarse de tomar en consideración los requerimientos del proceso de auditoría de TI, el *Marco Referencial* de COBIT y los *Objetivos de Control* de Alto Nivel, y las Consideraciones de Control que se muestran aquí.

RELACIÓN ENTRE LOS OBJETIVOS DE CONTROL Y LAS DIRECTRICES DE AUDITORÍA

Los objetivos han sido desarrollados a partir de una orientación al proceso porque la administración está buscando asesoría a proactivo sobre cómo tratar el problema de mantener TI bajo control. Los *Objetivos de Control* ayudan a la administración a establecer el control sobre el proceso, las Directrices *de Auditoría* ayudan al auditor o asesor a asegurar que el proceso está realmente bajo control, de tal manera que los requerimientos de información necesarios para lograr los objetivos del negocio serán satisfechos.

La relación entre estos dos conceptos es el proceso, por lo que las Directrices *de Auditoría* han sido desarrollados para cada uno de los procesos, en oposición para cada uno de los objetivos de control.



En cuanto al marco referencial de control representado por el modelo de cascada, las *Directrices de Auditoría* pueden verse como los elementos que proporcionan retroalimentación a partir de los procesos de control para los objetivos del negocio. Los objetivos de control son la guía que baja por la cascada para tener el proceso de TI bajo control. Las *Directrices de Auditoría* son la guía para regresar a la parte superior de la cascada con la pregunta: “¿Hay seguridad de que se logre el objetivo del negocio?” Algunas veces, las *Directrices de Auditoría* son traducciones literales de los *Objetivos de Control*; con mayor frecuencia, las *Directrices* buscan la evidencia de que el proceso esté bajo control.

OPORTUNIDADES Y RETOS PARA LAS TAREAS DE EVALUACIÓN

La utilización del *Marco Referencial*, los *Objetivos de Control* y las *Directrices de Auditoría* como fundamento para la tarea de auditoría/valoración nos presenta algunas ventajas definitivas:

- Permite dar prioridad a las actividades de auditoría y áreas bajo revisión, utilizando las calificaciones Primaria y Secundaria de los criterios de información;
- Conduce a áreas de investigación que normalmente –sin un marco referencial o modelo- no serían tratadas; Puede desarrollarse una planeación y secuencia de entrevistas más lógica conforme los auditores avanzan en el proceso;

- Las investigaciones pueden enfocarse utilizando el indicador de qué recurso es más importante en qué proceso; y
- Como un estándar para definir las áreas de TI auditables para el plan estratégico de auditoría, con el fin de asegurar
 - La cobertura eficaz de la auditoría
 - La adquisición/desarrollo oportuno de las habilidades necesarias para la auditoría.

Sin embargo, existen algunos retos en cuanto a la integración del marco referencial y de los objetivos dentro del trabajo de auditoría:

- El cambio nunca es fácil (actitud, conjunto de herramientas, conjunto de habilidades, ...);
- La naturaleza detallada hace difícil la aplicación inicial, especialmente cuando se está verificando la consumación y aplicabilidad de los objetivos de control para el área bajo revisión;

Existe un grado necesario de repetición en las *Directrices de Auditoría* porque rara vez hay una relación uno-a-uno entre el objetivo de control y los mecanismos de control, un mecanismo contribuye de varias maneras a varios objetivos, un objetivo necesitando de varios mecanismos para poder lograrlo; y

- Refuerza cierto formalismo (por ejemplo, registrar información previa) que puede parecer innecesario.

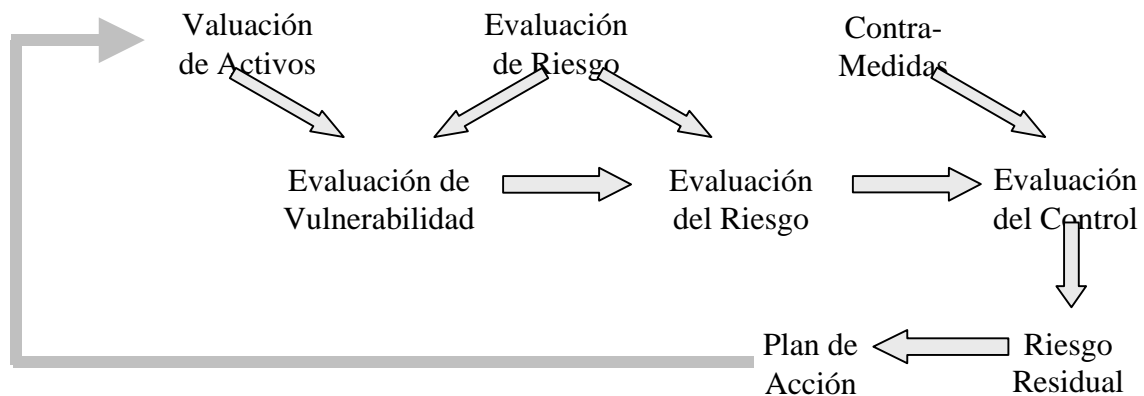
ANÁLISIS DE RIESGOS COMO UN ENFOQUE ALTERNATIVO DE EVALUACIÓN

El balance entre costo y riesgo es el siguiente problema a tratar, esto es, tomar una decisión consciente de cómo se va implementar cada uno de los objetivos de control y si se van a implementar. Los enfoques de análisis de riesgos tratan esta decisión, a pesar de que permanece el principio proactivo; los objetivos de control deberán aplicarse en primera instancia para lograr unos criterios de control de información (eficacia, eficiencia, confidencialidad, disponibilidad, integridad, cumplimiento y confiabilidad). Es evidente que la administración necesita utilizar alguna forma de evaluación de riesgos del negocio para definir las medidas a implementar (vea CO PO9). Los auditores también realizarán alguna forma de evaluación de riesgos cuando elijan los dominios del proceso y los objetivos de control para la revisión.

Un enfoque comúnmente aceptado para el análisis de riesgos en TI es el siguiente: El modelo comienza a partir de la valoración de los activos, que dentro del *Marco Referencial* de COBIT consiste en la información que tiene

los criterios requeridos para ayudar a lograr los objetivos del negocio (incluyendo todos los recursos necesarios para producir dicha información). El siguiente paso es el análisis de vulnerabilidad[†] que trata de la importancia de los criterios de información dentro del proceso bajo revisión, por ejemplo, si un proceso del negocio es vulnerable a la pérdida de integridad, entonces se requieren medidas específicas. Luego se tratan las amenazas, esto es, aquello que puede provocar una vulnerabilidad. La probabilidad de la amenaza, el grado de vulnerabilidad y la severidad del impacto se combinan para concluir acerca de la evaluación del riesgo. Esto es seguido por la selección de contramedidas (controles) y una evaluación de su eficacia, que también identifica el riesgo residual. La conclusión es un plan de acción después del cual el ciclo puede comenzar nuevamente.

[†] El resultado de un análisis de vulnerabilidad es la identificación de amenazas relevantes y el resultado de un análisis de amenazas es la identificación de vulnerabilidades relevantes.

Marco Referencial del Análisis de Riesgo

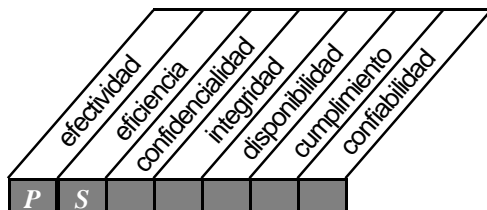
DIRECTRICES DE AUDITORÍA

PLANEACIÓN & ORGANIZACIÓN

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:

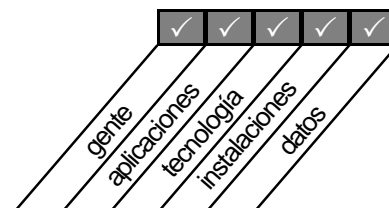
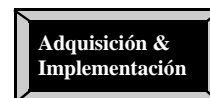
Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.

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 tecnológica²¹
- cambios organizacionales
- estudios de factibilidad oportunos
- evaluación de sistemas existentes



²¹ Vigilancia tecnológica (technology watch)

PO 1 DEFINIR UN PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVOS DE CONTROL

- 1 Tecnología de Información como parte del Plan a largo y corto plazo
- 2 Plan a largo plazo de Tecnología de Información
- 3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura
- 4 Cambios al Plan a largo plazo de Tecnología de Información
- 5 Planeación a corto plazo para la Función de Servicios de Información
- 6 Evaluación de los sistemas existentes

TANTO LOS OBJETIVOS DE CONTROL DETALLADOS COMO LOS DE ALTO NIVEL SON AUDITADOS MEDIANTE:

La obtención de un entendimiento a través de:

- ⇒ **Entrevistas:**
 - Director General
 - Director de Operaciones
 - Director de Finanzas
 - Director de TI
 - Miembros del comité planeador de la función de servicios de información.
 - Presidencia y personal de recursos humanos de la función de servicios de información
- ⇒ **Obteniendo:**
 - Políticas y procedimientos inherentes al proceso de planeación.
 - Tareas y responsabilidades de planeación de la Presidencia.
 - Objetivos y planes a corto y largo plazo organizacionales.
 - Objetivos y planes a corto y largo plazo de tecnología de información.
 - Reportes de estatus y minutas de las reuniones del comité planeador.

Evaluar los controles:

- ⇒ **Considerando sí:**

Las políticas y procedimientos de negocios de la función de servicios de información siguen un enfoque de planeación estructurado. Se ha establecido una metodología para formular y modificar los planes y que cubran, como mínimo:

 - misión y las metas de la organización
 - iniciativas de tecnología de información para soportar la misión y las metas de la organización
 - oportunidades para las iniciativas de tecnología de información
 - estudios de factibilidad de las iniciativas de tecnología de información
 - evaluación de los riesgos de las iniciativas de tecnología de información
 - inversión óptima de las inversiones en tecnología de información actuales y futuras
 - reingeniería de las iniciativas de tecnología de información para reflejar los cambios en la misión y las metas de la organización.
 - evaluación de las estrategias alternativas para las aplicaciones de datos, tecnología y organización

Los cambios organizacionales, la evolución tecnológica, los requerimientos regulatorios, la reingeniería de los procesos de negocios, las fuentes externas e internas, etc. están siendo consideradas y dirigidas adecuadamente en el proceso de planeación.

Existen planes de tecnología de información a corto y largo plazo, si éstos son actuales, están dirigidos adecuadamente a la empresa en general, si su misión y proyectos de tecnología de información para las funciones clave de negocios están soportados por la documentación apropiada según lo definido en la metodología de planeación de tecnología de información.

Existen puntos de revisión para asegurar que los objetivos de tecnología de información y los planes a corto y largo plazo continúan satisfaciendo los objetivos y los planes a corto y largo plazo organizacionales.

Los propietarios de procesos y la Presidencia de los planes de tecnología de información llevan a cabo revisiones y aprobaciones formales.

El plan de la tecnología de información evalúa los sistemas de información existentes en términos del grado de automatización, funcionalidad, estabilidad, complejidad, costos, fortalezas y debilidades del negocio.

Evaluar la suficiencia:

▸ **Probando que:**

Las minutas de las reuniones del comité planeador de la función de servicios de información reflejan el proceso de planeación.

Los elementos entregables y liberables de la metodología de planeación existen según lo indicado.

Se incluyen iniciativas de tecnología de información en los planes a corto y largo plazos de la función de servicios de información (por ejemplo, cambios de hardware, planeación de capacidad, arquitectura de información, desarrollo u obtención de nuevos sistemas, planeación de recuperación en caso de desastre, instalación de plataformas para nuevos procesamiento, etc.).

Las iniciativas de tecnología de información soportan la investigación, el entrenamiento, la asignación de personal, las instalaciones, el hardware y el software.

Se hayan identificado las implicaciones para las iniciativas de tecnología de información

Se haya tomado en consideración la optimización de inversiones de tecnología de información actuales y futuras

Los planes a corto y largo plazo de tecnología de información son consistentes con los planes a corto y largo plazo de la organización, así como con los requerimientos de ésta.

Se han modificado los planes para reflejar condiciones cambiantes.

Los planes a largo plazo de tecnología de información son traducidos periódicamente en planes a corto plazo.

Existen tareas para implementar los planes.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Evaluar el riesgo de los objetivos de control no cumplidos:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de planes estratégicos de tecnología de información contra organizaciones similares o buenas prácticas industriales reconocidas/estándares internacionales apropiados.

Una revisión detallada de los planes de TI para asegurar que las iniciativas de tecnología de información reflejen la misión y las metas de la organización.

Una revisión detallada de los planes de TI para determinar si, como parte de las soluciones de tecnología de información contenidas en los planes, se han identificado áreas de debilidad dentro de la organización que requieren ser mejoradas.

▸ **Identificando:**

Fallas en la tecnología de información para satisfacer la misión y las metas de la organización.

Fallas en la tecnología de información para concordar los planes a corto y largo plazo.

Fallas en la tecnología de información para satisfacer planes a corto plazo.

Fallas en la tecnología de información para satisfacer lineamientos de costos y tiempos.

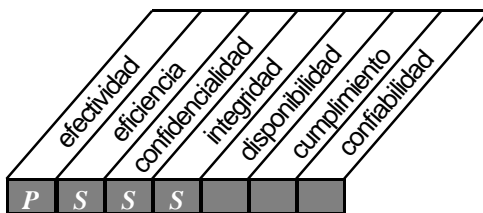
Oportunidades de negocios no aprovechadas.

Oportunidades de tecnología de información no aprovechadas.

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:

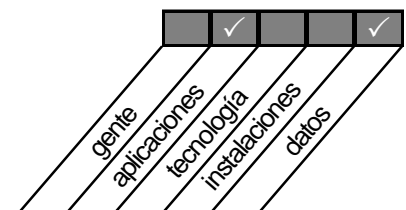
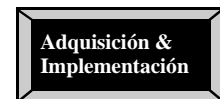
organizar de la mejor manera los sistemas de información

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 severidad²²



²² Severidad (criticality)

PO 2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN

OBJETIVOS DE CONTROL

- 1 Modelo de la Arquitectura de Información
- 2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación
- 3 Esquema de Clasificación de Datos
- 4 Niveles de Seguridad

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

La obtención de un entendimiento a través de:

- ⇒ **Entrevistas:**
 - Director de TI
 - Miembros del comité planeador de la función de servicios de información.
 - Presidencia de la función de servicios de información.
 - Funcionario de Seguridad
- ⇒ **Obteniendo:**
 - Políticas y procedimientos sobre la arquitectura de información.
 - Modelo de la arquitectura de información.
 - Documentos que soporten el modelo de la arquitectura de información, incluyendo el modelo de datos corporativo.
 - Diccionario de datos corporativo
 - Política de propiedad de datos
 - Funciones y responsabilidades de planeación de la Presidencia. Objetivos y planes a corto y largo plazo de tecnología de información
 - Reporte de estatus y minutas de las reuniones del comité planeador

Evaluar los controles::

- ⇒ **Considerando sí:**
 - Las políticas y procedimientos de la función de los servicios de información dirigen el desarrollo y mantenimiento del diccionario de datos.
 - El proceso utilizado para actualizar el modelo de la arquitectura de información toma como base los planes a corto y largo plazo, considera los costos y riesgos asociados y asegura que las aprobaciones formales de la Presidencia sean obtenidas antes de hacer modificaciones al modelo.
 - Se utiliza algún proceso para mantener actualizados el diccionario de datos y las reglas de sintaxis de datos.
 - Se utiliza algún medio para distribuir el diccionario de datos para asegurar que éste sea accesible para las áreas de desarrollo y que los cambios sean reflejados inmediatamente.

Las políticas y procedimientos de la función de servicios de información dirigen la clasificación de los datos, incluyendo categorías de seguridad y propiedad de datos, y si las reglas de acceso para las clases de datos están claras y apropiadamente definidas.

Los estándares definen la clasificación "default" para los activos de datos que no contienen un identificador de clasificación.

Las políticas y procedimientos de la función de servicios de información dirigen lo siguiente:

- la existencia de un proceso de autorización que requiera que el propietario de los datos (tal como lo define la política de propiedad de datos) autorice todos los accesos a éstos datos, así como los atributos de seguridad de los mismos.
 - los niveles de seguridad estén definidos para cada clasificación de datos.
 - los niveles de acceso estén definidos y sean apropiados para la clasificación de datos.
- el acceso a datos delicados requiera de niveles de acceso explícitos y que los datos sean únicamente proporcionados si existe una verdadera necesidad de acceder a ellos.

Evaluar la suficiencia:

▸ **Probando que:**

Estén identificados los cambios realizados al modelo de arquitectura de información para confirmar que dichos cambios reflejan la información de los planes a largo y corto plazo, así como los costos y los riesgos.

La evaluación del impacto de cualquier modificación realizada al diccionario de datos y cualquier cambio realizado al diccionario de datos para asegurar que éstos han sido comunicados efectivamente.

Varios sistemas de aplicación operacional y proyectos de desarrollo para confirmar que el diccionario de datos es utilizado para la definición de datos.

La adecuación de la documentación del diccionario de datos para confirmar que éste define los atributos de datos y los niveles de seguridad para cada elemento de datos.

La propiedad de la clasificación de datos, de los niveles de seguridad, de los niveles de acceso y "defaults".

Cada clasificación de datos defina claramente:

- quién puede tener acceso
- quién es responsable de determinar el nivel de acceso apropiado
- la aprobación específica requerida para el acceso
- los requerimientos especiales para el acceso (por ejemplo, acuerdo de confidencialidad)

Evaluar el riesgo de los objetivos de control no cumplidos:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") del modelo de arquitectura de información contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas.

Una revisión detallada del diccionario de datos para asegurar que es completo en lo referente a elementos clave.

Una revisión detallada de los niveles de seguridad definidos para datos delicados, con el fin de verificar que se haya obtenido la autorización apropiada para el acceso y que el acceso sea consistente con los niveles de seguridad definidos en las políticas y procedimientos de la función de servicios de información.

▸ **Identificando:**

Inconsistencias en el modelo de arquitectura de información y en el modelo de datos corporativo, en el diccionario de datos corporativo, en los sistemas de información asociados y en los planes a largo y corto plazo de tecnología de información.

Elementos obsoletos en el diccionario de datos corporativo y reglas de sintaxis de datos en las que se haya perdido tiempo debido a cambios realizados inadecuadamente al diccionario de datos.

Elementos de datos en los que la propiedad no haya sido claramente y/o apropiadamente determinada

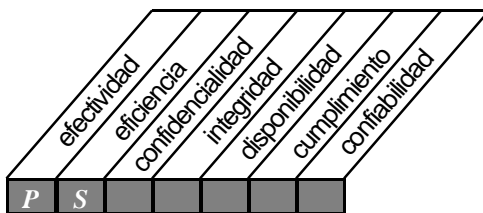
Clases de datos que hayan sido definidos de manera no apropiada.

Niveles de seguridad de datos inconsistentes con la regla de "necesidad de acceso" ("need to know").

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:

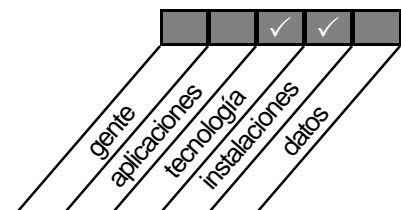
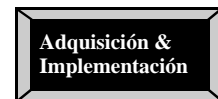
aprovechar la tecnología disponible o tecnología emergente

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



PO 3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Planeación de la Infraestructura Tecnológica |
| 2 | Monitoreo de Tendencias y Regulaciones Futuras |
| 3 | Contingencias en la Infraestructura Tecnológica |
| 4 | Planes de Adquisición de Hardware y Software |
| 5 | Estándares de Tecnología |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

La obtención de un entendimiento a través de:

- **Entrevistas:**
 - Director General
 - Director de Operaciones
 - Director de Finanzas
 - Director de TI
 - Miembros del comité planeador de la función de servicios de información
 - Presidencia de la función de servicios de información
- **Obteniendo:**
 - Políticas y procedimientos relacionados con la planeación y el monitoreo de la infraestructura tecnológica.
 - Tareas y responsabilidades de planeación de la Presidencia.
 - Objetivos y planes a largo y corto plazo de la organización.
 - Objetivos y planes a largo y corto plazo de tecnología de información.
 - Plan de adquisición de hardware y software de tecnología de información.
 - Plan de infraestructura tecnológica.
 - Estándares de tecnología.
 - Reportes de estatus y minutas de las reuniones del comité planeador.

Evaluar los controles::

- **Considerando sí:**
 - Existe un proceso para la creación y la actualización regular del plan de infraestructura tecnológica para confirmar que los cambios propuestos estén siendo examinados primero para evaluar los costos y riesgos inherentes, y que la aprobación de la Presidencia sea obtenida antes de realizar cualquier cambio al plan.
 - El plan de infraestructura tecnológica está siendo comparado contra los planes a largo y corto plazo de tecnología de información.
 - Existe un proceso para la evaluación de la situación tecnológica actual de la organización para asegurar que abarca aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

La política y procedimientos de la función de los servicios de información aseguran la consideración de la necesidad de evaluar y monitorear las tendencias y condiciones regulatorias tecnológicas presentes y futuras, y si éstas son tomadas en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

Se planean el impacto logístico y ambiental de las adquisiciones tecnológicas.

Las políticas y procedimientos de la función de servicios de información aseguran que se considere la necesidad de evaluar sistemáticamente el plan tecnológico para aspectos de contingencia (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).

La administración de la función de los servicios de información evalúa tecnologías de vanguardia, e incorpora tecnologías apropiadas a la infraestructura de servicios de información actual.

Los planes de adquisición de hardware y software suelen satisfacer las necesidades identificadas en el plan de infraestructura tecnológica y si éstos son aprobados apropiadamente.

Se encuentran establecidos los estándares de tecnología para los componentes tecnológicos descritos en el plan de infraestructura tecnológica.

Evaluar la suficiencia:

► Probando que:

La administración de la función de servicios de información comprende y utiliza el plan de infraestructura tecnológica. Se hayan realizado cambios al plan de infraestructura tecnológica para identificar los costos y riesgos inherentes, y que dichos cambios reflejen las modificaciones a los planes a largo y corto plazo de tecnología de información.

La administración de la función de servicios de información comprende el proceso de monitoreo y evaluación de nuevas tecnologías, y que incorpora tecnologías apropiadas a la infraestructura de servicios de información actual.

La administración de la función de servicios de información comprende el proceso de evaluar sistemáticamente el plan de tecnología en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).

La existencia de un ambiente físico de la función de servicios de información adecuado para alojar el hardware/software actualmente instalado, así como nuevo hardware/software a ser añadido según el plan de adquisiciones actual aprobado.

El plan de adquisición de hardware y software cumple con los planes a largo y corto plazo de tecnología de información, reflejando las necesidades identificadas en el plan de infraestructura tecnológica.

El plan de infraestructura tecnológica dirige la utilización de tecnología actual y futura.

Se cumpla con los estándares de tecnología y que éstos sean agregados e incorporados como parte del proceso de desarrollo.

El acceso permitido sea consistente con los niveles de seguridad definidos en las políticas y procedimientos de la función de servicios de información, y que se haya obtenido la autorización apropiada para el acceso.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Evaluar el riesgo de los objetivos de control no cumplidos:

▸ **Llevando a cabo:**

- Mediciones ("Benchmarking") de la planeación de infraestructura tecnológica contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas.
- Una revisión detallada del diccionario de datos para verificar que es completo en lo referente a elementos clave.
- Una revisión detallada de los niveles de seguridad definidos para datos delicados.

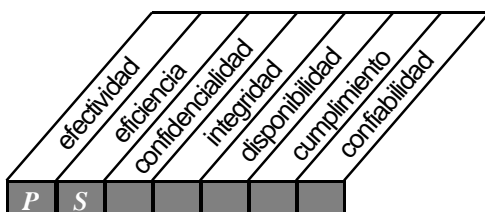
▸ **Identificando:**

- Inconsistencias en el modelo de arquitectura de información y en el modelo de datos corporativo, en el diccionario de datos corporativo, en los sistemas de información asociados y en los planes a largo y corto plazo de tecnología de información.
- Elementos de diccionario de datos y reglas de sintaxis de datos obsoletos.
- Aspectos de contingencia no considerados en el plan de infraestructura tecnológica.
- Planes de adquisición de hardware y software de tecnología de información que no reflejen las necesidades de plan de infraestructura tecnológica.
- Estándares de tecnología que no sean consistentes con el plan de infraestructura tecnológica o con los planes de adquisición de hardware y software de tecnología de información.
- Un plan de infraestructura tecnológica o planes de adquisición de hardware y software de tecnología de información que no sean consistentes con los estándares de tecnología.
- Elementos clave omitidos en el diccionario de datos.

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:

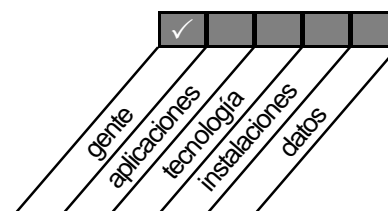
- comité de dirección
- responsabilidades a nivel de alta gerencia o del consejo
- propiedad, custodia
- supervisión
- segregación de funciones
- roles y responsabilidades
- descripción de puestos
- niveles de asignación de personal
- personal clave

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



PO 4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS DEFINICIONES DE TI

OBJETIVOS DE CONTROL

- 1 Comité de planeación o dirección de la función de servicios de información
- 2 Ubicación de los servicios de información en la organización
- 3 Revisión de Logros Organizacionales
- 4 Funciones y Responsabilidades
- 5 Responsabilidad del aseguramiento de calidad
- 6 Responsabilidad de la Seguridad Lógica y Física
- 7 Propiedad y Custodia
- 8 Propiedad de Datos y Sistemas
- 9 Supervisión
- 10 Segregación de Funciones
- 11 Asignación de Personal para Tecnología de Información
- 12 Descripción de Puestos para el Personal de la Función de Servicios de Información
- 13 Personal Clave de Tecnología de Información
- 14 Procedimientos para personal por contrato
- 15 Relaciones

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

La obtención de un entendimiento a través de:

- **Entrevistas:**
 - Director General
 - Director de Operaciones
 - Director de Finanzas
 - Director de TI
 - Oficial de Aseguramiento de Calidad
 - Oficial de Seguridad de Información
 - Miembros del comité planeador de la función de servicios de información, recursos humanos y Presidencia.
- **Obteniendo:**
 - Funciones y responsabilidades de planeación de la Presidencia.
 - Objetivos y planes a largo y corto plazo organizacionales.
 - Objetivos y planes a largo y corto plazo de tecnología de información.
 - Organigrama organizacional que muestre la relación entre la función de servicios de información y otras funciones.
 - Políticas y procedimientos relacionadas con la organización y las relaciones de tecnología de información.
 - Políticas y procedimientos relacionados con el aseguramiento de la calidad.
 - Políticas y procedimientos utilizados para determinar los requerimientos de asignación de personal de la función de servicios de información. Organigrama organizacional de la función de servicios de información.

Funciones y responsabilidades de la función de servicios de información.
 Descripción de los puestos clave de la función de servicios de información.
 Reportes de estatus y minutas de las reuniones del comité de planeación.

Evaluar los controles::

► **Considerando sí:**

- Las políticas y los comunicados de la Presidencia aseguran la independencia y la autoridad de la función de los servicios de información.
- Se han definido e identificado la calidad de miembro, las funciones y las responsabilidades del comité de planeación de la función de servicios de información.
- Los estatutos del comité de planeación de la función de servicios de información alinean las metas del comité con los objetivos y los planes a largo y corto plazo de la organización y con los objetivos y planes a largo y corto plazo de tecnología de información.
- Se han establecido procesos para incrementar el conocimiento la conciencia, la comprensión y la habilidad para identificar y resolver problemas de administración de la información.
- Las políticas consideran la necesidad de evaluar y modificar la estructura organizacional para satisfacer objetivos y circunstancias cambiantes.
- Existen procesos e indicadores de desempeño para determinar la efectividad y aceptación de la función de servicios de información.
- La Presidencia se asegura que las funciones y responsabilidades están siendo llevadas a cabo.
- Existen políticas que determinen las funciones y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control y seguridad internos.
- Existen campañas regulares para incrementar la conciencia y disciplina en cuanto al control y la seguridad interna.
- Existen políticas y funciones de aseguramiento de la calidad.
- La función de aseguramiento de la calidad cuenta con la independencia suficiente con respecto al personal de desarrollo de sistemas y con una asignación de personal y experiencia adecuados para llevar a cabo sus responsabilidades.
- Existen procedimientos establecidos dentro del aseguramiento de la calidad para calendarizar recursos y asegurar el cumplimiento de las pruebas y aprobación del aseguramiento de la calidad antes de que se implementen nuevos sistemas o cambios a los sistemas.
- La Gerencia ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formalicen de políticas y procedimientos de control y seguridad internos (tanto lógicos como físicos) a algún funcionario de seguridad de la información.
- El funcionario de seguridad de la información comprende adecuadamente las funciones y responsabilidades y si éstas han mostrado consistencia con respecto a la política de seguridad de la información de la organización.
- La política de seguridad de la organización define claramente las responsabilidades sobre la seguridad de la información que cada propietario de activos (por ejemplo, usuarios, administración y administradores de seguridad) debe llevar a cabo.
- Existen políticas y procedimientos que cubran datos y propiedad de sistemas para todas las fuentes de datos y sistemas más importantes.
- Existen procedimientos para revisar y mantener cambios en la propiedad de los datos y los sistemas regularmente.
- Existen políticas y procedimientos que describan las prácticas de supervisión para asegurar que las funciones y responsabilidades sean ejercidas apropiadamente y que todo el personal cuente con suficiente autoridad y recursos para llevar a cabo sus funciones y responsabilidades.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Existe una segregación de funciones entre los siguientes pares de unidades:

- desarrollo y mantenimiento de sistemas
- desarrollo y operaciones de sistemas
- desarrollo/mantenimiento de sistemas y seguridad de la información.
- operaciones y control de datos
- operaciones y usuarios
- operaciones y seguridad de la información

La asignación de personal y la competencia de la función de servicios de información es mantenida para asegurar su habilidad para proporcionar soluciones tecnológicas efectivas.

Existen políticas y procedimientos para la evaluación y revalidación de las descripciones de puestos de la función de servicios de información.

Existen funciones y responsabilidades para procesos clave, incluyendo actividades del ciclo de vida de desarrollo de sistemas (requerimientos, diseño, desarrollo, pruebas), seguridad de la información, adquisición y planeación de capacidad.

Se utilizan indicadores clave de desempeño y/o factores críticos de éxito al medir los resultados de la función de servicios de información en el logro de objetivos organizacionales.

Existen políticas y procedimientos en la función de servicios de información para controlar las actividades de consultores y demás personal por contrato, asegurando así la protección de los activos de la organización.

Existen procedimientos aplicables a tecnología de información por contrato que sean adecuados y consistentes con las políticas de adquisición organizacionales.

Existen procesos para coordinar, comunicar y documentar los intereses dentro y fuera del directorio de la función de servicios de información.

Evaluar la suficiencia:

▸ Probando que:

El comité planeador de la función de servicios de información vigila a la función de servicios de información y sus actividades.

La propiedad de la jerarquía de reporte para la función de servicios de información.

La efectividad de la localización de la función de servicios de información dentro de la organización en cuanto a facilitar una relación de sociedad con la alta Gerencia.

La Presidencia de la función de servicios de información comprenda cuáles son los procesos utilizados para monitorear, medir y reportar el desempeño de la función de servicios de información.

La utilización de indicadores clave para evaluar el desempeño.

Los procesos para analizar los resultados reales contra los niveles meta, con el fin de determinar las acciones correctivas realizadas cuando los resultados reales no alcanzan los niveles meta.

Las acciones realizadas por la administración en cuanto a cualquier variación significativa con respecto a los niveles esperados de desempeño.

La administración de usuarios/propietarios evalúa la capacidad de respuesta y la habilidad de la función de servicios de información para proporcionar soluciones de tecnología de información que satisfagan las necesidades de usuarios/propietarios.

La Gerencia de la función de servicios de información conoce sus funciones y responsabilidades.

- Aseguramiento de la calidad se involucre en la prueba y aprobación de los planes de proyectos de la función de servicios de información.
- El personal de seguridad de la información revisa los sistemas operativos y los sistemas de aplicación esenciales.
- La adecuación de los reportes o documentación de la función de seguridad de la información al evaluar la seguridad de la información (tanto lógica como física) ya existente o en desarrollo.
- Existe suficiente conocimiento, conciencia y una aplicación consistente de las políticas y procedimientos de seguridad de la información.
- El personal asiste a los entrenamientos de seguridad y control interno.
- La propiedad de los datos y sistemas se encuentra definida para todos los activos de información.
- Los propietarios de datos y sistemas hayan aprobado los cambios realizados a dichos datos y sistemas.
- Todos los datos y sistemas cuentan con un propietario o custodio que sea responsable del nivel de control sobre los datos y sistemas.
- El acceso a todos los activos de datos y sistemas es aprobado por el/los propietario(s) de los activos.
- La línea directa de autoridad y supervisión asociada con el puesto está en conformidad con las responsabilidades del beneficiado.
- Las descripciones de puestos delinean claramente tanto la autoridad como la responsabilidad.
- Las descripciones de puestos describen claramente las aptitudes de negocios, relaciones y técnicas requeridas.
- Las descripciones de puestos hayan sido comunicadas con precisión y hayan sido comprendidas por el personal.
- Las descripciones de puestos para la función de servicios de información contienen indicadores clave de desempeño que han sido comunicados al personal.
- Las funciones y responsabilidades del personal de la función de servicios de información corresponden tanto a las descripciones de puestos publicadas como al organigrama.
- Existan descripciones de puestos para las posiciones clave y que éstas incluyan los mandatos de la organización relativos a sistemas de información, control y seguridad internos.
- La precisión de las descripciones de puestos comparadas contra las responsabilidades actuales de los encargados de dichas posiciones.
- La naturaleza y el alcance de la suficiencia de la segregación de funciones deseada y de las limitaciones de funciones dentro de la función de servicios de información.
- El mantenimiento de la competencia del personal de tecnología de información.
- La propiedad de las descripciones de puestos como base para la adecuación y la claridad de las responsabilidades, autoridad y criterios de desempeño.
- Las responsabilidades de administración por contrato hayan sido asignadas al personal apropiado.
- Los términos de los contratos sean consistentes con los estándares normales para contratos de la organización y que los términos y condiciones contractuales estándar hayan sido revisados y evaluados por un consultor legal, cuyo acuerdo haya sido obtenido.
- Los contratos contienen cláusulas apropiadas con respecto al cumplimiento de: políticas de seguridad corporativa y control interno y estándares de tecnología de información.
- Existen procesos y/o estructuras que garantizan una coordinación efectiva y eficiente para lograr relaciones exitosas.

Evaluar el riesgo de los objetivos de control no cumplidos:

▸ **Llevando a cabo:**

- Mediciones ("Benchmarking") de la organización y de las relaciones contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas por la industria apropiadas.
- Una revisión detallada para determinar el impacto sobre la organización causada por un comité de planeación de la función de servicios de información no efectivo.
- Una revisión detallada para medir el progreso de la función de servicios de información al tratar con problemas de sistemas de información e implementar soluciones tecnológicas.
- Una revisión detallada para evaluar la estructura organizacional, las aptitudes del personal, las funciones y responsabilidades asignadas, la propiedad de datos y sistemas, supervisión, segregación de funciones, etc.
- Una revisión detallada de la función de aseguramiento de la calidad para determinar su efectividad en la satisfacción de los requerimientos de la organización.
- Una revisión detallada de la función de seguridad de la información para determinar su efectividad para proporcionar seguridad general en la organización (tanto lógica como física) y entrenamiento de conocimiento y conciencia de seguridad.
- Una revisión detallada de una muestra de contratos para confirmar que éstos hayan sido ejecutados apropiadamente por ambas partes y que cumplan con los términos contractuales estándar de la organización.

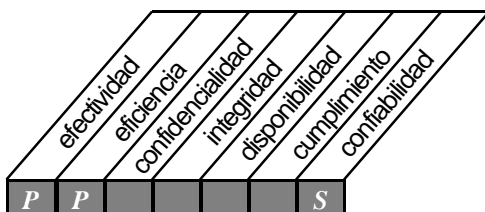
▸ **Identificando:**

- Debilidades en la función de servicios de información y sus actividades ocasionadas por una vigilancia no efectiva por parte del comité de planeación de dicha función.
- Lagunas, traslapes, etc. en la estructura organizacional que traen como resultado ineffectividad e ineficiencia en la función de servicios de información.
- Estructuras organizacionales inapropiadas, funciones faltantes, personal insuficiente, deficiencias en competencia, funciones y responsabilidades no apropiadas, confusión en la propiedad de datos y sistemas, problemas de supervisión, falta de segregación de funciones, etc.
- Sistemas en proceso de desarrollo, modificados o implementados que cumplen con los requerimientos de aseguramiento de la calidad.
- Sistemas en proceso de desarrollo, modificados o implementados que cumplen con los requerimientos de seguridad (lógica, física, o ambos).
- Contratos que no cumplen con los requerimientos contractuales de la organización.
- Coordinación y comunicación no efectivas entre la función de servicios de información y otros intereses dentro y fuera de esta función.

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:

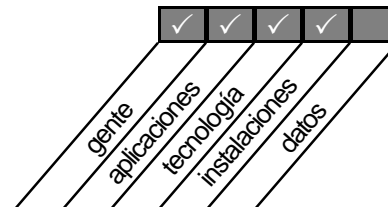
asegurar el financiamiento y el control de desembolsos de recursos financieros

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



PO 5 MANEJO DE LA INVERSIÓN EN TECNOLOGÍA DE INFORMACIÓN

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Presupuesto Operativo Anual para la Función de Servicios de Información |
| 2 | Monitoreo de Costos |
| 3 | Justificación de Costos |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

La obtención de un entendimiento a través de:

► **Entrevistas:**

Director de Finanzas
 Director de TI
 Miembros del comité de planeación de la función de servicios de información
 Presidencia de la función de servicios de información

► **Obteniendo:**

Políticas, métodos y procedimientos organizacionales relacionados con la elaboración del presupuesto y las actividades de costeo.
 Políticas y procedimientos de la función de servicios de información relacionadas con la elaboración del presupuesto y las actividades de costeo.
 Presupuesto operativo actual y del año inmediato anterior para la función de servicios de información.
 Objetivos y planes organizacionales a corto y largo plazo.
Objetivos y planes a corto y largo plazo de tecnología de información.
 Funciones y responsabilidades de planeación de la Presidencia.
 Reportes de variaciones y otros comunicados relacionados con el control y monitoreo de variaciones.
 Reportes de estatus y minutas de las reuniones del comité de planeación.

Evaluar los controles::

► **Considerando sí:**

El proceso de elaboración del presupuesto de la función de servicios de información es consistente con el proceso de la organización.
 Existen políticas y procedimientos para asegurar la preparación y la aprobación adecuada de un presupuesto operativo anual para la función de servicios de información, que sea consistente con el presupuesto y los planes a corto y largo plazo de la organización y los planes a corto y largo plazo de tecnología de información.
 El proceso de elaboración del presupuesto está vinculado con la administración de las unidades más importantes de la función de servicios de información que contribuyen a su preparación.
 Existen políticas y procedimientos para monitorear regularmente los costos reales y compararlos con los costos proyectados y si los costos reales tienen como base el sistema de contabilidad de costos de la organización.
 Existen políticas y procedimientos para garantizar que la entrega y liberación de servicios por parte de la función de servicios de información se justifican en cuanto a costos y están en línea con los costos de la industria.

Evaluar la suficiencia:**▸ Probando que:**

El soporte en el presupuesto de la función de servicios de información es el adecuado para justificar el plan operativo anual de dicha función.

Las categorías de gastos de la función de servicios de información son suficientes, apropiadas y han sido clasificadas adecuadamente.

El sistema para registrar, procesar y reportar los costos asociados con las actividades de la función de servicios de información en forma rutinaria es adecuado.

El proceso de monitoreo de costos compara adecuadamente los costos reales contra los presupuestados.

Los análisis costo/beneficio llevados a cabo por la administración de los grupos de usuarios afectados, la función de servicios de información y la Presidencia de la organización son revisados adecuadamente.

Las herramientas utilizadas para monitorear los costos son usadas efectiva y apropiadamente.

Evaluar el riesgo de los objetivos de control no cumplidos:**▸ Llevando a cabo:**

Mediciones ("Benchmarking") de presupuestos y costos contra organizaciones y buenas prácticas reconocidas en la industria/estándares internacionales apropiados.

Una revisión detallada del presupuesto actual y del año inmediato anterior contra los resultados reales, variaciones y acciones correctivas aplicadas.

▸ Identificando:

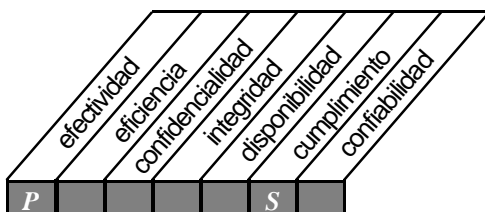
Presupuestos de la función de sistemas de información que no estén en línea con el presupuesto y los planes a corto y largo plazo de la organización y con los planes a corto y largo plazo de tecnología de información.

Los costos reales de la función de servicios de información que no hayan sido capturados

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:

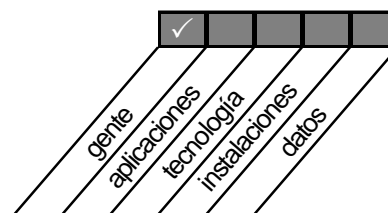
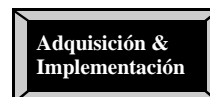
asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones

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



PO 6 MANEJO DE LA INVERSIÓN EN TECNOLOGÍA DE INFORMACIÓN

OBJETIVOS DE CONTROL

- 1 Ambiente Positivo de Control de la Información
- 2 Responsabilidad de la Gerencia en cuanto a Políticas
- 3 Comunicación de las Políticas de la Organización
- 4 Recursos para la Implementación de Políticas
- 5 Mantenimiento de Políticas
- 6 Cumplimiento de Políticas, Procedimientos y Estándares
- 7 Compromiso con la Calidad
- 8 Política sobre el Marco Referencial para la Seguridad y el Control Interno
- 9 Derechos de la Propiedad Intelectual
- 10 Políticas para Situaciones Específicas
- 11 Comunicación de la Sensibilización de Seguridad de la TI

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

La obtención de un entendimiento a través de:

► **Entrevistas:**

Director General
 Director de Operaciones
 Director de Finanzas
 Director de TI
 Funcionario de Seguridad
 Miembros del comité de planeación de la función de servicios de información
 Presidencia de la función de servicios de información

► **Obteniendo:**

Políticas y procedimientos relacionados con el marco referencial de control positivo y el programa de conocimiento y conciencia de la administración, con el marco referencial de seguridad y control interno y con el programa de calidad de la función de servicios de información.
 Las funciones y responsabilidades de planeación de la Presidencia.
 Objetivos y planes a corto y largo plazo organizacionales..
 Objetivos y planes a corto y largo plazo de tecnología de información.
 Reportes de estatus y minutas de las reuniones del comité de planeación.
 Un programa de comunicación.

Las políticas y procedimientos de la organización crean un marco referencial y un programa de conocimiento y conciencia, prestando atención específica a la tecnología de información, propiciando un ambiente de control positivo y considerando aspectos como:

- Integridad
- valores éticos
- código de conducta
- seguridad y control interno
- competencia del personal
- filosofía y estilo operativo de la administración
- responsabilidad, atención y dirección proporcionadas por el consejo directivo o su equivalente

La alta gerencia promueve un ambiente de control positivo a través del ejemplo.

La administración ha aceptado la responsabilidad total sobre la formulación, el desarrollo, la documentación, la promulgación, el control y la revisión regular de las políticas que rigen las metas y directivas generales.

Existe un programa de conocimiento y conciencia formal para proporcionar comunicación y entrenamiento relacionados con el ambiente positivo de control de la administración.

Existen políticas y procedimientos organizacionales para asegurar que los recursos adecuados y apropiados son asignados para implementar las políticas de la organización de manera oportuna.

Existen procedimientos apropiados para asegurar que el personal comprende las políticas y procedimientos implementados, y que se cumple con dichas políticas y procedimientos.

Las políticas y procedimientos de la función de servicios de información definen, documentan y mantienen una filosofía, políticas y objetivos formales que rigen la calidad de los sistemas y servicios producidos, y que éstos son consistentes con la filosofía, políticas y objetivos de la organización.

La administración de la función de servicios de información asegura que la calidad de la filosofía, las políticas y objetivos sea comprendida, implementada y mantenida a todos los niveles de la función de servicios de información.

Existen procedimientos que consideren la necesidad de revisar y aprobar periódicamente estándares, directivas, políticas y procedimientos clave relacionados con tecnología de información.

La Presidencia ha aceptado la responsabilidad total sobre el desarrollo de un marco referencial para el enfoque general de seguridad y control interno.

El documento del marco referencial de seguridad y control interno especifica la política, propósito, objetivos, estructura administrativa, alcance dentro de la organización, asignación de responsabilidades y definición de sanciones y acciones disciplinarias de seguridad y control interno asociados con la falta de cumplimiento de las políticas de seguridad y control interno.

Las políticas de seguridad y control interno identifican el proceso de control interno de la organización e incluye componentes de control tales como:

- ambiente de control
- reevaluación de riesgos
- actividades de control
- información y comunicación
- monitoreo

Existen políticas para asuntos especiales para documentar las decisiones administrativas sobre actividades, aplicaciones, sistemas y tecnologías particulares.

Evaluar los controles:

▸ **Probando que:**

Los esfuerzos de la administración para fomentar un control positivo cubren los aspectos clave tales como: integridad, valores éticos, código de conducta, seguridad y control interno, competencia del personal, filosofía y estilo operativo de la administración, y responsabilidad, atención y dirección proporcionados.

Los empleados han recibido el código de conducta y que lo comprenden.

Se da el proceso de comunicación de las políticas de la administración relacionadas con el ambiente de control interno de la organización.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- Existe el compromiso de la administración en cuanto a los recursos para formular, desarrollar, documentar, promulgar y controlar políticas que cubren el ambiente de control interno.
- La propiedad y habilidad para adaptarse a condiciones cambiantes de las revisiones regulares de estándares, directivas, políticas y procedimientos por parte de la administración.
- Los esfuerzos de monitoreo de la administración aseguran la asignación adecuada y apropiada de recursos para implementar las políticas de la organización de manera oportuna.
- Los esfuerzos de reforzamiento por parte de la administración con respecto a los estándares, directivas, políticas y procedimientos relacionados con su ambiente de control interno están asegurando su cumplimiento a través de toda la organización.
- La filosofía, políticas y objetivos de calidad determinan el cumplimiento y la consistencia con la filosofía, políticas y procedimientos corporativos y de la función de servicios de información.
- La administración de la función de servicios de información y el personal de desarrollo y operaciones determinan la filosofía de calidad y su política relacionada, y que los procedimientos y objetivos son comprendidos y cumplidos por todos los niveles dentro de la función de servicios de información.
- Los procesos de medición aseguran que los objetivos de la organización sean alcanzados.
- Miembros seleccionados de la administración están involucrados y comprenden el contenido de las actividades de seguridad y control interno (por ejemplo, reportes de excepción, conciliaciones, comparaciones, etc.) bajo su responsabilidad.
- Las funciones individuales, las responsabilidades y líneas de autoridad se comunican claramente y se comprenden en todos los niveles de la organización.
- Los departamentos seleccionados evalúan procedimientos para monitorear en forma rutinaria actividades de seguridad y control interno (por ejemplo, reportes de excepción, conciliaciones, comparaciones, etc.) y que se da en proceso para proporcionar retroalimentación a la administración.
- La documentación del sistema seleccionado confirma que las decisiones administrativas del sistema específico han sido documentadas y aprobadas de acuerdo con las políticas y procedimientos organizacionales.
- La documentación del sistema seleccionado confirma que las decisiones administrativas con respecto a actividades, sistemas de aplicación o tecnologías particulares han sido aprobadas por la Presidencia.

Evaluar el riesgo de los objetivos de control no cumplidos:

► **Llevando a cabo:**

- Mediciones ("Benchmarking") del marco referencial de control de la información y del programa de conocimiento y conciencia de la administración contra organizaciones similares o estándares internacionales/buenas prácticas de la industria reconocidas adecuadas.
- Una revisión detallada de una muestra de proyectos aprobados de seguridad y control interno para determinar que los proyectos fueron aprobados y tomaron como base un análisis de riesgos y costo/beneficio.

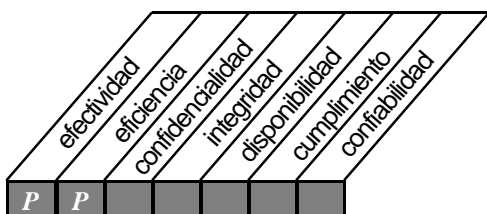
► **Identificando:**

- Un marco referencial de control débil que ponga en duda el compromiso de la administración en cuanto al fomento de un ambiente de control interno positivo a través de la organización.
- Fallas en la administración para comunicar efectivamente sus políticas relacionadas con el ambiente de control interno de la organización.
- Falta de recursos asignados para formular, desarrollar, documentar, promulgar y controlar políticas que cubran el ambiente de control interno.
- Estándares, directivas, políticas y procedimientos no actuales.
- Incumplimiento por parte de la administración para asegurar el respeto a los estándares, directivas, políticas y procedimientos a través de la organización.
- Deficiencias en la función de servicios de información en su compromiso con la calidad o en su habilidad para definir, documentar, mantener y comunicar efectivamente una filosofía, políticas y objetivos de calidad.
- Debilidades en el marco referencial de seguridad y control interno de la organización y/o en la función de servicios de información.
- Ausencia de políticas para asuntos específicos requeridas para dirigir actividades, aplicaciones y 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:

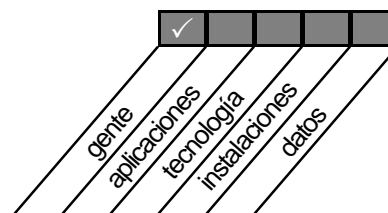
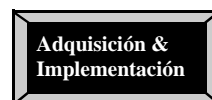
maximizar las contribuciones del personal a los procesos de TI

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



PO 7 ADMINISTRACIÓN DE RECURSOS HUMANOS

OBJETIVOS DE CONTROL

- | | |
|---|--|
| 1 | Reclutamiento y Promoción de Personal |
| 2 | Personal Calificado |
| 3 | Entrenamiento de Personal |
| 4 | Entrenamiento Cruzado o Personal de Respaldo |
| 5 | Procedimientos de Acreditación de Personal |
| 6 | Evaluación de Desempeño de los Empleados |
| 7 | Cambio de Puesto y Despido |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

La obtención de un entendimiento a través de:

► **Entrevistas:**

Funcionario de Recursos Humanos de la Organización y personal seleccionado
 Funcionario de Seguridad
 Personal seleccionado de seguridad
 Administrador de la función de servicios de información
 Funcionario de Recursos Humanos de la función de servicios de información
 Administradores seleccionados de la función de servicios de información
 Personal seleccionado de la función de servicios de información
 Personal seleccionado asociado con posiciones sensibles en la función de servicios de información

► **Obteniendo:**

Políticas y procedimientos relacionadas con la administración de recursos humanos
 Descripciones de puestos, formas de evaluación del desempeño y formas de desarrollo y entrenamiento
 Expedientes de personal de posiciones y personal seleccionado

Evaluar los controles:

► **Considerando sí:**

Se utilizan criterios para reclutar y seleccionar personal para cubrir posiciones vacantes.
 Las especificaciones de las habilidades y conocimientos requeridos para las posiciones staff toman en consideración requerimientos relevantes de profesionales cuando sea apropiado.
 La administración y los empleados aceptan el proceso de competencia del puesto.
 Los programas de entrenamiento son consistentes con los requerimientos mínimos documentados de la organización relacionados con la educación, el conocimiento y la conciencia generales que cubren los asuntos de seguridad de la información.
 La administración está comprometida con el entrenamiento y el desarrollo profesional de sus empleados.

Las brechas técnicas y administrativas están identificadas y si se están llevando a cabo las acciones apropiadas para manejar estas brechas.

Se dan los procesos de entrenamiento cruzado y respaldo de personal regularmente para las funciones de posiciones críticas.

Considerando si, *continúa*

Se da reforzamiento la política de vacaciones ininterrumpidas.

Si el proceso de liquidación de seguridad de la organización es adecuado.

Los empleados son evaluados tomando como base un conjunto estándar de perfiles de competencia para la posición y si se llevan a cabo evaluaciones en forma periódica.

Los procesos de despido y cambio de puesto aseguran la protección de los recursos de la organización.

Las políticas y procedimientos de recursos humanos concuerdan con leyes y regulaciones aplicables.

Evaluar la suficiencia:

▸ **Probando que:**

Las acciones de reclutamiento y/o selección, así como los criterios de selección reflejan objetividad y relevancia con respecto a los requerimientos de la posición.

El personal cuenta con los conocimientos adecuados de las operaciones para la función de su posición o áreas de responsabilidad.

Existen descripciones de puestos, y que éstas sean revisadas y se mantienen actualizadas.

Los expedientes del personal contienen un reconocimiento del personal en cuanto a la comprensión del programa general de educación, conciencia y conocimiento de la organización.

Se da el proceso de entrenamiento y educación continua para el personal apropiado asignado a funciones críticas.

El personal de seguridad de la información ha recibido el entrenamiento apropiado en procedimientos y técnicas de seguridad.

La administración y el personal de la función de servicios de información tienen conocimiento, conciencia y comprenden las políticas y procedimientos organizacionales.

Los procedimientos de investigación de despidos de seguridad son consistentes con leyes aplicables que rigen la confidencialidad.

El conocimiento de los objetivos del negocio por parte del personal asignado a las funciones críticas de servicios de información incluye la filosofía de los controles internos y los conceptos de control y seguridad de sistemas de información.

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de las actividades de recursos humanos contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria adecuados.

Una revisión detallada de las actividades de la administración de recursos humanos de la función de servicios de información.

▸ **Identificando:**

Causas y objeciones/quejas por parte de candidatos al puesto potenciales/reales.

Discrepancias en las actividades de reclutamiento, transferencia, promoción y despido relacionadas con:

- políticas y procedimientos no seguidos
- acciones no aprobadas por parte de la administración apropiada.
- acciones no basadas en especificaciones de puestos y calificación del personal.

Personal:

- calificado no apropiadamente
- cuyas oportunidades de entrenamiento y desarrollo no están ligadas a las brechas de competencia.
- cuyas evaluaciones de desempeño no existen o no dan soporte a la posición ocupada y/o funciones llevadas a cabo.
- cuya investigación de seguridad asociada con la contratación no fue llevada a cabo.
- cuyas investigaciones periódicas de seguridad no han sido llevadas a cabo.

Insuficiencias en los programas de entrenamiento y en las actividades de desarrollo personal.

Insuficiencias en el entrenamiento cruzado y respaldo de personal clave.

Reconocimientos de políticas de seguridad que no hayan sido firmados.

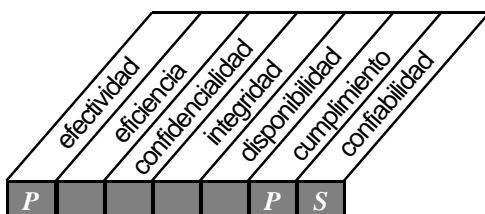
Presupuestos y tiempos inadecuados asignados al entrenamiento y desarrollo del personal.

Reportes de asistencia del personal que lleva a cabo funciones críticas que no indiquen que se han tomado días de asue-
to y vacaciones.

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:

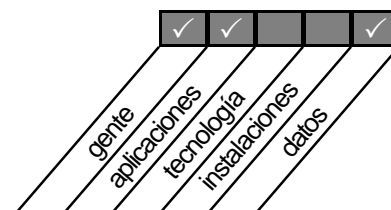
cumplir con obligaciones legales, regulatorias y contractuales

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 regulatorias
- revisiones regulares en cuanto a cambios
- búsqueda de asistencia legal y modificaciones
- seguridad y ergonomía
- privacidad
- propiedad intelectual
- flujo de datos



PO 8 ASEGURAMIENTO DEL CUMPLIMIENTO DE REQUERIMIENTOS EXTERNOS

OBJETIVOS DE CONTROL

- | | |
|---|--|
| 1 | Revisión de Requerimientos Externos |
| 2 | Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos |
| 3 | Cumplimiento de los Estándares de Seguridad y Ergonomía |
| 4 | Confidencialidad y Flujo de Datos |
| 5 | Comercio Electrónico |
| 6 | Cumplimiento con los Contratos de Seguros |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Consejo legal de la organización
 Funcionario de Recursos Humanos de la Organización
 Presidencia de la función de servicios de información

▸ **Obteniendo:**

Requerimientos relevantes gubernamentales o externos (por ejemplo, leyes, legislaciones, guías, regulaciones y estándares) con respecto a relaciones y revisiones de requerimientos externos, aspectos de seguridad y salud (incluyendo ergonomía), aspectos de confidencialidad, requerimientos de seguridad de sistemas de información y transmisión de datos criptográficos - tanto nacional como internacional.

Estándares/declaraciones contables nacionales o internacionales relacionadas con el uso de comercio electrónico

Reglamentos sobre impuestos relacionados con el uso de comercio electrónico

Estándares, políticas y procedimientos sobre:

- revisiones de requerimientos externos
- seguridad y salud (incluyendo ergonomía)
- confidencialidad
- seguridad
- clasificación de sensibilidad de datos ingresados, procesados, almacenados, extraídos y transmitidos
- comercio electrónico
- seguros

Copias de todos los contratos con socios de intercambio electrónico y con el proveedor de intercambio electrónico de datos (EDI), si aplica

Copias de todos los contratos de seguros relacionados con la función de servicios de información

Orientación del consejo legal sobre los requerimientos "uberrimae fidei" (de buena fe) para los contratos de seguros (Uberrimae fidei requiere que ambas partes divulguen completamente a la otra todo lo relacionado con el riesgo. En caso de no mostrarse buena fe en este sentido, el contrato será anulable por la parte agraviada y no podrá ser puesto en vigor nuevamente por la parte culpable).

Reportes de auditoría de auditores externos, proveedores de servicios como terceras partes y dependencias gubernamentales.

Evaluar los controles:▸ **Considerando sí:**

Existen políticas y procedimientos para:

- asegurar las acciones correctivas apropiadas relacionadas con la revisión oportuna de los requerimientos externos y si existen procedimientos para asegurar un cumplimiento continuo.
- coordinar la revisión de los requerimientos externos, con el fin de asegurar que se aplican oportunamente las acciones correctivas que garantizan el cumplimiento de los requerimientos externos.
- dirigir protección apropiada, así como objetivos de seguridad y salud.
- asegurar que se proporcionan entrenamiento y educación en seguridad y salud apropiadamente a todos los empleados.
- monitorear el cumplimiento de las leyes y regulaciones aplicables de seguridad y salud.
- proporcionar la dirección/enfoque adecuados sobre confidencialidad de tal manera que todos los requerimientos legales caigan dentro de este alcance.
- informar a los aseguradores acerca de todos los cambios materiales realizados al ambiente de la función de servicios de información.
- asegurar el cumplimiento con los requerimientos de los contratos de seguros
- asegurar que se lleven a cabo las actualizaciones necesarias cuando de inicia un contrato de seguros nuevo/modificado.

Los procedimientos de seguridad van de acuerdo con todos los requerimientos legales y si éstos están siendo tomados en cuenta adecuadamente, incluyendo:

- protección con "passwords" o contraseñas y software para limitar el acceso
- procedimientos de autorización
- medidas de seguridad de terminales
- medidas de encriptamiento de datos
- controles contra incendios
- protección contra virus
- seguimiento oportuno de reportes de violaciones

Evaluar la suficiencia:▸ **Probando que:**

Las revisiones de los requerimientos externos:

- son actuales, completos y suficientes en cuanto a aspectos legales, gubernamentales y regulatorios
- traen como resultado una pronta acción correctiva

Las revisiones de seguridad y salud son llevadas a cabo dentro de la función de servicios de información para asegurar el cumplimiento de los requerimientos externos

Las áreas problemáticas que no cumplan con los estándares de seguridad y salud sean rectificadas

El cumplimiento de la función de servicios de información en cuanto las políticas y procedimientos de confidencialidad y seguridad.

Los datos transmitidos a través de las fronteras internacionales no violan las leyes de exportación

Los contratos existentes con los proveedores de comercio electrónico consideren adecuadamente los requerimientos

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

especificados en las políticas y procedimientos organizacionales

Los contratos de seguros existentes consideren adecuadamente los requerimientos especificados en las políticas y procedimientos organizacionales

En donde se hayan impuesto límites regulatorios a los tipos de encriptamiento que pueden ser utilizados (por ejemplo, la longitud de la llave), la encriptamiento aplicada cumpla con las regulaciones

En donde las regulaciones o procedimientos internos requieran la protección y/o encriptamiento especial de ciertos elementos de datos (por ejemplo, números PIN bancarios, Números de expedientes de Impuestos, de Inteligencia Militar), dicha protección/encriptamiento sea proporcionada a estos datos.

Los procesos EDI reales desplegados por la organización aseguran el cumplimiento con las políticas y procedimientos organizacionales y con los contratos individuales del socio de comercio electrónico (y del proveedor EDI, en caso de aplicar)

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") del cumplimiento de los requerimientos externos, actividades EDI y requerimientos de contratos de seguros contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiados

Una revisión detallada de los archivos de requerimientos externos para asegurar que se han llevado a cabo acciones correctivas, o bien, que están siendo implementadas

Una revisión detallada de los reportes de seguridad para evaluar si la información sensible/confidencial (definida como tal por procedimientos internos o por regulaciones externas) está siendo protegida apropiadamente en cuanto a seguridad y confidencialidad

▸ **Identificando:**

Requerimientos externos que no hayan sido cumplidos por la organización

Acciones significativas no resueltas/no corregidas en respuesta a las revisiones de requerimientos externos

Riesgos de seguridad y salud (incluyendo ergonomía) en el ambiente de trabajo que no hayan sido considerados

Debilidades en la confidencialidad y la seguridad relacionadas con flujos de datos y/o flujo de datos internacional

Interrupciones en el comercio electrónico

Debilidades en los contratos con socios comerciales relacionadas con procesos de comunicación, mensajes de transacción, seguridad y/o almacenamiento de datos

Debilidades en las relaciones de confianza con socios comerciales

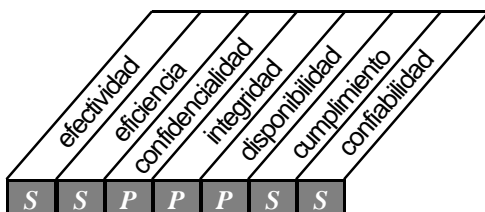
Debilidades/equivocaciones en la cobertura del seguro

Incumplimientos de los términos del contrato

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:

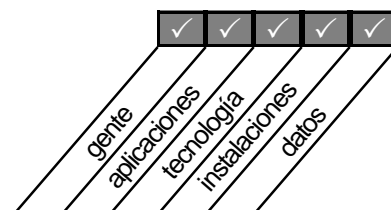
- diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.)
- alcance: global o de sistemas específicos
- actualización de evaluación de riesgos
- metodología de evaluación de riesgos
- medición de riesgos cualitativos y/o cuantitativos
- plan de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

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



PO 9 EVALUACIÓN DE RIESGOS

OBJETIVOS DE CONTROL

- | | |
|---|-----------------------------------|
| 1 | Evaluación del Riesgo del Negocio |
| 2 | Enfoque de Evaluación de Riesgos |
| 3 | Identificación de Riesgos |
| 4 | Medición de Riesgos |
| 5 | Plan de Acción contra Riesgos |
| 6 | Aceptación de Riesgos |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Presidencia de la función de servicios de información
 Personal seleccionado de la función de servicios de información
 Personal seleccionado de manejo de riesgos

▸ **Obteniendo:**

Políticas y procedimientos relacionados con la evaluación de riesgos
 Documentos de evaluación de riesgos del negocio
 Documentos de evaluación de riesgos operativos
 Documentos de evaluación de riesgos de la función de servicios de información
 Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos
 Expedientes de personal para personal seleccionado de evaluación de riesgos
 Políticas de seguros que cubren el riesgo residual

Evaluar los controles:

▸ **Considerando sí:**

Existe un marco referencial para la evaluación sistemática de riesgos, incorporando los riesgos de información relevantes para el logro de los objetivos de la organización y formando una base para determinar la forma en la que los riesgos deben ser manejados a un nivel aceptable.
 El enfoque de evaluación de riesgos asegura la evaluación actualizada regular de riesgos tanto a nivel global como a nivel específico de sistemas.
 Existen procedimientos de evaluación de riesgos para determinar que los riesgos identificados incluyen factores tanto externos como internos y toman en consideración los resultados de las auditorías, inspecciones, e incidentes identificados.
 Los objetivos de toda la organización están incluidos en el proceso de identificación de riesgos.

Los procedimientos para el monitoreo de cambios en la actividad de procesamiento de sistemas determinan que los riesgos y exposición de los sistemas son ajustados oportunamente.

Existen procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos y controles de mitigación.

La documentación de evaluación de riesgos incluye:

- una descripción de la metodología de evaluación de riesgos
- la identificación de exposiciones significativas y los riesgos correspondientes
- los riesgos y exposiciones correspondientes considerados

Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos.

El personal asignado a evaluación de riesgos está adecuadamente calificado

Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones.

Se utilizan cálculos y otros métodos en la medición de riesgos, amenazas y exposiciones

El plan de acción contra riesgos es utilizado en la implementación de medidas apropiadas para mitigar los riesgos, amenazas y exposiciones.

La aceptación del riesgo residual toma en cuenta:

- la política organizacional
- la identificación y medición de riesgos
- la incertidumbre inherente al enfoque de evaluación de riesgos mismo
- el costo y la efectividad de implementar salvaguardas y controles

La cobertura de los seguros compensan el riesgo residual

Evaluar la suficiencia:

▸ **Probando que:**

Se cumple con el marco referencial de evaluación de riesgos en cuanto a que las evaluaciones de riesgos con actualizadas regularmente para reducir el riesgo a un nivel aceptable.

La documentación de evaluación de riesgos cumple con el marco referencial de evaluación de riesgos y es mantenido y preparado apropiadamente.

La administración y el personal de la función de servicios de información tienen conocimiento y conciencia y están involucrados en el proceso de evaluación de riesgos

La administración comprende los factores relacionados con los riesgos y la probabilidad de amenazas

El personal relevante comprende y acepta formalmente el riesgo residual

Los reportes emitidos a la Presidencia para su revisión y acuerdo con los riesgos identificados y utilización en el monitoreo de actividades de reducción de riesgos sean oportunos

El enfoque utilizado para analizar los riesgos traiga como resultado una medición cuantitativa o cualitativa (o combinada) de la exposición al riesgo

Los riesgos, amenazas y exposiciones identificados por la administración y atributos relacionados con los riesgos sean utilizados para detectar cada ocurrencia de una amenaza específica.

El plan de acción contra riesgos es actual e incluye controles económicos y medidas de seguridad para mitigar la exposición al riesgo

Existen prioridades desde la más alta hasta la más baja, y que existe una respuesta apropiada para cada riesgo:

- control planeado preventivo de mitigación.
- control secundario detectivo
- control terciario correctivo

Los escenarios de riesgo versus control están documentados, son actuales y son comunicados al personal apropiado

Existe suficiente cobertura de seguros con respecto al riesgo residual aceptado y que éste es considerado contra varios escenarios de amenaza, incluyendo:

- incendio, inundaciones, terremotos, tornados, terrorismo y otros desastres naturales no predecibles
- violaciones a las responsabilidades fiduciarias del empleado
- interrupción del negocio, ganancias perdidas, clientes perdidos, etc.
- otros riesgos no cubiertos generalmente por la tecnología de información y planes de riesgo/continuidad del negocio

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") del marco referencial de evaluación de riesgos contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiados

Una revisión detallada del enfoque de evaluación de riesgos utilizado para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual

▸ **Identificando:**

Riesgos no identificados

Riesgos que no hayan sido medidos

Riesgos no considerados/manejados a un nivel aceptable

Evaluaciones de riesgos obsoletos y/o evaluaciones de información en riesgo obsoleta

Medidas incorrectas cuantitativas y/o cualitativas de riesgos, amenazas y exposiciones

Planes de acción contra riesgos que no aseguren controles económicos y medidas de seguridad

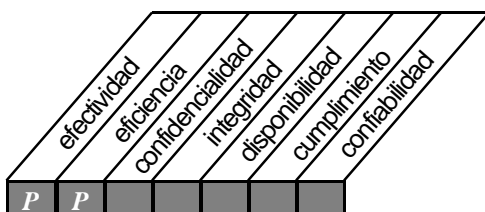
Falta de aceptación formal del riesgo residual

Cobertura de seguros inadecuada

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:

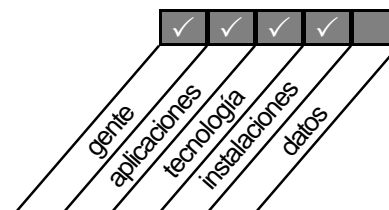
- la propiedad de los proyectos
- el involucramiento de los usuarios
- la estructuración jerárquica de tareas y los puntos de revisión
- asignación de responsabilidades
- aprobación de fases y proyecto
- presupuestos de costos y horas hombre
- planes y metodología de aseguramiento de calidad

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



PO 10 ADMINISTRACIÓN DE PROYECTOS**OBJETIVOS DE CONTROL**

- 1 Marco Referencial para la Administración de Proyectos
- 2 Participación del Departamento Usuario en la Iniciación de Proyectos
- 3 Miembros y Responsabilidades del Equipo del Proyecto
- 4 Definición del Proyecto
- 5 Aprobación del Proyecto
- 6 Aprobación de las Fases del Proyecto
- 7 Plan Maestro del Proyecto
- 8 Plan de Aseguramiento de la Calidad de Sistemas
- 9 Planeación de Métodos de Aseguramiento
- 10 Manejo Formal de Riesgos de Proyectos
- 11 Plan de Prueba
- 12 Plan de Entrenamiento
- 13 Plan de Revisión Post-Implementación

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Administrados de Calidad de la Organización
 Administrador/Coordinador de Calidad de Proyectos
 Propietarios/patrocinadores del Proyecto
 Líder del equipo del Proyecto
 Coordinador de Aseguramiento de Calidad
 Funcionario de Seguridad
 Miembros del comité de planeación de la función de servicios de información
 Administración de la función de servicios de información

▸ **Obteniendo:**

Políticas y procedimientos relacionados con el marco referencial de administración de proyectos
 Políticas y procedimientos relacionados con la metodología de administración de proyectos
 Políticas y procedimientos relacionados con los planes de aseguramiento de la calidad
 Políticas y procedimientos relacionados con los métodos de aseguramiento de la calidad
 Plan Maestro del Proyecto de Software (Software Project Master Plan (SPMP))
 Plan de Aseguramiento de la Calidad del Software (Software Quality Assurance Plan (SQAP))
 Reportes de estatus del proyecto
 Reportes de estatus y minutas de las reuniones del comité de planeación
 Reportes de Calidad del Proyecto

Evaluar los controles:▸ **Considerando sí:**

El marco referencial de administración de proyectos:

- define el alcance y los límites para la administración de proyectos
- asegura que las demandas del proyecto sean revisadas en cuanto a su consistencia con el plan operativo aprobado y si los proyectos son priorizados de acuerdo con este plan
- define la metodología de administración de proyectos a ser adoptada y aplicada en cada proyecto emprendido, incluyendo:
 - planeación del proyecto
 - asignación de personal
 - asignación de responsabilidades y autoridad
 - distribución de tareas
 - presupuestos de tiempo y recursos
 - puntos de revisión
 - puntos de verificación
 - aprobaciones
- suficiencia y actualización
- asegura la participación de la administración del departamento usuario afectado (propietario/patrocinador) en la definición y autorización de un proyecto de desarrollo, implementación o modificación
- especifica la base sobre la cual los miembros del personal son asignados a los proyectos
- define las responsabilidades y la autoridad de los miembros del equipo del proyecto
- asegura la creación de estatutos claros por escrito que definan la naturaleza y alcance del proyecto antes de comenzar a trabajar sobre el mismo
- proporciona un documento inicial de definición del proyecto que incluya estatutos claros sobre la naturaleza y alcance del proyecto
- incluye las siguientes razones para llevar a cabo el proyecto, entre ellas:
 - una definición del problema a ser resuelto o del proceso a ser mejorado
 - una definición de la necesidad del proyecto expresada en términos de incrementar la habilidad de la organización para alcanzar metas
 - un análisis de las deficiencias en sistemas relevantes existentes
 - las oportunidades que se abrirían al incrementar la eficiencia y hacer más económica la operación
 - el control interno y la necesidad de seguridad que sería satisfecha por los proyectos
- considera la manera en la que los estudios de factibilidad de los proyectos propuestos deben ser preparados y aprobados por la Presidencia, incluyendo:
 - el ambiente del proyecto - hardware, software, telecomunicaciones
 - el alcance del proyecto - lo que este incluirá y excluirá en la primera implementación y en las subsecuentes
 - las limitaciones del proyecto - lo que debe retenerse durante este proyecto, aún cuando las oportunidades de mejora a corto plazo parezcan obvias
 - los beneficios y costos a ser realizados por el patrocinador o propietario/patrocinador del proyecto
- delinea la manera en la que cada fase del proceso de desarrollo (por ejemplo, preparación de estudios de factibilidad, definición de requerimientos, diseño del sistema, etc.) debe ser aprobada antes de proceder a la si-

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

guiente fase del proyecto (por ejemplo, programación, pruebas del sistema, pruebas de transacciones, pruebas en paralelo, etc.)

- requiere el desarrollo de un SPMP para cada proyecto y especifica la manera en la que el control deberá ser mantenido a través de la vida del proyecto, así como períodos (puntos de revisión) y presupuestos del mismo
- cumple con el estándar organizacional para SPMPs o, en caso de no existir éste, con algún otro estándar apropiado
- requiere el desarrollo de un SQAP para cada proyecto, asegura que éste se encuentre integrado con el SPMP y que sea revisado y acordado formalmente por todas las partes involucradas
- delinea la manera en la que el programa de manejo formal de riesgos del proyecto elimina o minimiza los riesgos relacionados con el mismo
- asegura el desarrollo de un plan de pruebas para cada proyecto de desarrollo, implementación y modificación
- asegura el desarrollo de un plan adecuado para el entrenamiento de personal propietario/patrocinador y de las funciones de servicios de información para cada proyecto de desarrollo, implementación y modificación

Se monitorean y reportan a la Presidencia los puntos de revisión y compra de software, compra de hardware, programación por contrato, actualizaciones de redes, etc.)

Los puntos de revisión y costos que excedan los montos y tiempos presupuestados requieren la aprobación de la administración apropiada de la organización

SQAP cumple con el estándar organizacional para SQAPs, o en caso de no existir éste, con los criterios seleccionados anteriormente

Las tareas de aseguramiento SQAP soportan la acreditación de sistemas nuevos o modificados y aseguran que los estatutos de control interno y seguridad cumplen con los requerimientos

Todos los propietarios/patrocinadores del proyecto han comentado sobre el SPMP y el SQAP y están de acuerdo sobre los elementos entregables y liberables finales.

El proceso de post-implementación es una parte integral del marco referencial de la administración del proyecto para asegurar que los sistemas de información nuevos o modificados han aportado los beneficios planeados

Evaluar la suficiencia:

▸ Probando que:

La metodología de administración de proyectos y todos los requerimientos fueron seguidos con consistencia

La metodología de administración de proyectos fue comunicada a todo el personal apropiado involucrado en el proyecto

La definición escrita de la naturaleza y alcance del proyecto concuerda con un patrón estándar

La naturaleza y alcance del involucramiento del propietario/patrocinador en la definición y autorización del proyecto, así como la conformidad con el involucramiento esperado del propietario/patrocinador según lo estipulado por el marco referencial de administración de proyectos

La asignación de los miembros del personal al proyecto y la definición de responsabilidades y autoridad de los miembros del equipo del proyecto sean respetadas

Existe evidencia de una definición por escrito clara de la naturaleza y alcance del proyecto antes de comenzar a trabajar sobre el mismo

Se ha aprobado y preparado un estudio de factibilidad

Se obtienen las aprobaciones por parte de la administración de la función de sistemas de información y de los propietarios / patrocinadores para cada fase del proyecto de desarrollo

Cada fase del proyecto es completada y que se obtienen las aprobaciones apropiadas según los requerimientos del SPMP

Se han desarrollado y aprobado el SPMP y el SQAP de acuerdo con el marco referencial de la administración de proyectos

El SPMP y el SQAP son suficientemente específicos y detallados

Las actividades/reportes obligatorios identificados han sido realmente ejecutados/producidos (por ejemplo, que se han llevado a cabo reuniones del Comité Ejecutivo de Planeación, reuniones para el proyecto o similares, que se han registrado minutas de las reuniones y que éstas han sido distribuidas a las partes relevantes, que se preparan y distribuyen reportes a las partes relevantes)

Se ha desarrollado y aprobado un plan de pruebas de acuerdo con el marco referencial de administración de proyectos y que éste es suficientemente específico y detallado

Las actividades/reportes obligatorios identificados en el plan de pruebas han sido realmente ejecutados/producidos

Existen criterios de acreditación utilizados para el proyecto y que éstos:

- se derivan de metas e indicadores de desempeño
- se derivan de requerimientos cuantitativos acordados
- aseguran que los requerimientos de control interno y seguridad son satisfechos
- están relacionados con el "Qué" esencial versus el "cómo" arbitrario
- definen un proceso formal de aprobación/no aprobación
- son capaces de una demostración objetiva dentro de un período de tiempo limitado
- no redefinen simplemente los requerimientos de los documentos de diseño

El programa de manejo de riesgos ha sido utilizado para identificar y eliminar o por lo menos minimizar los riesgos relacionados con el proyecto

Se ha cumplido con el plan de pruebas, que los propietarios/patrocinadores, así como las funciones de programación y aseguramiento de la calidad, han creado revisiones de las pruebas, y que se ha cumplido con un proceso de aprobación según lo esperado

Se ha preparado un plan para el entrenamiento del personal de las funciones de servicios de información y para los propietarios/patrocinadores, que éste ha dado el tiempo suficiente para completar las actividades de entrenamiento requeridas, y que ha sido utilizado para el proyecto

Se ha cumplido y seguido un plan de revisión post-implementación para el proyecto

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") del marco referencial de administración de proyectos contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de:

- el plan maestro del proyecto para determinar el alcance de la participación del propietario/patrocinador y la adecuación del proceso general para definir, autorizar y ejecutar el proyecto, incluyendo:
- definición de las funciones del sistema
- factibilidad, dadas las limitaciones del proyecto
- determinación de los costos y beneficios del sistema
- propiedad de los controles del sistema
- impacto e integración en otros sistemas propietarios/patrocinadores
- compromiso de recursos (de personal y económicos) por parte del propietario/patrocinador
- definición de responsabilidades y autoridad de los participantes en el proyecto
- criterios de aceptación deseables y alcanzables
- puntos de revisión y verificación en la autorización de las diferentes fases del proyecto

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- elaboración de gráficas de Gantt, bitácoras de problemas, resúmenes de reuniones, etc. en la administración del proyecto
- reportes de calidad para determinar si existen problemas sistemáticos en el proceso de planeación de aseguramiento de la calidad de sistemas en la organización
- el programa de manejo formal de riesgos del proyecto para determinar si se han identificado y eliminado, o por lo menos minimizado los riesgos.
- la ejecución del plan de pruebas para determinar que éste probó completamente todo el proyecto de desarrollo, implementación o modificación del sistema
- la ejecución del plan de entrenamiento para determinar que éste ha preparado adecuadamente a propietarios/patrocinadores y al personal de la función de servicios de información en el uso del sistema
- la revisión post-implementación para determinar si los beneficios otorgados corresponden a los planeados

► **Identificando:**

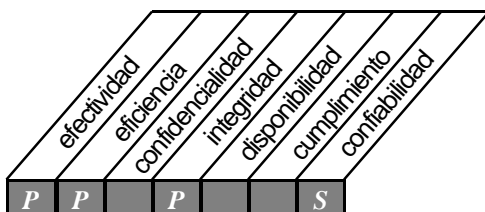
Proyectos que:

- sean administrados inadecuadamente
- hayan excedido fechas claves
- hayan excedido costos
- sean obsoletos
- no hayan sido autorizados
- no sean técnicamente factibles
- no sean económicos
- no otorguen los beneficios planeados
- no contengan puntos de verificación
- no sean aprobados en puntos de verificación claves
- no hayan sido acreditados para implementación
- no satisfagan los requerimientos de control interno y seguridad
- no eliminen o mitiguen los riesgos
- no hayan sido probados completamente
- necesitaran un entrenamiento no llevado a cabo o inadecuado para el sistema en proceso de implementación
- no hayan contado con una revisión post-implementación

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:

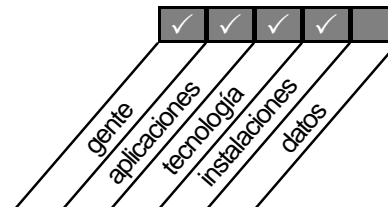
- estructura del plan de calidad
- responsabilidades de aseguramiento de la calidad
- metodología del ciclo de vida de desarrollo de sistemas
- pruebas y documentación de sistemas y programas
- revisiones y reporte de aseguramiento de calidad

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



PO 11 ADMINISTRACIÓN DE CALIDAD

OBJETIVOS DE CONTROL	
1	Plan General de Calidad
2	Enfoque de Aseguramiento de Calidad
3	Planeación del Aseguramiento de Calidad
4	Revisión del Aseguramiento de Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información
5	Metodología del Ciclo de Vida de Desarrollo de Sistemas
6	Metodología del Ciclo de Vida de Desarrollo de Sistemas par Cambios Mayores a la Tecnología Actual
7	Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas
8	Coordinación y Comunicación
9	Marco Referencial de Adquisición y Mantenimiento para la Infraestructura de Tecnología
10	Relaciones con Terceras Partes como Implementadores
11	Estándares para la Documentación de Programas
12	Estándares para Pruebas de Programas
13	Estándares para Pruebas de Sistemas
14	Pruebas Piloto/En Paralelo
15	Documentación de las Pruebas del Sistema
16	Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo
17	Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información
18	Reportes de Revisiones de Aseguramiento de la Calidad
19	Reportes de Revisión de Aseguramiento de Calidad

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

- **Entrevistas:**
 - Director General
 - Miembros del comité de planeación de la función de servicios de información
 - Director de TI
 - Funcionario de Seguridad
 - Administrador de la Calidad de la Organización
 - Administrador de la Calidad de la Función de Servicios de Información
 - Administración de la función de servicios de información
 - Propietarios/patrocinadores del sistema
- **Obteniendo:**
 - Políticas y procedimientos relacionados con el aseguramiento de la calidad, el ciclo de vida del desarrollo de sistemas y la documentación de sistemas
 - Funciones y responsabilidades de planeación de la Presidencia

Plan estratégico, política de calidad, manual de calidad y plan de calidad de la organización del Plan estratégico, política de calidad, manual de calidad, plan de calidad y plan de administración de la configuración de la función de servicios de información

Gráficas de todas las funciones de aseguramiento de la calidad

Minutas de las reuniones individuales de planeación de la calidad

Minutas de las reuniones convocadas para la revisión de la metodología del ciclo de vida del desarrollo de sistemas

Copias de las revisiones a la metodología del ciclo de vida del desarrollo de sistemas

Reportes de estatus y minutas de las reuniones del comité de planeación

Evaluar los controles:

► **Considerando sí:**

El plan de calidad:

- toma como base los planes a corto y largo plazo de la organización
- fomenta la filosofía de mejora continua y responde a las preguntas básicas qué, quién y cómo
- es completo y actual

El plan de calidad de la función de servicios de información:

- toma como base el plan general de calidad de la organización y los planes a corto y largo plazo de tecnología de información
- fomenta la filosofía de mejora continua y responde a las preguntas básicas qué, quién y cómo
- es completo y actual

Si el enfoque estándar de calidad existe, y si éste:

- es aplicable tanto a las actividades generales como a las específicas del proyecto
- es escalable y, de esta manera, aplicable a todos los proyectos
- es comprendido por todo el personal involucrado en un proyecto y en actividades de aseguramiento de la calidad
- fue aplicable a través de todas las fases de un proyecto

El enfoque estándar de aseguramiento de la calidad prescribe los tipos de actividades de aseguramiento de la calidad (y específicas revisiones, auditorías, inspecciones, etc.) a ser llevados a cabo para alcanzar los objetivos del plan general de calidad

La planeación de aseguramiento de la calidad prescribe el alcance y calendarización de las actividades de aseguramiento de la calidad

Las revisiones de aseguramiento de la calidad evalúan el cumplimiento general de los estándares, políticas y procedimientos de la función de servicios de información

La Presidencia ha definido e implementado estándares, políticas y procedimientos de servicios de información, incluyendo una metodología formal de ciclo de vida del desarrollo de sistemas adquirida, desarrollada internamente o una combinación de ambas

La metodología del ciclo de vida del desarrollo de sistemas:

- rige el proceso de desarrollar, adquirir, implementar y mantener sistemas de información computarizados y tecnología afín
- soporta y fomenta los esfuerzos de desarrollo/modificación que cumplen con los planes a corto y largo plazos de la función de servicios de información y de la organización
- requiere un proceso de desarrollo y modificación estructurado que contenga puntos de revisión en momentos clave de decisión, así como la autorización para proceder con el proyecto en cada punto de revisión
- es completa y actual

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- es capaz de ser adaptada/escalada para acoplarse a todos los tipos de desarrollo que ocurren dentro de la organización
- es aplicable a la creación y mantenimiento tanto de software adquirido como desarrollado internamente
- cuenta con provisiones documentadas para cambios tecnológicos
- ha construido un marco referencial general en cuanto a la adquisición y mantenimiento de la infraestructura tecnológica
- cuenta con pasos a seguir (tales como adquisición, programación, documentación y pruebas, establecimiento de parámetros, y "applying fixes") que deben ser regidos por, y estar en línea con el marco referencial de adquisición y mantenimiento de la infraestructura tecnológica
- fomenta la provisión de criterios para la aceptación de terceras partes como implementadores, manejo de cambios, manejo de problemas, funciones participantes, instalaciones, herramientas y estándares y procedimientos de software
- requiere el mantenimiento de documentación detallada de programación y de sistemas (por ejemplo, diagramas de flujo, diagramas de flujo de datos, narrativas escritas de programación, etc.), y que dichos requerimientos hayan sido comunicados a todo el personal involucrado
- requiere que la documentación se mantenga actualizada al ocurrir cambios
- requiere la aplicación de pruebas rigurosas y sólidas de programas/sistemas
- define las circunstancias bajo las cuales deben conducirse pruebas piloto o en paralelo de sistemas nuevos o modificados
- requiere, como parte de cada proyecto de desarrollo, implementación o modificación de sistemas, que las pruebas sean verificadas, documentadas y retenidas en forma independiente

El enfoque de aseguramiento de la calidad de la organización:

- requiere que se lleve a cabo una revisión post-implementación para asegurar que todos los sistemas nuevos o modificados sean desarrollados y puestos en producción de acuerdo con la metodología del ciclo de vida del desarrollo de sistemas, mismo que debe ser respetado por el equipo del proyecto
- requiere una revisión de la medida en la que los sistemas nuevos o modificados han alcanzado los objetivos establecidos para ellos por la administración
- trae como resultado reportes, los cuales propician el llevar a cabo el desarrollo de sistemas y las recomendaciones de efectividad para la administración (tanto para los usuarios como para la función de servicios de información) como corresponda
- cuenta con recomendaciones a las que se les da seguimiento periódicamente y que son reportadas a los funcionarios de la Presidencia apropiados

La administración de la función de servicios de información de la Presidencia revisa y actualiza apropiadamente la metodología del ciclo de vida del desarrollo de sistemas con regularidad para asegurar su suficiencia para tecnología nueva y de desarrollo/modificación

Existe una variación de niveles de control para los distintos tipos de proyectos de desarrollo y mantenimiento (por ejemplo, si los proyectos grandes reciben mayor control que los pequeños)

El logro de una coordinación y comunicación estrecha a través del ciclo de vida de desarrollo de sistemas entero se da entre los clientes de la función de servicios de información y los implementadores del sistema

Existe un compromiso apropiado por parte de las diferentes funciones/personas dentro de la organización (por ejemplo, administración de la función de servicios de información, funcionario de seguridad, personal legal, personal de aseguramiento de la calidad, personal de auditoría, usuarios, etc.)

Existen medidas para medir los resultados de las actividades, permitiendo una evaluación sobre si se han logrado las metas de calidad

Evaluar la suficiencia:**▸ Probando que:**

Los procedimientos para el desarrollo del Plan de Calidad de la función de servicios de información incluyen las siguientes entradas:

- Planes a corto y largo plazo de la organización
- Planes a corto y largo plazo de la función de servicios de información
- Política de Calidad de la organización
- Política de Calidad de la función de servicios de información
- Plan de Calidad de la organización
- Plan de administración de la configuración de la función de servicios de información

El Plan de Calidad de la función de servicios de información toma como base los planes a corto y largo plazo de la función de servicios de información, los cuales definen:

- los esfuerzos y/o adquisiciones de desarrollo de sistemas de aplicación
- interfases con otros sistemas (internos y externos)
- la plataforma/infraestructura de la función de servicios de información requerida para soportar los sistemas e interfases
- los recursos (tanto financieros como humanos) para desarrollar/soportar el ambiente de la función de servicios de información planeado
- el entrenamiento requerido para desarrollar y soportar ambiente de la función de servicios de información planeado

El Plan de Calidad de la función de servicios de información considera lo siguiente:

- en términos medibles no ambiguos, el nivel planeado del servicio a ser otorgado a los clientes (internos o externos)
- en términos medibles no ambiguos, los "outages" planeados máximos para cada sistema y plataforma
- las estadísticas de desempeño requeridas para monitorear los objetivos planeados de desempeño/"outage", incluyendo la manera en la que deben ser reportados y a quién deben ser distribuidos
- los procesos de monitoreo/revisión necesarios para asegurar el desarrollo/modificación/transición en el ambiente/infraestructura de la función de servicios de información identificados en la función de servicios de información
- los planes a corto y largo plazo: están correctamente planeados, monitoreados, probados, documentados, implementados y cuentan con el entrenamiento y los recursos necesarios
- los intervalos en los que el Plan de Calidad debe ser actualizado

El personal de aseguramiento de la Calidad cumple consistentemente con el enfoque y el plan de aseguramiento de la calidad y otros procedimientos operativos establecidos

La metodología del ciclo de vida de desarrollo de sistemas asegura apropiadamente:

- controles suficientes durante el proceso de desarrollo para sistemas y tecnologías nuevas
- comunicación con todos los empleados apropiados involucrados en el desarrollo y mantenimiento de sistemas
- se utilizan procedimientos para los cambios tecnológicos
- se utilizan procedimientos para asegurar la aceptación y aprobación de los usuarios
- la adecuación de los acuerdos de terceras partes como implementadores

Los usuarios comprenden los controles y requerimientos de la metodología del ciclo de vida del desarrollo de sistemas

Los mecanismos de control de cambios dentro de la metodología del ciclo de vida del desarrollo de sistemas permiten el llevar a cabo cambios a la metodología y que ésta es un documento "vivo"

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- El registro de las revisiones y modificaciones a la metodología del ciclo de vida del desarrollo de sistemas de la organización refleja los nuevos sistemas y tecnologías considerados actualmente y esperados en el futuro
- Los resultados completos de las pruebas de programas y sistemas (incluyendo resultados de pruebas en paralelo/piloto) son revisados y retenidos para pruebas futuras
- Existe un proceso para resolver problemas encontrados durante las pruebas
- Se ha llevado a cabo una revisión post-implementación por parte del personal de aseguramiento de la calidad
- Los representantes del departamento usuario involucrados en los proyectos de desarrollo de sistemas están satisfechos con el uso actual de la metodología
- El personal de aseguramiento de la calidad comprende claramente su función dentro de la organización
- Se requiere el llevar a cabo una revisión de aseguramiento de la calidad subsecuente al término de todas las pruebas del sistema y de la revisión y aprobación de los resultados de las pruebas por parte del personal de la administración de la función de servicios de información apropiada, de aseguramiento de la calidad y de los usuarios
- La revisión de aseguramiento de la calidad trae como resultado acciones correctivas por parte de la administración
- Se llevan a cabo revisiones post-implementación, que los resultados son comunicados a la Presidencia y que se requieren planes de acción para las áreas de implementación con necesidad de mejoras.
- Los resultados de las mediciones de las metas de calidad, existen y se trabaja con ellos

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de la metodología del ciclo de vida del desarrollo de sistemas contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de las medidas de desempeño incluidas en el Plan de Calidad y asegurar sí éstas:

- son alcanzables
- satisfacen los requerimientos/expectativas de la corporación
- satisfacen los requerimientos/expectativas de los usuarios
- son medibles

Una revisión detallada de una muestra de proyectos para asegurar que:

- se ha cumplido con la metodología del ciclo de vida del desarrollo de sistemas
- toda adaptación/escalamiento de la metodología del ciclo de vida del desarrollo de sistemas es apropiada y ha sido aprobada
- se han obtenido aprobaciones en todos los puntos de revisión y por parte de todo el personal clave de control (por ejemplo, funcionario de seguridad de la función de servicios de información, personal de aseguramiento de la calidad, representantes de los usuarios, etc.)
- se han dado una coordinación y comunicación estrechas entre los usuarios de la función de servicios de información y los implementadores de sistemas (internos o terceras partes)
- se ha seguido el marco referencial para la adquisición y el mantenimiento para la infraestructura técnica, junto con cualquier paso relevante involucrado
- el desarrollo/las modificaciones fueron terminados satisfactoria y oportunamente
- se terminaron los reportes apropiados de aseguramiento de la calidad y se llevaron a cabo las acciones correctivas necesarias de manera oportuna

Una revisión detallada de la manera en la que la documentación de la programación y los sistemas es preparada, revisada, aprobada y mantenida

Una revisión detallada de la manera en la que las pruebas de programas y sistemas (incluyendo pruebas piloto/en paralelo) y la documentación son preparadas, aprobadas y mantenidas

Una revisión detallada del proceso de verificación de post-implementación de aseguramiento de la calidad para asegurar que los reportes consideran el cumplimiento de las provisiones del proceso del ciclo de vida del desarrollo de sistemas, así como los aspectos de efectividad y calidad de los sistemas nuevos/modificados

► **Identificando:**

Planes de calidad que no se relacionen con los planes a corto y largo plazo

Instancias en la que no se utilice la metodología del ciclo de vida del desarrollo de sistemas y aquellas situaciones de sobreutilización de la metodología (por ejemplo demasiada estructura en proyectos pequeños, y no suficiente en proyectos mayores)

Las instancias en las que la metodología del ciclo de vida del desarrollo de sistemas haya sido utilizada inapropiadamente (por ejemplo, aplicar la metodología del ciclo de vida del desarrollo de sistemas para desarrollos internos en la implementación de un paquete de software "off-the-shelf", sin modificarla de manera correspondiente)

Instancias en las que la coordinación y la comunicación entre el personal involucrado en el proceso del ciclo de vida del desarrollo de sistemas (incluyendo terceras partes como implementadores) sean pobres o inexistentes

Instancias en las que los distintos pasos a seguir en la adquisición y mantenimiento de la infraestructura de tecnología (por ejemplo, adquisición, programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y "applying fixes") no hayan sido seguidas adecuadamente

Situaciones en las que no exista documentación de los programas y/o sistemas, en donde ésta sea inadecuada o no esté actualizada

Instancias en las que las pruebas de programas y/o sistemas (incluyendo pruebas piloto/en paralelo) no hayan sido llevadas a cabo, hayan sido realizadas inadecuadamente y/o no hayan sido documentadas o hayan sido documentadas inadecuadamente

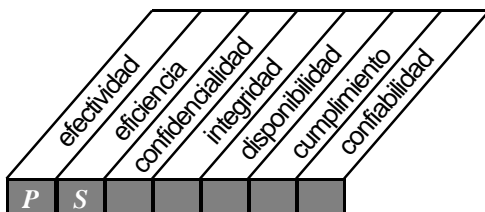
Situaciones en las que las verificaciones de revisiones/post implementación de aseguramiento de la calidad no hayan sido llevadas a cabo o hayan sido realizadas inadecuadamente

Situaciones en las que las verificaciones de revisiones/post implementación de aseguramiento de la calidad hayan sido ignoradas por la administración y en las que se hayan implementado sistemas que no deberían haber sido implementados

ADQUISICIÓN & IMPLEMENTACIÓN

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:

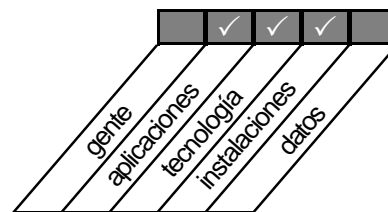
asegurar el mejor enfoque para cumplir con los requerimientos del usuario

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



AI 1 ADMINISTRACIÓN DE SOLUCIONES

OBJETIVOS DE CONTROL

- 1 Definición de Requerimientos de Información
- 2 Formulación de Acciones Alternativas
- 3 Formulación de la Estrategia de Adquisición
- 4 Paquetes de Software de Aplicación
- 5 Estudio de Factibilidad Tecnológica
- 6 Estudio de Factibilidad Económica
- 7 Arquitectura de Información
- 8 Reporte de Análisis de Riesgos
- 9 Controles Económicos de Seguridad
- 10 Diseño de Pistas de Auditoría
- 11 Ergonomía
- 12 Selección del Software del Sistema
- 13 Control de Abastecimiento
- 14 Adquisición de Productos de Software
- 15 Mantenimiento de Software de Terceras Partes
- 16 Contratos de Programación de Aplicaciones
- 17 Aceptación de Instalaciones
- 18 Aceptación de Tecnología

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

► **Entrevistas:**

Director de TI
 Funcionario de Seguridad
 Presidencia de la función de servicios de información
 Propietarios/patrocinadores del proyecto
 Administración de contratos

► **Obteniendo:**

Políticas y procedimientos relacionados con el ciclo de vida de desarrollo de sistemas y con la adquisición de software
 Objetivos y planes a corto y largo plazo de tecnología de información
 Documentación seleccionada del proyecto, incluyendo definición de requerimientos, análisis de alternativas, estudios de factibilidad tecnológica, estudios de factibilidad económica, análisis de modelos de datos de la empresa / arquitectura de información, análisis de riesgos, estudios de economía sobre control/seguridad interna, análisis de pistas de auditoría, estudios ergonómicos, y planes de aceptación y resultados de pruebas de instalaciones y tecnología específica
 Contratos seleccionados relacionados con la compra, desarrollo o mantenimiento de software

Evaluar los controles:▸ **Considerando sí:**

Existen políticas y procedimientos que requieren que:

- los requerimientos de usuarios satisfechos por el sistema existente o a ser satisfechos por el nuevo sistema propuesto o modificado sean claramente definidos antes de la aprobación de cualquier proyecto de desarrollo, implementación o modificación
- los requerimientos de los usuarios sean revisados y aprobados por escrito por el propietario/patrocinador enterado antes de la aprobación de cualquier proyecto de desarrollo, implementación o modificación
- los requerimientos operativos y funcionales de la solución sean satisfechos incluyendo desempeño, seguridad, confiabilidad, compatibilidad y legislación
- las soluciones alternativas a los requerimientos de los usuarios sean estudiadas y analizadas antes de seleccionar una u otra solución de software
- se lleve a cabo la identificación de paquetes de software comercial que satisfagan los requerimientos del usuario para un proyecto específico de desarrollo o modificación antes de tomar la decisión final
- las alternativas para la adquisición de los productos de software están claramente definidos en términos de practicidad, internamente desarrollados, a través del contacto o mejorar el software existente o una combinación de todos los anteriores
- el propietario/patrocinador enterado prepare, analice y apruebe un estudio de factibilidad técnica para cada alternativa con el fin de satisfacer los requerimientos del usuario establecidos para el desarrollo de un proyecto de sistemas nuevo o modificado
- en cada proyecto de desarrollo, modificación o implementación de sistemas, se lleve a cabo un análisis de los costos y los beneficios asociados con cada alternativa considerada para satisfacer los requerimientos del usuario
- el propietario/patrocinador enterado prepare, analice y apruebe un estudio de factibilidad económica antes de tomar la decisión respecto a desarrollar o modificar un proyecto de sistemas nuevo o modificado propuesto
- se preste atención al modelo de datos de la empresa mientras se identifica y analiza la factibilidad de las soluciones
- en cada proyecto de desarrollo, implementación o modificación de sistemas propuesto, se prepare y documente un análisis de las amenazas a la seguridad, de las debilidades y los impactos potenciales y las salvaguardas factibles de seguridad y control interno para reducir o eliminar el riesgo identificado
- los costos y los beneficios de seguridad sean examinados cuidadosamente para garantizar que los costos de los controles no exceden los beneficios
- se obtenga una aprobación formal del estudio costo/beneficio por parte de la administración
- se requieran controles y pistas de auditoría apropiados para ser aplicados en todos los sistemas modificados o nuevos propuestos durante la fase de diseño del proyecto
- las pistas de auditoría y los controles dan la posibilidad de proteger a los usuarios contra la identificación o mal uso de su identidad por parte de otros usuarios (ej., ofreciendo anonimato, pseudónimos, ausencia de vínculos y confidencialidad)
- cada proyecto de desarrollo, implementación o modificación de sistemas propuesto preste atención a los problemas ergonómicos asociados con la introducción de sistemas automatizados
- la administración de la función de servicios de información identifique todos los programas de software de sistemas potenciales que satisfarán sus requerimientos operativos
- los productos sean revisados y probados antes de ser adquiridos y utilizados
- la compra de productos de software siga las políticas de adquisición de la organización definiendo el marco referencial para la creación de la solicitud de propuesta, la selección del proveedor de software y la negociación del contrato.
- para el software con licencia adquirido de terceras partes, los proveedores cuenten con procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de software
- la adquisición de servicios de programación por contrato se justifique a través de una requisición de servicios por

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- escrito por parte de un miembro designado de la función de servicios de información
- se acuerde en el contrato con el proveedor un plan de aceptación de las instalaciones y que dicho plan defina los procedimientos y criterios de aceptación
- los productos finales de los servicios de programación por contrato terminados sean revisados y probados de acuerdo con los estándares establecidos por el grupo de aseguramiento de la calidad de la función de servicios de información y otras partes interesadas antes de pagar por el trabajo realizado y aprobar el producto final
- se acuerde en el contrato con los proveedores un plan de aceptación para tecnología específica, y que dicho plan defina los procedimientos y criterios de aceptación
- la adquisición de servicios de programación por contrato sea justificada a través de una requisición por escrito de servicios por parte de un miembro designado de la función de servicios de información

Se lleve a cabo un análisis de riesgos en línea con el marco referencial general de evaluación de riesgos

Existen los mecanismos para asignar o mantener los atributos de seguridad para la exportación e importación de datos, y para interpretarlos correctamente.

La administración haya desarrollado e implementado un enfoque de adquisición central, que describa un conjunto común de procedimientos y estándares a ser seguidos en la adquisición de servicios de hardware, software y servicios de tecnología de información

Los contratos estipulen que el software, la documentación y otros elementos entregables y liberables sean sujetos a pruebas y revisiones antes de ser aceptados

Las pruebas incluidas en las especificaciones del contrato consisten en pruebas de 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 para evitar cualquier falla inesperada del sistema

Las pruebas de aceptación de instalaciones son llevadas a cabo para garantizar que éstas y el ambiente, satisfacen los requerimientos especificados en el contrato

Las pruebas de aceptación de tecnología específica deberían incluir inspección, pruebas de funcionalidad y de carga de trabajo

Evaluar la suficiencia:

▸ Probando que:

Los requerimientos de los usuarios satisfechos por el sistema existente y a ser satisfechos por el sistema nuevo o modificado propuesto hayan sido claramente definidos, revisados y aprobados por escrito por parte del usuario enterado antes del desarrollo, implementación o modificación del proyecto

Los requerimientos de las soluciones funcionales y operativas sean satisfechos incluyendo desempeño, seguridad, confiabilidad, compatibilidad y legislación

Todas las debilidades y deficiencias de procesamiento en el sistema existente hayan sido identificadas y sean tomadas en cuenta y resueltas completamente por el sistema nuevo o modificado propuesto

Los cursos de acción alternativos que satisfarán los requerimientos de los usuarios, establecidos para un sistema nuevo o modificado propuesto, hayan sido analizados apropiadamente

Los paquetes de software comercial que satisfagan las necesidades de un proyecto particular de desarrollo o modificación de sistemas hayan sido identificados y considerados apropiadamente

Todos los costos y beneficios identificables asociados con cada alternativa hayan sido soportados apropiadamente e incluidos como parte del estudio de factibilidad económica requerido

Se haya prestado atención al modelo de datos de arquitectura de información/empresa al identificar y analizar su factibilidad

El reporte de análisis de riesgos en cuanto a amenazas a la seguridad, vulnerabilidades e impactos potenciales y las salvaguardas factibles de seguridad y control interno sea preciso, completo y suficiente

- Los problemas de seguridad y control interno hayan sido tomados en cuenta apropiadamente en la documentación del diseño del sistema
- La aprobación de la administración en cuanto a que los controles existentes y planeados son suficientes y aportan beneficios apropiados comparados con los costos de compensación
- Existen mecanismos disponibles para las pistas de auditoría o que éstos pueden ser desarrollados para la solución identificada y seleccionada
- Se ha tomado en cuenta un diseño amigable al usuario para mejorar las habilidades finales de éste durante el diseño del sistema y el desarrollo de diseño de pantallas, formatos de reporte, instalaciones de ayuda en línea, etc.
- Se han considerado aspectos ergonómicos durante el diseño y el desarrollo del sistema
- Se han incluido aspectos de desempeño de usuarios (por ejemplo, tiempo de respuesta del sistema, capacidades de carga/descarga, y reportes "ad hoc") en las especificaciones de requerimientos del sistema antes de su diseño y desarrollo
- La identificación de todos los programas de software de sistemas potenciales que satisfacen los requerimientos operativos
- La función de servicios de información cumpla con un conjunto común de procedimientos y estándares en la adquisición de hardware, software y servicios relacionados con tecnología de información
- Los productos adquiridos sean revisados y probados antes de ser usados y costeados completamente
- El acuerdo de compra de software permite al usuario tener una copia del código fuente el programa, si aplica
- Las actualizaciones, renovaciones de tecnología y "fixes" son especificados en los documentos de adquisición
- El mantenimiento de terceras partes incluye los requerimientos de validación protección y mantenimiento de la integridad del producto de software
- El personal de programación por contrato trabaja sujetándose al mismo nivel de pruebas, revisión y aprobaciones que se exige a los programadores propios de la organización
- La función de aseguramiento de la calidad de la organización es responsable de la revisión y aprobación del trabajo llevado a cabo por los programadores por contrato
- La propiedad y suficiencia del plan de aceptación de instalaciones, incluyendo los procedimientos y criterios de aceptación
- La propiedad y suficiencia del plan específico de aceptación de tecnología, incluyendo inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ Llevando a cabo:

Mediciones ("Benchmarking") de la identificación de los requerimientos de los usuarios para lograr soluciones automatizadas contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de:

- la identificación de soluciones automatizadas para satisfacer los requerimientos del usuario (incluyendo la definición de requerimientos del usuario, formulación de cursos de acción alternativos; identificación de paquetes de software comercial y elaboración de estudios de factibilidad de desempeño tecnológico, de factibilidad económica, de arquitectura de información y de análisis de riesgos)
- la seguridad, los controles internos (incluyendo la consideración de diseños amigables al usuario, ergonomía, etc.) y las pistas de auditoría disponibles o "desarrollables" para la solución identificada y seleccionada
- la selección e implementación del software del sistema
- las políticas y procedimientos existentes de adquisición de software para la adecuación y el cumplimiento del control interno de la organización
- la manera en la que se administra el mantenimiento de terceras partes

- la manera en la que la programación de aplicación por contrato ha sido monitoreada y administrada
- la identificación de todo lo especificado en el contrato por parte de la administración de la función de servicios de información
- el proceso de aceptación de tecnología específica para asegurar que las inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo satisfacen los requerimientos especificados en el contrato

► **Identificando:**

Las deficiencias en la metodología del ciclo de vida del desarrollo de sistemas de la organización

Soluciones que no satisfacen los requerimientos del usuario

Tentativas de desarrollo de sistemas que:

- no hayan considerado cursos alternativos de acción, trayendo como resultado una solución más costosa
- no hayan considerado los paquetes de software comercial que podrían haber sido implementados en menos tiempo y a un menor costo
- no hayan considerado la factibilidad tecnológica de las alternativas o hayan considerado inapropiadamente la factibilidad tecnológica de la solución elegida, trayendo como resultado la incapacidad para implementar la solución como fue diseñada originalmente
- hayan hecho suposiciones equivocadas en el estudio de factibilidad económica, trayendo como resultado la elección del curso de acción incorrecto
- no hayan considerado el modelo de datos de la arquitectura de información/empresa, trayendo como resultado la elección del curso de acción incorrecto
- no hayan conducido análisis de riesgos sólidos, y consecuentemente, no hayan identificado adecuadamente los riesgos (incluyendo amenazas, vulnerabilidades e impactos potenciales) o los controles internos y de seguridad para reducir o eliminar los riesgos identificados

Soluciones que:

- estuvieran ya sea sobre controladas o no controladas suficientemente debido a que la economía de los controles y la seguridad fueron examinados inapropiadamente
- no hayan contado con pistas de auditoría adecuadas
- no hayan considerado los aspectos ergonómicos y de diseño amigable para el usuario, trayendo como resultado errores en la entrada de datos que podrían haber sido evitados
- no hayan seguido el enfoque de adquisiciones establecido por la organización, trayendo como resultado costos adicionales creados por la organización

La falta de software de sistemas necesario

La ineffectividad del software de sistemas debido al establecimiento incorrecto de parámetros

Mantenimiento de software de terceras partes que no haya satisfecho los términos del contrato, afectando negativamente a la organización en el logro de su misión y/o metas

Programas de aplicación por contrato que no hayan satisfecho los términos del contrato, trayendo como consecuencia costos adicionales a la organización, atraso en la implementación de los sistemas, etc.

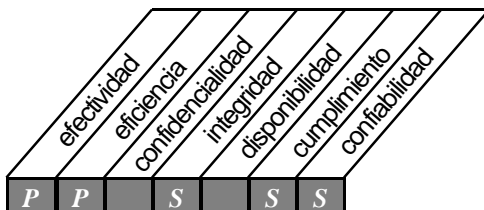
Situaciones en las que las instalaciones hayan sido aceptadas sin probar completamente el ambiente, trayendo como consecuencia no satisfacer los requerimientos de los usuarios y/o no cumplir con los términos del contrato

Las instancias en las que se haya aceptado una tecnología específica, pero que no se hayan llevado a cabo adecuadamente inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo, trayendo como resultado el que la tecnología no satisfaga los requerimientos del usuario y/o no cumpla con los términos del contrato

Cualquier falla del sistema

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:

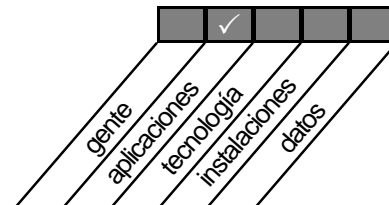
proporcionar funciones automatizadas que soporten efectivamente al negocio

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



AI 2 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN**OBJETIVOS DE CONTROL**

- 1 Métodos de Diseño
- 2 Cambios Significativos a Sistemas Actuales
- 3 Aprobación del Diseño
- 4 Definición y Documentación de Requerimientos de Archivos
- 5 Especificaciones de Programas
- 6 Diseño para la Recopilación de Datos Fuente
- 7 Definición y Documentación de Requerimientos de Entrada de Datos
- 8 definición de Interfases
- 9 Interfase Usuario - Máquina
- 10 Definición y Documentación de Requerimientos de Procesamiento
- 11 Definición y Documentación de Requerimientos de Salida de Datos
- 12 Controlabilidad
- 13 Disponibilidad como Factor Clave de Diseño
- 14 Estipulaciones de Integridad TI para Software de Programas de Aplicación
- 15 Pruebas de Software de Aplicación
- 16 Materiales de Consulta y Soporte para Usuario
- 17 Reevaluación del Diseño del Sistema

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

- **Entrevistas:**
 - Director de TI
 - Funcionario de Seguridad
 - Presidencia de la función de servicios de información
 - Propietarios / patrocinadores de proyectos
- **Obteniendo:**
 - Políticas y procedimientos relacionados con la metodología del ciclo de vida del desarrollo de sistemas
 - Objetivos y planes a corto y largo plazo de tecnología de información
 - Documentación seleccionada del proyecto, incluyendo aprobaciones de diseños, definición de requerimientos de archivo, especificaciones de programas, diseño de recopilación de datos fuente, definición de requerimientos de entrada, interfase usuario - máquina, definición de requerimientos de procesamiento, definición de requerimientos de salida, requerimientos de control interno/seguridad, requerimientos de disponibilidad, provisiones para la integridad de tecnología de información, plan de pruebas y resultados del software de aplicación, materiales de soporte y referencia para usuarios y reevaluación del diseño del sistema

Evaluar los controles:**► Considerando sí:**

Las políticas y procedimientos aseguran:

- la metodología del ciclo de vida de desarrollo de sistemas de la organización aplica tanto para el desarrollo de nuevos sistemas como para la modificación de sistemas existentes y participación del usuario
- el vínculo con el usuario al crear las especificaciones de diseño y al verificar éstas contra los requerimientos del usuario
- en el caso de cambios mayores a los sistemas existentes, se observe un proceso de ciclo de vida de desarrollo de sistemas similar al del utilizado en los casos de desarrollo de nuevos sistemas
- las especificaciones de diseño sean aprobadas por la administración, los departamentos usuarios afectados y la Presidencia de la organización, cuando esto sea apropiado para todos los proyectos nuevos de modificación y desarrollo de sistemas
- se aplica un proceso apropiado para definir y documentar el formato de archivos para cada proyecto nuevo de desarrollo o modificación de sistemas, incluyendo que se requiera el respeto de las reglas de diccionario de datos
- se preparan especificaciones detalladas de programas para cada proyecto de desarrollo o modificación de información, y que estas especificaciones concuerdan con las especificaciones del diseño del sistema
- se especifican los mecanismos adecuados para la recolección y captura de datos para cada desarrollo nuevo del sistema o proyecto de modificación
- se especifican los mecanismos adecuados para la recopilación y entrada de datos para cada nuevo proyecto de desarrollo o modificación de sistemas
- existen mecanismos adecuados para la definición y documentación de los requerimientos de entrada para cada proyecto nuevo de desarrollo o modificación de sistemas
- existe el desarrollo de una interfase entre el usuario y la máquina fácil de utilizar y autodocumentable (por medio de funciones de ayuda en línea)
- existen mecanismos adecuados para la definición y documentación de los requerimientos de procesamiento para cada nuevo proyecto de desarrollo o modificación de sistemas
- existen mecanismos adecuados para la definición y documentación de los requerimientos de salida para cada nuevo proyecto de desarrollo o modificación de sistemas
- se especifican mecanismos adecuados para asegurar los requerimientos de seguridad y control internos para cada proyecto nuevo de desarrollo o modificación de sistemas
- los requerimientos de seguridad y control interno incluyen controles de aplicación que garantizan la precisión, suficiencia y autorización de entradas y salidas
- se considera la disponibilidad en el proceso de diseño de sistemas nuevos o modificados en la etapa más temprana posible, y que esta consideración debe analizar, en caso necesario, un incremento a través de mejoras de mantenimiento y confiabilidad
- los programas de aplicación contienen provisiones que verifican rutinariamente las tareas llevadas a cabo por el software para ayudar a asegurar la integridad de los datos
- el software de aplicación es probado de acuerdo con el plan de pruebas del proyecto y los estándares establecidos antes de ser aprobado por el usuario
- se preparan manuales adecuados de soporte y referencia para usuarios (preferiblemente en formato electrónico) como parte del proceso de desarrollo o modificación de cada sistema
- el diseño del sistema es reevaluado siempre que ocurren discrepancias tecnológicas y/o lógicas significativas durante el desarrollo o el mantenimiento del sistema

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- La metodología del ciclo de vida de desarrollo de sistemas asegura que los materiales de soporte y referencia para usuarios son actualizados de manera precisa y oportuna
- La metodología de ciclo de vida de desarrollo de sistemas requiere el llevar a cabo una evaluación de sensibilidad durante la iniciación del desarrollo o modificación de nuevos sistemas
- La metodología de ciclo de vida de desarrollo de sistemas requiere la evaluación de los aspectos básicos de seguridad y control interno de un sistema nuevo a ser desarrollado o modificado, junto con el diseño conceptual del sistema, con el fin de integrar los conceptos de seguridad en el diseño lo más pronto posible
- La metodología del ciclo de vida de desarrollo de sistemas requiere que los aspectos de seguridad lógica y de las aplicaciones sean considerados e incluidos en el diseño de nuevos sistemas o modificaciones de sistemas existentes
- La evaluación de los aspectos de control internos y de seguridad está basada en un buen marco referencial
- Los sistemas de Inteligencia Artificial están funcionando en una interacción o en el marco referencial con los operadores humanos para asegurar que las decisiones importantes sean aprobadas.
- La exposición de la información sensible que se utiliza durante las pruebas de la aplicación se reduce ya sea con limitaciones severas de acceso o la despersonalización de los datos históricos.

Evaluar la suficiencia:

► Probando que:

- La participación del usuario en el proceso de ciclo de vida de desarrollo de sistemas es significativa
- La metodología del ciclo de vida de desarrollo de sistemas asegura que existe un proceso que considera apropiadamente todos los aspectos de diseño de sistemas (por ejemplo, entrada, procesamiento, salida, controles internos, seguridad, recuperación en caso de desastre, tiempo de respuesta, reportes, control de cambios, etc.)
- Los usuarios clave de los sistemas están involucrados en el proceso del diseño del sistema
- Que la revisión del diseño y el proceso de aprobación aseguran que todos los problemas han sido resueltos antes de comenzar a trabajar sobre la siguiente fase del proyecto
- Los cambios mayores a los sistemas existentes aseguran que éstos han sido desarrollados utilizando una metodología de ciclo de vida de desarrollo de sistemas similar a la utilizada para el desarrollo de nuevos sistemas
- Existen los procedimientos de aprobación del diseño para asegurar que la programación del sistema no se inicie hasta que se hayan obtenido las aprobaciones correspondientes
- Los requerimientos de archivo y la documentación del sistema, así como el diccionario de datos, son consistentes con los estándares
- Se aprueban las especificaciones finales de archivos
- Las especificaciones de programación concuerdan con las especificaciones del diseño del sistema
- Las especificaciones del diseño de recolección de datos y de entrada de datos concuerdan
- Existen las especificaciones del diseño de la interfase usuario - máquina
- Las especificaciones usuario - máquina es fácil de utilizar y que autodocumentación (utilizando instalaciones de ayuda en línea) funciona
- Se documenten las interfaces internas y externas
- Los requerimientos de procesamiento forman parte de las especificaciones del diseño
- Los requerimientos de salida forman parte de las especificaciones del diseño
- Los requerimientos de seguridad y control interno forman parte de las especificaciones del diseño
- Las especificaciones de diseño de los requerimientos de controles de aplicación garantizan la precisión, suficiencia, oportunidad y autorización de las entradas y las salidas
- Los requerimientos de seguridad y control interno han sido incluidos en el diseño conceptual del sistema (ya sea nuevo

- o modificado) lo más tempranamente posible
- El funcionario de seguridad está involucrado activamente en el proceso de diseño, desarrollo e implementación del proyecto del nuevo sistema o de modificación del sistema
- El diseño del sistema determina si se han cuantificado las mejoras de disponibilidad/confiabilidad en términos de tiempo y de procedimientos más eficientes en comparación con métodos anteriores, en caso de aplicar
- Las provisiones de programas de aplicación verifican rutinariamente las tareas llevadas a cabo por el software para asegurar la integridad de los datos
- Existen estándares de pruebas establecidos
- Existe un plan de pruebas del proyecto y un proceso de aprobación del usuario
- Los materiales de soporte y referencia para usuarios, así como las instalaciones de ayuda en línea están disponibles
- La función de "help desk" apoya efectivamente a los usuarios para solucionar problemas de procesamiento cada vez más complejos
- El proceso para escalar los problemas del help desk incluye el seguimiento, monitoreo y reporte de tales problemas a la administración de la función de servicios de información apropiada
- Se requiere la existencia de mecanismos para actualizar la documentación de los usuarios
- Existe la comunicación sobre los cambios a la documentación de los usuarios
- Se da el proceso de reevaluación siempre que ocurren discrepancias tecnológicas y/o lógicas significativas

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ Llevando a cabo:

Mediciones ("Benchmarking") de los costos de adquirir y desarrollar software de aplicación contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de:

- documentación seleccionada del diseño del sistema para evaluar la adecuación de las especificaciones del diseño y el cumplimiento del diseño en cuanto a dichas especificaciones
- proyectos seleccionados de desarrollo o modificación de nuevos sistemas, determinando si los documentos de especificación del diseño han sido revisados y aprobados por la administración de la función de servicios de información y las funciones de los usuarios afectados, así como por la Presidencia de la organización cuando esto sea apropiado
- documentación seleccionada del software para asegurar que los requerimientos de archivo (por lo menos para los archivos mencionados a continuación) son comprendidos claramente por el equipo de implementación del proyecto y están siendo estructurados por sistema y requerimientos del usuario, así como por las reglas de diccionario de datos de la organización:
 - Maestro
 - Transacciones
 - Comando
 - Programa
 - Control
 - Tablas
 - Reportes
 - Impresión
 - Bitácora
 - Transmisión
- proyectos de desarrollo o modificación de nuevos sistemas para asegurar que los archivos, programas, instrumentos de recopilación de datos fuente, entradas, interfaces usuario - máquina, pasos de procesamiento y salidas identificados en diagramas de flujo/diagramas de flujo de datos, corresponden a las especificaciones varias del diseño del sistema
- proyectos de desarrollo o modificación de nuevos sistemas para determinar que siempre que se identifiquen discrepancias técnicas y/o lógicas, ocurra un proceso efectivo de reevaluación del diseño del sistema

- proyectos de desarrollo o modificación de nuevos sistemas para determinar la existencia de cualquier discrepancia de diseño técnico o cualquier cambio funcional necesario
- proyectos de desarrollo o modificación de nuevos sistemas y diseños conceptuales de sistemas para evaluar la adecuación de las provisiones de seguridad y control interno que aseguren la precisión, la suficiencia, la oportunidad y la autorización de las entradas y salidas, así como la integración de los conceptos de seguridad en el diseño lo más tempranamente posible
- proyectos de desarrollo o modificación de nuevos sistemas para evaluar el diseño a la luz de una mayor confiabilidad y disponibilidad para el usuario final, así como de "mantenibilidad" para el personal de mantenimiento de la función de servicios de información
- proyectos para evaluar la adecuación de la verificación de integridad de los datos de los programas de aplicación
- proyectos de desarrollo o modificación de nuevos sistemas para asegurar que los materiales de referencia para los usuarios son actuales y consistentes con la documentación del sistema y que éstos satisfacen completamente las necesidades del usuario

Una revisión detallada de la efectividad de:

- el proceso de especificación de programas para asegurar que éstos están escritos de acuerdo a las especificaciones del diseño del usuario
- el proceso de especificación de entradas para asegurar que los programas están escritos de acuerdo a las especificaciones del diseño del usuario
- el proceso de especificación de interfase usuario - máquina para asegurar que los programas están escritos de acuerdo a las especificaciones del diseño del usuario
- el proceso de especificación de procesamiento para asegurar que los programas están escritos de acuerdo a las especificaciones del diseño del usuario
- el proceso de especificación de salidas para asegurar que los programas están escritos de acuerdo a las especificaciones del diseño del usuario

Una revisión detallada de los estándares de prueba de la organización y la implementación de los planes de pruebas relacionados para proyectos seleccionados de desarrollo y modificación de nuevos sistemas

Una revisión detallada de la satisfacción del usuario con el sistema, sus reportes, la documentación y material de referencia para el usuario, las instalaciones de ayuda, etc.

► **Identificando:**

Deficiencias en la metodología de ciclo de vida de desarrollo de sistemas utilizada para los proyectos de desarrollo o modificación de nuevos sistemas

Especificaciones de diseño que no reflejen los requerimientos del usuario

Requerimientos de archivo que no sean consistentes con las reglas de diccionario de datos de la organización

Proyectos de desarrollo o modificación de nuevos sistemas que contengan archivos, programas, selección de datos fuente, entradas, interfaces usuario - máquina, procesamiento, requerimientos de salida y/o Controlabilidad inadecuadamente definidos

Proyectos de desarrollo o modificación de nuevos sistemas en los que la disponibilidad no haya sido considerada en el proceso de diseño

Deficiencias en la integridad de los datos en software de programas de aplicación en proyectos de desarrollo o modificación de nuevos sistemas

Deficiencias en los estándares de pruebas de la organización, trayendo como consecuencia la implementación de sistemas que procesan incorrectamente los datos, y emiten incorrectamente reportes

Deficiencias en los planes de prueba en proyectos nuevos de desarrollo o modificación de sistemas

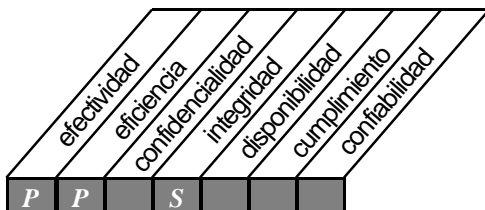
Deficiencias en los materiales de soporte y referencia para usuarios en proyectos nuevos de desarrollo o modificación de sistemas

Discrepancias técnicas y/o lógicas significativas que hayan ocurrido durante el desarrollo o mantenimiento del sistema que no hayan traído como consecuencia la reevaluación del diseño del sistema, y por lo mismo, no hayan sido corregidos o hayan traído como resultado correcciones provisionales no económicas en el sistema

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:

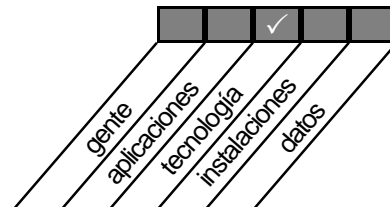
proporcionar las plataformas apropiadas para soportar aplicaciones de negocios

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



AI 3 ADQUISICIÓN Y MANTENIMIENTO DE ARQUITECTURA DE TECNOLOGÍA

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Evaluación de Nuevo Hardware y Software |
| 2 | Mantenimiento Preventivo para Hardware |
| 3 | Seguridad del Software del Sistema |
| 4 | Instalación del Software del Sistema |
| 5 | Mantenimiento del Software del Sistema |
| 6 | Controles para Cambios del Software del Sistema |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

- **Entrevistas:**
 - Director de TI
 - Funcionario de Seguridad
 - Presidencia de la función de servicios de información
 - Propietarios / patrocinadores de proyectos
- **Obteniendo:**
 - Políticas y procedimientos relacionados con la metodología del ciclo de vida del desarrollo de sistemas
 - Objetivos y planes a corto y largo plazo de tecnología de información
 - Documentación seleccionada del proyecto, incluyendo aprobaciones de diseños, definición de requerimientos de archivo, especificaciones de programas, diseño de recopilación de datos fuente, definición de requerimientos de entrada, interfase usuario - máquina, definición de requerimientos de procesamiento, definición de requerimientos de salida, requerimientos de control interno/seguridad, requerimientos de disponibilidad, provisiones para la integridad de tecnología de información, plan de pruebas y resultados del software de aplicación, materiales de soporte y referencia para usuarios y reevaluación del diseño del sistema

Evaluar los controles:

- **Considerando sí:**

Existen políticas y procedimientos que aseguran que:

 - se prepara un plan de evaluación formal para evaluar el nuevo hardware y software en cuanto a cualquier impacto sobre el desempeño global del sistema
 - la posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de información operativa es limitada
 - la preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema
 - se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema

- el software del sistema es instalado y mantenido de acuerdo con el marco referencial de adquisición y mantenimiento de la infraestructura de tecnología
- los proveedores de software del sistema proporcionan estatutos de aseguramiento de la integridad como parte de su software y todas las modificaciones al mismo
- la prueba global (por ejemplo, utilizando una metodología de ciclo de vida de desarrollo de sistemas) de software del sistema ocurre antes de que éste sea introducido al ambiente de producción
- los passwords o contraseñas de instalación proporcionados por el proveedor de software son modificados al momento de la instalación y que los cambios al software del sistema son controlados en línea con los procedimientos de administración de cambios de la organización

Existen políticas y procedimientos para el mantenimiento preventivo de hardware (tanto el operado por la función de servicios de información como por las funciones de los usuarios afectados) para reducir la frecuencia y el impacto de las fallas de desempeño

Se cumple con los pasos y la frecuencia de mantenimiento preventivo prescritos por el proveedor para cada dispositivo de hardware operado por la función de servicios de información y las funciones de los usuarios afectados

Evaluar la suficiencia:

► Probando que:

Existen los estatutos de aseguramiento de la integridad del software entregados por el proveedor de software del sistema para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema

La evaluación del desempeño trae como resultado la comparación con los requerimientos del sistema

Existe un proceso formal de evaluación del desempeño

El calendario de mantenimiento preventivo asegura que el mantenimiento de hardware programado no tendrá ningún impacto negativo sobre aplicaciones críticas o sensibles

El mantenimiento programado asegura que no ha sido planeado para períodos pico de carga de trabajo y que la función de servicios de información y las operaciones de los grupos de usuarios afectados son suficientemente flexibles para adaptar el mantenimiento preventivo rutinario planeado

Los programas operativos de servicios de información aseguran que existen las preparaciones adecuadas para manejar anticipadamente los tiempos muertos de hardware ocasionados por mantenimiento no programado

Los parámetros del software del sistema aseguran que fueron elegidos los correctos por parte del personal apropiado de la función de sistemas de información con el fin de asegurar la integridad de los datos y los programas almacenados en el sistema

El acceso se restringe únicamente a un número limitado de operadores dentro de la función de servicios de información

El software del sistema es instalado y mantenido de acuerdo con el marco referencial de adquisición y mantenimiento para la infraestructura de tecnología

Se llevan a cabo pruebas completas (utilizando una metodología de ciclo de vida de desarrollo de sistemas) para todo el software del sistema antes de autorizar su introducción al ambiente de producción

Todos los passwords o contraseñas de instalación del software del sistema proporcionados por los proveedores fueron cambiados al momento de la instalación

Todos los cambios al software del sistema fueron controlados de acuerdo con los procedimientos de administración de cambios de la organización

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

La administración del sistema (por ejemplo, adición de nuevos usuarios al sistema y a las redes; creación y respaldo de bases de datos, asignación de espacio para almacenamiento de datos, prioridades del sistema, etc.) se restringen únicamente a un número limitado de operadores dentro de la función de servicios de información

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de la adquisición, implementación y mantenimiento de hardware y software contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión de tallada de:

- la documentación seleccionada de sistemas operacionales o proyectos de desarrollo o modificación de sistemas para determinar si los requerimientos formales de desempeño de hardware y software (incluyendo referencias para volumen de transacción, tiempos de procesamiento y respuesta, tamaños de archivos y bases de datos, volúmenes de redes y compatibilidad de protocolos de comunicaciones) existen para todos los sistemas
- prácticas de mantenimiento de hardware para determinar si el mantenimiento está siendo llevado a cabo de acuerdo con los lineamientos del proveedor y calendarizado de tal manera que no afecte el desempeño global del sistema
- documentación seleccionada de sistemas operacionales y sistemas en desarrollo o modificación para evaluar las habilidades potenciales para burlar las restricciones de seguridad de acceso lógicas existentes proporcionadas por el software del sistema
- instalación, mantenimiento del sistema y controles de cambio para asegurar el cumplimiento con el marco referencial de adquisición y mantenimiento para la infraestructura de tecnología y la integridad del sistema

▸ **Identificando:**

Evaluaciones de desempeño que hayan afectado el desempeño global del sistema

Problemas de mantenimiento preventivo que hayan afectado el desempeño global del sistema Debilidades en la preparación, instalación y mantenimiento de software del sistema (incluyendo la selección de parámetros inapropiados de software del sistema) que hayan amenazado la seguridad de los datos y los programas almacenados en el sistema

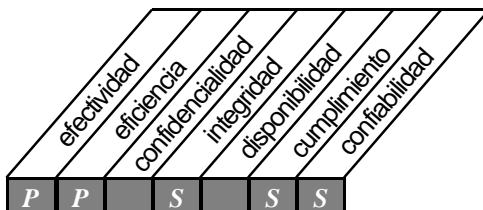
Debilidades en las pruebas de software del sistema que pudieran amenazar la seguridad de los datos y los programas almacenados en el sistema

Debilidades en el proceso de control de cambios del software del sistema que pudieran amenazar la seguridad de los datos y los programas almacenados en el sistema

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:

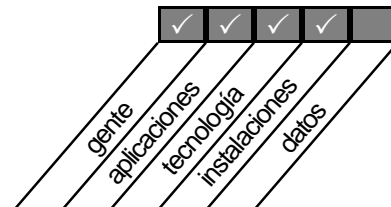
asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas

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



AI 4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVOS DE CONTROL

- 1 Futuros Requerimientos y Niveles de Servicios Operacionales
- 2 Manual de Procedimientos para Usuario
- 3 Manual de Operaciones
- 4 Material de Entrenamiento

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

► **Entrevistas:**

Desarrollo de aplicaciones de la función de servicios de información
 Mantenimiento de la función de servicios de información
 Control de cambios de la función de servicios de información
 Operaciones de la función de servicios de información
 Recursos humanos/entrenamiento de la función de servicios de información
 Administración de aseguramiento de la calidad de la función de servicios de información
 Usuarios seleccionados de recursos de sistemas de información

► **Obteniendo:**

Políticas y procedimientos organizacionales relacionados con:
 Planeación estratégica y objetivos del negocio, planeación de sistemas de información y desarrollo de aplicaciones
 Políticas y procedimientos de las funciones de servicios de información relacionadas con el desarrollo del sistema, incluyendo: organigrama, metodología del ciclo de vida de desarrollo de sistemas, planeación de capacidad, manuales de usuarios y operaciones, materiales de entrenamiento, pruebas y migración a estatus de producción y documentos de planeación de reanudación/ contingencia

Evaluar los controles:

► **Considerando sí:**

Los requerimientos operativos fueron determinados con estadísticas históricas de desempeño disponibles y entregadas del usuario con respecto a incrementos/decrementos esperados

El nivel de servicio y las expectativas de desempeño están o suficientemente detallados para permitir el seguimiento, la emisión de reportes y las oportunidades de mejora

Los requerimientos operativos y los niveles de servicio están determinados utilizando tanto desempeño histórico y ajustes de usuario como mediciones o "benchmarks" de la industria

Los niveles de servicio y requerimientos de procesamiento son un paso integral en la planeación de nuevos sistemas

Los manuales de procedimientos de usuarios, el manual de operaciones y los materiales de entrenamiento están desarrollados como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información, y se mantienen actualizados

Evaluar la suficiencia:▸ **Probando que:**

Existen requerimientos operacionales y que éstos reflejan tanto las expectativas de operación como las de los usuarios
El desempeño operacional está siendo medido, comunicado y corregido en donde existen deficiencias

El personal de operaciones y los usuarios están conscientes y tienen conocimiento de los requerimientos de desempeño

El personal de operaciones cuenta con manuales de operaciones para todos los sistemas y procesamientos bajo su responsabilidad

Todo el movimiento de programas de desarrollo de aplicaciones a producción requiere la actualización o creación de un manual de operaciones

Existen manuales de entrenamiento de usuarios para todas las aplicaciones, y reflejan actualmente la funcionalidad de la aplicación

Existen manuales de entrenamiento para todos los sistemas existentes y nuevos, y que éstos apoyan a los usuarios, reflejando el uso del sistema en la práctica diaria

Los manuales de usuario incluyen, pero no se limita a:

- visión global de los sistemas y el ambiente
- explicación de todas la entradas, programas, salidas e integración (con otros sistemas) de los sistemas
- explicación de todas las pantallas de entrada y despliegue de datos
- explicación de todos los mensaje de error y la respuesta apropiada
- procedimientos y/o recursos de escalamiento de problemas

El manual de operación incluyen, pero no se limita a:

- nombre del sistema, nombre de los programas, secuencia de ejecución
- definición de los nombres de todos los archivos de entrada, proceso y de salida y del formato del medio
- calendarización para las corridas diarias, semanales, mensuales, trimestrales, cuatrimestrales, fin de año, etc.
- comandos y parámetros de consola que requieran entradas por parte del operador
- mensajes y respuestas de mensajes de error
- procedimientos de respaldo, reinicio y recuperación en varios puntos o al darse una terminación anormal
- formatos o procedimientos de salidas especiales; distribución de reportes/salidas
- procedimiento de solución en caso de emergencia, si aplica

Se llevan a cabo el entrenamiento y el mantenimiento continuo de la documentación de aplicación, manuales de operación y de usuario

Evaluar el riesgo de los objetivos de control no alcanzados:▸ **Llevando a cabo:**

Para una selección de proyectos de desarrollo de sistemas, revisiones y aprobaciones de documentación en cuanto a:

- la consideración de futuros requerimientos y niveles de servicio de usuarios
- la tarea, entrega y liberación para la creación y mantenimiento de manuales de usuario
- la tarea, entrega y liberación para la creación y mantenimiento del manual de operación
- la tarea, entrega y liberación de entrenamiento para el usuario para comprender y utilizar nuevos sistemas o nuevas modificaciones

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Entrevistas a los usuarios para confirmar la suficiencia de las tentativas de desarrollo de sistemas, incluyendo los manuales desarrollados y el entrenamiento proporcionado

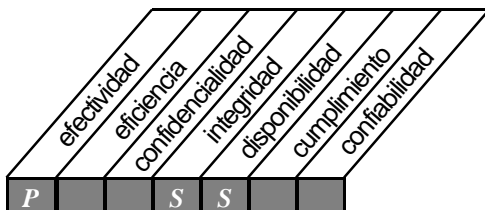
El análisis tanto de manuales de usuario como de operaciones en cuanto a actualidad y mantenimiento continuo

▸ **Identificando:**

- deficiencias en los manuales de usuarios, operaciones y entrenamiento
- la no existencia de acuerdos de niveles servicio entre el proveedor y la función de servicios de información
- Vendedor y función de servicios de información
- función y usuarios de servicios de información
- debilidades organizacionales para desarrollar y correr las aplicaciones requeridas

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:

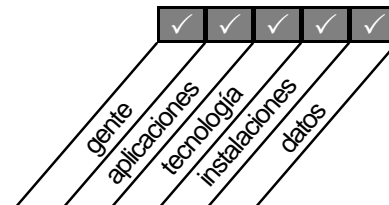
- capacitación
- conversión / carga de datos
- pruebas específicas
- acreditación
- revisiones post implementación

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



AI 5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS

OBJETIVOS DE CONTROL

- 1 Entrenamiento
- 2 Adecuación del Desempeño del Software de Aplicación
- 3 Conversión
- 4 Pruebas de Cambios
- 5 Criterios y Desempeño de Pruebas en Paralelo/Piloto
- 6 Prueba de Aceptación Final
- 7 Pruebas y Acreditación de Seguridad
- 8 Prueba Operacional
- 9 Promoción a Producción
- 10 Evaluación de la Satisfacción de los Requerimientos del Usuario
- 11 Revisión Gerencial Post - Implementación

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

► **Entrevistas:**

Director de TI

Administración de la función de servicios de información

Entrenamiento, desarrollo de aplicaciones, seguridad, aseguramiento de la calidad y administración de operaciones de la función de servicios de información

Funcionario de Seguridad

Administración seleccionada de sistemas recientemente desarrollados/en desarrollo

Contratos con proveedores para recursos de desarrollo de sistemas

► **Obteniendo:**

Políticas y procedimientos organizacionales relacionados con la planeación del ciclo de vida de desarrollo de sistemas

Políticas y procedimientos de la función de servicios de información relacionadas con políticas y comités de seguridad, planeación del ciclo de vida de desarrollo de sistemas para programas, unidades, planes de prueba del sistema, entrenamiento de usuarios, migración de sistemas de prueba a producción, aseguramiento de la calidad y entrenamiento

Plan y calendarización del ciclo de vida de desarrollo de sistemas, estándares de programación de ciclo de vida de desarrollo de sistemas, incluyendo procesos de requisición de cambios

Reportes muestra de estatus de tentativas de desarrollo de sistemas

Reportes post-implementación de tentativas de desarrollo anteriores

Evaluar los controles:

► **Considerando sí:**

Existen políticas y procedimientos relacionados con el proceso de ciclo de vida de desarrollo de sistemas

Existe una metodología formal de ciclo de vida de desarrollo de sistemas para la instalación y acreditación de sistemas, incluyendo, pero no limitándose a, un enfoque en fases sobre: entrenamiento, adecuación del desempeño, plan de conversión, pruebas de programas, grupos de programas (unidades) y del sistema total, un plan de pruebas prototipo o paralelo, pruebas de aceptación, pruebas y acreditación de seguridad, pruebas operativas, controles de cambio, revisión y modificación de implementación y post-implementación

Se lleva a cabo el entrenamiento de usuarios como parte de cada tentativa de desarrollo

Los controles de los programas/sistema son consistentes con los estándares de seguridad de la organización y con las políticas, procedimientos y estándares de la función de servicios de información

Existen varias librerías de desarrollo, prueba y producción para los sistemas en proceso

Existen criterios predeterminados para probar el acierto, las fallas y la terminación de tentativas futuras

El proceso de aseguramiento de la calidad incluye la migración independiente de desarrollo a las librerías de producción y la suficiencia de la aceptación requerida de los usuarios y grupos de operación

Los planes de prueba para simulación de volúmenes, intervalos de proceso y disponibilidad y acreditación de salidas forman parte del proceso

El programa de entrenamiento asociado con una muestra de varias tentativas de desarrollo de sistemas contiene: diferencias con respecto al sistema anterior, cambios que afecten las entradas, procesamiento, calendarización, distribución, interfaces con otros sistemas, errores y corrección de errores

Las herramientas automatizadas optimizan los sistemas desarrollados, en producción, y si estas herramientas son utilizadas para oportunidades de eficiencia

La solución de problemas ocurre en relación con un desempeño por debajo de lo óptimo

Evaluar la suficiencia:

► Probando que:

Se ha incluido en todas las tentativas de desarrollo de nuevos sistemas un plan formal para el entrenamiento de usuarios

El personal está consciente, comprende y tiene conocimiento de la necesidad de controles formales de desarrollo de sistemas y entrenamiento de usuarios para cada instalación e implementación de desarrollo

La consciencia, comprensión y conocimiento de usuarios seleccionados con respecto a sus responsabilidades en el diseño, aprobación, pruebas, entrenamiento, conversión y proceso de implementación es conocida y considerada

Se da seguimiento a los costos reales del sistema comparados con los costos estimados, y al desempeño real contra el esperado de los sistemas nuevos o modificados

Existe un plan de pruebas que cubre todas las áreas de recursos de sistemas de información: software de aplicación, instalaciones, tecnología y usuarios

Los usuarios comprenden todas las fases y responsabilidades en el desarrollo de sistemas, incluyendo:

- especificaciones de diseño, incluyendo iteraciones durante el ciclo de desarrollo
- análisis costo/beneficio y estudio de factibilidad
- aprobación en cada paso del proceso de desarrollo del sistema
- compromiso y evaluación del plan de pruebas y los resultados de las pruebas al ocurrir éstas
- aprobación y aceptación del sistema a través del ciclo de desarrollo
- aprobación final y aceptación del sistema
- evaluación de la suficiencia del entrenamiento recibido para sistemas recientemente entregados y liberados

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

El personal de desarrollo y la administración aseguran la estabilidad de los requerimientos de los usuarios una vez acordados éstos

La satisfacción del usuario es medida contra los elementos entregables y liberables de los proveedores, en comparación con los productos internos

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de la instalación y acreditación de sistemas contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de:

- el cumplimiento del grupo de desarrollo con las fechas límite y tareas en relación con la satisfacción del usuario la funcionalidad del sistema una vez completado
- el material de entrenamiento asociado con sistemas anteriores
- la revisión independiente y migración de los sistemas del ambiente de prueba al estatus y las librerías de producción por parte de la función de aseguramiento de la calidad
- las herramientas y monitoreo de redes y recursos utilizados para recopilar estadísticas para mantenimiento y optimización, asegurando el soporte a las aplicaciones desarrolladas para lograr un desempeño máximo a un costo mínimo
- registros de una tentativa de desarrollo para determinar la disponibilidad de:
 - Entrenamiento de usuarios
 - Seguridad
 - Desempeño de software
 - Documentación y resultados de pruebas
 - Plan de conversión
 - Migración a producción
 - Control de cambios durante el desarrollo
 - Satisfacción de las necesidades del usuario
 - Pruebas piloto o en paralelo
 - Revisión post-implementación
- conclusiones de auditoría interna o externa con respecto al proceso de diseño de sistemas
- resultados de las pruebas para confirmar si éstos satisfacen los criterios predefinidos y si todas las funciones del sistema fueron incluidas en los planes de prueba
- discusiones de la administración sobre los resultados de las pruebas, así como cualquier prueba terminada o proyecto de desarrollo
- participación del usuario en el proceso de desarrollo
- pistas de auditoría dirigidas a recrear una actividad o el análisis de errores según sea necesario
- participación del proveedor en la tentativa de desarrollo incluyendo:
 - lo razonable de los costos
 - el cumplimiento con las fechas límite
 - la funcionalidad entregada y liberada

▸ **Identificando:**

Para una selección de proyectos recientes de ciclo de vida de desarrollo de sistemas:

- compromiso del usuario y aprobación formal en cada fase del proceso de desarrollo de sistemas
- plan de pruebas para programas, unidades, sistemas (incluyendo prototipo o en paralelo), conversión, implementación, y revisión post-implementación
- consistencia apropiada con los estándares de seguridad y control interno
- tareas y calendarización apropiadas para la conversión de datos
- la realización de pruebas independientemente de aquellas de desarrollo, modificación o mantenimiento del sistema
- aceptación formal por parte de los usuarios con respecto a la funcionalidad, seguridad, integridad y riesgo remanente del sistema

Los manuales de operación para calendarización, corridas, recuperación/reinicio, respaldo / "backout" y solución de errores consideran:

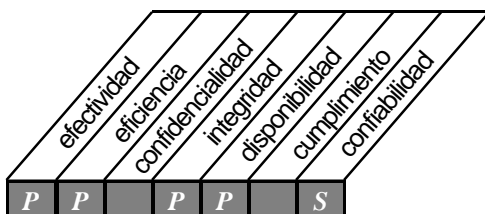
- la separación física y lógica de las librerías de productos con respecto a las de desarrollo o pruebas
- los procedimientos de solución entre las expectativas de los usuarios y la funcionalidad del sistema entregado y liberado, cuando éstos se encuentren en conflicto

Para los proveedores:

- la formalidad de las relaciones con los proveedores y la existencia de contratos
- la consideración de servicios específicos y costos
- que el desempeño del proveedor es controlado también por la metodología del ciclo de vida de desarrollo de sistemas de la organización
- el cumplimiento del proveedor en cuanto a desempeño, fechas límite y especificaciones de costos de los contratos

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:

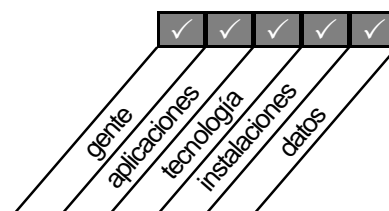
- identificación de cambios
- procedimientos de categorización, priorización y emergencia
- evaluación del impacto
- autorización de cambios
- manejo de liberación
- distribución de software

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



AI 6 ADMINISTRACIÓN DE CAMBIOS

OBJETIVOS DE CONTROL

- 1 Inicio y Control de Requisiciones de Cambio
- 2 Evaluación del Impacto
- 3 Control de Cambios
- 4 Documentación y Procedimientos
- 5 Mantenimiento Autorizado
- 6 Política de Liberación de Software
- 7 Distribución de Software

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Director de TI

Administración de la función de servicios de información

Administración de desarrollo de sistemas, aseguramiento de la calidad de control de cambios, operaciones y seguridad

Administración de usuarios seleccionada involucrada en el diseño y utilización de aplicaciones de sistemas de información

▸ **Obteniendo:**

Políticas y procedimientos organizacionales relacionadas con: planeación de sistemas de información, control de cambios, seguridad y ciclo de vida de desarrollo de sistemas

Políticas y procedimientos de la función de servicios de sistemas de información relacionadas con: metodología del ciclo de vida de desarrollo de sistemas, estándares de seguridad, aseguramiento independiente de la calidad, implementación, distribución, mantenimiento, cambios de emergencia, liberación de software y control de versiones del sistema.

Plan de desarrollo de aplicaciones

Formato y bitácora de requisiciones de control de cambios

Contratos con proveedores relacionados con servicios de desarrollo de aplicación

Evaluar los controles:

▸ **Considerando sí:**

Existe y se utiliza una metodología para priorizar los requerimientos de cambios al sistema de los

Se consideran procedimientos de cambios de emergencia en los manuales de operaciones

El control de cambios es un procedimiento formal tanto para los usuarios como para los grupos de desarrollo

La bitácora de control de cambios asegura que todos los cambios mostrados fueron resueltos

El usuario está satisfecho con el resultado de los cambios solicitados - calendarización y costos

Para una selección de cambios en la bitácora de control de cambios:

- el cambio trajo como resultado modificaciones en los programas y operaciones
- los cambios hayan sido llevados a cabo como fueron documentados
- la documentación actual refleja el ambiente modificado

El proceso de cambios es monitoreado en cuanto a mejoras en el conocimiento, efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso

El mantenimiento al sistema de Intercambio de rama privada o Exchange Private Branch (PBX) se incluye en los procedimientos de control de cambios

Evaluar la suficiencia:

► **Probando que:**

Para una muestra de cambios, la administración ha aprobado los siguientes puntos:

- solicitud de cambios
- especificación del cambio
- acceso al programa fuente
- finalización del cambio por parte del programador
- solicitud para mover el programa fuente al ambiente de prueba
- finalización de pruebas de aceptación
- solicitud de compilación y paso a producción
- determinación y aceptación del impacto general y específico
- desarrollo de un proceso de distribución

La revisión del control de cambios en cuanto a la inclusión de:

- fecha del cambio solicitado
- persona(s) que lo solicitan
- solicitud aprobada de cambios
- aprobación del cambio realizado - función de servicios de información
- aprobación del cambio realizado – usuarios
- fecha de actualización de documentación
- fecha de paso a producción
- aprobación del cambio por parte de aseguramiento de la calidad
- aceptación por parte de operaciones

Los tipos de análisis de cambios realizados al sistema para la identificación de tendencias

La evaluación de la adecuación de las librerías de la función de servicios de información y la determinación de la existencia de niveles de código base para prevenir la regresión de errores

Existen procedimientos de entradas y salidas ("check in/check out) para cambios

Todos los cambios en la bitácora fueron resueltos a satisfacción de los usuarios y que no se llevaron a cabo cambios que no hayan sido registrados en la bitácora

Los usuarios tienen consciencia y conocimiento de la necesidad de procedimientos formales de control de cambios

El proceso de reforzamiento del personal asegura el cumplimiento de los procedimientos de control de cambios

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de la administración de control de cambios contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Para sistemas seleccionados de la función de servicios de información:

- una verificación en cuanto a si la documentación determina el requerimiento o si el cambio del sistema ha sido aprobado y priorizado por parte de la administración de las áreas usuarias afectadas y el proveedor de servicios
- la confirmación de la existencia y adecuación de evaluación del impacto en formas de control de cambios
- la obtención del conocimiento del cambio a través de un acuse de recibo de solicitud de cambios de la función de servicios de información
- la asignación del cambio a los recursos apropiados de desarrollo
- la adecuación de los sistemas y los planes de prueba de los usuarios y sus resultados
- la migración formal de prueba a producción vía grupo de aseguramiento de la calidad
- la actualización de los manuales de usuario y de operación para reflejar el cambio
- la distribución de la nueva versión a los usuarios apropiados

▸ **Identificando:**

Para una selección de cambios de información que:

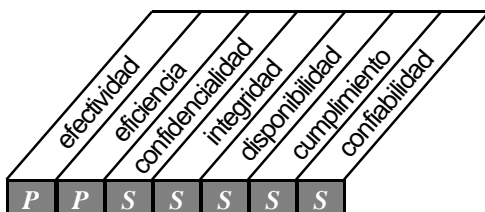
- sólo se llevaron a cabo cambios aprobados
- todos los cambios han sido considerados
- las librerías actuales (fuente y objeto) reflejan los cambios más recientes
- las variaciones en el procedimiento de control de cambios entre:
 - aplicaciones adquiridas e internas
 - software de aplicación y de sistemas
 - tratamiento del control de cambios por parte del proveedor

ENTREGA & SOPORTE

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:

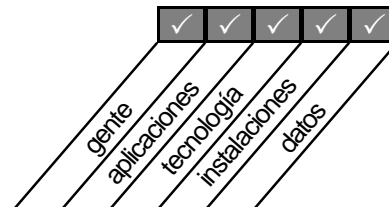
- convenios formales
- definición de responsabilidades
- tiempos y volúmenes de respuesta
- dependencias
- cargos
- garantías de integridad
- convenios de confidencialidad

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



DS 1 DEFINICIÓN DE NIVELES DE SERVICIO

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Marco de Referencia para el Convenio de Nivel de Servicio |
| 2 | Aspectos sobre los Acuerdos de Nivel de Servicio |
| 3 | Procedimientos de Ejecución |
| 4 | Monitoreo y Reporte |
| 5 | Revisión de Convenios y Contratos de Nivel de Servicio |
| 6 | Elementos sujetos a Cargo |
| 7 | Programa de Mejoramiento del Servicio |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Director de Información
 Presidencia de la función de servicios de información
 Administrador del nivel de servicio/contrato de servicios de información
 Administrador de operaciones de la función de servicios de información
 Administración de usuarios

▸ **Obteniendo:**

Políticas y procedimientos generales para la organización asociadas a las relaciones proveedor/usuario
 Políticas y procedimientos de la función de servicios de información relacionadas con:

- Acuerdos de nivel de servicio
- Contenido de emisión de reportes operativos, tiempos y distribución
- Métodos de seguimiento de desempeño
- Actividades de acción correctiva

Documentación de la función de servicios de información relacionada con:

- Reportes de desempeño de nivel de servicio
- Algoritmos de cargo y metodología para calcular cargos
- Programas de mejora del servicio
- Recurso resultante de un bajo desempeño

Acuerdos de nivel de servicio con usuarios y proveedores internos y externos

Evaluar los controles:

▸ **Considerando sí:**

Se identifica por política un proceso de acuerdo de nivel de servicio
 La participación en el proceso por parte del usuario se requiere para la creación y modificación de acuerdos
 Están definidas las responsabilidades de usuarios y proveedores
 La administración monitorea y emite reportes sobre el logro de los criterios de desempeño de servicio especificados y sobre todos los problemas encontrados

Existe un proceso de revisión regular llevado a cabo por la administración

Se identifica un proceso de recurso en caso de un bajo desempeño

Los acuerdos de nivel de servicio incluyen, pero no se limitan a contar con:

- definición de servicio
- costo del servicio
- nivel de servicio mínimo cuantificable
- nivel de soporte por parte de la función de servicios de información
- disponibilidad, confiabilidad y capacidad de crecimiento
- planeación de recuperación en caso de desastre/contingencia
- requerimientos de seguridad
- procedimientos de cambio para cualquier parte del acuerdo
- acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio
- revisión/renovación/no renovación del período efectivo y del nuevo período
- contenido y frecuencia del reporte de desempeño y pago de servicios
- cargos realistas comparados contra la historia, la industria y las buenas prácticas
- cálculo de cargos
- compromiso de mejoras al servicio

Evaluar la suficiencia:

► Probando que:

Para una muestra de acuerdos pasados y en proceso, el contenido incluye:

- definición del servicio
- costo del servicio
- nivel de servicio mínimo cuantificable
- nivel de soporte por parte de la función de servicios de información
- disponibilidad, confiabilidad y capacidad de crecimiento
- procedimiento de cambios para cualquier parte del acuerdo
- planeación de recuperación en caso de desastre/contingencia
- requerimientos de seguridad
- acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio
- revisión/renovación/no renovación del período efectivo y nuevo período
- contenido y la frecuencia del reporte de desempeño el pago de servicios
- cargos realistas comparados con la historia, la industria y las buenas prácticas
- cálculos de cargos
- compromiso de mejoras al servicio
- aprobación formal por parte de usuarios y proveedores

Los usuarios apropiados están conscientes, tienen conocimiento y comprenden los procesos y procedimientos del acuerdo de nivel de servicio

El nivel de satisfacción del usuario en cuanto al proceso y acuerdos reales del nivel de servicio actuales es suficiente

El servicio proporciona registros para asegurar razones para un bajo desempeño ("non-performance") y para asegurar que existe un programa para la mejora del desempeño

La precisión de los cargos reales concuerda con el contenido del acuerdo

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Se da seguimiento al desempeño histórico comparándolo contra el compromiso de mejora al servicio determinado anteriormente

Los reportes sobre el logro del desempeño de servicio especificado son utilizados apropiadamente por la administración para asegurar un desempeño satisfactorio

Los reportes sobre todos los problemas encontrados son utilizados apropiadamente para asegurar que se toman las acciones correctivas correspondientes

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones ("Benchmarking") de los acuerdos del nivel de servicio contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria

Una revisión:

- del acuerdo de nivel de servicio para determinar que se definen y alcanzan las provisiones cualitativas y cuantitativas que confirman las obligaciones
- del acuerdo de nivel de servicio seleccionado para confirmar que los procedimientos de solución de problemas, específicamente el desempeño bajo sean incluidos y llevados a cabo

▸ **Identificando:**

La conveniencia de las provisiones que describen, coordinan y comunican la relación entre el proveedor y el usuario de los servicios de información

Cálculos incorrectos para categorías seleccionadas de información

Revisiones continuas y acciones correctivas llevadas a cabo por la administración de reportes del nivel de servicio

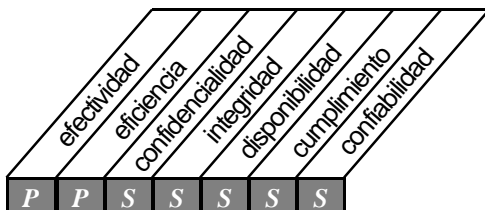
La conveniencia de las mejoras a los servicios propuestos en comparación con el análisis costo/beneficio

La conveniencia de la capacidad de los proveedores para alcanzar en el futuro los objetivos comprometidos de mejoras

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:

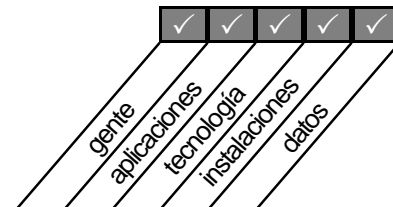
asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

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



DS 2 ADMINISTRACIÓN DE SERVICIOS PRESTADOS POR TERCEROS

OBJETIVOS DE CONTROL

- 1 Interfases con Proveedores
- 2 Relaciones de propietarios
- 3 Contratos con Terceros
- 4 Calificaciones de Terceros
- 5 Contratos con Fuentes Externas
- 6 Continuidad de Servicios
- 7 Relaciones de Seguridad
- 8 Monitoreo

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Director de Información
 Presidencia de la función de servicios de información
 Administrador de contrato/nivel de servicio de servicios de información
 Administración de las operaciones de la función de servicios de información
 Funcionario de seguridad de la función de servicios de información

▸ **Obteniendo:**

Políticas generales para la organización asociadas con los servicios adquiridos y en particular, con las relaciones con proveedores como terceras partes
 Políticas y procedimientos de la función de servicios de información asociadas con: relaciones con terceras partes, procedimientos de selección de proveedores, contenido del control de dichas relaciones, seguridad lógica y física, mantenimiento de la calidad por parte de los proveedores, planeación de contingencias y fuentes externas
 Una lista de todas las relaciones actuales con terceras partes y de los contratos reales asociados con ellas
 El reporte del nivel de servicio relacionado con las relaciones y servicios proporcionados por terceras partes
 Las minutas de las reuniones en las que se discuten la revisión de los contratos, la evaluación del desempeño y la administración de las relaciones
 Los acuerdos de confidencialidad para todas las relaciones con terceras partes
 Las listas de seguridad de acceso con los perfiles y recursos disponibles para los vendedores

Evaluar los controles:

▸ **Considerando sí:**

Existen políticas y procedimientos de la función de servicios de información asociadas con las relaciones con terceras partes, y si éstas son consistentes con las políticas generales de la organización
 Existen políticas que consideran específicamente la necesidad de contratos, de una definición del contenido de los mismos, del propietario o administrador de las relaciones responsable de asegurar la creación, mantenimiento, monitoreo y renegociación de los contratos

Considerando si, continúa

Las interfaces están definidas para agentes independientes involucrados en la conducción del proyecto y demás partes como los subcontratados.

Los contratos representan un registro completo de las relaciones con los proveedores como terceras partes

Los contratos están establecidos específicamente para la continuidad de los servicios, y que dichos contratos incluyen una planeación de contingencias por parte del proveedor para asegurar la continuidad del servicio a los usuarios de éstos

El contenido de los contratos incluye por lo menos lo siguiente:

- aprobación formal administrativa y legal
- entidad legal que proporciona los servicios
- servicios proporcionados
- acuerdos cualitativos y cuantitativos de nivel de servicio
- costo de los servicios y frecuencia de su pago
- proceso de solución de problemas
- sanciones por bajo desempeño
- proceso de disolución
- proceso de modificación
- reporte de servicio - contenido, frecuencia y distribución
- funciones entre las partes del contrato durante la vida del mismo
- aseguramiento de continuidad que indica que el servicio será proporcionado por el proveedor
- usuarios de los servicios y procesos y frecuencia de las comunicaciones del proveedor
- duración del contrato
- nivel de acceso proporcionado por el proveedor
- requerimientos de seguridad
- garantías de confidencialidad
- derecho a acceso y a auditar

Los acuerdos de depósito se han negociado en su momento

Los terceros en potencia se han calificado adecuadamente mediante la evaluación de su habilidades para proveer el servicio requerido (vencimiento del trabajo)

Evaluar la suficiencia:**▸ Probando que:**

La precisión y existencia de la lista de contratos y de los contratos

Ningún servicio es proporcionado por algún proveedor no incluido en la lista de contratos mencionada

Los proveedores mencionados en los contratos efectivamente están llevando a cabo los servicios definidos

La administración/los propietarios de los proveedores comprenden su responsabilidad dentro del contrato

Las políticas y procedimientos de la función de servicios de información asociadas con las relaciones con terceras partes existen y son consistentes con las políticas generales de la organización

Existen políticas que consideran específicamente la necesidad de establecer contratos, la definición del contenido de los mismos, del propietario o administrador de la relación responsable de asegurar que los contratos sean creados, mantenidos, monitoreados y renegociados según se requiera

Los contratos representan un registro completo de las relaciones con los proveedores como terceras partes

Los contratos están establecidos para asegurar específicamente la continuidad de los servicios, y que dichos contratos

incluyen una planeación de contingencias por parte del proveedor para asegurar el servicio continuo a los usuarios
El contenido de los contratos incluyen por lo menos lo siguiente:

- aprobación formal administrativa y legal
- entidad legal para proporcionar los servicios
- servicios proporcionados
- acuerdos cuantitativos y cualitativos del nivel de servicio
- costo y frecuencia de los servicios y su pago
- proceso de solución de problemas
- sanciones por bajo desempeño
- proceso de disolución
- proceso de modificación
- reporte de servicios - contenido, frecuencia y distribución
- funciones entre las partes del contrato durante la vida del mismo
- aseguramiento de la continuidad de los servicios prestados por el proveedor
- usuarios de los servicios y frecuencia del proceso de comunicaciones del proveedor
- duración del contrato
- nivel de acceso proporcionado por el proveedor
- requerimientos de seguridad
- garantías de confidencialidad
- derecho de acceso y de auditar

Los usuarios tienen consciencia, conocimiento y comprenden la necesidad de contar con políticas de contratos y con los contratos mismos para proporcionar servicios

Existe una independencia adecuada entre el proveedor y la organización

Se dan independientemente la búsqueda y la selección de proveedores

La lista de seguridad de acceso incluye únicamente un número mínimo de proveedores requeridos, y que dicho acceso es el mínimo necesario

El acceso de hardware y software a los recursos de la organización es administrado y controlado para minimizar su utilización por parte de los proveedores

El nivel real de servicios proporcionados se compara en gran medida con las obligaciones contractuales

Las instalaciones, personal, operaciones y controles de fuentes externas aseguran un nivel de desempeño requerido comparable con el esperado

El monitoreo continuo de liberación y entrega de servicios por parte de terceros es llevado a cabo por la administración

Se llevan a cabo auditorías independientes de las operaciones de la parte contratante

Existen los reportes de evaluación para terceros con el fin de evaluar sus capacidades para entregar el servicio requerido

Las interfases de los agentes independientes involucrados en la conducción del proyecto están documentadas en el contrato.

La historia de la actividad de litigación - actual y anterior

Los contratos con proveedores PBX están y cubiertos

Evaluar el riesgo de los objetivos de control no alcanzados:**▸ Llevando a cabo:**

Mediciones ("Benchmarking") de los servicios de terceras partes contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria

Una revisión detallada de cada uno de los contratos de terceras partes para determinar provisiones cualitativas y cuantitativas que confirmen la definición de las obligaciones

▸ Identificando:

Provisiones que describen, coordinan y comunican la relación entre el proveedor y el usuario de los servicios de información

Facturas de terceras partes que reflejan cargos precisos por servicios por contrato seleccionados

El vínculo de la organización con los proveedores como terceras partes que asegura la comunicación de problemas de contrato entre las partes y los usuarios de los servicios

La aprobación de todos los contratos por parte de la administración y el consejo legal

La puesta en práctica de evaluaciones de riesgos para confirmar la necesidad de las relaciones o la necesidad de modificar la relación

La revisión continua y las acciones correctivas sobre los reportes de contratos llevadas a cabo por la administración

Lo razonable de la aplicación de los cargos en comparación con el desempeño interno, externo y de la industria

La existencia de planes de contingencia para todos los servicios contratados, específicamente para los servicios de recuperación en caso de desastre de la función de servicios de información

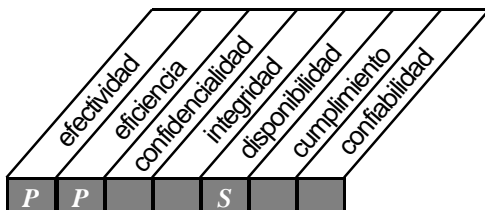
Para las funciones de fuentes externas, defectos aparentes u oportunidades para mejorar el desempeño o reducir costos

La implementación de recomendaciones contenidas en auditorías independientes llevadas a cabo por la parte contratante

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:

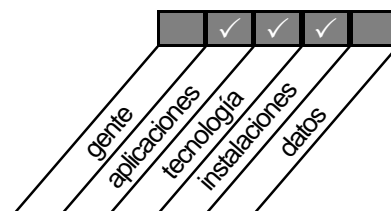
asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado

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



Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo

DS 3 ADMINISTRACIÓN DE DESEMPEÑO Y CAPACIDAD

OBJETIVOS DE CONTROL

- 1 Requerimientos de Disponibilidad y Desempeño
- 2 Plan de Disponibilidad
- 3 Monitoreo y Reporte
- 4 Herramientas de Modelado
- 5 Manejo de Desempeño Proactivo
- 6 Pronóstico de Carga de Trabajo
- 7 Manejo de Capacidad de Recursos
- 8 Disponibilidad de Recursos
- 9 Calendarización de Recursos

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Presidencia de la función de servicios de información
 Administración de operaciones de la función de servicios de información
 Administración de la capacidad de la función de servicios de información
 Administración de redes de la función de servicios de información

▸ **Obteniendo:**

Políticas y procedimientos globales para la organización relacionados con la disponibilidad, monitoreo y reporte del desempeño, pronóstico de la carga de trabajo, administración de la capacidad y calendarización
 Políticas y procedimientos de la función de servicios de información relacionadas con: el enlace de la capacidad con el plan del negocio, la disponibilidad de los servicios, la planeación de la disponibilidad, el monitoreo continuo y la administración del desempeño
 Representaciones del producto por parte del proveedor con respecto a las normas de capacidad y desempeño
 Una lista de todos los productos actuales del proveedor en lo referente a hardware, software, comunicaciones y periféricos
 Reportes de monitoreo de redes de comunicación
 Minutas de las reuniones en las que se discuten la planeación de la capacidad, las expectativas de desempeño y la "afinación" del desempeño
 Documentos de disponibilidad, capacidad, carga de trabajo y planeación de recursos
 Presupuesto de TI anual incluyendo las suposiciones relacionadas con la capacidad y el desempeño
 Reportes relacionados con el desempeño operativo dentro de la función de servicios de información, incluyendo el reporte y la historia de la solución de problemas

Evaluar los controles:

▸ **Considerando sí:**

Los períodos de tiempo y el nivel de servicio están definidos para todos los servicios proporcionados por la función de

servicios de información

Los períodos de tiempo y los niveles de servicio reflejan los requerimientos del usuario

Los períodos de tiempo y los niveles de servicio son consistentes con las expectativas de desempeño del potencial del equipo

Existe un plan de disponibilidad, si éste es actual y refleja los requerimientos del usuario

Se lleva a cabo y se reporta un monitoreo continuo del desempeño de todo el equipo y de la capacidad, y si la falta de un desempeño adecuado es considerada por la administración y si se consideran formalmente las oportunidades de mejoras al desempeño

Se monitorea el desempeño óptimo de configuración utilizando herramientas de modelado para maximizar el desempeño y al mismo tiempo, minimizar la capacidad a los niveles requeridos

Los usuarios y los grupos de desempeño operativo revisan proactivamente la capacidad, el desempeño, y si se llevan a cabo modificaciones a la calendarización de la carga de trabajo

El pronóstico de la carga de trabajo incluye las entradas hechas por los usuarios debido a demandas cambiantes y por los proveedores debido a nueva tecnología o a mejoras a los productos actuales

Evaluar la suficiencia:

▸ Probando que:

Las estadísticas sobre reportes de desempeño, capacidad y disponibilidad son precisas, incluyendo una comparación entre las explicaciones de las variaciones de desempeño históricas y las pronosticadas

El proceso de cambios para modificar los documentos de planeación de disponibilidad, capacidad y carga de trabajo refleja los cambios en la tecnología o los requerimientos del usuario

Los reportes de análisis de flujo de trabajo consideran las oportunidades de eficiencia de procesos adicionales

El reporte de información del desempeño para los usuarios relacionado con el uso y la disponibilidad, existe, incluyendo capacidad calendarización de carga de trabajo y tendencias

Existen procedimientos de escalamiento, que éstos son seguidos y son apropiados para la solución de problemas

La fase de post - implementación de la metodología de desarrollo de sistemas incluye criterios para determinar el crecimiento futuro y los cambios a las expectativas de desempeño

Los niveles de soporte proporcionados por la función de servicios de información son suficientes para apoyar las metas de la organización

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ Llevando a cabo:

Mediciones ("Benchmarking") de la administración del desempeño y la capacidad contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Pruebas de las necesidades continuas del negocio, para asegurar que los términos y requerimientos de disponibilidad de TI reflejan adecuadamente estas necesidades

Una revisión del proceso de planeación de capacidad y recursos para asegurar la modificación oportuna de los planes, tomando como base las necesidades cambiantes del negocio

Una verificación para asegurar que las expectativas de desempeño están siendo alcanzadas en lo referente a capacidad, respuesta y disponibilidad

Una comparación de los requerimientos de desempeño desde una perspectiva de análisis costo/beneficio, para asegurar

que no existen excedentes de capacidad o recursos

Una verificación periódica del reporte de desempeño producido y revisado por la administración

Identificando:

Reportes de desempeño en cuanto a oportunidades de mejora o solución de debilidades

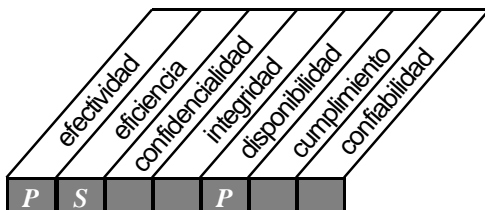
Las expectativas de desempeño de los usuarios están siendo satisfechas, y que las modificaciones basadas en cambios de requerimientos están siendo reflejadas en el plan

Bitácoras o reportes de problemas que confirmen que los problemas ocurridos durante el procesamiento fueron considerados oportunamente y que se llevaron a cabo las acciones correctivas apropiadas

Problemas específicos encontrados y el aseguramiento de la efectividad del proceso de solución de problemas

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:

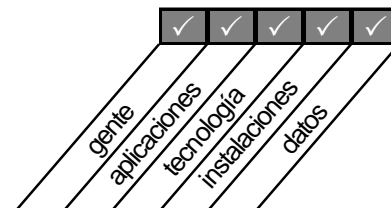
- clasificación de severidad
- plan documentado
- procedimientos alternativos
- respaldo y recuperación
- pruebas y entrenamiento sistemáticos y regulares

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



DS 4 ASEGURAMIENTO DE SERVICIO CONTINUO

OBJETIVOS DE CONTROL

- 1 Marco de Referencia para Continuidad de TI
- 2 Estrategia y Filosofía del Plan de Continuidad de TI
- 3 Contenido del Plan de Continuidad de TI
- 4 Reducción de los Requerimientos de la Continuidad de TI
- 5 Mantenimiento del Plan de Continuidad de TI
- 6 Prueba del Plan de Continuidad de TI
- 7 Capacitación para el Plan de Continuidad de TI
- 8 Distribución del Plan de Continuidad de TI
- 9 Procedimientos de Respaldo del Procesamiento Alterno en el Departamento Usuario
- 10 Recursos de TI Críticos
- 11 Respaldo del Sitio y Hardware
- 12 Procedimientos de Involucramiento

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Presidencia de la función de servicios de información
 Administración de operaciones de la función de servicios de información
 Administración de contingencias de la función de servicios de información
 Administración de recursos humanos o entrenamiento
 Organizaciones de usuarios con necesidades de reanudación/contingencia
 Administrador del centro de cómputo de recuperación del proveedor
 Administrador del almacenamiento fuera del centro de cómputo
 Administrador de riesgos/seguros

▸ Obteniendo:

Políticas y procedimientos generales para la organización relacionados con el proceso de planeación de recuperación/ contingencia
 Políticas y procedimientos de la función de servicios de información relacionadas con: el marco referencial, el plan, la filosofía, la estrategia, la priorización de aplicaciones, el plan de pruebas, los respaldos y rotaciones regulares y el entrenamiento de recuperación de desastres/contingencia
 El plan de recuperación de desastres/contingencia de la función de servicios de información
 Los usuarios de los servicios de planes de reanudación del negocio/contingencia
 Los resultados de las pruebas de los planes para usuario de recuperación de desastre/contingencia y reanudación del negocio/contingencia más recientes
 La metodología para determinar la priorización de aplicaciones en caso de desastre
 Los contratos de los proveedores que dan soporte a los servicios de recuperación/soporte
 Políticas de seguros por interrupción del negocio

Evaluar los controles:‣ **Considerando sí:**

Las políticas organizacionales requieren de un marco referencial de recuperación/contingencia y de un plan como parte de los requerimientos normales de operación tanto para la función de servicios de información como para todas las organizaciones dependientes de los recursos de sistemas de información

Las políticas y procedimientos de la función de servicios de información requieren de:

- una filosofía y un marco referencial consistentes en relación con el desarrollo de un plan de recuperación de desastres/contingencia
- una priorización de las aplicaciones con respecto a los tiempos de recuperación y regreso
- una evaluación de riesgos y la consideración de seguros por pérdidas del negocio en situaciones de recuperación de desastre/contingencia para la función de servicios de información, así como para los usuarios de los recursos
- una determinación de funciones y responsabilidades específicas con respecto a la planeación de recuperación de desastres/contingencia con pruebas, mantenimiento y requerimientos de actualización específicos
- un acuerdo de contrato formal con los proveedores que prestan servicios para proporcionar servicios en caso de desastre, incluyendo instalaciones de centro de cómputo o relaciones de respaldo, anticipándose a una necesidad real
- la inclusión de los siguientes puntos como contenido mínimo en cada plan de recuperación de desastre/contingencia:
 - Procedimientos de emergencia para garantizar la seguridad de todos los miembros del personal afectados
 - Funciones y responsabilidades de la función de servicios de información, de los proveedores que prestan servicios de recuperación de desastres, de los usuarios de los servicios y del personal administrativo de soporte
 - Un marco referencial de recuperación de desastres consistente con un plan de contingencias a largo plazo
 - Una lista de los recursos de sistemas que requieren alternativas (hardware, periféricos, software)
 - Una lista de las aplicaciones mayores y menores, de los tiempos de recuperación requeridos y de las normas de desempeño esperadas
 - Funciones administrativas para comunicar y proporcionar servicios de soporte tales como beneficios, nómina, comunicación externa, seguimiento de costos, etc. en caso de desastre
 - Escenarios de desastre varios, desde las pérdidas mínimas hasta la pérdida total de la capacidad y respuesta en suficiente detalle para llevar a cabo una ejecución paso a paso.
 - La identificación de equipo específico y necesidades de suministros tales como impresoras de alta velocidad, firmas, formatos, equipo de comunicación, teléfonos, etc., así como de una fuente y fuente
 - El entrenamiento, la consciencia y el conocimiento de las funciones individuales y de equipo en el plan de recuperación de desastre
 - La calendarización de las pruebas, los resultados de la última prueba y las acciones correctivas llevadas a cabo tomando como base la(s) prueba(s) anterior(es)
 - El detalle de los proveedores de servicios contratados, de los servicios y de la expectativas de respuesta
 - La información logística de la localización recursos clave, incluyendo el centro de cómputo de respaldo para la recuperación de sistemas operativos, aplicaciones, archivos de datos, manuales de operación y documentación de programas/sistema/usuarios
 - Los nombres, direcciones, números de teléfono/ "localizadores" (pagers) actuales del personal clave
 - La inclusión de los planes de reconstrucción para la recuperación en la localidad original de todos los sistemas y recursos
 - Las alternativas de reanudación del negocio para todos los usuarios para el establecimiento de localidades de

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

trabajo alternativas, una vez que los recursos de sistemas de información estén disponibles (por ejemplo, el sistema ha sido recuperado en el centro de cómputo alternativo pero el edificio de los usuarios sufrió un incendio y no está disponible)

Los requerimientos de la agencia reguladora con respecto a la planeación de contingencia están siendo satisfechos

Los planes de contingencia para usuarios son desarrollados tomando como base la no disponibilidad de los recursos físicos para llevar a cabo procesamiento críticos - manuales y computarizados

Los sistemas de telefonía, Correo de Voz, fax y sistemas de imágenes son parte del plan de continuidad

Los sistemas de imágenes, los sistemas de fax, los documentos en papel y los medios de almacenamiento masivo son parte del plan de continuidad.

Evaluar la suficiencia:

▸ Probando que:

Existen planes de recuperación de desastre/contingencia, que éste es actual y que es comprendido por todas las partes afectadas

Se ha proporcionado a todas las partes involucradas un plan regular de entrenamiento de contingencia y recuperación en caso de desastre

Se han seguido todas las políticas y procedimientos relacionadas con el desarrollo del plan

El contenido del plan tiene como base el contenido descrito anteriormente, y que:

- los objetivos del plan de contingencia han sido alcanzados
- se ha seleccionado a las personas apropiadas para llevar a cabo funciones de liderazgo
- el plan ha recibido las revisiones y aprobaciones apropiadas por parte de la administración
- el plan ha sido probado recientemente y que éste trabajó de acuerdo con lo esperado, o que cualquier deficiencia encontrada trajo como resultado la aplicación de correcciones al plan
- existe un vínculo entre el plan de recuperación en caso de desastres y el plan de negocios de la organización
- los procedimientos manuales alternativos son documentados y probados como parte de la prueba global

Se han dado el entrenamiento, la consciencia y el conocimiento de los usuarios y del personal de la función de servicios de información en cuanto a funciones, tareas y responsabilidades específicas dentro del plan

Las relaciones y tiempos del proveedor contratado son consistentes con las expectativas y necesidades del usuario

El contenido del centro de cómputo de respaldo está actualizado y es suficiente con respecto a los procedimientos normales de rotación fuera del centro de cómputo

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ Llevando a cabo:

Mediciones ("Benchmarking") de la planeación de recuperación de desastres/contingencias contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de:

- los objetivos del plan para asegurar una estrategia apropiada y una interfase con la estrategia de continuidad general del negocio
- la comprensión apropiada del personal con respecto a proporcionar liderazgo como coordinadores del plan
- el plan verificado y aprobado por los niveles apropiados de la presidencia
- los miembros seleccionados de la función de servicios de información y del departamento usuario para verificar que las necesidades del negocio están incluidas en el plan de contingencia

- los procedimientos de usuario para el procesamiento de datos manual alternativo para asegurar que éstos están documentados por los departamentos usuarios con el fin de ser utilizados cuando ocurra un desastre, y hasta que haya posibilidad de restaurar las operaciones después del desastre
- los suministros de aplicación específicos, para asegurar que existe inventario suficiente en un centro de cómputo exterior (por ejemplo, cintas magnéticas, reserva de cheques, reserva de certificados, etc.)

► **Identificando:**

Los contratos de los proveedores para verificar los tiempos para obtener suministros y la suficiencia de detalles del servicio, oportunidad, niveles de servicio y costos

Las provisiones para adquirir componentes de redes o de telecomunicaciones especializadas

Escenarios varios a corto plazo y permanentes como parte del plan

La priorización de aplicaciones ocurridas en forma consistente con las expectativas de los usuarios

Que existen contratos por escrito para instalaciones de centro de cómputo externas proporcionales a las necesidades

Velocidad, respuesta, disponibilidad y soporte de procesamiento del centro de cómputo alternativo, suficientes para los requerimientos de los usuarios

Plan(es) de recuperación de desastre del (de los) proveedor(es) para asegurar la continuidad de sus servicios en caso de desastre

La lejanía de los servicios alternativos del proveedor con respecto al centro de cómputo original, con el fin de eliminar la posibilidad de desastres mutuos

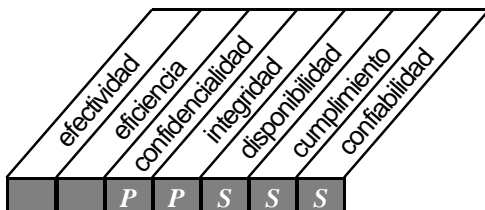
Pruebas periódicas del plan, habiendo ocurrido ajustes al plan basándose en pruebas

Al personal usuario y de la función de servicios de información, asegurándose que haya recibido regularmente entrenamiento en recuperación de desastres

La existencia de equipos, funciones y responsabilidades de reconstrucción similares, así como pruebas para migrar el procesamiento desde el lugar de procesamiento alternativo al centro de cómputo original

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:

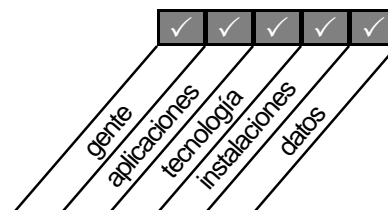
- autorización
- autenticación
- acceso
- perfiles e identificación de usuarios
- administración de llaves criptográficas
- manejo, reporte y seguimiento de incidentes
- Prevención y detección de virus
- *Firewalls*

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



DS 5 GARANTIZAR LA SEGURIDAD DE SISTEMAS

OBJETIVOS DE CONTROL

- 1 Manejo de las Medidas de Seguridad
- 2 Identificación, Autenticación y Acceso
- 3 Seguridad de Acceso a Datos en Línea
- 4 Administración de Cuentas de Usuario
- 5 Revisión Gerencial de Cuentas de Usuario
- 6 Control de Usuario de las Cuentas de Usuario
- 7 Vigilancia de Seguridad
- 8 Clasificación de Datos
- 9 Administración Centralizada de Identificación y Derechos de Acceso
- 10 Reportes de Actividades de Violación y Seguridad
- 11 Manejo de Incidentes
- 12 Re-acreditación
- 13 Confianza en el Colega
- 14 Autorización de Transacción
- 15 No Rechazo
- 16 Ruta Confiable
- 17 Protección de las Funciones de Seguridad
- 18 Administración de Llaves Criptográficas
- 19 Prevención, Detección y Corrección del Software Dañino
- 20 Arquitectura de Firewalls y Conexiones con las Redes Públicas
- 21 Protección del Valor Electrónico

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Oficial de seguridad Senior de la organización
 Administración de la seguridad y presidencia de la función de servicios de información
 Administrador de la base de datos de la función de servicios de información
 Administrador de la seguridad de la función de servicios de información
 Administración de desarrollo de aplicaciones de la función de servicios de información

▸ Obteniendo:

Políticas y procedimientos globales para la organización referentes a la seguridad y el acceso de los sistemas de información
 Políticas y procedimientos de la función de servicios de información relacionadas con: seguridad y acceso a los sistemas de información
 Políticas y procedimientos relevantes, así como requerimientos de seguridad legales y regulatorios de los sistemas de información (por ejemplo, leyes, regulaciones, lineamientos, estándares industriales) incluyendo:

- procedimientos de administración de cuentas de usuario
- política de seguridad del usuario o de protección de la información
- estándares relacionados con el comercio electrónico
- esquema de clasificación de datos
- inventario de software de control de acceso
- plano de los edificios/habitaciones que contienen recursos de sistemas de información
- inventario o esquema de los puntos de acceso físico a los recursos de sistemas de información (por ejemplo, módems, líneas telefónicas y terminales remotas)
- procedimientos de control de cambios de software de seguridad
- procedimientos de seguimiento, solución y escalamiento de problemas
- reportes de violaciones a la seguridad y procedimientos de revisión administrativa
- inventario de dispositivos de encriptación de datos y de estándares de encriptación
- lista de los proveedores y clientes con acceso a los recursos del sistema
- lista de los proveedores de servicios utilizados en la transmisión de datos
- prácticas de administración de redes relacionadas con pruebas continuas de seguridad
- copias de los contratos de los proveedores de servicios de transmisión de datos
- copias de documentos firmados de seguridad y conocimiento de los usuarios
- contenido del material de entrenamiento de seguridad para nuevos empleados
- reportes de auditoría de auditores externos, proveedores de servicios como terceras partes y dependencias gubernamentales relacionadas con la seguridad de los sistemas de información

Evaluar los controles:

► **Considerando sí:**

Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario con propósitos de consistencia

Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema

Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido

Se cuenta con perfiles de seguridad de usuario que representen “los menos accesos requeridos” y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación

El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus

Se cuenta con reportes de violaciones a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir:

- intentos no autorizados de acceso al sistema (sign on)
- intentos no autorizados de acceso a los recursos del sistema
- intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad
- privilegios de acceso a recursos por ID de usuario
- modificaciones autorizadas a las definiciones y reglas de seguridad
- accesos autorizados a los recursos (seleccionados por usuario o recurso)
- cambio de estatus de la seguridad del sistema
- accesos a las tablas de parámetros de seguridad del sistema operativo

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Existen módulos criptográficos y procedimientos clave de mantenimiento, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión

Existen estándares de administración criptográfica claves tanto para la actividad centralizada como para la de los usuarios

Los controles de cambios al software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de sistemas

Los mecanismos de autenticidad en uso proveen las siguientes facilidades:

- uso individual de datos de autenticidad (ej., passwords y no re- utilizables)
- autenticación múltiple (ej., se utilizan dos o más mecanismos de autenticidad diferentes)
- autenticidad basada en la política (ej., capacidad para especificar procedimientos de autenticidad aparte en los eventos específicos)
- autenticidad a demanda (ej., capacidad de volver a autenticar al usuario, en ocasiones, después de la autenticación inicial)

El número de sesiones concurrentes correspondientes al mismo usuario están limitadas

Al entrar, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.

Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales

Al lograrse la sesión exitosamente, se despliega el historial de los intentos exitosos y fallidos de acceso a la cuenta del usuario

La política de password incluye:

- cambio inicial de password la primera vez de uso
- longitud adecuada mínima del password
- la frecuencia obligada mínima de cambio de password
- verificación del password en la lista de valores no permitidos (ej., verificación de diccionario)
- protección adecuada para los passwords de emergencia

El procedimiento formal para resolución de problemas incluye:

- ID de usuario suspendido después de 5 intentos de entrada fallidos
- Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado de las entradas
- El tiempo de autenticidad se limita a 5 minutos, después del cual se concluye la sesión
- Se le informa al usuario la suspensión, pero no la razón de la misma

Los procedimientos de marcación incluyen la marcación anterior o autenticidad base prueba

Los métodos de control de locación se utilizan para aplicar restricciones adicionales a las locaciones específicas

El acceso al servicio VoiceMail y el sistema PBX está controlado con los mismos controles físicos y lógicos de los sistemas computacionales

Ocurren el refuerzo a las políticas de posición delicada, incluyendo:

- se les pide a los empleados en puestos delicados que permanezcan alejados de la organización durante un periodo adecuado cada año gregoriano; durante este tiempo su ID de usuario se suspende; y las personas que lo sustituyen deben notificar a la administración en caso de advertirse cualquier anomalía de seguridad
- la rotación de personal sin previa notificación al personal en áreas delicadas se realiza de tiempo en tiempo

El hardware y software de seguridad, como los módulos de encriptación, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la “necesidad de conocimiento”

El acceso a los datos de seguridad como el manejo de la seguridad, datos de transacción delicados, passwords y claves de encriptación se limita a la base de la “necesidad de conocimiento”

Se utilizan rutas confiables para transmitir información delicada no encriptados

Para evitar la suspensión del servicio por ataques con faxes basura, se toman medidas de seguridad como:

- evitar la publicación de números de fax fuera de la organización en la base de “necesidad de conocimiento”

- las líneas de fax utilizadas para solicitudes del negocio no se utilizan con otros fines

Las medidas preventivas y detectoras de control se han establecido con respecto a los virus de computadoras

Para reforzar la integridad de los valores electrónicos, se toman las medidas:

- facilidades de lector de tarjeta protegido contra la destrucción, publicación o modificación de la información de la tarjeta
- la información de la tarjeta (NIP y demás información) se protege contra la divulgación del intruso
- se evita la falsificación de las tarjetas

Para reforzar la protección de las facilidad de seguridad, se toman medidas:

- el proceso de identificación y autenticidad requiere ser repetido después de un cierto periodo de inactividad
- un sistema de candado, un botón de fuerza o una secuencia de salida se puede activar cuando la terminal se deja encendida

Evaluar la suficiencia:

▸ **Probando que:**

La función de servicios de información cumple con los estándares de seguridad relacionados con:

- autenticación y acceso
- administración de clasificación de perfiles de usuario y seguridad de datos
- reportes y revisión gerencial de las violación e incidentes de seguridad
- estándares criptográficos administrativos clave
- detección de virus, solución y comunicación
- clasificación y propiedad de datos

Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema

Existen procedimientos para el acceso externo de recursos del sistema, por ejemplo, "logon", "ID", "password" o contraseña y "dial back"

Se lleva un inventario de los dispositivos del sistema para verificar su suficiencia

Los parámetros de seguridad del sistema operativo tienen como base estándares locales/del proveedor

Las prácticas de administración de seguridad de la red son comunicadas, comprendidas e impuestas

Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad

Existen procedimientos de "logon" reales para sistemas, usuarios y para el acceso de proveedores externos

Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes

El acceso a las llaves y módulos criptográficos se limita a necesidades reales de consulta

Existen llaves secretas para la transmisión

Los procedimientos para la protección contra software maligno incluyen:

- todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso
- existe una política por escrito para bajar archivos (downloads), aceptación o uso de aplicaciones gratuitas y compartidas y esta política está vigente
- el software para aplicaciones altamente sensibles está protegido por MAC (Message Authentication Code- Código de Autenticación de Mensajes) o firma digital, y fallas de verificación para evitar el uso del software
- los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos
- existe una política y un procedimiento vigente para la verificación de disquetes externos al programa de compra normal de la organización

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Los firewalls poseen por lo menos las siguientes propiedades:

- todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles digitales, debe reforzarse físicamente)
- sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local
- los firewalls por sí misma es inmune a la penetración
- el tráfico se intercambia en firewalls a la capa de aplicación únicamente
- la arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación
- la arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transportación
- la arquitectura del firewall debe estar configurada de acuerdo a la “filosofía de arte mínima”
- la arquitectura del firewall debe desplegar sólida autenticación para la administración y sus componentes
- la arquitectura del firewall oculta la estructura de la red interna
- la arquitectura del firewall provee una auditoría de todas las comunicaciones hacia o a través del sistema del firewall y activará alarmas cuando se detecte alguna actividad sospechosa
- el host de la organización, que provee el soporte para las solicitudes de entrada al servicio de las redes públicas, permanece fuera del firewall
- la arquitectura del firewall se defiende de los ataques directos (ej., a través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico)
- todo código ejecutable se explora en busca de códigos malignos ej., virus, applets dañinos) antes de introducirse a la red interna

Evaluar el riesgo de los objetivos de control no alcanzados:

► **Llevando a cabo:**

Mediciones (“Benchmarking”) de la seguridad de los sistemas de información contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión detallada de la seguridad de los sistemas de información, incluyendo evaluaciones de penetración de la seguridad física y lógica de los recursos computacionales, de comunicación, etc.

Entrevistas a los nuevos empleados para asegurar el conocimiento y la conciencia en cuanto a seguridad y en cuanto a las responsabilidades individuales, por ejemplo, confirmar la existencia de declaraciones de seguridad firmadas y el entrenamiento para nuevos empleados en cuanto a seguridad

Entrevistas a usuarios para asegurar que el acceso está determinado tomando como base la necesidad (“menor necesidad”) y que la precisión de dicho acceso es revisada regularmente por la gerencia

► **Identificando:**

Accesos inapropiados por parte de los usuarios a los recursos del sistema

Inconsistencias con el esquema o inventario de redes en relación con puntos de acceso faltantes, accesorios faltantes, etc.

Deficiencias en los contratos en cuanto a la propiedad y responsabilidades relacionadas con la integridad y seguridad de los datos en cualquier punto de la transmisión entre en envío y la recepción

Empleados no verificados como usuarios legítimos o antiguos empleados que cuenten aún con acceso

Requisiciones informales o no aprobadas de acceso a los recursos del sistema

Software de monitoreo de redes que no indique a la administración de redes las violaciones a la seguridad

Defectos en los procedimientos de control de cambios del software de redes

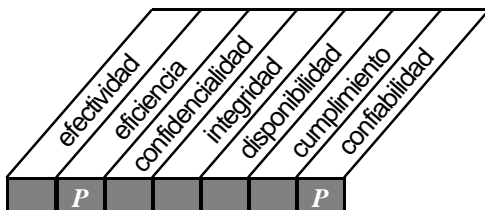
La no utilización de llaves secretas en los procedimientos de emisión/recepción de terceras partes

Deficiencias en los protocolos para generación de llaves, almacenamiento de distribución, entrada, uso, archivo y protección

La falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones

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:

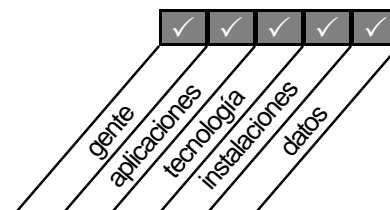
- recursos identificables y medibles
- procedimientos y políticas de cargo
- tarifas

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



DS 6 IDENTIFICACIÓN Y ASIGNACIÓN DE COSTOS

OBJETIVOS DE CONTROL

- | | |
|---|--|
| 1 | Elementos Sujetos a Cargo |
| 2 | Procedimientos de Costeo |
| 3 | Procedimientos de Cargo y Facturación a Usuarios |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

► **Entrevistas:**

Gerencia administrativa o de asignación de costos de la función de servicios de información

Administración de usuarios seleccionada facturada y absorbente de costos

► **Obteniendo:**

Políticas y procedimientos generales para la organización relacionadas con la planeación y la preparación del presupuesto

Políticas y procedimientos de la función de servicios de información relacionadas con la agregación de costos, facturación, metodología y reportes de desempeño/costos

Los siguientes elementos de la función de servicios de información:

- Presupuesto actual y del año anterior
- Reportes de seguimiento de la utilización de los recursos de los sistemas de información
- Datos fuente utilizados en la preparación de los reportes de seguimiento
- Metodología o algoritmo de asignación de costos
- Reportes históricos de facturación

Los siguientes elementos de la administración de usuarios:

- Presupuesto actual y del año anterior para los costos de la función de servicios de información
- Plan de desarrollo y mantenimiento de sistemas de información del año en curso
- Gastos presupuestados para los recursos de sistemas de información, incluyendo aquellos facturados o absorbidos

Evaluar los controles:

► **Considerando sí:**

La función de servicios de información cuenta con un grupo responsable de reportar y emitir facturas a los usuarios

Existen procedimientos que:

- creen un plan anual de desarrollo y mantenimiento con la identificación de prioridades por parte del usuario en cuanto a desarrollo, mantenimiento y gastos operacionales
- permitan a los usuarios una determinación de muy alto nivel en cuanto a en qué se gastan los recursos de la función de servicios de información
- generen un presupuesto anual para la función de servicios de información, incluyendo:
 - Cumplimiento con los requerimientos organizacionales en cuanto a la preparación de presupuestos
 - Consistencia en cuanto a cuáles costos deben ser asignados por los departamentos usuarios

- Comunicación de costos históricos, suposición de nuevos costos – para la comprensión del usuario en cuanto a cuáles costos son incluidos y facturados
- Autorización del usuario de todos los costos presupuestados a ser asignados por la función de servicios de información
- Frecuencia de la emisión de reportes y cargo real de costos a los usuarios
- seguimiento de los costos asignados de todos los recursos de los sistemas de información en cuanto (pero sin limitarse) a:
 - Hardware operacional
 - Equipo periférico
 - Utilización de telecomunicaciones
 - Desarrollo y soporte de aplicaciones
 - Generales administrativos
 - Costos de servicios de proveedores externos
 - Help desk
 - Instalaciones y mantenimiento
 - Costos directos e indirectos
 - Gastos fijos y variables
 - Costos discrecionales
- asistan en la emisión regular de reportes para los usuarios en cuanto al desempeño para las distintas categorías de costos
- reporten a los usuarios en cuanto a mediciones (“benchmarks”) externas relacionadas con la efectividad de costos, con el fin de permitir una comparación contra las expectativas de la industria u otras fuentes alternativas de servicios para los usuarios
- permitan la modificación oportuna de la asignación de costos para reflejar los cambios en las necesidades del negocio
- aprueben y acepten formalmente los cargos al ser recibidos
- identifiquen las oportunidades de mejora de la función de servicios de información para reducir las facturaciones o para obtener un mejor valor por los cargos

Los reportes aseguran que los elementos sujetos a costo son identificables, medibles y predecibles

Los reportes capturan y resaltan los cambios en los componentes de costos o en el algoritmo de asignación

Evaluar la suficiencia:

▸ Probando que:

Existe una metodología de asignación de costos, que los usuarios están de acuerdo en cuanto a su equidad, y que genera tanto costos como reportes

Existe un programa de mejora para reducir costos o aumentar el desempeño de los recursos de los sistemas de información

Los procesos de asignación y reporte fomentan un uso más apropiado, efectivo y consistente de los recursos computacionales, que éstos aseguran el tratamiento justo de los departamentos usuarios y sus necesidades, y que los cargos reflejan los costos asociados con la prestación de servicios

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ Llevando a cabo:

Mediciones (“Benchmarking”) de la contabilidad de costos y de la metodología de facturación contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Un recálculo de la facturación a partir de datos fuente, a través de un algoritmo de asignación de facturación y dentro del flujo de reportes a usuarios

La precisión de los datos en el reporte de desempeño, como:

- utilización de CPU
- utilización de periféricos
- utilización de DASD
- líneas de código escritas
- líneas/páginas impresas
- modificaciones a programas llevadas a cabo
- número de PCs, teléfonos, archivos de datos
- consultas al help desk
- número, duración de las transmisiones

La compilación de los datos fuente de recursos en el reporte de desempeño es correcta

Se cuenta con el algoritmo real para compilar y asignar costos a facturación

La precisión de la facturación a usuarios específicos sea probada frecuentemente

Las facturaciones a usuarios sean aprobadas

Se lleven a cabo revisiones de consistencia de la facturación entre los diferentes usuarios

El progreso en el plan de desarrollo de usuarios tenga como base los costos expendidos

Se lleve a cabo una revisión de la distribución de reportes en cuanto a utilización e información de costos

La satisfacción del usuario en cuanto a :

- lo razonable de la facturación comparada con las expectativas presupuestadas
- el plan de desarrollo anual contra los costos
- lo razonable de la facturación comparada con las fuentes alternativas, por ejemplo “benchmarks”
- la comunicación de tendencias que incrementaría/decrementaría la facturación
- solución de las variaciones comparadas contra la facturación esperada

► **Identificando:**

Oportunidades para una mayor efectividad y propiedad de la metodología de facturación

- incluyendo más componentes de costos
- modificando los índices o unidades de medida de asignación de costos
- modificando el algoritmo mismo de costos
- mecanizando o integrando la función de contabilidad con equipo y reportes generadores de aplicaciones

Inconsistencias dentro del algoritmo de asignación

Inconsistencias de asignación entre diferentes usuarios

Oportunidades para la mejora de recursos de sistemas

Oportunidades para el usuario con el fin de aplicar de una mejor manera los recursos de servicios de información para alcanzar los requerimientos de negocios del usuario

Mejoras en la eficiencia de los procesos de recopilación, acumulación, asignación, reporte y comunicación, los cuales de traducirán en un mejor desempeño o menor costo para los usuarios de los servicios proporcionados

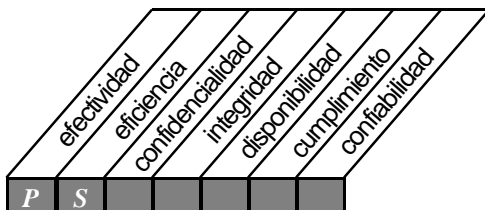
Que las tendencias de costos reflejadas por las variaciones y el análisis hayan sido traducidas a cargos modificados en los períodos siguientes y hayan sido reflejadas en la estructura de costos

Que existen oportunidades para hacer de la función de servicios de información un centro de provecho y beneficios al proporcionar servicios a otros usuarios internos o externos

Si la función de servicios de información es un centro de provecho y beneficios, que la contribución de dichos beneficios contra el plan y el presupuesto sea alcanzada y que destaquen las oportunidades para aumentar los beneficios

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:

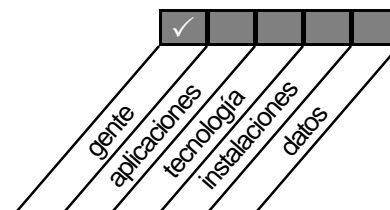
- curriculum de entrenamiento
- campañas de concientización
- técnicas de concientización

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



DS 7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS

OBJETIVOS DE CONTROL

- | | |
|---|--|
| 1 | Identificación de necesidades de entrenamiento |
| 2 | Organización de Entrenamiento |
| 3 | Entrenamiento sobre principios y conciencia de Seguridad |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Administrador de entrenamiento o recursos humanos de la organización
 Administrador de entrenamiento o de recursos humanos de la función de servicios de información
 Administradores y empleados seleccionados de la función de servicios de información
 Administradores y empleados seleccionados de los departamentos usuarios

▸ **Obteniendo:**

Políticas y procedimientos generales para la organización con respecto al entrenamiento sobre controles y conciencia de seguridad, beneficios para los empleados enfocados al desarrollo, programas de entrenamiento para los usuarios de servicios, instalaciones educacionales y requerimientos de educación continua profesional
 Programas, políticas y procedimientos de entrenamiento y de educación de la función de servicios de información relacionados con controles y conciencia de seguridad, seguridad técnica y controles
 Programas de entrenamiento disponibles (tanto internos como externos) para seguridad y conciencia de controles introductorios y continuos, así como para entrenamiento dentro de la organización

Evaluar los controles:

▸ **Considerando sí:**

Existen políticas y procedimientos relacionados con una conciencia continua de seguridad y controles
 Se cuenta con un programa de educación/entrenamiento enfocado a los principios de seguridad de los sistemas de información y de control
 Los nuevos empleados tienen conocimiento y conciencia de la responsabilidad de seguridad y control con respecto a la utilización y la custodia de los recursos de sistemas de información
 Se cuenta con políticas y procedimientos vigentes relacionados con entrenamiento y si éstos están actualizados con respecto a la configuración técnica de los recursos de sistemas de información
 Existe disponibilidad de oportunidades de entrenamiento interno, considerando también la asistencia de los empleados
 Existe disponibilidad de oportunidades de entrenamiento técnico externo, considerando también la asistencia de los empleados
 Si una función de entrenamiento asesora las necesidades de entrenamiento del personal con respecto a seguridad y controles, trasladando estas necesidades en oportunidades de entrenamiento interno o externo
 Se requiere a todos los empleados asistir a entrenamientos de conciencia de control y seguridad continuamente, los cuales incluirían, sin limitarse a:

- principios generales de seguridad de sistemas

- conducta ética de la función de servicios de información
- prácticas de seguridad para la protección contra daños ocasionados por fallas que afecten la disponibilidad, confidencialidad, integridad y desempeño de las funciones en una forma segura
- existen las responsabilidades asociadas con la custodia y utilización de los recursos de sistemas de información
- la seguridad de la información y los sistemas de información cuando se utilizan externamente al lugar

La capacitación sobre la sensibilización a la seguridad incluye una política para evitar la exposición de la información sensible a través de conversaciones (ej., avisando el estatus de la información a todas las personas que toman parte en la conversación)

Evaluar la suficiencia:

▸ **Probando que:**

Los nuevos empleados tienen conciencia y conocimiento de la seguridad, controles y responsabilidades fiduciarias de poseer y utilizar recursos de sistemas de información

Las responsabilidades de los empleados con respecto a la confiabilidad, integridad, disponibilidad, confidencialidad y seguridad de todos los recursos de los sistemas de información es comunicada continuamente

Un grupo de la función de servicios de información es formalmente responsable del entrenamiento, conciencia de seguridad y controles y mantenimiento de programas de educación continua para certificaciones profesionales

Se considera continuamente la evaluación de las necesidades de entrenamiento para empleados

El desarrollo o la participación en los programas de entrenamiento relacionados con seguridad y controles es parte de los requerimientos de entrenamiento

Existen programas reales nuevos y a largo plazo de entrenamiento sobre conciencia de seguridad para empleados

Los acuerdos de confidencialidad son firmados por todos los empleados

No faltan estatutos de confidencialidad y conflicto de intereses para empleados

No faltan evaluaciones de necesidades de entrenamiento para empleados

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Una revisión de los manuales de entrenamiento en cuanto a su adecuación y suficiencia con respecto a controles de seguridad, confidencialidad, confiabilidad, disponibilidad e integridad

Entrevistas al personal de la función de servicios de información para determinar la identificación de necesidades de entrenamiento y la extensión o satisfacción de tales necesidades

▸ **Identificando:**

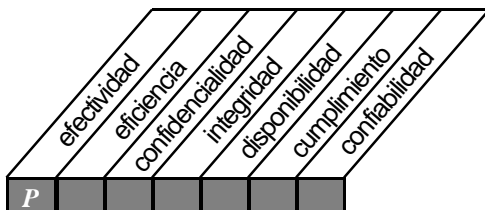
Inconsistencias en el currículum ofrecido como respuesta a las necesidades de entrenamiento

Deficiencias en la conciencia de los usuarios en cuanto a problemas de seguridad relacionados con la utilización de los recursos de los sistemas de información

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

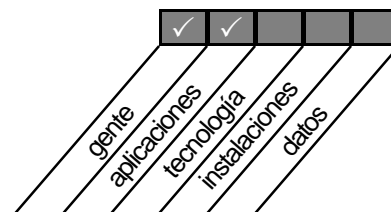
Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo

⁵⁵ Buró de ayuda (*help desk*)



DS 8 APOYO Y ASISTENCIA PARA LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVOS DE CONTROL

- 1 Buró de Ayuda
- 2 Registro de preguntas del Usuario
- 3 Escalamiento de preguntas del cliente
- 4 Monitoreo de atención a clientes
- 5 Análisis y reporte de tendencias

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Administrador de soporte del buró de ayuda de la función de sistemas de información
 Usuarios seleccionados de los servicios de información

▸ **Obteniendo:**

Políticas y procedimientos generales para la organización relacionados con el soporte a usuarios de la función de servicios de información
 Organigrama, misión, políticas y procedimientos de la función de servicios de información relacionados con las actividades de buró de ayuda
 Reportes relacionados con la preguntas de los usuarios, su solución y estadísticas de desempeño del buró de ayuda
 Cualquier estándar de desempeño para las actividades del buró de ayuda
 Acuerdos de nivel de servicios entre la función de servicios de información y usuarios diversos
 Archivos personales que muestren las credenciales y experiencia profesional del personal del buró de ayuda

Evaluar los controles:

▸ **Considerando sí:**

La naturaleza de la función del buró de ayuda (por ejemplo, la forma en la que las requisiciones de ayuda son procesadas y la ayuda es proporcionada) es efectiva
 Existen instalaciones reales, divisiones o departamentos que lleven a cabo la función del buró de ayuda, así como personal o posiciones responsables del buró de ayuda
 El nivel de documentación para las actividades del buró de ayuda es adecuado y actual
 Existe un proceso real para registrar requisiciones de servicios y si se hace uso de dicha bitácora
 El proceso para la escalación de preguntas y la intervención de la administración para su solución son suficientes
 El período de tiempo para atender las preguntas recibidas es adecuado
 Existen los procedimientos para el seguimiento de tendencias y reportes de las actividades del buró de ayuda
 Se identifican y ejecutan formalmente iniciativas de mejora de desempeño
 Se alcanzan y se cumple con los acuerdos de nivel de servicio y los estándares de desempeño
 El nivel de satisfacción del usuario periódicamente se revisa y se reporta

▸ **Probando que:**

Las políticas y procedimientos son actuales y precisos en relación con las actividades del buró de ayuda

Los compromisos de nivel de servicio son conservados y que las variaciones son explicadas

Las preguntas son atendidas de una forma oportuna

El análisis y reporte de tendencias asegura que los reportes:

- son emitidos y que se toman las medidas necesarias para mejorar el servicio
- incluyen problemas específicos, análisis de tendencias y tiempos de respuesta
- son enviados a las personas responsables con la autoridad para resolver los problemas

Se obtienen para una muestra de requisiciones de ayuda, confirmación de la precisión, oportunidad y suficiencia de la respuesta

Las encuestas sobre el nivel de satisfacción del usuario existen y se trabaja con ellas

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Entrevistas con usuarios seleccionados para determinar su satisfacción en cuanto a:

- actividades de buró de ayuda
- reporte de actividades
- cumplimiento de los compromisos de nivel de servicio

Una revisión de la competencia y capacidad del personal del buró de ayuda con respecto a la realización de sus tareas

Una revisión de preguntas seleccionadas escaladas en cuanto a lo adecuado de sus respuestas

Una revisión de los reportes de tendencias y posibles oportunidades de mejoras de desempeño

▸ **Identificando:**

Interacciones inadecuadas de las actividades del buró de ayuda con respecto a otras funciones dentro de la función de servicios de información, así como a las organizaciones usuarias

Procedimientos y actividades insuficientes relacionadas con problemas en el reporte de recepción, registro, seguimiento, escalamiento y solución de preguntas

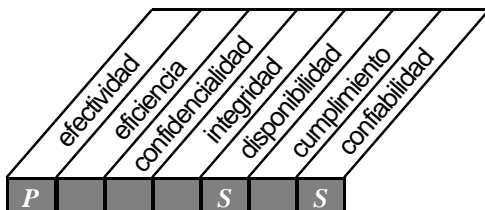
Deficiencias en el proceso de escalamiento con respecto a la falta de involucramiento por parte de la administración o a acciones correctivas efectivas

Oportunidad inadecuada en el reporte de problemas o insatisfacción del usuario en cuanto al proceso de reporte de problemas.

OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS9



Control sobre el proceso de TI de:

Administración de la configuración

que satisface los requerimientos de negocio de:

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

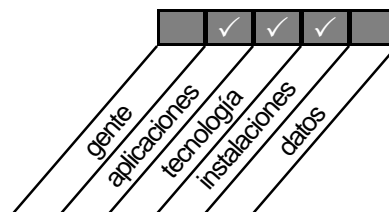
- registro de activos
- administración de cambios en la configuración
- chequeo de software no autorizado
- controles de almacenamiento de software

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



DS 9 ADMINISTRACIÓN DE LA CONFIGURACIÓN

OBJETIVOS DE CONTROL

- | | |
|---|------------------------------|
| 1 | Registro de la Configuración |
| 2 | Base de la Configuración |
| 3 | Estado de Cuenta |
| 4 | Control de la Configuración |
| 5 | Software no Autorizado |
| 6 | Almacenamiento de Software |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Administración de operaciones de la función de servicios de información
 Administración de soporte de sistemas de la función de servicios de información
 Administración de desarrollo de aplicaciones de la función de servicios de información
 Administración de instalaciones
 Personal de soporte de proveedores de software
 Personal de administración de activos relacionados con computación
 Administrador de aseguramiento de la calidad

▸ Obteniendo:

Un inventario de la configuración: hardware, software de sistema operativo, software de aplicaciones, instalaciones y archivos de datos –dentro y fuera de las instalaciones
 Políticas y procedimientos organizacionales relacionados con la adquisición, inventario y disposición de software y equipo computacional comprado, rentado o arrendado
 Políticas organizacionales relacionadas con la utilización de software o equipo no autorizado
 Políticas y procedimientos de la función de servicios de información relacionados específicamente con la adquisición, disposición y mantenimiento de los recursos de la configuración
 Políticas y procedimientos de la función de servicios de información relacionados con las funciones de aseguramiento de la calidad y de control de cambios en cuanto a la transferencia independiente y el registro de la migración del desarrollo de software nuevo y modificado hacia los archivos y estatus de producción
 Información de la base de la configuración
 Registros contables de activos fijos y arrendamientos relacionados con los recursos de sistemas
 Reportes relacionados con adiciones, eliminaciones y cambios a la configuración de los sistemas
 Listas del contenido de las distintas librerías – prueba, desarrollo y producción
 Inventario del contenido del almacenamiento fuera de las instalaciones– equipo, archivos, manuales y formas – incluyendo material en manos de los proveedores

► **Considerando sí:**

El proceso para crear y controlar las bases de la configuración (el punto en el diseño y desarrollo de un elemento de la configuración más allá del cual no ocurren más avances sin llevar a cabo un estricto control de la configuración) es apropiado

Existen funciones para mantener la base de la configuración

Existe un proceso para controlar los estados de cuenta de los recursos adquiridos y arrendados – incluyendo entradas, salidas e integración con otros procesos

Los procedimientos de control de la configuración incluyen:

- integridad en la base de la configuración
- controles de autorización de acceso programados en el sistema de administración de cambios
- la recuperación de los elementos de la configuración y las requisiciones de cambios en cualquier momento
- la terminación de la configuración y de los reportes que evalúan lo adecuado de los procedimientos de registro de la configuración
- evaluaciones periódicas de la función de registro de la configuración
- el personal responsable de la revisión del control de la configuración satisfaga los requisitos de conocimientos, destrezas y habilidades
- la existencia de procedimientos para revisar el acceso a las bases del software
- los resultados de las revisiones sean proporcionados a la administración para llevar a cabo acciones correctivas

Se lleva a cabo regularmente una revisión periódica de la configuración con registros de inventario y de cuentas

La base de la configuración cuenta con historia suficiente para dar seguimiento a los cambios

Existen procedimientos de control de cambios de software para:

- establecer y mantener una librería de programas de aplicación con licencia
- asegurar que la librería de programas de aplicación con licencia sea controlada adecuadamente
- asegurar la confiabilidad e integridad del inventario de software
- asegurar la confiabilidad e integridad del inventario de software autorizado utilizado y revisar la existencia de software no autorizado
- asignar responsabilidades sobre el control de software no autorizado a un miembro específico del personal
- registrar el uso de software no autorizado y reportar a la administración para llevar a cabo acciones correctivas
- determinar si la administración llevó a cabo acciones correctivas sobre las violaciones

Los procesos de migración de aplicaciones de desarrollo al ambiente de pruebas y finalmente al estatus de producción interactúan con el reporte de la configuración

El proceso de almacenamiento de software incluye:

- definir un área segura de almacenamiento de archivos (librería) para todo el software válido en fases apropiadas del ciclo de vida de desarrollo de sistemas
- requerir separación de las librerías de almacenamiento de software entre ellas y con respecto a las áreas de almacenamiento de archivos de desarrollo, pruebas y producción
- requerir la existencia dentro de las librerías fuente que permitan la colocación temporal de módulos fuente a ser transferidos al período de ciclo de producción
- requerir que cada miembro de todas las librerías cuente con un propietario designado
- definir controles de acceso lógicos y físicos
- establecer responsabilidades sobre el software

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- establecer un seguimiento de auditoría
- detectar, documentar y reportar a la administración todas las instancias en las que no se cumpla con este procedimiento
- determinar si la administración llevó a cabo acciones correctivas

Existe una coordinación entre el desarrollo de aplicaciones, el aseguramiento de la calidad y las operaciones con respecto a la actualización de la base de la configuración al realizarse cambios

Evaluar la suficiencia:

► Probando que:

Todos los elementos de la configuración se encuentran bajo un control base

Las políticas y procedimientos relacionados con el reporte de la configuración son actuales y precisos

Se cumple con los estándares de desempeño con respecto al mantenimiento y reporte de la configuración

Se lleva a cabo una comparación entre el inventario físico del equipo y los registros de contabilidad de activos

Existe independencia de la migración de pruebas a producción y registros de los cambios

Para una selección de salidas de base:

- se lleve una base precisa, apropiada y aprobada de los elementos de la configuración
- los registros de la configuración reflejen el estatus actual de todos los elementos de la configuración, incluyendo la historia de cambios
- la administración revise y evalúe periódicamente la consistencia de la configuración, y que se lleven a cabo acciones correctivas
- las librerías de archivos hayan sido definidas conveniente y adecuadamente y en fases apropiadas del ciclo de vida de desarrollo de sistemas
- para todas las computadoras personales que contengan software no autorizado se reporten violaciones y la administración lleve a cabo acciones correctivas
- los registros de la configuración con respecto a producto, versión y modificaciones de los recursos proporcionados por los proveedores sean precisos
- los registros históricos de cambios a la configuración sean precisos
- existan mecanismos para asegurar que no exista software no autorizado en las computadoras, incluyendo:
 - Políticas y estatutos
 - Entrenamiento y conciencia de responsabilidades potenciales (legales y de producto)
 - Formas firmadas de cumplimiento por parte de todo el personal que utilice computadoras
 - Control centralizado del software computacional
 - Revisión continua del software computacional
 - Reportes de los resultados de la revisión
 - Acciones correctivas por parte de la administración basadas en los resultados de las revisiones
- el almacenamiento de programas de aplicación y código fuente sea definido durante el ciclo de desarrollo y que el impacto de los registros de la configuración sea determinado
- la suficiencia e integridad de los registros de proveedores y fuera del site relacionados con la configuración, así como la precisión en los registros de la configuración sean anticipados y considerados
- se definan procedimientos de base de la configuración para:

- Registrar el evento que creó la base, el establecimiento de la base y los elementos de la configuración que deben ser controlados en la base
- Modificar la base, incluyendo la autoridad requerida para aprobar los cambios a las bases de la configuración aprobadas previamente
- Registrar los cambios a la base y a los elementos de la configuración que deben ser controlados en la base
- Asegurar que todos los elementos de la configuración son registrados dentro de los productos de base
- Existe el reporte de estado de cuenta para:
 - El tipo de información a ser recopilada, almacenada, procesada y reportada (Esto deberá incluir el estatus de la base, los hallazgos en las revisiones de la base, requisiciones de cambios y estatus; revisión y aprobación/desaprobación del control de la configuración (sí aplica); modificaciones realizadas; reportes de problemas y estatus y la historia de la revisión de la configuración)
 - La manera en la que los problemas de requisiciones de cambio son resueltos con un estado de cuenta incompleto
 - Los tipos de reportes de estados de cuenta a ser generados y su frecuencia
 - La manera en la que el acceso a estos datos de estatus será controlado

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Una revisión detallada de la frecuencia y la oportunidad de las revisiones administrativas de los registros de la configuración, los cambios a los registros y la conciliación de los registros de inventario, cuenta y proveedor

Un análisis del software de varias librerías en cuanto a posible duplicación, identificación de código objeto faltante y en cuanto a la eliminación de archivos de datos o programas innecesarios -- y su reflejo en los registros de la configuración

▸ **Identificando:**

Las debilidades en la conciencia y en el conocimiento de la administración y el personal en cuanto a las políticas organizacionales con respecto a:

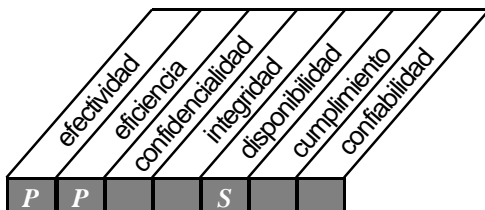
- Los registros de la configuración y los cambios realizados a estos registros
- La colocación de controles de configuración en el ciclo de vida de desarrollo de sistemas La integración de los registros de configuración, cuenta y proveedor
- La no utilización de software no autorizado en computadoras personales

Posibles mejoras inadecuadas en la efectividad y la eficiencia de la función de creación y mantenimiento de la función de creación y mantenimiento de la base de la configuración

Deficiencias en los cambios de proveedores al ser reflejados en los registros de la configuración, en los registros de seguridad, o cambios a los registros por parte de los proveedores reflejados apropiadamente

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:

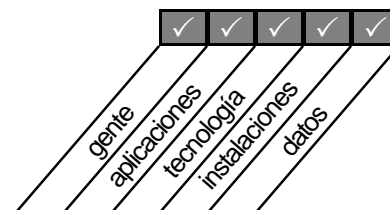
- suficientes pistas de auditoría de problemas y soluciones
- resolución oportuna de problemas reportados
- procedimientos de escalamiento
- reportes de incidentes

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



DS 10 MANEJO DE PROBLEMAS E INCIDENTES

OBJETIVOS DE CONTROL

- | | |
|---|--|
| 1 | Sistema de manejo de Problemas |
| 2 | Escalamiento de Problemas |
| 3 | Seguimiento de Problemas y Pistas de Auditoría |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Personal de soporte de operaciones de la función de servicios de información
 Personal de soporte del buró de ayuda de la función de servicios de información
 Personal de soporte de sistemas de la función de servicios de información
 Personal de soporte de aplicaciones de la función de servicios de información
 Usuarios seleccionados de los recursos de los sistemas de información

▸ Obteniendo:

Un resumen de las instalaciones y posiciones de manejo de problemas que realizan la función de manejo de problemas
 Políticas y procedimientos de la función de servicios de información relacionados con el manejo de problemas, incluyendo procesos de reconocimiento, registro, solución, escalamiento, seguimiento y reporte
 Una lista de los problemas reportados durante un período representativo, incluyendo la fecha de ocurrencia, la fecha de escalamiento (sí aplica), la fecha de solución y los tiempos de solución
 Una lista de las aplicaciones críticas que son escaladas inmediatamente a la atención de la presidencia para darles prioridad de solución, o que son reportables como problemas críticos
 Un conocimiento de cualquier aplicación de manejo de problemas, y en particular un método para asegurar que todos los problemas son capturados, resueltos y reportados según lo requerido

Evaluar los controles:

▸ Considerando sí:

Existe un proceso de manejo de problemas que asegure que todos los eventos operacionales que no son parte de las operaciones estándar son registrados, analizados y resueltos de manera oportuna, y que se generan reportes de incidentes para problemas significativos
 Existen procedimientos de manejo de problemas para:

- definir e implementar un sistema de manejo de problemas
- registrar, analizar y resolver de manera oportuna todos los eventos no-estándar
- establecer reportes de incidentes para los eventos críticos y la emisión de reportes para usuarios
- identificar tipos de problemas y metodología de priorización que permitan una variedad de soluciones tomando el riesgo como base
- definir controles lógicos y físicos de la información de manejo de problemas

- distribuir salidas con una base de “necesidad de conocimiento”
- seguir las tendencias de los problemas para maximizar recursos y reducir la rotación
- recolectar entradas de datos precisas, actuales, consistentes y utilizables para la emisión de reportes
- notificar los escalamientos al nivel apropiado de administración
- determinar si la administración evalúa periódicamente el proceso de manejo de problemas en cuanto a una mayor efectividad y eficiencia
- asegurar la suficiencia de los seguimientos de auditoría para los problemas de sistemas
- asegurar la integración entre los cambios, la disponibilidad, el sistema y el personal de manejo de la configuración

Evaluar la suficiencia:

▸ **Probando que:**

Una muestra seleccionada de salidas de procesos cumple con los procedimientos establecidos relacionados con:

- problemas no-críticos
- problemas críticos/de alta prioridad que requieren escalamiento
- el reporte de los requerimientos, el contenido, la precisión, la distribución y las acciones llevadas a cabo
- la satisfacción del usuario con el proceso de manejo de problemas y los resultados

Vía entrevistas, el conocimiento y la conciencia del proceso de manejo de problemas

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Para una selección de problemas reportados, pruebas que aseguren que los procedimientos de manejo de problemas fueron seguidos para todas las actividades no-estándar, incluyendo:

- registro de todos los eventos no-estándar por proceso
- seguimiento y solución de todos y cada una de los eventos
- nivel apropiado de respuesta tomando como base la prioridad del evento
- escalamiento de problemas para eventos críticos
- reporte apropiado dentro de la función de servicios de información y grupos usuarios
- revisiones regulares de efectividad y eficiencia de procesos en cuanto a mejoras
- expectativas y éxito de programa de mejoras del desempeño

▸ **Identificando:**

Ocurrencias de problemas no controlados formalmente por el proceso de manejo de problemas

Ocurrencias de problemas reconocidos pero no resueltos por proceso de manejo de problemas

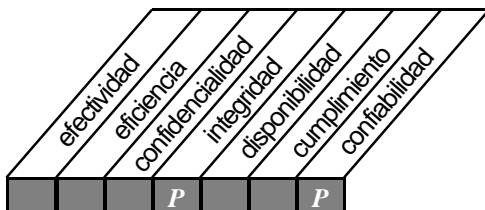
Variaciones entre los eventos de procesos reales y formales con respecto a la solución de problemas

Deficiencias de los usuarios en el proceso de manejo de problemas, en la comunicación de problemas y su solución -- en cuanto a posibles oportunidades de mejora

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:

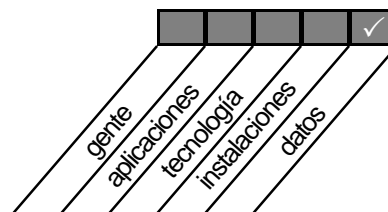
- diseño de formatos
- controles de documentos fuente
- controles de entrada
- controles de procesamiento
- controles de salida
- identificación, movimiento y administración de la librería de medios
- administración de almacenamiento y respaldo de medios
- autenticación e integridad

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



DS 11 ADMINISTRACIÓN DE DATOS

OBJETIVOS DE CONTROL

- 1 Procedimientos de Preparación de Datos
- 2 Procedimientos de Autorización de Documentos Fuente
- 3 Recopilación de Datos de Documentos Fuente
- 4 Manejo de Errores de Documentos Fuente
- 5 Retención de Documentos Fuente
- 6 Procedimientos de Autorización de Entrada de Datos
- 7 Revisiones de Precisión, Suficiencia y Autorización
- 8 Manejo de Errores en la Entrada de Datos
- 9 Integridad de Procesamiento de Datos
- 10 Validación y Edición de Procesamiento de Datos
- 11 Manejo de Errores en el Procesamiento de Datos
- 12 Manejo y Retención de Salida de Datos
- 13 Distribución de Salida de Datos
- 14 Balanceo y Conciliación de Datos de Salida
- 15 Revisión de Salida de Datos y Manejo de Errores
- 16 Provisiones de Seguridad para Reportes de Salida
- 17 Protección de Información Sensible
- 18 Protección de Información Sensible Desechada
- 19 Administración de Almacenamiento
- 20 Períodos de Retención y Términos de Almacenamiento
- 21 Sistema de Administración de la Librería de Medios
- 22 Responsabilidades de la Administración de la Librería de Medios
- 23 Respaldo y Restauración
- 24 Funciones de Respaldo
- 25 Almacenamiento de Respaldo
- 26 Archivo
- 27 Protección de mensajes sensibles
- 28 Autenticación e Integridad
- 29 Integridad de Transacciones Electrónicas
- 30 Integridad continua de Datos Almacenados

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

- Administración de operaciones de la función de servicios de información
- Administración de bases de datos de la función de servicios de información
- Administración de desarrollo de aplicaciones de la función de servicios de información
- Administración de entrenamiento/recursos humanos de la función de servicios de información
- Administración de soporte de sistemas de la función de servicios de información
- Administración de la seguridad de respaldos
- Administraciones de usuarios varias para aplicaciones críticas de la misión

► **Obteniendo:**

Políticas y procedimientos organizacionales relacionados con la naturaleza y administración de datos, incluyendo:

- flujo de datos dentro de la función de servicios de información y entre usuarios de datos
- puntos en la organización en los que los datos son originados, concentrados en grupos o tandas (“batched”), editados, capturados, procesados, extraídos, revisados, corregidos y remitidos, y distribuidos a los usuarios
- proceso de autorización de documentos fuente
- procesos de recolección, seguimiento y transmisión de datos
- procedimientos para asegurar la suficiencia, precisión, registro y transmisión de documentos fuente completos para captura
- procedimientos utilizados para identificar y corregir errores durante la creación original de datos
- procedimientos para asegurar la integridad, confidencialidad y aceptación de los mensajes delicados transmitidos por Internet o cualquier otra red pública
- métodos utilizados por la organización para retener documentos fuente (archivo, imagen, etc.), para definir qué documentos deben ser retenidos, los requerimientos de retención legales y regulatorios, etc.
- sistemas de interfase que proporcionen y utilicen datos para las funciones de servicios de información
- contratos de proveedores para llevar a cabo tareas de administración de datos
- reportes administrativos utilizados para monitorear actividades e inventarios

Una lista de todas las aplicaciones mayores, así como de la documentación de usuario relacionada con:

- módulos que lleven a cabo revisiones de precisión, suficiencia y autorización de captura
- funciones que lleven a cabo entradas de datos para cada aplicación
- funciones que lleven a cabo rutinas de corrección de errores de entrada de datos
- métodos utilizados para prevenir (por medios manuales y programados), detectar y corregir errores
- control de la integridad de los procesos de datos emitidos
- edición y autenticación de la validación del procesamiento de datos tan cerca del punto de origen como sea posible
- manejo y retención de salidas creadas por aplicaciones
- salidas, distribución de salidas y sistemas de interfase que utilizan salidas
- procedimientos de balanceo de salidas para control de totales y conciliación de variaciones
- revisión de la precisión de los reportes de salida y de la información
- seguridad en los reportes de procesamiento de salidas distribuidos
- seguridad de los datos transmitidos y entre aplicaciones
- disposición de documentación sensible de entrada, proceso y salida
- procedimientos de control de proveedores como terceras partes con respecto a preparación, entrada, procesamiento y salida

Políticas y procedimientos relacionados con cualquier depósito de bases de datos de la organización, incluyendo:

- organización de la base de datos y diccionario de datos
- procedimientos de mantenimiento y seguridad de bases de datos
- determinación y mantenimiento de la propiedad de las bases de datos
- procedimientos de control de cambios sobre el diseño y contenido de la base de datos
- reportes administrativos y seguimientos de auditoría que definen actividades de bases de datos

Políticas y procedimientos relacionados con la librería de medios y con el almacenamiento de datos fuera del site, incluyendo:

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- administración de la librería de medios y del sistema de administración de la librería
- requerir la identificación externa de todos los medios
- requerir el inventario actual de todos los contenidos y procesos para actividades de control
- procesos de administración para proteger los recursos de datos
- procedimientos de conciliación entre registros reales y de datos
- reciclaje de datos y rotación de medios de datos
- datos de pruebas pasadas de pruebas de inventario y recuperación llevadas a cabo
- funciones del personal de los medios y fuera del site en los planes de manejo de desastres y recuperación del negocio

Evaluar los controles:

► Considerando sí:

Para la preparación de datos:

- los procedimientos de preparación de datos aseguran suficiencia, precisión y validez
- existen procedimientos de autorización para todos los documentos fuente
- existe una separación de funciones entre el origen, la aprobación y la conversión de documentos fuente a datos
- los datos autorizados permanecen completos, precisos y válidos a través de la creación original de documentos fuente
- los datos son transmitidos de una manera oportuna
- se lleva a cabo una revisión periódica de los documentos fuente en cuanto a su suficiencia y aprobaciones apropiadas
- se lleva a cabo un manejo apropiado de documentos fuente erróneos
- existe un control adecuado de información sensible en documentos fuente en cuanto a protección contra transgresiones
- los procedimientos aseguran suficiencia y precisión de documentos fuente, contabilidad apropiada para documentos fuente y conversión oportuna
- la retención de documentos fuente es lo suficientemente larga para permitir: la reconstrucción en caso de pérdida, la disponibilidad para revisiones y auditoría, las averiguaciones de litigación o los requerimientos regulatorios

Para la entrada de datos:

- los documentos fuente siguen un proceso de aprobación apropiada antes de su captura
- existe una separación de funciones apropiada entre las actividades de envío, aprobación, autorización y entrada de datos
- existen códigos únicos de terminal o estación e identificaciones seguras de operadores
- existen procesos de uso, mantenimiento y control de códigos de estación e identificadores de operador
- se lleva a cabo un seguimiento de auditoría para identificar la fuente de entrada
- existen verificaciones de rutina o revisiones de edición de los datos capturados tan cerca del punto de origen como sea posible
- existen procesos apropiados de manejo de datos de entrada erróneos
- se asignan claramente las responsabilidades para hacer cumplir una autorización apropiada de los datos

Para el procesamiento de datos:

Los programas contienen rutinas de prevención, detección y corrección de errores:

- los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición)
- los programas deben validar todas las transacciones contra una lista maestra
- los programas deben rechazar la anulación de condiciones de error

Los procesos de manejo de errores incluyen:

- la aprobación de la corrección y del reenvío de errores
- la definición de las responsabilidades individuales para archivos suspendidos
- la generación de reportes de errores no resueltos por parte de los archivos en suspenso
- la disponibilidad del esquema de priorización de archivos suspendidos tomando como base la edad y el tipo

Existen bitácoras de los programas ejecutados y las transacciones procesadas/rechazadas para propósitos de auditoría

Existe un grupo de control para monitorear las actividades de entrada e investigar los eventos no-estándar, así como balancear las cuentas de registros y totales de control para todos los datos procesados

Todos los campos son editados apropiadamente, aún si uno de los campos contiene algún error

Las tablas utilizadas en la validación son revisadas frecuentemente

Existen procedimientos por escrito para la corrección y reenvío de datos con errores incluyendo una solución no descriptiva para reprocesamiento

Las transacciones reenviadas son procesadas exactamente como fueron procesadas originalmente

La responsabilidad de la corrección de errores reside dentro de la función de envío original

Los sistemas de Inteligencia Artificial están colocados en un marco referencial de control interactivo con operadores humanos que aseguran que las decisiones importantes se aprueben

Para las salidas, interfaces y distribución:

El acceso a las salidas está restringido física y lógicamente a personal autorizado

Se lleva a cabo una revisión continua de necesidades de salidas

Las salidas son balanceadas rutinariamente con respecto a totales de control

Existen seguimientos de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de datos confusos

La precisión de los reportes de salidas es revisada y los errores contenidos en las salidas son revisados por personal capacitado

Existe una definición clara de problemas de seguridad durante las salidas, interfaces y distribución

Las violaciones a la seguridad durante cualquier fase son comunicadas a la administración, se llevan a cabo acciones correctivas sobre ellas y son reflejadas apropiadamente en nuevos procedimientos

El proceso y la responsabilidad de la disposición de salidas está claramente definida

La destrucción de materiales utilizados pero no requeridos después de procesados es presenciada por alguien

Todos los medios de entrada y salida son almacenados en localidades fuera del site en caso de requerirse en un futuro

La información marcada como eliminada cambia de tal forma que no se pueda recuperar

Para la librería de medios:

El contenido de la librería de medios es inventariada sistemáticamente

Las discrepancias descubiertas por el inventario son solucionadas oportunamente

Se toman medidas para mantener la integridad de los medios magnéticos almacenados en la librería

Existen procesos de administración para proteger el contenido de la librería de medios

Las responsabilidades de la administración de la librería de medios han sido asignadas a miembros específicos del personal de la función de servicios de información

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Existen estrategias de respaldo y restauración de medios

Los respaldos de medios se llevan a cabo de acuerdo con la estrategia de respaldos y si la utilidad de los respaldos es verificada regularmente

Los respaldos de medios son almacenados con seguridad y si las localidades de almacenamiento son revisadas periódicamente en cuanto a la seguridad de sus acceso físico y a la seguridad de los archivos de datos y otros elementos

Los periodos de retención y almacenamiento están definidos por documentos, datos, programas, reportes y mensajes (de entrada y salida) así como los los datos (claves, certificados) utilizados para su encriptación y autenticación

Los procedimientos adecuados están activos en relación al archivo de información (datos y programas) en línea con los requerimientos legales y del negocio y reforzando la capacidad de respuesta y reproducción

Para la autenticación e integridad de información:

La integridad de los archivos de datos se verifica periódicamente

Las solicitudes externas a la organización recibidas por vía telefónica o correo de voz se verifican confirmado por teléfono o algún otro medio de autenticación

Un método preestablecido se utiliza independiente a la verificación de la autenticación de la fuente y el contenido de las solicitudes de transacción recibida vía fax o sistemas de imágenes

La firma electrónica o la certificación se utilizan para verificar la integridad y autenticidad de los documentos electrónicos que entran

Evaluar la suficiencia:

► **Probando que:**

La preparación de datos:

Para una muestra seleccionada de documentos fuente, existe consistencia evidente con respecto a los procedimientos establecidos relacionados con la autorización, aprobación, precisión, suficiencia y recepción de entrada de datos y si la entrada de datos es oportuna

El personal de las fuentes, entradas y conversión tiene conciencia y comprende los requerimientos de control en la preparación de datos

La entrada de datos:

Se envían de datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo revisiones de precisión, suficiencia y autorización

Para transacciones seleccionadas se comparan los archivos maestros antes y después de la captura

Existe una apropiada revisión de retención, solución y de la integridad en el manejo de errores

Los procedimientos y acciones de manejo de errores cumplen con las políticas y controles establecidos

El procesamiento de datos:

Se utilizan efectivamente los totales de control corrida-a-corrida y los controles de actualización de archivos maestros

Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo la validación, autenticación y edición de procesamiento de datos tan cerca del punto de origen como sea posible

El proceso de manejo de errores es llevado a cabo de acuerdo con los procedimientos y controles establecidos

Se llevan a cabo la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente

Los procedimientos y acciones del manejo de errores cumplen con los procedimientos y controles establecidos

La Salida, Interfase y Distribución de Datos:

La salida es balanceada rutinariamente contra totales de control relevantes

Los seguimientos de auditoría son proporcionados para facilitar el seguimiento del procesamiento de transacciones en la conciliación de datos confusos o erróneos

Los reportes de salida son revisados en cuanto a su precisión por parte del proveedor y los usuarios relevantes

Existen la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente

Los procedimientos y acciones de manejo de errores cumplen con las políticas y controles establecidos

Los reportes de salidas son asegurados al esperar ser distribuidos, así como aquéllos ya distribuidos a los usuarios de acuerdo con los procedimientos y controles establecidos

Existe la protección adecuada para la información sensible durante la transmisión y transporte contra los accesos no autorizados y las modificaciones

Existe una protección adecuada de información sensible durante la transmisión y transporte en cuanto a accesos y modificaciones no autorizadas

Los procedimientos y acciones de información sensible dispuesta cumplen con los procedimientos y controles establecidos

La Librería de Medios:

El contenido de la librería de medios es inventariado sistemáticamente, que todas las discrepancias encontradas son solucionadas oportunamente y se toman medidas para mantener la integridad de los medios almacenados en la librería

Los procedimientos de administración diseñados para proteger el contenido de la librería de medios existen y funcionan adecuadamente

Las responsabilidades de la administración de la librería de medios son asignadas apropiadamente

La librería de medios es independiente de las funciones de preparación, entrada, procesamiento y salida

La estrategia de respaldos y restauración de medios es apropiada

Los respaldos de medios se llevan a cabo apropiadamente de acuerdo con la estrategia de respaldo definida

Los sites de almacenamiento de medios son seguros físicamente y que su inventario está actualizado

El almacenamiento de datos considera los requerimientos de recuperación y la economía o efectividad de costos

Los períodos de retención y los términos de almacenamiento son apropiados para documentos, datos, programas y reportes

El riesgo de maldireccionar mensajes (por carta, fax o e-mail) se reduce con los procedimientos adecuados

Los controles normalmente se aplican a un proceso de transacción específico, como faxes o contestadores telefónicos automáticos, también aplica a sistemas computacionales que soportan la transacción o proceso (ej., software de fax en las computadoras personales)

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Mediciones (“Benchmarking”) de la administración de datos contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Para una selección de transacciones, la confirmación de la propiedad del procesamiento durante:

- la preparación de datos
- el procesamiento de entradas
- el procesamiento de datos
- la salida, distribución o integración

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

- el manejo de errores en todas las fases del procesamiento
- la integridad de los datos a través del manejo de errores en todas las fases del procesamiento
- retención y destrucción

Pruebas específicas para lo siguiente:

- suficiencia, precisión y validez durante cada fase del procesamiento
- aprobaciones y autorizaciones aprobadas
- existencia de controles preventivos, detectivos y correctivos dentro del procesamiento o vía funciones manuales/procedimientos de grupos de control
- retención de documentos fuente para la revisión posterior de la consistencia con respecto a los requerimientos de retención
- recuperación de una selección de documentos fuente y medios de transacciones para confirmar la existencia y la precisión
- análisis de la disponibilidad del seguimiento de auditoría: existencia, identificación de fuente/operador y asegurar que cualquier sistema de interfase cuenta con niveles iguales de control sobre las transacciones
- edición de las funciones de programas de entrada y procesamiento, incluyendo, pero sin limitarse a:
 - Blancos en campos requeridos
 - Validación de códigos de transacciones
 - Montos negativos
 - Cualquier otra condición apropiada
- suficiencia de las pruebas de validación internas al procesamiento
- archivos suspendidos con transacciones defectuosas, incluyendo los siguientes controles:
 - Identificación inmediata del operador que comete el error y aviso del error
 - Todas las transacciones de error son transferidas a estos archivos suspendidos
 - El registro es mantenido hasta que la transacción es resuelta y eliminada
 - Las transacciones muestran código de error, fecha y hora de captura, operador y máquina
 - Los archivos de suspenso crean reportes de seguimiento para la revisión administrativa, el análisis de tendencias y entrenamiento correctivo
- separación de las funciones de origen, entrada, procesamiento, verificación y distribución

Para una selección de transacciones de salida:

- revisar una muestra de listas de transacciones procesadas en cuanto a su suficiencia y precisión
- revisar una muestra de reportes de salida en cuanto a precisión y suficiencia
- revisar los calendarios de retención de salidas en cuanto a su adecuación y cumplimiento de los procedimientos
- confirmar que la distribución real de una muestra de salidas fue llevada a cabo con precisión
- confirmar el procesamiento integrado confirmando la salida de una bitácora de procesamiento de transacciones de un sistema con la entrada de la bitácora de otro sistema
- revisar los procedimientos de balanceo para todas las entradas, salidas de procesamiento y otras transacciones de uso de sistemas
- confirmar que únicamente personal autorizado tiene acceso a reportes sensibles
- confirmar la destrucción o relocalización de almacenamientos fuera del site para todos los medios de datos por políticas y procedimientos de retención
- confirmar los períodos reales de retención contra los procedimientos de retención
- atestiguar la entrega o transmisión real de salidas sensibles y el cumplimiento con los procedimientos de procesamiento, distribución y seguridad

- confirmar la creación e integridad de los respaldos en asociación con el procesamiento normal, así como para los requerimientos del plan de recuperación en caso de desastre

Para la librería de medios:

- revisar el acceso de los usuarios a los servicios sensibles: determinar que el acceso es apropiado
- seleccionar una muestra de medios a ser destruida y observar el proceso completo; verificar el cumplimiento de los procedimientos aprobados
- determinar la adecuación de los controles para los datos en almacenamientos fuera del site y mientras los datos están en tránsito
- obtener resultados del inventario de la librería de medios más reciente; confirmar su precisión
- confirmar que los procesadores de registro son suficientes para acceder los medios necesarios
- revisar los controles en cuanto a las desviaciones o “bypass” restringidos de reglas de etiquetado internas e internas
- probar el cumplimiento de los controles internos y externos vía revisión de medios seleccionados
- revisar los procedimientos de creación de respaldos para asegurar la existencia de datos suficientes en caso de desastre
- confirmar las inspecciones de la librería de medios por requerimientos calendarizados

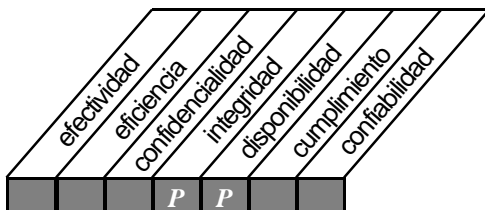
► **Identificando:**

- cuando los archivos de producción son accedidos directamente por los operadores que “antes” y “después” no creen ni se mantengan imágenes de archivos
- formas de entrada y salida sensibles (por ejemplo, certificados de reservas) no protegidas
- bitácoras no llevadas y mantenidas para totales batch y de control para todas las fases del procesamiento
- reportes de salidas no útiles a los usuarios: datos relevantes y útiles, reportes necesarios, distribución apropiada, formato y frecuencia adecuados, acceso en línea a los reportes tomado en consideración
- datos transmitidos sin controles adicionales, incluyendo:
 - Accesos de envío/recepción de transmisiones limitados
 - Autorización e identificación apropiadas del emisor y del receptor
 - Medios seguros de transmisión
 - Encriptación de datos transmitidos y algoritmos de decodificación apropiados
 - Pruebas de integridad de la transmisión en cuanto a su suficiencia
 - Procedimientos de retransmisión
- contratos de proveedores con controles faltantes como servicios de destrucción
- deficiencias fuera del site con respecto a amenazas al ambiente tales como fuego, agua, fallas eléctricas y accesos no autorizados

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:

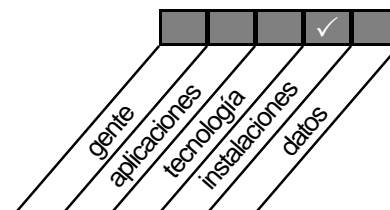
- acceso a instalaciones
- identificación del centro de cómputo
- seguridad física
- salud y seguridad del personal
- protección contra amenazas ambientales

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



DS 12 ADMINISTRACIÓN DE INSTALACIONES

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Seguridad Física |
| 2 | Bajo Perfil de las Instalaciones de Tecnología de Información |
| 3 | Escolta de Visitantes |
| 4 | Salud y Seguridad del Personal |
| 5 | Protección contra Factores Ambientales |
| 6 | Suministro Ininterrumpido de Energía |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Administrador de las Instalaciones
 Oficial de Seguridad
 Administrador de Riesgos
 Administración de operaciones de la función de servicios de información
 Administrador de la seguridad de la función de servicios de información

▸ Obteniendo:

Políticas y procedimientos organizacionales relacionados con la administración, disposición o plano, seguridad, inventario de activos fijos e inventario de las instalaciones, así como adquisición/arrendamiento de capital
 Políticas y procedimientos de la función de servicios de información relacionados con la disposición o plano de las instalaciones, la seguridad física y lógica, acceso, mantenimiento, visitantes, salud, seguridad y requerimientos ambientales, mecanismos de entrada y salida, reporte de seguridad, contratos de seguridad y mantenimiento, inventario de equipo, procedimientos de vigilancia, y requerimientos regulatorios
 Una lista de los individuos que tienen acceso a las instalaciones y la disposición o plano de las instalaciones
 Una lista de los acuerdos de desempeño, capacidad y nivel de servicios con respecto a las expectativas de desempeño de los recursos de los sistemas de información (equipo e instalaciones), incluyendo estándares industriales
 Copia del documento de planeación de recuperación/contingencia en caso de desastre

Evaluar los controles:

▸ Considerando sí:

La localización de las instalaciones no es obviamente externa, se encuentra en el área u organización menos accesible, y si el acceso es limitado al menor número de personas
 Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones
 Los procedimientos y prácticas de administración de llave ("Key") y lectora de tarjetas ("card reader") son adecuados, incluyendo la actualización y revisión continuas tomando como base una "menor necesidad de acceso"

Las políticas de acceso y autorización de entrada/salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles

Se llevan a cabo revisiones periódicas de los perfiles de acceso, incluyendo revisiones administrativas

Existen y se llevan a cabo los procesos de revocación, respuesta y escalamiento en caso de violaciones a la seguridad

Existe el proceso de “signage” con respecto a la no identificación de áreas sensibles, y si es consistente con los requerimientos de seguro, código de construcción local y regulatorios

Las medidas de control de seguridad y acceso incluyen a los dispositivos de información portátiles utilizados fuera del sitio

Se lleva a cabo una revisión de los registros de visitantes, asignación de pases, escolta, persona responsable del visitante, bitácora para asegurar tanto los registros de entradas como de salidas y el conocimiento de la recepcionista con respecto a los procedimientos de seguridad

Se lleva a cabo una revisión de los procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma, así como las respuestas esperadas en los distintos escenarios para los diferentes niveles de emergencias ambientales

Se lleva a cabo una revisión de los procedimientos de control de aire acondicionado, ventilación, humedad y las respuestas esperadas en los distintos escenarios de pérdida o extremos no anticipados

Existe una revisión del proceso de alarma al ocurrir una violación a la seguridad, que incluya:

- definición de la prioridad de la alarma (por ejemplo, apertura de la puerta por parte de una persona armada que ha entrado en las instalaciones)
- escenarios de respuesta para cada alarma de prioridad
- responsabilidades del personal interno versus personal de seguridad local o proveedores
- interacción con las autoridades locales
- revisión del simulacro de alarma más reciente

La organización es responsable del acceso físico dentro de la función de servicios de información, incluyendo:

- desarrollo, mantenimiento y revisiones continuas de políticas y procedimientos de seguridad
- establecimiento de relaciones con proveedores relacionados con la seguridad
- contacto con la administración de las instalaciones en cuanto a problemas de tecnología relacionados con seguridad
- coordinación del entrenamiento y conciencia sobre seguridad para la organización
- coordinación de actividades que afecten en control de acceso lógico vía aplicaciones centralizadas y software de sistema operativo
- proporcionar entrenamiento y crear conciencia de seguridad no sólo dentro de la función de servicios de información, sino para los servicios de usuarios

Se llevan a cabo prácticas de distribuidores automáticos y servicios de conserjería para investigación del personal en las instalaciones de la organización

Se llevan a cabo la actualización y negociación del contenido de los contratos de servicio

Los procedimientos de pruebas de penetración y los resultados

- coordinan los escenarios de prueba de penetración física
- coordinan la prueba de penetración física con proveedores y autoridades locales

Se cumple con las regulaciones de salud, seguridad y ambiente

La seguridad física es tomada en cuenta en el plan de recuperación/contingencia en caso de desastre y abarca una seguridad física similar en las instalaciones aprovisionadas

Existen elementos de infraestructura específicos alternativos necesarios para implementar seguridad:

- fuente de poder ininterrumpida (UPS)
- alternativas o reruteo de líneas de telecomunicación
- recursos alternativos de agua, gas, aire acondicionado y humedad

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Evaluar la suficiencia:

▸ Probando que:

- El personal tiene conciencia y comprende la necesidad de seguridad y controles
- Los armarios cableados están físicamente protegidos con el acceso posible autorizado y el cableado se encuentra bajo tierra o conductos protegidos tanto como sea posible
- El proceso de “signage” identifica rutas de emergencia y qué hacer en caso de una emergencia o violación a la seguridad
- Los directorios de teléfono en otra partes de la instalación no identifican localidades sensibles
- La bitácora de visitantes sigue apropiadamente los procedimientos de seguridad
- Existen los procedimientos de identificación requeridos para cualquier acceso dentro o fuera vía observación
- Las puertas, ventanas, elevadores, ventilas y ductos o cualquier otro modo de acceso están identificados
- El site computacional está separado, cerrado y asegurado y es accesado únicamente por personal de operaciones y gente de mantenimiento tomando como base un “acceso necesario”
- El personal de las instalaciones rota turnos y toma vacaciones y descansos apropiados
- Existen los procedimientos de mantenimiento y registro para un desempeño de trabajo oportuno
- Las variaciones de las políticas y procedimientos en las operaciones de los turnos segundo y tercero son reportadas
- Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones
- Los registros y el equipo de monitoreo ambiental y de seguridad --debajo, en, sobre, y alrededor – son mantenidos
- No se almacenan útiles peligrosos
- Existe el seguimiento de auditoría de control de acceso sobre software de seguridad o reportes clave de administración
- Se ha dado seguimiento a toda emergencia ocurrida en el pasado o a su documentación
- El personal con acceso son empleados reales
- Se llevan a cabo verificaciones de suficiencia de administración clave de acceso
- Se otorga una educación en seguridad física y conciencia de seguridad
- Existe una cobertura y experiencia de seguros para los gastos asociados con algún evento de seguridad, pérdida del negocio y gastos para recuperar la instalación
- El proceso para la implementación de acceso a cambios de llaves y controles de procesos lógicos es continuo y conocido
- El ambiente cumple con los requerimientos regulatorios establecidos
- Las bitácoras de mantenimiento de alarmas no pueden ser modificadas inapropiadamente
- La frecuencia de cambios a los códigos de acceso y revisiones de perfil – involucramiento de usuario e instalaciones – es documentada

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ Llevando a cabo:

- Mediciones (“Benchmarking”) de administración de instalaciones contra organizaciones similares o estándares internacionales/buenas prácticas reconocidas en la industria apropiadas
- Comparaciones de la disposición o plano físico contra bosquejos del edificio y dispositivos de seguridad
- Determinaciones sobre:
 - la no aparición de la instalación en sí como una localidad de servicios de sistemas, ni siquiera sugerida indirectamente vía direcciones, señalamientos de estacionamiento, etc.
 - la limitación del número de puertas por códigos locales de construcción/seguro
 - la suficiente protección de las instalaciones a través de barreras físicas para evitar el acceso inapropiado de vehículos y personas
 - patrones de tránsito para asegurar que el flujo no dirige a las personas hacia las áreas de seguridad
 - la suficiencia del monitoreo con videos y la revisión de cintas

- la existencia de espacio apropiado para el equipo computacional en cuanto a acceso, temperatura y mantenimiento
- la suficiencia y disponibilidad de las cubiertas para el equipo contra agua o elementos externos en caso de emergencia
- la revisión de las bitácoras de mantenimiento de alarmas y el reporte del último reporte de simulacro

Pruebas sobre temperatura, humedad, electricidad – sobre y debajo de los pisos falsos; si han ocurrido anomalías, cuáles fueron las actividades de investigación/solución resultantes

Revisiones de todos los seguros y bisagras (bisagras dentro de la habitación)

Una visita de las instalaciones sin portar gafete para determinar si se llevan a cabo detenciones e interrogatorios sobre el hecho de no portar gafete

Revisiones de la cobertura del guardia/recepcionista cuando un visitante es escoltado a través de las instalaciones

Pruebas de seguridad de penetración de las instalaciones

▸ **Identificando:**

Suficiencia de “signage”, extinguidores de incendios, sistemas de aspersión, UPS, drenaje, cableado y mantenimiento regular

Para las ventanas: asegurar que ningún recurso es visible desde el exterior, que no existan “aparadores” en el centro de datos

Determinación de pruebas de seguridad de penetración

Pruebas de visitantes, incluyendo registro, gafete, escolta, inspección, salida

Discrepancias en la bitácora de visitantes y en los gafetes de visitantes

Evaluación de los perfiles e historia de acceso tomando como base el reporte clave de la administración incluyendo el reemplazo de gafetes/tarjetas maestras y artículos perdidos inactivos

Revisión de estadísticas de desastres locales

Desarrollo de escenarios de penetración en caso de desastre

Contratos de proveedores para asegurar que se llevan a cabo una investigación de personal y el cumplimiento con los requerimientos de salud y seguridad

Pruebas de UPS y verificar que los resultados cumplan con los requerimientos operacionales y de capacidad para sostener las actividades críticas de procesamiento de datos

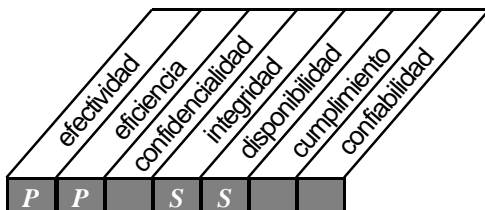
Pruebas de acceso de información (bitácoras, cintas, registros) para asegurar que éstos son revisados por los usuarios y la administración en cuando a su propiedad

Pruebas de procedimientos de monitoreo de entrada a la instalación cerca del área

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:

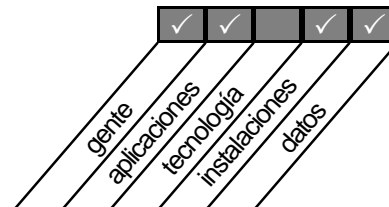
- manual de procedimiento de operaciones
- documentación de procedimientos de arranque
- administración de servicios de red
- calendarización de personal y cargas de trabajo
- proceso de cambio de turno
- registro de eventos de sistemas

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



DS 13 MANEJO DE OPERACIONES

OBJETIVOS DE CONTROL

- 1 Manual de Procedimientos de Operación e Instrucciones
- 2 Documentación del Proceso de Inicio y de Otras Operaciones
- 3 Calendarización de Trabajos
- 4 Salidas de la Calendarización de Trabajos Estándar
- 5 Continuidad de Procesamiento
- 6 Bitácoras de Operación
- 7 Operaciones Remotas

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Administración de operaciones de la función de servicios de información
 Administración de la planeación de recuperación/contingencia en caso de desastre de la función de servicios de información
 Presidencia de la función de servicios de información
 Usuarios seleccionados de los recursos de la función de servicios de información
 Proveedores seleccionados que proporcionan servicios o productos de software por contrato

▸ Obteniendo:

Políticas y procedimientos organizacionales relacionados con la administración de operaciones y el rol de sistemas de información en el cumplimiento de los objetivos del negocio
 Políticas y procedimientos de la función de servicios de información relacionados con el rol operacional, las expectativas de desempeño, la calendarización de trabajos, los acuerdos de nivel de servicio, las instrucciones para el operador, la rotación de personal, la planeación de recuperación/contingencia en caso de desastre y las operaciones de instalaciones remotas
 Instrucciones operacionales para la función general de inicio, término, calendarización de la carga de trabajo, estándares, acuerdos de nivel de servicio, procedimientos fijos de emergencia, respuestas de procesamiento anormal, bitácoras de consola, seguridad física y lógica, separación de librerías de desarrollo y producción y procedimientos de problemas de escalamiento
 Una muestra seleccionada de instrucciones operacionales para aplicaciones clave incluyendo, calendarización, entradas, tiempo de procesamiento, mensajes de error, instrucciones de fin anormal, reinicio, procedimientos de problemas de escalamiento, trabajos antes y después y archivos fuera del site

Evaluar los controles:▸ **Considerando sí:**

Existe evidencia sobre:

- la suficiencia de todos los procesamientos llevados a cabo, reinicios y recuperaciones
- la suficiencia de la carga de programa inicial (IPL) y del procedimiento de término
- estadísticas de suficiencia del calendario para confirmar el término completo y exitoso de todos los requerimientos
- la separación física y lógica de las librerías fuente y objeto, de pruebas/desarrollo/producción y los procedimientos de control de cambios para trasladar programas de una librería a otra
- estadísticas de desempeño para actividades operacionales, incluyendo, aunque sin limitarse a:
 - Capacidad, utilización y desempeño de hardware y periféricos
 - Utilización y desempeño de memoria
 - Utilización y desempeño de telecomunicaciones
- prueba de que el desempeño alcanza las normas de desempeño de producto, los estándares de desempeño definidos internamente y los compromisos de acuerdo de nivel de servicio de usuarios
- el mantenimiento, retención y revisión periódicos de las bitácoras de operación
- la oportunidad de mantenimiento realizado a todo el equipo
- la rotación de turnos, el disfrute de vacaciones y el mantenimiento de competencia de los operadores

Evaluar la suficiencia:▸ **Probando que:**

Los miembros del personal de operaciones tienen conciencia y comprenden:

- los procedimientos de operación por los que son responsables
- las expectativas de desempeño dentro de las instalaciones – normas de proveedores, estándares organizacionales y acuerdos de nivel de servicio con los usuarios
- el programa fijo de emergencia, así como los procedimientos de reinicio/recuperación
- los requerimientos y la revisión administrativa de los requerimientos de la bitácora de operaciones
- los procedimientos de escalamiento de problemas
- la comunicación de cambios de turno y las responsabilidades entre turnos
- procedimientos de cambio o rotación para trasladar programas de desarrollo a producción
- interacción con las instalaciones remotas de procesamiento y las instalaciones centrales de procesamiento
- las responsabilidades de comunicación de oportunidades de mejoras a la productividad a la administración

Evaluar el riesgo de los objetivos de control no alcanzados:▸ **Llevando a cabo:**

Una revisión de las estadísticas de desempeño operacional (equipo y personal) para asegurar lo adecuado de su utilización; compararlas contra organizaciones similares, normas de proveedores y estándares internacionales/buenas prácticas reconocidas en la industria apropiadas

Una revisión de una muestra limitada de manuales de operación de la función de servicios de información y determinar si cumplen con los requerimientos de las políticas y los procedimientos

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Un examen de la documentación de los procesos de inicio y término y confirmar que los procedimientos son probados y actualizados regularmente

Un examen de la calendarización de procesamiento para asegurar lo adecuado y la suficiencia del desempeño comparado contra el plan o calendario

▸ **Identificando:**

Usuarios seleccionados y asegurando la suficiencia del desempeño operacional relacionado con actividades continuas y acuerdos de nivel de servicio

Una muestra de términos anormales (ABENDS) para trabajos y determinando la solución a los problemas ocurridos

Las experiencias de entrenamiento, rotación de turnos y vacaciones de los operadores

Una muestra de bitácoras de consola para revisar la precisión, las tendencias en el desempeño y la revisión administrativa de la solución de problemas – evaluar el escalamiento de problemas si aplica

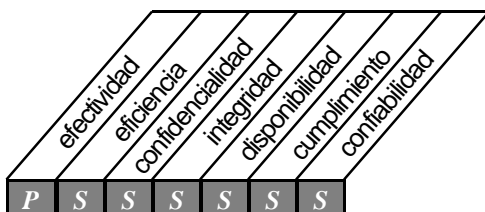
A usuarios para determinar la satisfacción con el compromiso del acuerdo de nivel de servicio

Procedimientos de mantenimiento preventivo completados en todo el equipo por sugerencia del proveedor

MONITOREO

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:

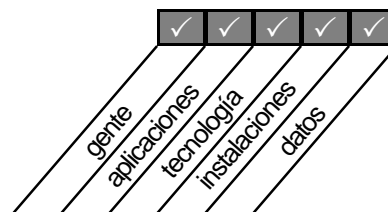
- indicadores clave de desempeño
- factores críticos de éxito
- evaluación de la satisfacción de clientes
- reportes gerenciales

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



M 1 MONITOREAR LOS PROCESOS

OBJETIVOS DE CONTROL

- | | |
|---|-------------------------------------|
| 1 | Recolectar Datos de Monitoreo |
| 2 | Evaluar el Desempeño |
| 3 | Evaluar la Satisfacción del Cliente |
| 4 | Reporte Administrativo |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Director Ejecutivo
 Director de Información
 Director de auditoría interna
 Director de servicios de información y administración de control de calidad
 Gerente de auditoría externa
 Usuarios seleccionados de recursos de la función de servicios de información
 Miembros del comité de auditoría, si aplica

▸ Obteniendo:

Políticas y procedimientos organizacionales relacionadas con la planeación, administración, monitoreo y reporte del desempeño
 Políticas y procedimientos de la función de servicios de información relacionadas con el monitoreo y el reporte del desempeño, estableciendo iniciativas de mejoramiento del desempeño y frecuencia de las revisiones
 Reportes de las actividades de la función de servicios de información incluyendo, pero no limitados a: reportes internos, reportes de auditorías internas, reportes de auditorías externas, reportes de usuarios, encuestas de satisfacción de los usuarios, planes de desarrollo de sistemas y reportes de avance, minutas del comité de auditoría y cualquier otro tipo de evaluación del uso de los recursos de la función de servicios de información de la organización.
 Documentos de planeación de la función de servicios de información con objetivos para cada grupo de recursos y el desempeño real en comparación con dichos planes.

Evaluar los controles:

▸ Considerando sí:

Los datos identificados para monitorear los recursos de la función de servicios de información son apropiados
 Se usan indicadores clave del desempeño y/o factores críticos para el éxito para medir el desempeño de la función de servicios de información en comparación con los niveles deseables.
 Los reportes internos de la utilización de los recursos de la función de servicios de información (gente, instalaciones, aplicaciones, tecnología y datos) son adecuados.

Existe una revisión administrativa de los reportes de desempeño de los recursos de la función de servicios de información

Considerar si, continúa

Existen controles de monitoreo para proporcionar una retroalimentación confiable y útil de manera oportuna

La respuesta de la organización a las recomendaciones de mejoramiento de control de calidad, auditoría interna y auditoría externa es apropiada

Existen iniciativas y resultados de mejoramiento del desempeño deseado

Se está dando el desempeño organizacional en comparación con las metas establecidas dentro de la organización

La confiabilidad y utilidad de los reportes de desempeño para no usuarios es suficiente, tales como auditor externo, comité de auditoría y alta administración de la organización

La oportunidad de los reportes permite una respuesta rápida ante las excepciones o incumplimientos identificados del desempeño

Los reportes son suficientes en comparación con las políticas y procedimientos establecidos para el desempeño de las actividades (por ejemplo, reportes de desempeño)

Evaluar la suficiencia:

▸ **Probando que:**

Existen reportes de monitoreo del desempeño de la información

Existe revisión administrativa de los reportes de monitoreo del desempeño e iniciativas de acciones correctivas

Los empleados están conscientes y comprenden las políticas y procedimientos relativos al monitoreo del desempeño

La calidad y el contenido de los reportes internos se relacionan con:

- La recolección de datos de monitoreo del desempeño
- El análisis de los datos de monitoreo del desempeño
- El análisis de los datos del desempeño de los recursos
- Las acciones administrativas sobre problemas del desempeño
- El análisis de encuestas de satisfacción de los usuarios

La alta administración está satisfecha con los reportes sobre el monitoreo del desempeño

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Referencia del monitoreo del desempeño respecto a organizaciones similares o estándares internacionales/prácticas industriales reconocidas apropiados

Revisión de la relevancia de los datos dentro de los procesos que se están monitoreando

Revisión del desempeño real contra lo planeado en todas las áreas de la función de servicios de información

Satisfacción real contra lo anticipado de los usuarios de todas las áreas de la función de servicios de información

Análisis del grado de cumplimiento de las metas de desempeño e iniciativas de mejoramiento

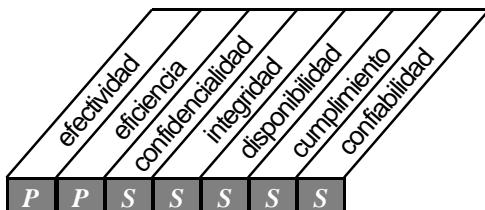
Análisis del nivel de implantación de las recomendaciones de la administración

▸ **Identificando:**

La responsabilidad, autoridad e independencia del personal de monitoreo dentro de la organización de sistemas de información

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:

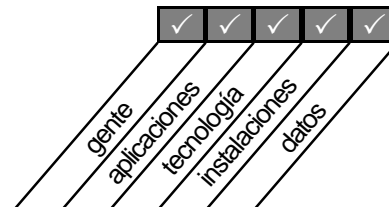
- monitoreo permanente de control interno
- comparación con mejores prácticas
- reportes de errores y excepciones
- autoevaluaciones
- reportes gerenciales

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



M 2 EVALUAR LA SUFICIENCIA DEL CONTROL INTERNO

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Monitoreo del Control Interno |
| 2 | Operación Oportuna de los Controles Internos |
| 3 | Reportes del Nivel de Control Interno |
| 4 | Aseguramiento de la Seguridad Operacional y del Control Interno |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ Entrevistas:

Director Ejecutivo
 Director de Información
 Director de auditoría interna
 Director de servicios de información y administración de control de calidad
 Gerente de auditoría externa
 Usuarios seleccionados de los recursos de la función de servicios de información
 Miembros del comité de auditoría, si aplica

▸ Obteniendo:

Políticas y procedimientos organizacionales relacionadas con la planeación, administración, monitoreo y reporte de los controles internos
 Políticas y procedimientos de la función de servicios de información relacionadas con el monitoreo y el reporte de los controles internos y la frecuencia de las revisiones
 Reportes de las actividades de la función de servicios de información incluyendo, pero no limitados a: reportes internos, reportes de auditorías internas, reportes de auditorías externas, reportes de usuarios, encuestas de satisfacción de los usuarios, planes de desarrollo de sistemas y reportes de avance, minutas del comité de auditoría y cualquier otro tipo de evaluación de los controles internos de la función de servicios de información
 Políticas y procedimientos específicos de la función de servicios de información relativos al aseguramiento de la seguridad operacional y del control interno

Evaluar los controles:

▸ Considerando sí:

Los datos identificados para monitorear los controles internos de la función de servicios de información son apropiados
 Los reportes internos de los datos de control interno de la función de servicios de información son adecuados
 Existe una revisión administrativa de los controles internos de la función de servicios de información
 Existen controles de monitoreo para proporcionar retroalimentación confiable y útil de manera oportuna
 La respuesta de la organización a las recomendaciones de mejoramiento del control de calidad, auditoría interna y auditoría externa es apropiada

Existen iniciativas y resultados de mejoramiento del control interno deseable

Se está dando el desempeño organizacional en comparación con las metas establecidas dentro de la organización

La información concerniente a errores, inconsistencias y excepciones de control interno se mantiene de manera sistemática y se reporta a la administración

La confiabilidad y utilidad de los reportes de control interno para no usuarios, tales como auditor externo, comité de auditoría y alta administración de la organización, es suficiente

La oportunidad de los reportes permite una respuesta rápida ante las excepciones o incumplimientos identificados del control interno

Los reportes de control interno son suficientes en comparación con las políticas y procedimientos establecidos para el desempeño de las actividades (por ejemplo, reportes de control interno)

Evaluar la suficiencia:

▸ **Probando que:**

Existen reportes de monitoreo del control interno

Está habiendo revisión administrativa de los reportes de control interno e iniciativas de acciones correctivas

Los empleados están conscientes y comprenden las políticas y procedimientos relativos al monitoreo del control interno

La calidad y el contenido de los reportes internos se relacionan con:

- La recolección de datos de monitoreo del control interno
- El desempeño del cumplimiento del control interno
- Las acciones administrativas sobre problemas del control interno
- El aseguramiento de la seguridad operacional y del control interno

La alta administración está satisfecha con los reportes sobre la seguridad y el control interno

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Referencia de la evaluación del control interno respecto a organizaciones similares o estándares internacionales/prácticas industriales reconocidas apropiados

Revisión de la relevancia de los datos dentro de los procesos que se están monitoreando y en el reporte de los controles internos

Marco de referencia para la revisión de los controles internos de toda la organización y en particular de la función de servicios de información para asegurar la suficiencia de la cobertura y de los diversos niveles de detalle para los responsables del proceso

Revisión del control interno real contra lo planeado en todas las áreas de la función de servicios de información

Análisis del grado de cumplimiento de las metas de control interno e iniciativas de mejoramiento

Revisión de la satisfacción del comité de auditoría con los reportes sobre los controles internos

Análisis del nivel de implantación de las recomendaciones de la administración

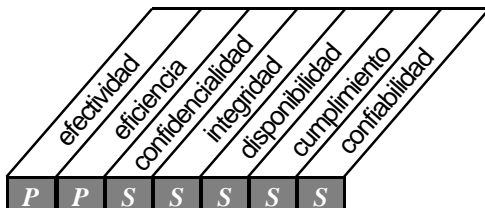
▸ **Identificando:**

Las áreas adicionales para el probable reporte de control interno, en consistencia con los requerimientos de servicios de información, auditoría, administración, auditores externos y regulativos

La responsabilidad, autoridad e independencia del personal de revisión de control interno dentro de la organización de sistemas de información

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:

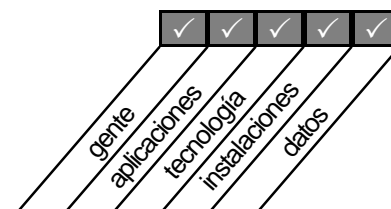
- certificaciones / acreditaciones independientes
- evaluaciones independientes de efectividad
- aseguramiento independiente sobre cumplimiento de requerimientos legales y regulatorios
- aseguramiento independiente de cumplimiento de compromisos contractuales
- revisiones a proveedores externos de servicios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

Planeación &
Organización

Adquisición &
Implementación

Entrega &
Soporte

Monitoreo



M 3 OBTENER ASEGURAMIENTO INDEPENDIENTE

OBJETIVOS DE CONTROL

- | | |
|---|---|
| 1 | Acreditación/Certificación Independiente de la Seguridad y el Control Interno de los Servicios de Tecnología de Información |
| 2 | Acreditación/Certificación Independiente de la Seguridad y el Control Interno de los Proveedores Externos de Servicios |
| 3 | Evaluación Independiente de la Eficacia de los Servicios de Tecnología de Información |
| 4 | Evaluación Independiente de la Eficacia de los Proveedores Externos de Servicios |
| 5 | Aseguramiento Independiente del Cumplimiento de Requerimientos Regulatorios y Legales y de Compromisos Contractuales |
| 6 | Aseguramiento Independiente del Cumplimiento de Requerimientos Regulatorios y Legales y de Compromisos Contractuales por parte de Proveedores Externos de Servicios |
| 7 | Responsabilidad de la Función de Aseguramiento Independiente |
| 8 | Involucramiento Proactivo de Auditoría |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

▸ **Entrevistas:**

Director Ejecutivo
 Director de Información
 Director de auditoría interna
 Director de la función de servicios de información
 Gerente de auditoría externa
 Gerente de la entidad de aseguramiento independiente

▸ **Obteniendo:**

Organigrama a nivel de toda la organización y manual de políticas y procedimientos
 Políticas y procedimientos relativas al proceso de aseguramiento independiente
 Contratos/Acuerdos de servicio con el proveedor del servicio de tecnología de información
 Requerimientos legales y regulatorios pertinentes y compromisos contractuales
 Contratos, presupuestos, reportes previos e historial de desempeño de aseguramiento independiente
 Historial de experiencia y educación continua del personal de aseguramiento independiente
 Reportes de auditorías previas

Evaluar los controles:

▸ **Considerando sí:**

Los contratos de aseguramiento independiente están debidamente establecidos/ejecutados para asegurar la cobertura de revisión adecuada (por ejemplo, certificación/acreditación, evaluación de eficacia y evaluaciones de cumplimiento)

- La acreditación/certificación independiente se obtiene antes de implantar servicios nuevos e importantes de tecnología de información
- La re-certificación/re-acreditación independiente de los servicios de tecnología de información se obtiene en un ciclo rutinario después de la implantación
- La certificación/acreditación independiente se obtiene antes de utilizar a los proveedores de servicios de tecnología de información
- La re-certificación/re-acreditación se obtiene en un ciclo rutinario
- La evaluación independiente de la eficacia de los servicios de tecnología de información se obtiene en un ciclo rutinario
- La evaluación independiente de la eficacia de los proveedores de servicios de tecnología de información se obtiene en un ciclo rutinario
- Las revisiones independientes del cumplimiento de la función de servicios de información con los requerimientos legales y regulativos y los compromisos contractuales se obtiene en un ciclo rutinario
- Las revisiones independientes del cumplimiento de proveedores externos de servicios con los requerimientos legales y regulativos y los compromisos contractuales se obtiene en un ciclo rutinario
- El personal de aseguramiento independiente es competente y realiza su tarea de acuerdo a los estándares profesionales apropiados
- El programa de educación profesional continua ayuda para proporcionar la capacitación técnica al personal de aseguramiento independiente
- La administración busca el involucramiento de auditoría antes de decidir sobre soluciones del servicio de tecnología de información

Evaluar la suficiencia:

► Probando que:

- La alta administración aprueba el desempeño de la entidad de aseguramiento independiente
- La certificación/acreditación independiente antes de la implantación de nuevos servicios importantes de tecnología de información es global, completa y oportuna
- La re-certificación/re-acreditación independiente de los servicios de tecnología de información se realiza en un ciclo rutinario después de la implantación, y que es global, completa y oportuna
- La certificación/acreditación independiente antes de utilizar proveedores de servicios de tecnología de información es global, completa y oportuna
- La re-certificación/re-acreditación independiente se realiza en un ciclo rutinario y es global, completa y oportuna
- La evaluación independiente de la eficacia de los servicios de tecnología de información se realiza en un ciclo rutinario y es global, completa y oportuna
- La evaluación independiente de la eficacia de los proveedores de servicios de tecnología de información se realiza en un ciclo rutinario y es global, completa y oportuna
- Las revisiones independientes del cumplimiento de la función de servicios de información con los requerimientos legales y regulativos y los compromisos contractuales se realizan en ciclos rutinarios y son globales, completas y oportunas
- Las revisiones independientes del cumplimiento de proveedores externos de servicios con los requerimientos legales y regulativos y los compromisos contractuales se realizan en ciclos rutinarios y son globales, completas y oportunas
- Los reportes de la función de aseguramiento independiente son relevantes en cuanto a hallazgos, conclusiones y recomendaciones

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

La función de aseguramiento independiente posee las habilidades y el conocimiento necesarios para realizar un trabajo competente

Está habiendo involucramiento proactivo, antes de decidir sobre soluciones del servicio de tecnología de información

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Referencia de las actividades de revisión de la entidad de aseguramiento independiente respecto a organizaciones similares o estándares internacionales/prácticas industriales reconocidas apropiados

Una revisión detallada que:

- verifique los contratos de aseguramiento independiente respecto a las actividades de revisión realizadas
- determine la suficiencia y oportunidad de las certificaciones/acreditaciones
- determine la suficiencia y oportunidad de las re-certificaciones/re-acreditaciones
- determine la suficiencia y oportunidad de las evaluaciones de eficacia
- determine la suficiencia y oportunidad de las revisiones de cumplimiento de requerimientos legales y regulatorios y de compromisos contractuales
- verifique la capacidad del personal de la función de aseguramiento independiente
- verifique el involucramiento proactivo de auditoría

▸ **Identificando:**

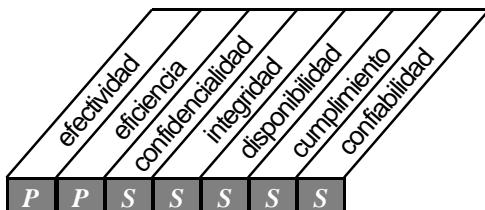
El valor agregado de las actividades de revisión de aseguramiento independiente

El desempeño real contra lo planeado con relación a los planes y presupuestos de aseguramiento independiente

El grado y la oportunidad del involucramiento proactivo de auditoría

OBJETIVOS DE CONTROL DE ALTO NIVEL MONITOREO

M4



Control sobre el proceso de TI de:

proveer auditoría independiente

que satisface los requerimientos de negocio de:

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

se hace posible a través de:

auditorías independientes desarrolladas en intervalos regulares

y toma en consideración:

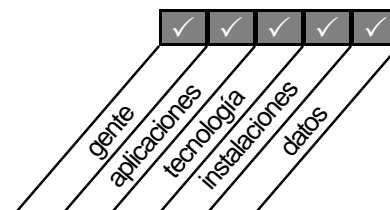
- independencia de auditoría
- involucramiento proactivo de auditoría
- ejecución de auditorías por parte de personal calificado
- aclaración de resultados y recomendaciones
- actividades de seguimiento

Planeación & Organización

Adquisición & Implementación

Entrega & Soporte

Monitoreo



M 4 PREPARAR AUDITORÍAS INDEPENDIENTES

OBJETIVOS DE CONTROL

- | | |
|---|--------------------------------------|
| 1 | Contratación de Auditoría |
| 2 | Independencia |
| 3 | Ética y Estándares Profesionales |
| 4 | Capacidad |
| 5 | Planeación |
| 6 | Realización del Trabajo de Auditoría |
| 7 | Reporte |
| 8 | Actividades de Seguimiento |

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

► **Entrevistas:**

Director Ejecutivo
 Director de Información
 Director de auditoría interna
 Director de la función de servicios de información y administración de control de calidad
 Gerente de auditoría externa
 Miembros del comité de auditoría, si aplica

► **Obteniendo:**

Organigrama a nivel de toda la organización y manual de políticas y procedimientos
 Código de conducta a nivel organización
 Políticas y procedimientos relativos al proceso de auditoría independiente
 Contratación de auditoría, misión, políticas, procedimientos y estándares, reportes previos y planes de auditoría
 Opiniones de auditoría externa, revisiones y planes de auditoría
 Historial de experiencia y educación continua del personal de auditoría independiente
 Evaluación del riesgo de auditoría, presupuesto e historial de desempeño
 Minutas de las reuniones del comité de auditoría, si aplica

Evaluar los controles:

► **Considerando sí:**

El comité de auditoría está debidamente establecido y se reúne con regularidad, si aplica
 La organización de auditoría interna está debidamente establecida
 Las auditorías externas contribuyen a la consecución del plan de auditoría
 La adherencia de la auditoría a los códigos profesionales aplicables es suficiente
 Considerar si, continúa
 La independencia del auditor está confirmada mediante declaraciones de conflicto de intereses firmadas

El plan de auditoría se basa en la metodología de evaluación de riesgos y en las necesidades generales del plan
 Las auditorías se planean y supervisan de manera adecuada
 El programa de educación profesional continua ayuda en la capacitación técnica de los auditores
 El personal de auditoría es competente y realiza sus tareas de acuerdo con los estándares profesionales de auditoría
 Existe un proceso adecuado de reporte de los hallazgos de la auditoría hacia la administración
 El seguimiento de todos los problemas de control se está realizando de manera oportuna
 La cobertura de la auditoría incluye todo el rango de auditoría de sistemas de información (por ejemplo, controles generales y de aplicaciones, ciclo de desarrollo del sistema, rentabilidad, economía, eficiencia, eficacia, enfoque proactivo de auditoría, etc.)

Evaluar la suficiencia:

▸ **Probando que:**

La alta administración aprueba el desempeño de la función de auditoría independiente
 Las actitudes de la alta administración son consistentes con la contratación de auditoría
 Referencias de auditoría interna respecto a los estándares profesionales
 La designación de auditores asegura la independencia y las habilidades necesaria
 Hay mejora continua en la experiencia profesional del personal de auditoría
 El contenido del reporte de auditoría es relevante respecto a las recomendaciones
 Existen reportes de seguimiento que resumen la oportunidad de la implantación

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Referencia de la función de auditoría respecto a organizaciones similares o estándares internacionales/prácticas industriales reconocidas apropiados

Una revisión detallada que:

- verifique que el plan de auditoría representa una revisión cíclica y continua
- la auditoría está contribuyendo al éxito del negocio y a los planes de Tecnología de Información
- la evidencia de la función de auditoría apoya las conclusiones y recomendaciones
- los hallazgos de la auditoría están siendo comunicados y se está tomando ventaja de los mismos o se están reduciendo riesgos
- las recomendaciones de la auditoría están siendo implantadas de manera consciente respecto al beneficio que representan

▸ **Identificando:**

El costo/beneficio de las recomendaciones de la auditoría
 El desempeño real contra lo planeado con relación al plan y presupuesto de auditoría
 El grado de integración entre la auditoría externa y la interna

APÉNDICE I

LISTA DE DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

PLANEACIÓN Y ORGANIZACIÓN

- 1.0 Definir un Plan Estratégico de TI**
 - 1.1 TI como Parte del Plan a Largo y Corto Plazo de la Organización
 - 1.2 Plan a Largo Plazo de TI
 - 1.3 Planeación a Largo Plazo de TI – Enfoque y Estructura
 - 1.4 Cambios en el Plan a Largo Plazo de TI
 - 1.5 Planeación a Corto Plazo para la Función de Servicios de Información
 - 1.6 Evaluación de los Sistemas Existentes
- 2.0 Definir la Arquitectura de la Información**
 - 2.1 Modelo de Arquitectura de la Información
 - 2.2 Diccionario de Datos Corporativos y Reglas de Sintaxis de Datos
 - 2.3 Esquema de Clasificación de Datos
 - 2.4 Niveles de Seguridad
- 3.0 Determinar el Rumbo Tecnológico**
 - 3.1 Planeación de la Infraestructura Tecnológica
 - 3.2 Monitoreo de Tendencias y Regulaciones Futuras
 - 3.3 Contingencia de Infraestructura Tecnológica
 - 3.4 Planes de Adquisición de Hardware y Software
 - 3.5 Estándares de Tecnología
- 4.0 Definir la Organización y las Relaciones de TI**
 - 4.1 Comité Directivo o de Planeación de la Función de Servicios de Información
 - 4.2 Lugar dentro del Organigrama de la Función de Servicios de Información
 - 4.3 Revisión de los Logros Organizacionales
 - 4.4 Funciones y Responsabilidades
 - 4.5 Responsabilidad por el Aseguramiento de Calidad
 - 4.6 Responsabilidad por la Seguridad Lógica y Física
 - 4.7 Propiedad y Custodia
 - 4.8 Propiedad de los Datos y del Sistema
 - 4.9 Supervisión
 - 4.10 Segregación de Obligaciones
 - 4.11 Personal de TI
 - 4.12 Descripciones de Puestos para el Personal de la Función de Servicios de Información
 - 4.13 Personal Clave de TI
 - 4.14 Procedimientos de Contratación de Personal

4.15 Relaciones

- 5.0 Administrar la Inversión de TI**
 - 5.1 Presupuesto Anual Operativo de la Función de Servicios de Información
 - 5.2 Monitoreo de Costo y Beneficio
 - 5.3 Justificación de Costo y Beneficio
- 6.0 Comunicar los Objetivos y el Rumbo Administrativo**
 - 6.1 Ambiente Positivo de Control de Información
 - 6.2 Responsabilidad de la Administración sobre las Políticas
 - 6.3 Comunicación de las Políticas Organizacionales
 - 6.4 Recursos para la Implantación de Políticas
 - 6.5 Mantenimiento de Políticas
 - 6.6 Cumplimiento de las Políticas, Procedimientos y Estándares
 - 6.7 Compromiso de Calidad
 - 6.8 Política de Marco de Referencia para la Seguridad y el Control Interno
 - 6.9 Derechos de Propiedad Intelectual
 - 6.10 Políticas para Asuntos Específicos
 - 6.11 Comunicación de la Consciencia de Seguridad de TI
- 7.0 Administrar los Recursos Humanos**
 - 7.1 Reclutamiento y Promoción de Personal
 - 7.2 Requerimientos del Personal
 - 7.3 Capacitación del Personal
 - 7.4 Capacitación Cruzada o Respaldo de Personal
 - 7.5 Procedimientos de Liquidación de Personal
 - 7.6 Evaluación del Desempeño de los Empleados
 - 7.7 Cambio de Puesto y Terminación
- 8.0 Asegurar el Cumplimiento de los Requerimientos Externos**
 - 8.1 Revisión de Requerimientos Externos
 - 8.2 Prácticas y Procedimientos para el Cumplimiento de los Requerimientos Externos
 - 8.3 Cumplimiento de la Seguridad y Ergonomía
 - 8.4 Privacidad, Propiedad Intelectual y Flujo de Datos
 - 8.5 Comercio Electrónico
 - 8.6 Cumplimiento de Contratos de Aseguranza
- 9.0 Evaluar los Riesgos**
 - 9.1 Evaluación de Riesgos de Negocios

APÉNDICE I

LISTA DE DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

9.2	Enfoque de Evaluación de Riesgos	11.14	Pruebas Paralelas/Piloto
9.3	Identificación del Riesgo	11.15	Documentación de Pruebas del Sistema
9.4	Medición del Riesgo	11.16	Evaluación de Adherencia a los Estándares de Desarrollo de Aseguramiento de Calidad
9.5	Plan de Acción para el Riesgo	11.17	Revisión de la Consecución de los Objetivos de Aseguramiento de Calidad de la Función de Servicios de Información
9.6	Aceptación del Riesgo	11.18	Medición de la Calidad
10.0	Administrar los Proyectos	11.19	Reportes de Revisiones de Aseguramiento de Calidad
10.1	Marco de Referencia para la Administración de Proyectos		
10.2	Participación del Departamento del Usuario en la Iniciación del Proyecto		
10.3	Miembros y Responsabilidades del Equipo del Proyecto		
10.4	Definición del Proyecto		
10.5	Aprobación del Proyecto		
10.6	Aprobación de Fase del Proyecto		
10.7	Plan Maestro del Proyecto		
10.8	Plan del Sistema de Aseguramiento de Calidad		
10.9	Planeación de Métodos de Aseguramiento		
10.10	Manejo Formal del Riesgo del Proyecto		
10.11	Plan de Pruebas		
10.12	Plan de Capacitación		
10.13	Plan de Revisión Post-Implantación		
11.0	Administrar la Calidad		
11.1	Plan General de Calidad		
11.2	Enfoque de Aseguramiento de Calidad		
11.3	Planeación de Aseguramiento de Calidad		
11.4	Revisión de Adherencia a los Estándares y Procedimientos de Aseguramiento de Calidad de la Función de Servicios de Información		
11.5	Metodología del Ciclo de Desarrollo de Sistemas		
11.6	Metodología del Ciclo de Desarrollo de Sistemas para Cambios Importantes en Tecnología Existente		
11.7	Actualización de la Metodología del Ciclo de Desarrollo de Sistemas		
11.8	Coordinación y Comunicación		
11.9	Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura Tecnológica		
11.10	Relaciones con Implantadores Externos		
11.11	Estándares de Documentación de Programas		
11.12	Estándares de Prueba de Programas		
11.13	Estándares de Prueba de Sistemas		

ADQUISICIÓN E IMPLANTACIÓN

1.0 Identificar las Soluciones

- 1.1 Definición de los Requerimientos de Información
- 1.2 Formulación de Cursos de Acción Alternativos
- 1.3 Formulación de la Estrategia de Adquisición
- 1.4 Requerimientos de Servicios Externos
- 1.5 Estudio de Factibilidad Tecnológica
- 1.6 Estudio de Factibilidad Económica
- 1.7 Arquitectura de la Información
- 1.8 Reporte de Análisis de Riesgos
- 1.9 Controles Rentables de Seguridad
- 1.10 Diseño de Esquemas de Auditoría
- 1.11 Ergonomía
- 1.12 Selección del Software del Sistema
- 1.13 Control de Procuración
- 1.14 Adquisición del Software
- 1.15 Mantenimiento Externo del Software
- 1.16 Programa de Contrato de Aplicaciones
- 1.17 Aceptación de Instalaciones
- 1.18 Aceptación de Tecnología

2.0 Adquirir y Dar Mantenimiento al Software de Aplicación

- 2.1 Métodos de Diseño
- 2.2 Cambios Importantes en los Sistemas Existentes
- 2.3 Aprobación del Diseño
- 2.4 Definición y Documentación de los Requerimientos de Archivo
- 2.5 Especificaciones del Programa
- 2.6 Diseño de Recolección de Datos Fuente

APÉNDICE I

LISTA DE DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

- 2.7 Definición y Documentación de los Requerimientos de Datos de Entrada
- 2.8 Definición de Interfaces
- 2.9 Interfaz Usuario-Máquina
- 2.10 Definición y Documentación de los Requerimientos de Procesamiento de Datos
- 2.11 Definición y Documentación de los Requerimientos de Datos de Salida (Resultados)
- 2.12 Capacidad de Control
- 2.13 Disponibilidad como Factor Clave de Diseño
- 2.14 Provisiones de Integridad de TI en Software y Programas de Aplicación
- 2.15 Pruebas del Software de Aplicación
- 2.16 Material de Referencia y Apoyo para el Usuario
- 2.17 Re-evaluación del Diseño del Sistema
- 3.0 Adquirir y Dar Mantenimiento a la Arquitectura Tecnológica**
 - 3.1 Evaluación de Hardware y Software Nuevos
 - 3.2 Mantenimiento Preventivo del Hardware
 - 3.3 Seguridad del Software del Sistema
 - 3.4 Instalación del Software del Sistema
 - 3.5 Mantenimiento del Software del Sistema
 - 3.6 Cambio en los Controles del Software del Sistema
- 4.0 Desarrollar y Mantener Procedimientos de TI**
 - 4.1 Requerimientos Operativos y Niveles de Servicios Futuros
 - 4.2 Manual de Procedimientos del Usuario
 - 4.3 Manual de Operaciones
 - 4.4 Materiales de Capacitación
- 5.0 Instalar y Acreditar los Sistemas**
 - 5.1 Capacitación
 - 5.2 Ajuste de Desempeño del Software de Aplicación
 - 5.3 Conversión
 - 5.4 Pruebas de los Cambios
 - 5.5 Criterios y Desempeño de las Pruebas Paralelas/Piloto
 - 5.6 Prueba de Aceptación Final
 - 5.7 Acreditación y Pruebas de Seguridad
 - 5.8 Prueba Operativa
 - 5.9 Promoción para Producción
 - 5.10 Evaluación de Cumplimiento de los Requerimientos del Usuario
 - 5.11 Revisión Administrativa Post-Implementación
- 6.0 Manejar los Cambios**
 - 6.1 Iniciación y Control de la Solicitud de Cambios
 - 6.2 Evaluación del Impacto
 - 6.3 Control de los Cambios
 - 6.4 Documentación y Procedimientos
 - 6.5 Mantenimiento Autorizado
 - 6.6 Política de Lanzamiento de Software
 - 6.7 Distribución de Software

SUMINISTRO Y SOPORTE

1.0 Definir los Niveles de Servicio

- 1.1 Marco de Referencia de Acuerdos de Nivel de Servicio
- 1.2 Aspectos de los Acuerdos de Nivel de Servicio
- 1.3 Procedimientos de Desempeño
- 1.4 Monitoreo y Reporte
- 1.5 Revisión de los Acuerdos y Contratos de Nivel de Servicio
- 1.6 Artículos con Cargo
- 1.7 Programa de Mejoramiento de Servicio

2.0 Manejar los Servicios de Terceros

- 2.1 Interfaces de Proveedores
- 2.2 Relaciones con el Propietario
- 2.3 Contratos con Terceros
- 2.4 Requerimientos de Terceros
- 2.5 Contratos Externos
- 2.6 Continuidad de Servicios
- 2.7 Relaciones de Seguridad
- 2.8 Monitoreo

3.0 Administrar el Desempeño y la Capacidad

- 3.1 Requerimientos de Disponibilidad y Desempeño
- 3.2 Plan de Disponibilidad
- 3.3 Monitoreo y Reporte
- 3.4 Herramientas de Modelaje
- 3.5 Administración Proactiva del Desempeño
- 3.6 Pronóstico de la Carga de Trabajo
- 3.7 Administración de la Capacidad de los Recursos
- 3.8 Disponibilidad de los Recursos
- 3.9 Programación de Recursos

4.0 Asegurar el Servicio Continuo

- 4.1 Marco de Referencia de Continuidad de TI

APÉNDICE I

LISTA DE DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

- 4.2 Plan Estratégico y Filosofía de Continuidad de TI
- 4.3 Contenido del Plan de Continuidad de TI
- 4.4 Reducción de los Requerimientos de Continuidad de TI
- 4.5 Mantenimiento del Plan de Continuidad de TI
- 4.6 Pruebas del Plan de Continuidad de TI
- 4.7 Capacitación del Plan de Continuidad de TI
- 4.8 Distribución del Plan de Continuidad de TI
- 4.9 Procedimientos de Respaldo del Procesamiento Alternativo de Datos del Departamento del Usuario
- 4.10 Recursos Críticos de TI
- 4.11 Sitio y Hardware de Respaldo
- 4.12 Procedimientos de Wrap-up
- 5.0 Asegurar la Seguridad de los Sistemas**
 - 5.1 Manejo de las Medidas de Seguridad
 - 5.2 Identificación, Autenticación y Acceso
 - 5.3 Seguridad del Acceso a Datos En Línea
 - 5.4 Administración de las Cuentas del Usuario
 - 5.5 Revisión Administrativa de las Cuentas del Usuario
 - 5.6 Control del Usuario de las Cuentas del Usuario
 - 5.7 Vigilancia de Seguridad
 - 5.8 Clasificación de Datos
 - 5.9 Identificación de Central y Administración de Derechos de Acceso
 - 5.10 Reportes de Violación y Actividades de Seguridad
 - 5.11 Manejo de Incidentes
 - 5.12 Re-Acreditación
 - 5.13 Confianza de la Contraparte
 - 5.14 Autorización de Transacciones
 - 5.15 No-Repudio
 - 5.16 Ruta Confiable
 - 5.17 Protección de las Funciones de Seguridad
 - 5.18 Administración de la Clave Criptográfica
 - 5.19 Prevención, Detección y Corrección de Software Malicioso
 - 5.20 Arquitectura de Barreras de Protección y Conexiones con Redes Públicas
 - 5.21 Protección de Bienes Electrónicos
- 6.0 Identificar y Atribuir los Costos**
 - 6.1 Artículos Cobrables
 - 6.2 Procedimientos de Costeo
 - 6.3 Procedimientos de Facturación y Reembolso al Usuario
- 7.0 Educar y Capacitar a los Usuarios**
 - 7.1 Identificación de las Necesidades de Capacitación
 - 7.2 Organización de la Capacitación
 - 7.3 Capacitación de Consciencia y Principios de Seguridad
- 8.0 Ayudar y Aconsejar a los Clientes de TI**
 - 8.1 Oficina de Asistencia
 - 8.2 Registro de las Preguntas del Cliente
 - 8.3 Agravamiento de las Preguntas del Cliente
 - 8.4 Monitoreo de Habilidad
 - 8.5 Análisis y Reporte de Tendencias
- 9.0 Manejar la Configuración**
 - 9.1 Registro de la Configuración
 - 9.2 Fundamento de la Configuración
 - 9.3 Estatus de Contabilidad
 - 9.4 Control de la Configuración
 - 9.5 Software No Autorizado
 - 9.6 Almacenamiento de Software
- 10.0 Manejar los Problemas e Incidentes**
 - 10.1 Sistema de Manejo de Problemas
 - 10.2 Agravamiento de Problemas
 - 10.3 Rastreo y Ruta de Auditoría de Problemas
- 11.0 Manejar los Datos**
 - 11.1 Procedimientos de Preparación de Datos
 - 11.2 Procedimientos de Autorización de Documentos Fuente
 - 11.3 Recolección 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 Alimentación de Datos
 - 11.7 Chequeos de Precisión, Integridad y Autorización
 - 11.8 Manejo de Errores de Alimentación de Datos
 - 11.9 Integridad de Procesamiento de Datos
 - 11.10 Validación y Edición de Procesamiento de Datos
 - 11.11 Manejo de Errores de Procesamiento de Datos

APÉNDICE I

LISTA DE DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

11.12	Manejo y Retención de Datos de Salida (Resultados)	MONITOREO
11.13	Distribución de Resultados	1.0 Monitorear las Operaciones
11.14	Balance y Conciliación de Resultados	1.1 Recolección de Datos de Monitoreo
11.15	Revisión y Manejo de Errores de Resultados	1.2 Evaluación del Desempeño
11.16	Provisión de Seguridad para Reportes de Resultados	1.3 Evaluación de la Satisfacción del Cliente
11.17	Protección de Información Delicada Durante la Transmisión y el Transporte	1.4 Reporte Administrativo
11.18	Protección de Información Delicada Desechada	2.0 Evaluar la Suficiencia del Control Interno
11.19	Manejo del Almacenamiento	2.1 Monitoreo del Control Interno
11.20	Períodos de Retención y Plazos de Almacenamiento	2.2 Operación Oportuna de los Controles Internos
11.21	Sistema de Administración de Archivo de Medios	2.3 Reporte del Nivel de Control Interno
11.22	Responsabilidades de la Administración del Archivo de Medios	2.4 Aseguramiento de Seguridad Operativa y Control Interno
11.23	Respaldo y Restauración	3.0 Obtener Aseguramiento Independiente
11.24	Tareas de Respaldo	3.1 Certificación/Acreditación Independiente de la Seguridad y el Control Interno de los Servicios de TI
11.25	Almacenamiento del Respaldo	3.2 Certificación/Acreditación Independiente de Proveedores Externos de Servicios
11.26	Archivo	3.3 Evaluación Independiente de la Eficacia de los Servicios de TI
11.27	Protección de Mensajes Delicados	3.4 Evaluación Independiente de la Eficacia de los Proveedores Externos de Servicios
11.28	Autenticación e Integridad	3.5 Aseguramiento Independiente del Cumplimiento de los Requerimientos Legales y Regulatorios y Compromisos Contractuales
11.29	Integridad de las Transacciones Electrónicas	3.6 Aseguramiento Independiente del Cumplimiento de los Requerimientos Legales y Regulatorios y Compromisos Contractuales de Proveedores Externos de Servicios
11.30	Integridad Continua de los Datos Almacenados	3.7 Competencia de la Función de Aseguramiento Independiente
12.0	Manejar las Instalaciones	3.8 Involucramiento Proactivo de Auditoría
12.1	Seguridad Física	4.0 Preparar Auditorías Independientes
12.2	Perfil del Sitio de TI	4.1 Contrato de Auditoría
12.3	Escolta a Visitantes	4.2 Independencia
12.4	Salud y Seguridad del Personal	4.3 Ética y Estándares Profesionales
12.5	Protección Contra Factores Ambientales	4.4 Competencia
12.6	Suministro Ininterrumpido de Energía	4.5 Planeación
13.0	Manejar las Operaciones	4.6 Realización del Trabajo de Auditoría
13.1	Procedimientos de las Operaciones de Procesamiento y Manual de Instrucciones	4.7 Reporte
13.2	Documentación del Proceso de Inicio y Otras Operaciones	4.8 Actividades de Seguimiento
13.3	Programación de Tareas	
13.4	Desviaciones de la Programación Estándar de Tareas	
13.5	Continuidad de Procesamiento	
13.6	Bitácoras de Operaciones	
13.7	Operaciones Remotas	

APÉNDICE II – MATERIAL DE REFERENCIA PRINIPAL

COSO: Comité de las organizaciones patrocinadas de la Comisión Treadway. *Control Interno – Marco de Referencia Integrado*. 2 vols. Instituto Americano de Contadores Certificados, Nueva Jersy, 1994.

Directrices OECD: Organización para la Cooperación Económica y el Desarrollo. *Directrices para la Seguridad de la Información*, París, 1992.

Código DTI para el Manejo de la Seguridad de la Información: Departamento de Comercio e Industria y el Instituto Británico de Estándares. *Un Código para el Manejo de la Seguridad de la Información*, Londres, 1993, 1995.

ISO-9000-3: Organización Internacional de Estandarización. *Estándares de la Administración de Calidad y Aseguramiento de Calidad – Parte 3: Directrices para la aplicación del ISO-9001 para el desarrollo, abastecimiento y mantenimiento del software*, Suiza 1991.

Manual de Seguridad NIST: Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de E.U.A. *Una introducción a la Seguridad Computacional: El Manual NIST*, Washington, DC, 1995.

Prácticas del Manjeo de la TI del ITIL: Biblioteca de la Infraestructura de la Tecnología de la Información. Prácticas y Directrices desarrollados para la Agencia Central de Computación y Telecomunicaciones (CCTA), Londres, 1989.

Marco de Referencia IBAG: Marco de Referencia Preliminar del Grupo de Consultoría de Negocios para SOGIS (Grupo de Directores Ejecutivos de la Seguridad de Información, Recomendando a la Comisión Europea) Bruselas, Bélgica, 1994.

Declaraciones de la Oficina del Primer Ministro de NSW sobre las Mejores Prácticas y, las Técnicas y Manejo de la Información de Planeación: *Declaración de la Mejores Prácticas #1 a la #6*. Departamento del Primer Ministro de New South Wales, Gobierno de New South Wales, Australia, de 1990 a 1994.

Memorándum del Banco Central Holandés: *Memorándum sobre la Confiabilidad y Continuidad del Procesamiento electrónico de Datos en la Banca*. Banco de Nederlandsche, Reimpreso de Boletín Trimestral #3, Países Bajos, 1998.

Monografía EDPAF #7, EDI: Un Enfoque de Auditoría: Jamison, Rodger. *EDI. Un Enfoque de Auditoría*, Serie Monográfica #7, Fundación de Auditoría y Control de los Sistemas de Información; INC, Rolling Meadows, IL, Abril 1994.

Marco de Referencia Modelo de PCIE (Consultoría Presidencial sobre Integridad y Eficiencia: *Un Marco de Referencia Modelo para la Administración sobre los Sistemas de Información Autorizados*. Elaborado conjuntamente por el Consejo Presidencial para el Mejoramiento de la Administración y el Consejo Presidencial sobre Integridad y Eficiencia, Washington, DC, 1987.

Estándares de Auditoría para los Sistemas de Información en Japón: *Estándares de Auditoría para los Sistemas de Información de Japón*. Proporcionando por la cooperación de Auditoría Chuo, Tokio, Agosto 1994.

Controles de los OBJETIVOS DE CONTROL en un Ambiente de Sistema de Información: Directrices de Control y Procedimientos de Auditoría: Fundación de Auditores EDKP (ahora la Fundación de Control y Auditoría de los Sistemas de Información), cuarta Edición, Rolling Meadows, IL, 1992.

Análisis de Puesto CISA: Consejo de Certificación de la Asociación de Control y Auditoría de Sistema de Información. “Estudio de Análisis de Puesto de Auditor de Sistemas de Información Certificado”, Rolling Meadows, IL 1994.

Directrices de Controles Computacionales CICA: Instituto Canadiense de Peritos Contables, Toronto, 1986.

Directrices Internacionales IFAC para el Manejo de la Seguridad de la Información y Comunicaciones: Federación Internacional de Contadores, Nueva York, NY, 1997.

Directrices Internacionales IFAC sobre el Manejo de la Tecnología de Información – Manejo de la Planeación de la Tecnología de Información para el Impacto de Negocios (Borrador): Federación Internacional de Contadores, Nueva York, NY, 1998.

Estándares de Control Interno en el Gobierno Federal de E.U.A.: Oficina General de Tesorería de E.U.A., Washington, DC, 1983.

Guía para la Auditoría de Controles y Seguridad, un Enfoque del Grado de Vida de Desarrollo de Sistemas: *Publicación Especial NBS, 500-153*: Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de E.U.A., Washington, DC, 1998.

Estándares gubernamentales de Auditoría: Oficina General de Tesorería de EUA, Washington, Dc, 1994.

Prácticas generalmente aceptadas del Manejo de la TI en Dinamarca: El Inst. de Contadores Autorizados por el Estado, Dinamarca, 1994.

SPICE: Mejoras al Proceso del Software y Determinación de la capacidad. Un estándar sobre el mejoramiento del proceso del software, institución de Estándares Británico, Londres, 1995.

DRI Internacional, Prácticas Profesionales para planeadores de la continuidad del Negocio: Instituto Internal para la Recuperación en casos de Desastre, Guía para los planeadores de la Continuidad del Negocio, San Luis, MO, 1997.

IIA, Pantleto de Prácticas Profesionales 97-1, Comercio Electrónico: Instituto de la Fundación de Investigación de Auditores Internos, Alamonte Springs, FL, 1997.

Series de Referencias Técnicas E & Y: Ernest & Young, Guía de Auditoría, SAP R/3, Cleveland, OH 1996.

Guía de Auditoría C&L SAP R/3: Coopers & Lybrand, SAP R/3: Su Uso Control y Auditoría, Nueva York, NY, 1997
Tecnología de Información ISO IEC JTC

Tecnología de Información ISO IEC JTC1/SC27 – Seguridad: Organización Internacional de Estandarización, Comité Técnico para la Seguridad de la Tecnología de Información, Suiza, 1998.

ISO TC68/WGA, Directrices para la Seguridad de la Información para la Banca y Servicios Financieros Relacionados: Organización Internacional de Estandarización (ISO) Comité Técnico para la Banca y Servicios Financieros, Borrador, Suiza, 1997.

CCEB 96/011, Criterios Comunes para la Evaluación de la Seguridad de la Tecnología de Información: Consejo de implementación de los Criterios Comunes, Alineación y comparación de los criterios de seguridad de la TI Europeos, E.U. A. y Canadienses, Borrador, Washington, DC, 1997.

Práctica Recomendada para EDI: EDIFACT (EDI para la Administración de Comercio e Industria), París, 1987.

TICKIT: Guía para la Construcción y Certificación de software por Sistemas de Manejo de la Calidad, Departamento de Comercio e Industria Británico (DTI), Londres, 1994.

Control Base ESF – Comunicaciones: Foro de Seguridad Europeo, Londres, *Seguridad de Redes de Comunicaciones*, Septiembre 1991, *Controles Base para Redes de Área Local*, Septiembre 1994.

Control Base ESF – Microcomputadoras: Foro de Seguridad Europeo, Londres, *Cantidades de Base, Microcomputadoras Conectadas a la Red*, Junio 1990.

Manual de Auditoría de los Sistemas de Información Computalizados (CIS): Fundación de Auditores EDP (ahora la Fundación de Control y Auditoría de Sistema de Información), Rolling Meadows, IL, 1992.

APÉNDICE III – GLOSARIO DE TÉRMINOS

AICPA	Instituto Americano de Contadores Públicos Certificado. (<i>American Institute of Certified Public Accountants</i>)
CCEB	Criterios comunes para seguridad en tecnología de información. (<i>Common Criteria for Information Technology Security</i>)
CICA	Instituto Canadiense de Contadores. (<i>Canadian Institute of Chartered Accountants</i>)
CISA	Auditor Certificado de Sistemas de Información. (<i>Certified Information Systems Auditor</i>)
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" (<i>Committee of Sponsoring Organisations of the Tradeway Commission</i>).
DRI	Instituto Internacional de Recuperación de Desastres. (<i>Disaster Recovery Institute International</i>)
DTI	Departamento de Comercio e Industria del Reino Unido. (<i>Department of Trade and Industry of the United Kingdom</i>)
EDIFACT	Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria (<i>Electronic Data Interchange for Administration, Commerce and Trade</i>)
EDPAF	Fundación de Auditores de Procesamiento Electrónico de Datos (<i>Electronic Data Processing Auditors Foundation</i>), ahora ISACF .
ESF	Foro Europeo de Seguridad (<i>European Security Forum</i>), 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. (<i>U.S. General Accounting Office</i>)
I4	Instituto Internacional de Integridad de Información. (<i>International Information Integrity Institute</i>), asociación similar a ESF, con metas similares, pero con base principalmente en los Estados Unidos y dirigida por el Instituto de Investigaciones de Stanford (<i>Stanford Research Institute</i>)
IBAG	Grupo Consultivo de Negocios Infosec (<i>Infosec Business Advisory Group</i>), 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. (<i>International Federation of Accountants</i>)
IIA	Instituto de Auditores Internos. (<i>Institute of Internal Auditors</i>)
INFOSEC	Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (<i>Advisory Committee for IT Security Matters to the European Commission</i>)
ISACA	Asociación para la Auditoría y Control de Sistemas de Información. (<i>Information Systems Audit and Control Foundation</i>)
ISACF	Fundación para la Auditoría y Control de Sistemas de Información. (<i>Information Systems Audit and Control Foundation</i>)
ISO	Organización de Estándares Internacionales. (<i>International Standards Organisation</i>) (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. (<i>Information Technology Infrastructure Library</i>)
ITSEC	Criterios de Evaluación de Seguridad de Tecnología de Información (<i>Information Technology Security Evaluation Criteria</i>). 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 (<i>National Bureau of Standards of</i>

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

NIST	<i>the U.S.)</i> (antes NBS) Instituto Nacional de Estándares y Tecnología. (<i>National Institute of Standards and Technology</i>), con base en Washington D.C.
NSW	Nueva Gales del Sur, Australia. (<i>New South Wales, Australia</i>)
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. (<i>Organisation for Economic Cooperation and Development</i>)
OSF	Fundación de Software Público (<i>Open Software Foundation</i>)
PCIE	Consejo Presidencial de Integridad y Eficiencia. (<i>President's Council on Integrity and Efficiency</i>)
TCSEC	Criterios de Evaluación de Sistemas Computarizados Confiables. (<i>Trusted Computer System Evaluation Criteria</i>), conocido también como " <i>The Orange Book</i> ". 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)

APÉNDICE IV – PROCESO DE AUDITORÍA (PREPARADO POR EL CAPÍTULO NACIONAL DE ÁREA CAPITAL)

Los diagramas de flujo que se muestran a continuación tratan de cada uno de los pasos para la satisfacción de un solo *objetivo de control*. Define el objetivo del paso y especifica lo que el auditor debe haber alcanzado antes de continuar con el siguiente paso. Finalmente, un diagrama de flujo es la representación gráfica del proceso de recolección de información y toma de decisiones que deben ocurrir en cada uno de los pasos.

Dado que muchos de los objetivos son particulares, no sugerimos estos diagramas como una regla estricta. Resultan útiles como guía porque representan un marco de referencia conceptual preciso para cada una de las fases del trabajo de auditoría. Se presenta un glosario consolidado de términos después de cada diagrama. Los términos definidos se representan en *cursiva* a lo largo del texto.

PASO DE AUDITORÍA DE IDENTIFICACIÓN/DOCUMENTACIÓN

Objetivo del Paso – El objetivo del paso de auditoría de identificación/documentación es que el auditor se familiarice con la *tarea* cubierta por el *objetivo de control* y la manera en que la administración de SI cree que están siendo controlados.

Esto incluye la identificación de las personas, los procesos y la locación que realiza dicha *tarea*, y los *procedimientos establecidos* que los controlan.

Resultados Deseados del Paso – Al finalizar el paso de auditoría de identificación/documentación, el auditor deberá haber identificado, documentado y verificado:

- Quién realiza la *tarea* cubierta por el *objetivo de control*
- Dónde se realiza la *tarea*
- Cuándo se realiza la *tarea*
- Sobre qué *datos de entrada* se realiza la *tarea*
- Qué *datos de salida/resultados* se esperan de la *tarea*, y
- Cuáles son los *procedimientos establecidos* para realizar la *tarea*.

PASO DE AUDITORÍA DE EVALUACIÓN

Objetivo del Paso – El objetivo del paso de auditoría de evaluación es evaluar los *procedimientos establecidos* y determinar si los procedimientos brindan una estructura de control eficaz. Los procedimientos deben evaluarse contra los criterios identificados, las prácticas estándar de la industria y el criterio del auditor. Una estructura de control eficaz es eficiente en costos y proporciona aseguramiento razonable de que la *tarea* está siendo realizada y de que se están cumpliendo el *objetivo de control*.

Resultados Deseados del Paso – Al finalizar el paso de auditoría de evaluación, el auditor debe haber:

- Evaluado las leyes, regulaciones y criterios organizacionales en cuanto a su aplicación sobre los procedimientos
- Evaluado los *procedimientos establecidos* para determinar si son eficientes en costos y proporcionan *aseguramiento razonable* de que se está realizando la *tarea* y de que se está cumpliendo el *objetivo de control*
- Evaluado los *controles compensatorios* utilizados para apoyar procedimientos débiles
- Concluido si los *procedimientos establecidos* y los *controles compensatorios* proporcionan conjuntamente una estructura de control eficaz
- Identificado si son apropiadas las pruebas de cumplimiento.

PASO DE AUDITORÍA DE PRUEBAS DE CUMPLIMIENTO

Objetivo del Paso – El objetivo del paso de auditoría de pruebas de cumplimiento es analizar la adherencia de una organización a los controles prescritos. Deberá compararse los *procedimientos reales* y los *controles compensatorios* en relación con los *procedimientos establecidos*, y deberá realizarse entrevistas y revisión de documentos para determinar si los controles están debida y consistentemente aplicados. Las pruebas de cumplimiento solamente se realizan sobre la base de los procedimientos que han sido determinados como eficaces.

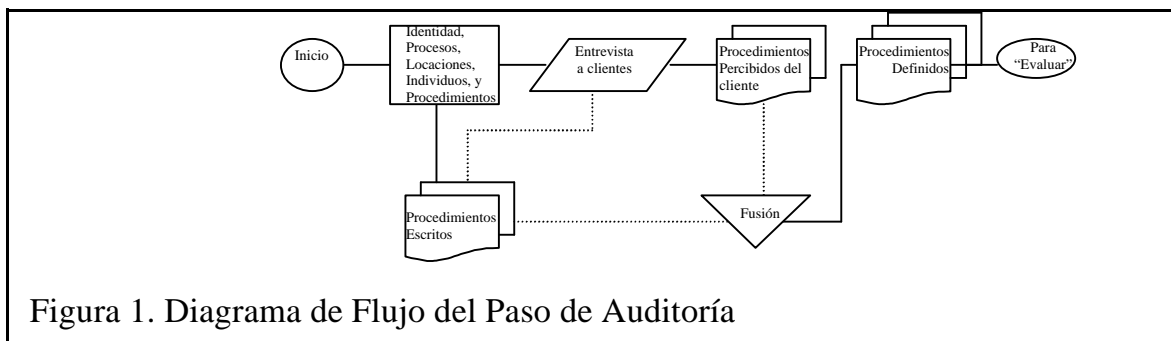


Figura 1. Diagrama de Flujo del Paso de Auditoría

APÉNDICE IV – PROCESO DE AUDITORÍA (PREPARADO POR EL CAPÍTULO NACIONAL DE ÁREA CAPITAL)

Resultados Esperados del Paso – Al finalizar el paso de auditoría de pruebas de cumplimiento, el auditor debe haber documentado la adherencia de la organización a los procedimientos identificados anteriormente y debe haber concluido si los *procedimientos establecidos* y los *controles compensatorios* están debida y consistentemente aplicados. Basándose en el nivel de cumplimiento, el auditor debe determinar el nivel de pruebas justificantes necesarias para brindar aseguramiento de que el proceso de control es adecuado.

PASO DE AUDITORÍA DE PRUEBAS JUSTIFICANTES

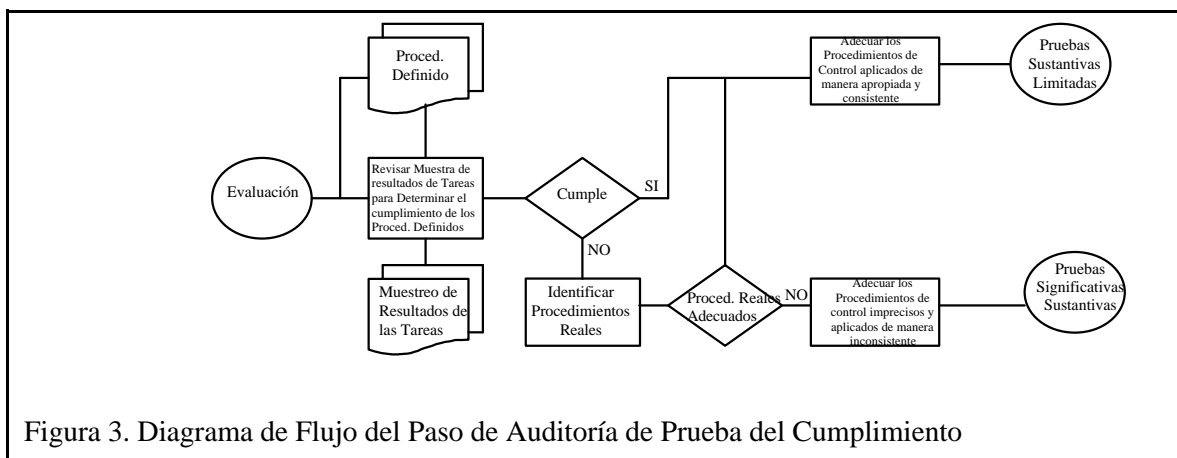
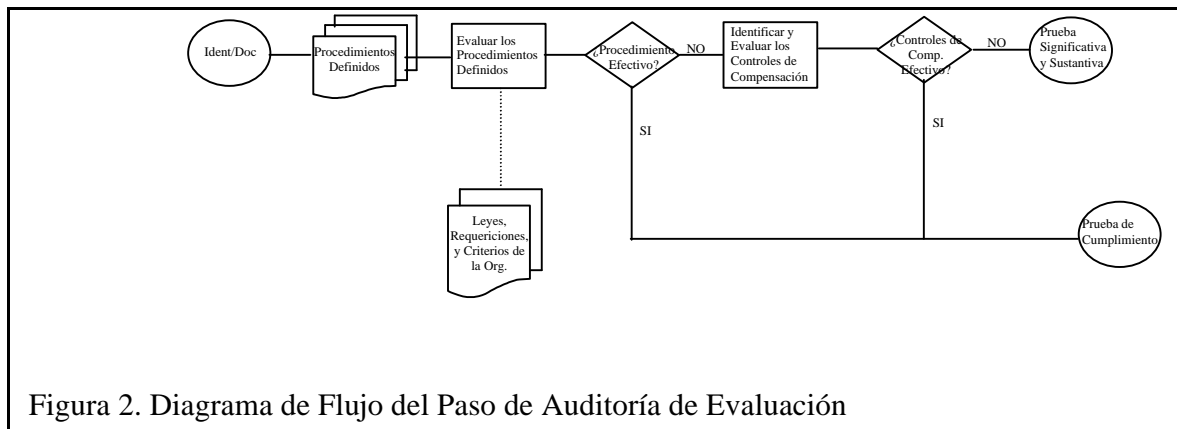
Objetivo del Paso – El objetivo del paso de auditoría de pruebas justificantes es realizar las pruebas de datos

necesarias para brindar aseguramiento o no-aseguramiento total a la administración sobre la consecución de un *objetivo de negocios* dado.

Resultados Deseados del Paso – Al finalizar el paso de auditoría de pruebas justificantes, el auditor deberá haber realizado pruebas suficientes sobre los resultados de la *tarea* para concluir si se está alcanzando un *objetivo de control* dado. Deberán realizarse pruebas justificantes significativas si:

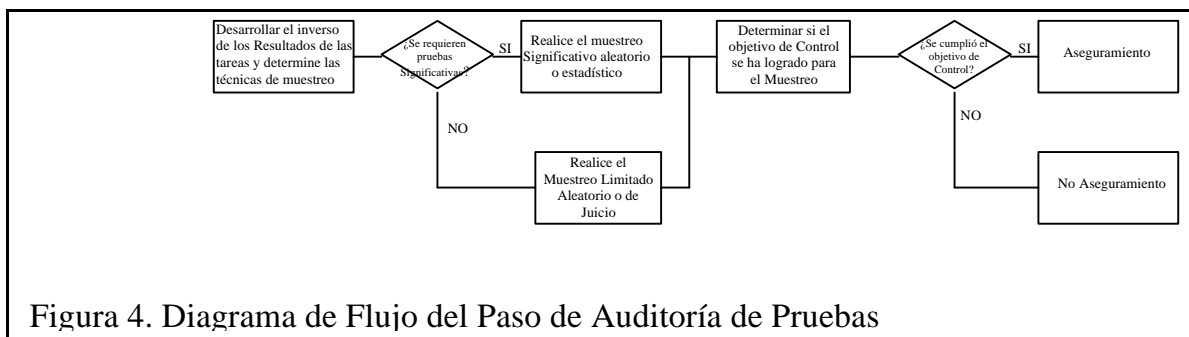
- No existen medidas de control
- Las medidas de control han sido calificadas como no satisfactorias, o

Las pruebas de cumplimiento indican que las medidas de control no han sido debida y consistentemente aplicadas.



APÉNDICE IV – PROCESO DE AUDITORÍA

(PREPARADO POR EL CAPÍTULO NACIONAL DE ÁREA CAPITAL)



APÉNDICE IV – PROCESO DE AUDITORÍA

GLOSARIO:

Procedimientos Reales – Son los procedimientos que están siendo realizados por la organización para satisfacer el objetivo de auditoría. Los procedimientos reales se identifican durante la fase de auditoría de pruebas de cumplimiento.

Controles Compensatorios – Son los pasos o procedimientos adicionales de control que no se relacionan directamente con el objetivo de control que se está probando, pero cuya presencia sirve para fortalecer los controles que sí se relacionan directamente con el objetivo de control. Los controles compensatorios se identifican durante la fase de pruebas de cumplimiento del trabajo de auditoría. Los controles compensatorios se procuran de manera activa solamente cuando la eficacia de los controles establecidos es cuestionable.

Objetivo de Control – El resultado deseado de cualquier procedimiento establecido para una organización. Desde el punto de vista de Sistemas de Información, el objetivo de control se utiliza para catalogar y definir el alcance del trabajo de auditoría que se está realizando.

Aseguramiento Razonable – Un estándar para la evaluación de la suficiencia de los procedimientos establecidos para cumplir con un objetivo de control en particular. El aseguramiento razonable involucra la aplicación del criterio, conocimiento y experiencia para desarrollar una opinión informada. El aseguramiento razonable requiere que un sistema de controles sea eficaz, pero no demasiado gravoso. El estándar de aseguramiento razonable también requiere que un sistema de controles sea eficiente en costos.

Procedimientos Establecidos – Controles que la organización cree establecidos y que se siguen para brindar aseguramiento de que se está cumpliendo el objetivo de control. Los procedimientos establecidos son lo que la administración cree que está sucediendo. Incluyen tanto procedimientos escritos, como procedimientos informales identificados por la administración. Los procedimientos establecidos se identifican en la fase de identificación/documentación del trabajo de auditoría y se comparan en relación con los procedimientos reales durante la fase de cumplimiento.

Tarea – El resultado deseado de una serie de procedimientos cubiertos por un objetivo de control. La tarea es lo que el objetivo de control está diseñado a asegurar.

Datos de Entrada y Resultados de la Tarea – Productos, reportes o información requerida para, asociada con o resultado de la realización de una tarea.

APÉNDICE V

Como una muestra de la aplicación del *Marco de Referencia* de COBIT a problemas específicos, así como también a procesos específicos, Robert Parker, ExPresidente de ISACA (AACSI), ha brindado una muestra de un lineamiento de auditoría aplicable al problema del Milenio – Año 2000, relacionado con los campos de datos de los programas de cómputo y las dificultades potenciales de procesamiento asociados con el cambio de los últimos dígitos de “99” a “00”. A manera de demostración, no pretende incluir todos los aspectos, sino más bien el ser de utilidad como un enfoque hacia el tema, utilizando el *Marco de Referencia* de COBIT para desarrollar un lineamiento de auditoría.

CUMPLIMIENTO DE LOS REQUERIMIENTOS DEL AÑO 2000

OBJETIVOS DE CONTROL

- 1 Asegurar que todos los programas de aplicación cumplan con los requerimientos del Año 2000
- 2 Asegurar que todo el hardware y software de sistema cumpla con los requerimientos del Año 2000
- 3 Asegurar que existan planes para monitorear el cumplimiento de los requerimientos del Año 2000 y que se efectúe la respuesta oportuna donde sea necesario

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Comprender a través de:

► Entrevistas:

Director General de Finanzas
 Director General de Información
 Miembros seleccionados del Comité Directivo de la Función de Servicios de Información
 Jefe del sub-comité especial para el Año 2000 de la organización
 Administración de la Función de Servicios de Información responsable de las iniciativas para el Año 2000
 Personal de la Función de Servicios de Información responsable de la implantación y los resultados de las iniciativas para el Año 2000
 Usuarios responsables de aplicaciones de comercio electrónico

► Obteniendo:

El plan para el Año 2000 de la organización, incluyendo tiempos específicos y costo presupuestado
 El reporte de evaluación para el Año 2000 de la organización
 El análisis, por parte de la función de servicios de información, del esfuerzo requerido para cumplir con los requerimientos del Año 2000, clasificado por aplicación, programas y utilidades de los sistemas, y dispositivos de hardware
 Información sobre certificación de cumplimiento de los requerimientos del Año 2000 de los distribuidores, y fecha anticipada de cumplimiento, si no están certificados todavía
 Minutas de las reuniones del sub-comité especial para el Año 2000
 Iniciativas importantes de la industria para resolver problemas a nivel industria (por ejemplo, comercio electrónico)

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Evaluar los controles:

► Considerando sí:

- La organización ha realizado una revisión de su utilización de la tecnología de información, incluyendo la preparación de un inventario apropiado, y ha evaluado adecuadamente los problemas potenciales y específicos del Año 2000
- La organización ha establecido un plan para asegurar que sus sistemas cumplan con los requerimientos del Año 2000 y ha dedicado tiempo suficiente para un cumplimiento total
- La organización ha desarrollado planes específicos para evaluar los sistemas antiguos que pueden no tener documentación o fuentes suficientes para permitir su modificación para que cumplan con los requerimientos del Año 2000
- La organización negocia electrónicamente con proveedores (EDI; EFI, etc.), y si ellos necesitan cumplir con los requerimientos del Año 2000, incluyendo la certificación apropiada
- La calidad de la documentación existente es suficiente para permitir que la organización cumpla con los requerimientos para el Año 2000
- Los sistemas operativos y otro software están certificados por su cumplimiento de los requerimientos para el Año 2000
- La organización ha utilizado “99” como una opción predeterminada en el diseño de sistemas, particularmente en políticas de retención (por ejemplo, 99365 para especificar una retención sin eliminar de los archivos guardados)
- La organización ha adoptado una política que requiere que todo el software nuevo cumpla con los requerimientos para el Año 2000
- La organización tiene la capacidad suficiente para llevar a cabo y finalizar las iniciativas para el Año 2000, incluyendo las pruebas de validación, en el tiempo requerido
- La organización ha adquirido y validado productos de software para ayudar en la implantación de su programa para el Año 2000
- La organización se apoya o se apoyará en fuentes externas para realizar su plan para el Año 2000, y si dichos recursos ya están contratados
- El plan para el Año 2000 de la organización incluye dispositivos controlados por computadora, tales como puertas, alarmas, elevadores, claves de seguridad, pases, máquinas de fax, etc.
- La organización probablemente evitará un problema de “creciente preocupación” dados el plan actual para el Año 2000 y el estatus de cualquier iniciativa para el Año 2000

Evaluar la suficiencia:

► Probando que:

- El inventario de aplicaciones, utilidades, APIs, etc., es preciso y completo, y que el estatus del cumplimiento con los requerimientos para el Año 2000 esté correcto
- Los planes para el Año 2000 sean razonables, completos y alcanzables, y que estén manejados apropiadamente
- Que las interfaces electrónicas con los proveedores cumplan con los requerimientos para el Año 2000
- La documentación es adecuada para permitir a la organización evaluar, actualizar y probar todos los programas requeridos para hacer que la organización cumpla con los requerimientos del Año 2000
- Los fabricantes, distribuidores y otros proveedores hayan certificado sus productos como en cumplimiento de los requerimientos del Año 2000, y que mantengan registros de dicha certificación
- Para los productos certificados para el Año 2000, la organización ha realizado las pruebas apropiadas en su ambiente normal/habitual de procesamiento, incluyendo las comunicaciones
- El uso de las opciones predeterminadas “99” ha sido apropiadamente resuelto
- Las políticas, procedimientos y estándares de la organización reflejan los requerimientos del Año 2000 y se cumple con ellos
- Todos los acuerdos de licencia de software y hardware actual especifican el cumplimiento de los requerimientos del Año 2000 y/o una fecha límite de cumplimiento especificada por el distribuidor/proveedor

La organización ha incluido tiempo de capacitación suficiente para asegurar que todos los empleados de la Función de Servicios de Información tengan los conocimientos para apoyar las iniciativas para el Año 2000 de la organización

Los acuerdos de licencia de software permiten a la organización realizar pruebas para el Año 2000 en sitios distintos de la locación principal con licencia

Las iniciativas para el Año 2000 de la organización incluyen la prueba y validación apropiada, incluyendo una prueba completa de los sistemas, y que los sitios remotos apropiados han sido asegurados para simular ambientes remotos de procesamiento y comunicaciones, y que han realizado dicha prueba

El plan comprende a los dispositivos, además de los sistemas computacionales

El plan permita a la organización continuar con sus actividades normales de negocios, sin interrupciones, después del Año 2000

Evaluar el riesgo de los objetivos de control no alcanzados:

▸ **Llevando a cabo:**

Referencia de los planes e iniciativas para el Año 2000 y de su estatus actual respecto a organizaciones similares o criterios razonables apropiados

Una revisión detallada de las diversas iniciativas para el Año 2000, incluyendo la evaluación del tiempo estimado, los recursos asignados, los conocimientos disponibles y el presupuesto establecido

Revisiones de los contratos con distribuidores y proveedores para calificar el grado de cumplimiento con los requerimientos del Año 2000

Revisiones de las pruebas para el Año 2000 de la organización para evaluar el cumplimiento de los sistemas individuales para cubrir los requerimientos del Año 2000 de la organización

Revisiones de los contratos externos para el Año 2000 y evaluación de los plazos y los resultados de los contratos

▸ **Identificando:**

Planes e iniciativas para el Año 2000 poco realistas o demasiado ambiciosos

Fondos, asignación de recursos, personal y conocimientos insuficientes para el Año 2000

Contratación inadecuada o inapropiada en el área de requerimientos para el Año 2000

Pruebas inadecuadas o inapropiadas de los sistemas y programas de aplicación que han sido modificados para cumplir con los requerimientos del Año 2000

Plazos, condiciones o temporalidad inadecuada o inapropiada para que el software suministrado por medio de distribuidores cumpla con los requerimientos del Año 2000

Pruebas inadecuadas o inapropiadas del software de distribuidores externos que ha sido “certificado por el distribuidor” como en cumplimiento de los requerimientos para el Año 2000

**Asociación de Auditoría y Control
de Sistemas de Información**

3701 ALGOLQUÍN ROAD, SUITE 1010
ROLLING MEADOWS, ILLINOIS 60008, USA

TELEPHONE: +1.847.253.1545
FACSMILE: +1.847.253.1443

E- MAIL: publication@isaca.org
WEB SITE: <http://www.isaca.org>

DÍGANOS QUÉ PIENSA DE COBIT

Nos interesa conocer su reacción a *COBIT: Objetivos de Control para la Información y Tecnología Relacionada*. Sírvase proporcionar sus comentarios a continuación. Las respuestas serán recopiladas y publicadas en *IS Audit and Control Journal*.

Nombre _____
Compañía _____
Dirección _____
Ciudad _____ Estado/Provincia _____
País _____ Código Postal _____
Número de Fax _____
Dirección Electrónica _____

- ? Estoy interesado en saber más sobre cómo puede utilizarse CobiT dentro de mi organización.
Favor de solicitar a un representante de la Asociación que se ponga en contacto conmigo.
- ? Envíenme más información sobre:
- ? Otros productos de CobiT
- ? Cursos de Capacitación de CobiT (privados o sesiones generales)
- ? Certificación de Auditor Certificado de Sistemas de Información [CISA (ACSI)]
- ? Conferencias de ISACA (AACSI)
- ? Membresía de la Asociación
- ? IS Audit & Control Journal
- ? Otras publicaciones de ISACA (AACSI)

¡Muchas Gracias!

Todas las encuestas serán tomadas en consideración.

DIRECTRIZ GENÉRICA PARA AUDITORÍAS

OBTENCIÓN DE UNA COMPRENSIÓN

Los pasos de auditoría a realizar para documentar las actividades subyacentes de los objetivos de control, así como también para identificar las medidas de control/procedimientos establecidos existentes.

Entrevistar al personal y directivos para obtener una comprensión de:

- Los requerimientos del negocio y los riesgos asociados
- La estructura organizacional
- Las funciones y responsabilidades
- Las políticas y procedimientos
- Las leyes y regulaciones
- Las medidas de control existentes
- El reporte administrativo (estatus, desempeño, puntos de acción)

Documentar los recursos de TI relacionados particularmente afectados por los procesos bajo revisión, los Indicadores Clave de Desempeño [ICD (KPI)] del proceso, las implicaciones del control, mediante una revisión paso a paso del proceso

EVALUACIÓN DE LOS CONTROLES

Los pasos de auditoría a realizar para la evaluación de la eficacia de las medidas de control existentes o el grado en que se logra un objetivo de control. Básicamente, trata de decidir qué y cómo probarlo.

Evaluar la suficiencia de las medidas de control para el proceso bajo revisión, por medio de considerar los criterios identificados y las prácticas estándar de la industria, los Factores Críticos de Éxito [FCE (CSF)] de las medidas de control, y la aplicación del criterio profesional del auditor.

- Existen procesos documentados
- Existen resultados apropiados
- Las responsabilidades son claras y eficaces
- Existen controles compensatorios, donde es necesario

Concluir el grado en el que se cumple el objetivo de control.

EVALUACIÓN DEL CUMPLIMIENTO

Los pasos de auditoría a realizar para asegurar que las medidas de control establecidas están funcionando como debiera, de manera consistente y continua, y concluir sobre la suficiencia del ambiente de control.

Obtener evidencia directa o indirecta para puntos/períodos seleccionados para asegurar que los procedimientos cumplieron en el periodo bajo revisión, utilizando evidencia directa o indirecta.

Realizar una revisión limitada de la suficiencia de los resultados del proceso.

Determinar el nivel de pruebas justificantes y el trabajo adicional necesarios para asegurar que el proceso de TI es adecuado.

JUSTIFICACIÓN DEL RIESGO

Los pasos de auditoría a realizar para justificar el riesgo de no cumplir con el objetivo de control mediante el uso de técnicas analíticas y/o consultando a fuentes alternativas. El objetivo es fundamentar la opinión y “cimbrar” a la administración para que tome acción. Los auditores deben ser creativos para encontrar y presentar esta información frecuentemente confidencial y delicada.

Documentar las debilidades del control, y las amenazas y los puntos vulnerables resultantes.

Identificar y documentar el impacto real y potencial; por ejemplo, mediante el análisis de causa-raíz.

Brindar información comparativa; por ejemplo, mediante puntos de referencia.