

Auditoría de Sistemas de Información

Autor: Cosachov Wolf, Gerardo

Edición y Corrección: Lic. Cristian Borghello, CISSP

Fecha Publicación: 18 de julio de 2009

Publicado en [Segu-Info](http://www.segu-info.com.ar)

Concepto

Es la revisión integral de todos los procesos desarrollados por la función Sistemas de Información a efectos de evaluar:

1. la efectividad y eficiencia en el uso de los recursos
2. la salvaguarda de los activos
3. el aseguramiento del cumplimiento de los atributos de confidencialidad, integridad y disponibilidad que debe reunir la información
4. la contribución al cumplimiento de los objetivos operacionales y de control del negocio
5. la detección y corrección de las vulnerabilidades de seguridad, en forma oportuna, y
6. el cumplimiento de la normativa interna y externa

En síntesis, Auditoría Interna debería asesorar e informar a la Dirección en materia de Gobernabilidad de Tecnología Informática, es decir acerca de: a) la alineación de TI con la estrategia general de la empresa b) la contribución de TI a la consecución de nuevos negocios y el valor agregado a los ya existentes, c) el uso responsable de los recursos y d) gerenciamiento de riesgos de sistemas de información.

Efectividad: se refiere a la relevancia y pertinencia de la información para el proceso de negocio y su entrega en forma oportuna, correcta, consistente y útil.

Eficiencia: se vincula con la provisión de información mediante el uso óptimo de los recursos.

Confidencialidad: protección de la información contra su divulgación no autorizada.

Integridad: se vincula con la exactitud y totalidad de la información así como también con su validez, de acuerdo con los valores y expectativas del negocio.

Disponibilidad: la información debe estar disponible cuando la necesite el proceso de negocio.

Procesos

Dentro de los procesos desarrollados por la función sistemas de información están comprendidos:

Planificación y organización: abarca la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología puede contribuir a los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Asimismo deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición e implementación: para llevar a cabo la estrategia de TI, las soluciones deben ser identificadas, desarrolladas ó adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además deben evaluarse los cambios y el mantenimiento realizados a sistemas existentes.

Entrega y Soporte: comprende la entrega ó prestación efectiva de los servicios requeridos, abarcando procesos tales como la administración de la configuración de los equipos, administración de datos, instalaciones y operaciones, así como también el aseguramiento de la continuidad del procesamiento y la protección de la información, garantizando su integridad y confidencialidad.

Monitoreo: comprende la evaluación de la calidad con que se desarrollan los procesos y el cumplimiento de los requerimientos de control.

Objetivos de Control

A continuación se enuncian objetivos de control generales en tecnología de información, los que deberían ser evaluados durante el desarrollo de las auditorías:

Preservar los atributos de la información: asegurar que la información generada y almacenada mediante el empleo de tecnología conserva los atributos necesarios (confidencialidad, integridad, disponibilidad), para ser útil y confiable a la empresa.

Protección del patrimonio: apoyar las medidas de protección para los bienes e inversiones de la empresa mediante el uso adecuado de los recursos financieros destinados a TI, y el desarrollo de las actividades de TI con apego a la normativa legal, regulatoria y contractual que corresponda .

Proteger la infraestructura de tecnología: proteger todos los recursos que conforman la infraestructura tecnológica de la empresa para preservar su integridad y funcionalidad, asegurando una adecuada segregación de funciones y responsabilidades, la protección de los equipos e instalaciones contra riesgos, y mediante la identificación y corrección de posibles debilidades en los procesos informáticos.

Eficiencia operativa: emplear la tecnología de información como soporte a la eficiencia de la operación de la empresa, procurando la reducción de costos.

Adecuado uso de los recursos de TI: utilizar los recursos disponibles en forma legal, eficiente, efectiva y en un todo alineado con los objetivos de la empresa.

Brindar apoyo competitivo: proporcionar soporte tecnológico a la operación y a la toma de decisiones de la empresa procurando que los recursos de TI se

asignen de acuerdo con las prioridades de la empresa, considerando los objetivos de los negocios.

Mantener una cultura informática adecuada: el personal de la empresa debe contar con conocimiento de los beneficios, riesgos, costos y responsabilidades relacionados con la tecnología de información aplicable a su negocio, y debe utilizar los recursos disponibles en forma adecuada.

Mantener una cultura organizacional adecuada entre el personal de TI, alineada con la cultura de la empresa: elevados valores personales, motivación para trabajar, identificación con la empresa y proceso de mejora continua para los procesos informáticos.

Mantener la continuidad operativa: los equipos e instalaciones de TI deben estar protegidos contra riesgos previendo mecanismos de recuperación y procesamiento alternativo en caso de contingencias.

Metodología

Los estándares generales que guían la actividad de auditoría de sistemas son COSO y COBIT (ver anexos). Adicionalmente se aplican otros estándares específicos como por ejemplo ISO 17799 “Código de práctica para la administración de la seguridad de la Información” y normas NIST - National Institute of Standards and Technology, y “The Standard Of Good Practice for Information Security” del Information Security Forum).

Alcance de las auditorías

Algunos de los alcances la auditoría pueden ser:

- Control de la gestión de la Dirección Sistemas de Información: plan estratégico de sistemas, organización, políticas y procedimientos, segregación de funciones, administración de inversiones, proceso de evaluación de riesgos.
- Revisión general del proceso de administración de seguridad física y lógica: usuarios habilitados, derechos de acceso, proceso de actualización de usuarios y permisos, logs.
- Revisión del ciclo de vida de desarrollo de aplicaciones: comprende la revisión de la metodología seguida para la definición de requerimientos por parte del usuario, el análisis funcional, diseño, programación y pruebas, y la elaboración de la documentación de las aplicaciones.
- Control sobre las operaciones de los Centros de Procesamiento de Datos.
- Revisión del control interno y seguridad en software aplicativo: evaluación de los controles “embebidos” en las aplicaciones que garanticen la integridad y confidencialidad de la información. Control de las interfases con otros sistemas. Esquema de seguridad de la aplicación. Trazabilidad de las transacciones.
- Evaluación de la seguridad de las redes corporativas y departamentales.
- Revisión de la seguridad en sistemas operativos y bases de datos.

- Evaluación de aspectos de seguridad y control interno en E-business / Internet.
- Análisis de los planes de continuidad del negocio y de recuperación ante desastres.
- Revisión de las compras y contrataciones de materiales y servicios de sistemas de información.
- Administración de servicios prestados por terceros.
- Cumplimiento de normas y regulaciones gubernamentales, nacionales y extranjeras, como por ejemplo la ley Sarbanes Oxley, y la ley de Habeas Data (Argentina)

Funciones de la Auditoría de Sistemas de Información

La Auditoría de Sistemas de Información comprende el desarrollo de las siguientes funciones:

- Realización de proyectos propios de auditoría sistemas de información.
- Apoyo al resto de equipos de auditoría para optimizar el desarrollo de los proyectos y garantizar la cobertura de los riesgos de sistemas de información correspondientes al proceso que está siendo auditado en cada Unidad de Negocio del Grupo.
- Testing de la eficacia del funcionamiento de los controles existentes en el reporting financiero (Sarbanes Oxley Act).
- Colaboración con la Dirección de Sistemas de Información en distintas áreas, como por ejemplo: el diseño y modificaciones importantes de aplicaciones informáticas, efectuando recomendaciones sobre control interno y seguridad; participación en pruebas de planes de recuperación ante desastres, etc.
- Desarrollo de programas de trabajo utilizando técnicas CAATS (Computer Assisted Audit Technics).

Estas funciones se llevarán a cabo sobre el universo de unidades auditables y de acuerdo con la metodología COBIT. Dicho universo de unidades auditables se divide en:

- Cuentas de la Dirección Sistemas de Información.
- Grandes sistemas de información: estándar y desarrollos ad-hoc.
- Centros de Cómputos.
- Sociedades Participadas.
- Procesos de sistemas (por ej., Servicios de Desarrollo, Administración de BBDD, Administración de Seguridad lógica, etc.)

Plan Anual de auditoría

A efectos del diseño del plan anual de auditorías de sistemas de información, se tomará en cuenta un esquema de evaluación de riesgos en el que se considerarán aspectos tales como, riesgo inherente, riesgo de control interno, aspecto económico, resultado última auditoría, etc.

Anexos

El informe COSO

El informe **COSO** (acrónimo de COMMITTEE OF SPONSORING ORGANIZATIONS de 1992), fue resultado de un grupo de trabajo integrado por la Comisión Treadway con el objetivo de definir un nuevo marco conceptual de control interno capaz de integrar las diversas definiciones y conceptos que se utilizaban hasta ese momento.

Se define al “control interno” como un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Confiabilidad de la información financiera
- Cumplimiento de las leyes y normas aplicables

Un sistema de control interno consta de cinco componentes relacionados entre sí e integrados al proceso de Dirección:

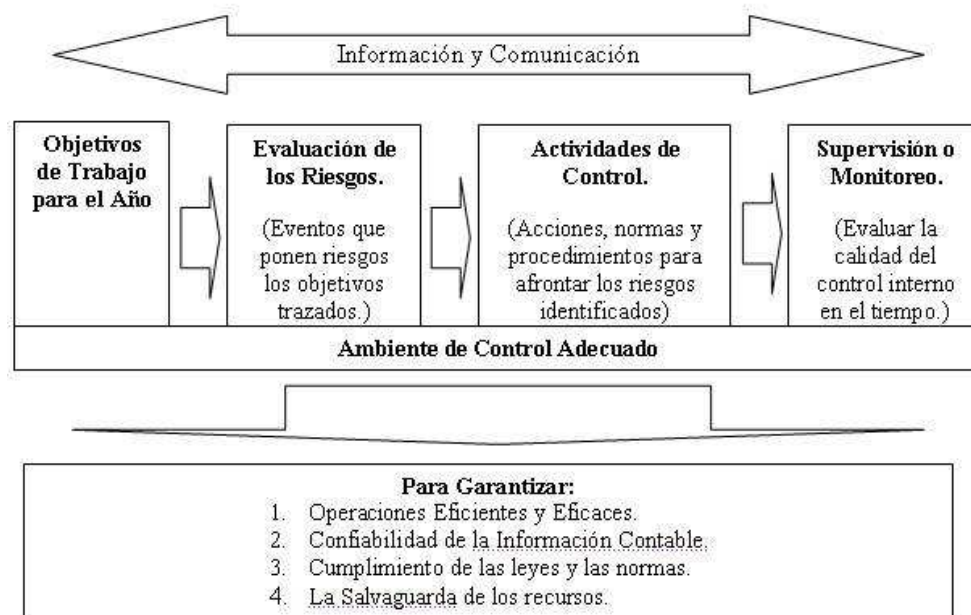
- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- supervisión

El sistema de control debe incorporarse de manera armónica con las actividades operativas de la organización. Esto ayuda a que se fomente la calidad de la delegación de poderes, se eviten pérdidas y haya una respuesta rápida ante los cambios.

Se presenta a continuación el denominado cubo COSO, donde se pueden visualizar los componentes del control interno y los objetivos.



El informe COSO plantea una estructura de control de la siguiente forma:



O sea, las empresas trazan objetivos anuales encaminados a la eficiencia y eficacia de las operaciones, la confiabilidad de la información financiera, el cumplimiento de las leyes y la salvaguarda de los recursos que mantiene. Identifican y evalúan los riesgos que ponen en peligro la consecución de estos objetivos; trazan actividades de control para minimizar el impacto de estos riesgos; y activan sistemas de supervisión para evaluar la calidad de este proceso. Todo lo anterior, con el sostén de un ambiente de control eficaz, y retroalimentado con un sistema de información y comunicación efectivo.

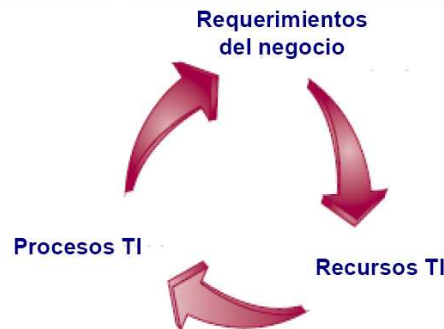
El control interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y a prevenir la pérdida de recursos, a la obtención de información financiera confiable y a reforzar la confianza en que la empresa cumple con la normativa aplicable.

Ahora bien, el sistema de control interno, no importa lo bien concebido que esté y lo bien que funcione, únicamente puede dar un grado de seguridad razonable, no absoluta, a la Dirección y al Consejo, en cuanto a la consecución de los objetivos de la entidad.

COBIT

COBIT (acrónimo de “Objetivos de Control para la Información y la Tecnología relacionada”), es un estándar de alto nivel orientado a la estrategia, con detalles precisos para el control de procesos, conjugando amplitud con profundidad.

El marco de trabajo COBIT se basa en el siguiente principio: proporcionar la información que la empresa requiere para lograr sus objetivos; la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información.



Criterios de Información de COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

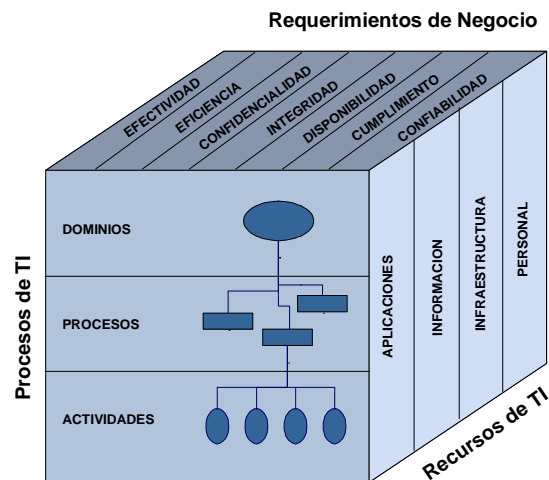
- La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La eficiencia consiste en que la información sea generada optimizando los recursos (más productivo y económico).
- La confidencialidad se refiere a la protección de información sensible contra revelación no autorizada. • La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.
- El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La confiabilidad significa proporcionar la información apropiada para que la gerencia administre la entidad y ejerce sus responsabilidades fiduciarias y de gobierno.

Recursos de TI

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (ej., implementando una cadena de suministro) que genere el resultado deseado (ej., mayores ventas y beneficios financieros).

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La información son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.
- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

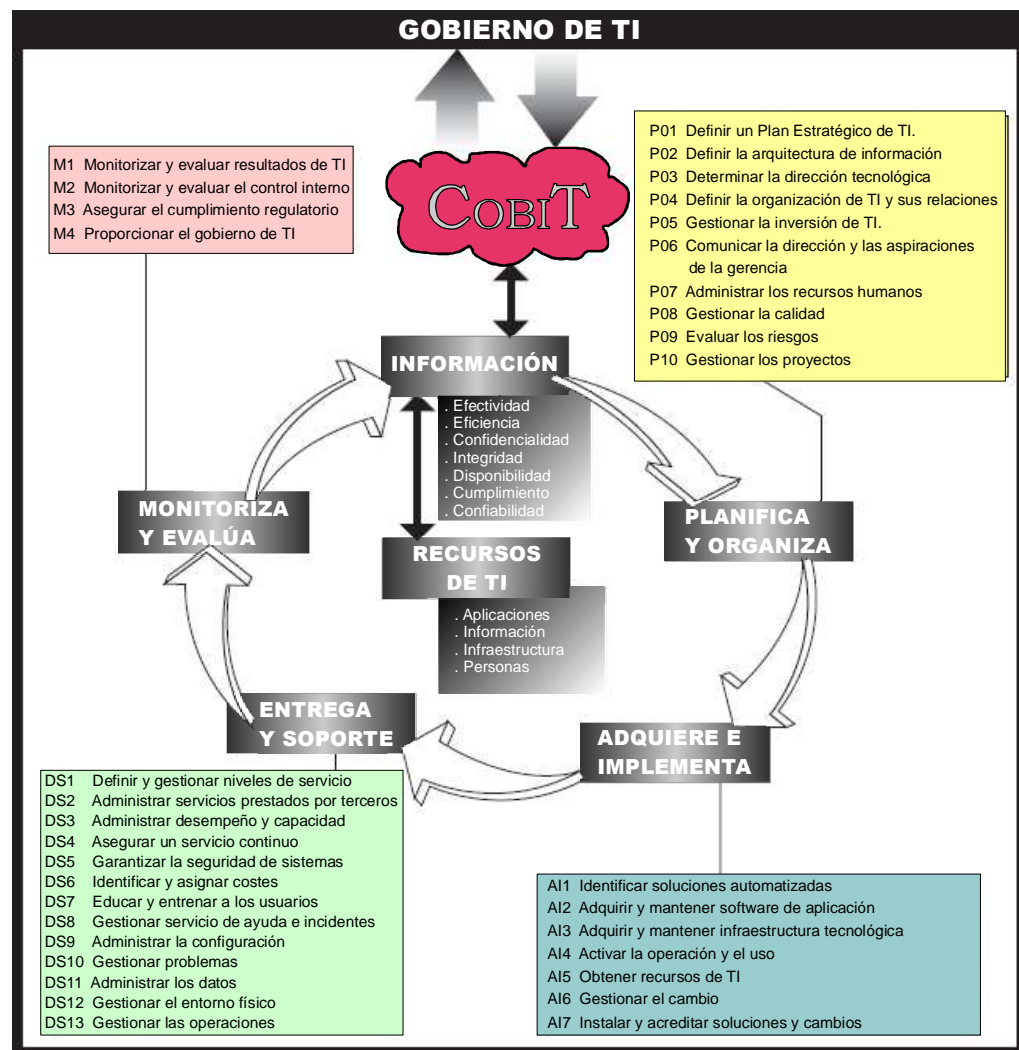


Procesos Orientados

COBIT define las actividades de TI en un modelo genérico de procesos, agrupados en cuatro dominios. Estos dominios son:

- PLANEAR y ORGANIZAR
- ADQUIRIR e IMPLEMENTAR
- ENTREGAR y DAR SOPORTE
- MONITOREAR y EVALUAR

Asimismo, dentro de cada dominio se definen procesos y actividades: un resumen de lo descrito puede apreciarse en el cuadro siguiente:



Las organizaciones encuentran razonable y conveniente usar **COBIT** porque está relacionado con otros marcos metodológico, tales como COSO, ITIL, ISO 17799 y CMM (Capability Maturity Model Integration).

COBIT puede coexistir y es compatible con las citadas metodologías. Está dirigido al control de procesos así como al control estratégico de TI en la empresa.

COBIT se ha convertido de facto en el estándar de control de las TI y como base para la función de gobierno de TI.