REVISTA CARIBEÑA DE CIENCIAS SOCIALES

**Octubre 2016 - ISSN: 2254-7630**

# EL CONTROL INTERNO PARA LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

**Byron Napoleón Cadena Oleas**[*]
Escuela Superior Politécnica de Chimborazo, Ecuador
napocadena@yahoo.com
**Irene García Rondón**[**]
Universidad de La Habana, Cuba
irene@fec.uh.cu

Para citar este artículo puede utilizar el siguiente formato:

Byron Napoleón Cadena Oleas e Irene García Rondón (2016): "El control interno para la gestión de tecnologías de la información", Revista Caribeña de Ciencias Sociales (octubre 2016). En línea: http://www.eumed.net/rev/caribe/2016/10/informacion.html

## Resumen

En la actualidad la información constituye uno de los principales recursos de una organización, el correcto proceso de datos que conlleve a generar información útil, permitirá a la administración a su vez llevar un adecuado proceso en la toma de decisiones. De aquí la necesidad de que el control como parte de proceso administrativo coadyuve a prevenir, detectar y corregir posibles irregularidades en la gestión de tecnologías de la información que pueda alterar el normal desarrollo de las actividades en una organización. En esta perspectiva en este artículo se realiza un análisis del control como parte del proceso administrativo, el control interno de tecnologías de la información y una visión de las normas generalmente aceptadas en lo que respecta a la gestión de tecnologías de la información.

---

[*] Ingeniero en Administración de Empresas
Máster en Informática Aplicada
Máster en Auditoría Integral
Aspirante a Doctor en Ciencias Económicas
Ponente en eventos científicos nacionales e internacionales
Autor de artículos científicos publicados en revistas indexadas

[**] Licenciada en Economías
Máster en Marketing y Diseño Comercial
Doctora en Ciencias Económicas
Ponente en eventos científicos nacionales e internacionales
Autor de artículos científicos publicados en revistas indexadas

**Palabras clave:** Control Interno de Tecnologías de la información, Tecnologías de la Información.

**Abstract**

At present the information is one of the main resources of an organization, proper data processing lead to generate useful information, will the administration in turn lead a proper process in decision-making. Hence the need for control as part of the administrative process contributes to prevent, detect and correct irregularities in the management of information technologies that can alter the normal development of activities in an organization. In this perspective in this article is an analysis of the control as part of the administrative process, internal control of information technology and a vision of the generally accepted standards regarding the management of information technology.

**Keywords:** Internal Control Information Technology, Information Technology.

## INTRODUCCIÓN

Como control se debe entender aquellos procedimientos destinados a evaluar el rendimiento real, comparar ese rendimiento con los objetivos fijados, o corregir las diferencias entre los resultados y los objetivos.[1]

EL control como parte de proceso administrativo es esencial, ya que de no existir, no podría conocerse si lo planificado, organizado y ejecutado se ha realizado correctamente, y por tanto ha funcionado bien.

Siendo el Control el tema fundamental de este artículo, se realiza un análisis inicialmente como elemento de la gestión empresarial, considerando lo que manifiesta Mairena Romero, quien, en un informe presentado analiza el control como una fase del proceso administrativo, analizando las diferentes definiciones empleadas por administradores como Stoner, Fayol, Robbins, entre otros; estudiando su importancia, su clasificación y las áreas de desempeño. El objetivo principal de su trabajo es estudiar el control como elemento clave de la administración, que permite detectar errores a tiempo y corregir fallas en su debido momento, aplicando así los mecanismos de control adecuado para cada caso.

[1] JURAN, Joseph M. Juran on Leadership for Quality: An executive handbook. New York: Free Press, 1989, p. 145.

## 1. EL CONTROL COMO FASE DEL PROCESO ADMINISTRATIVO[2]

Las organizaciones, ya sean formales o informales, tienen como propósito alcanzar una meta, a través de diversos planes establecidos y a través de los recursos que poseen. Es en ese momento cuando nace el sentido de la administración, es decir, aquel proceso que llevan a cabo los miembros de una organización para lograr alcanzar sus objetivos.

La administración en sentido formal, es aquella que se realiza en una empresa. Posee cuatro funciones específicas que son: la planificación, la organización, la dirección y el control; estas en conjunto se conocen como proceso administrativo y se puede definir como las diversas funciones que se deben realizar para que se logren los objetivos con la óptima utilización de los recursos.

**Definición de control**

El control es la función administrativa por medio de la cual se evalúa el rendimiento. Para Robbins (1996: 654) el control se define como "el proceso de regular actividades que aseguren que se están cumpliendo como fueron planificadas y corrigiendo cualquier desviación significativa".

Sin embargo Stoner (1996: 610) lo define de la siguiente manera: "El control administrativo es el proceso que permite garantizar que las actividades reales se ajusten a las actividades proyectadas".

Mientras que para Fayol, citado por Melinkoff (1990: 62), el control "Consiste en verificar si todo se realiza conforme al programa adoptado, a las órdenes impartidas y a los principios administrativos…Tiene la finalidad de señalar las faltas y los errores a fin de que se pueda repararlos y evitar su repetición".

Analizando todas las definiciones citadas notamos que el control posee ciertos elementos que son básicos y esenciales a considerar:

- En primer lugar, se debe llevar a cabo un proceso de supervisión de las actividades realizadas.
- En segundo lugar, deben existir estándares o patrones establecidos para determinar posibles desviaciones de los resultados.
- En un tercer lugar, el control permite la corrección de errores, de posibles desviaciones en los resultados o en las actividades realizadas.

[2] ROMERO, Mairena. El control como fase del proceso administrativo.

- Y en último lugar, a través del proceso de control se debe planificar las actividades y objetivos a realizar, después de haber hecho las correcciones necesarias.

En conclusión se define el control como la función que permite la supervisión y comparación de los resultados obtenidos contra los resultados esperados originalmente, asegurando además que la acción dirigida se esté llevando a cabo de acuerdo con los planes de la organización y dentro de los límites de la estructura organizacional.

**Importancia del control dentro el proceso administrativo**

El control se enfoca en evaluar y corregir el desempeño de las actividades de los subordinados para asegurar que los objetivos y planes de la organización se están llevando a cabo.

De aquí puede deducirse la gran importancia que tiene el control, pues es solo a través de esta función que se logrará precisar si lo realizado se ajusta a lo planeado y en caso de existir desviaciones, identificar los responsables y corregir dichos errores.

Sin embargo, es conveniente recordar que no debe existir solo el control a posteriori, sino que, al igual que el planteamiento, debe ser, por lo menos en parte, una labor de previsión. En este caso se puede estudiar el pasado para determinar lo que ha ocurrido y porque los estándares no han sido alcanzados; de esta manera se puede adoptar las medidas necesarias para que en el futuro no se cometan los errores del pasado.

Además, siendo el control la última de las funciones del proceso administrativo, esta cierra el ciclo del sistema al proveer retroalimentación respecto a desviaciones significativas contra el desempeño planeado. La retroalimentación de información pertinente a partir de la función de control puede afectar el proceso de planeación.

**Áreas de desempeño del control**

El control tiene muchas áreas de desempeño, todos los departamentos en los que se divide una organización necesitan ser controlados, por lo tanto, las áreas de desempeño dependen de los departamentos existentes en la empresa.

Entre las áreas del control dentro de una organización se tienen:

- Dentro del área de producción se encuentra el control de calidad. Este consiste en la verificación de la calidad (peso, resistencia, consistencia,

color, sabor, entre otros) para asegurar que cumplen con algunas normas preestablecidas. Es posible que este sea necesario en uno o varios puntos, desde el inicio, proceso y todas las etapas hasta el producto final. La detección temprana de una parte o proceso defectuoso puede ahorrar el costo de más trabajo en el producto.

- También existe el control de información. Para contribuir a la buena toma de decisiones del administrador se debe tener una información precisa, oportuna y completa. Para obtenerla de esta manera, la organización debe poseer sistemas tecnológicamente actualizados y eficaces ya que estos pueden contribuir a corregir un problema con mayor prontitud.

  Por lo que se puede decir que el control de información consiste en verificar que esta información sea veraz y comprobable, que permita a los administradores ser más eficientes y efectivos en la toma de decisiones.
- Dentro de una empresa debe existir otro tipo de control, como es el control de costo. Una de las labores de un buen administrador está el ahorrar en costos, es decir, no acarrear elevados gastos en la producción. El control de costo consiste en buscar la causa por la que se presentan desviaciones en los costos estándar por unidad. El gerente puede hacerse diferentes preguntas: ¿Se han incrementado los precios de los materiales?, ¿Se utiliza la mano de obra de manera eficiente?, ¿Necesitan los empleados capacitación adicional? La alta administración debe identificar en qué puntos radica el control.
- Además de los controles antes mencionados, podemos hablar del control de correspondencia. En toda empresa se redactan documentos legales que, en algunos casos, van dirigidos a otras organizaciones nacionales e internacionales, mayormente redactado por el staff legal de la compañía. Este tipo de control consiste en verificar cuidadosamente estos documentos, debido a que estas declaraciones llevan consigo mucho prestigio y autoridad de la organización.

## 2. EL CONTROL INTERNO DE TECNOLOGÍA DE LA INFORMACIÓN

### Definición de control interno

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que

puedan afectar al funcionamiento de un sistema para lograr o conseguir sus objetivos".[3]

El control interno será responsabilidad de cada institución y de las personas que tengan como finalidad crear las condiciones para el ejercicio del control.

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos. Constituyen componentes del control interno el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación, y el seguimiento.

El control interno está orientado a promover eficiencia y eficacia de las operaciones de una organización y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control.

**Objetivos del control interno**

El control interno de las instituciones, organizaciones para alcanzar la misión institucional, deberá contribuir al cumplimiento de los siguientes objetivos:

- Promover la eficiencia, eficacia y economía de las operaciones bajo principios éticos y de transparencia.
- Garantizar la confiabilidad, integridad y oportunidad de la información.
- Cumplir con las disposiciones legales y la normativa de la entidad para otorgar bienes y servicios de calidad.
- Proteger y conservar el patrimonio contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

**Responsables del control interno**

El diseño, establecimiento, mantenimiento, funcionamiento, perfeccionamiento, y evaluación del control interno es responsabilidad de la máxima autoridad, de los directivos y demás servidoras y servidores de la entidad, de acuerdo con sus competencias.

Los directivos, en el cumplimiento de su responsabilidad, pondrán especial cuidado en áreas de mayor importancia por su materialidad y por el riesgo e impacto en la consecución de los fines institucionales. Las servidoras y servidores de la entidad, son responsables de realizar las acciones y atender los

[3] Contraloría General del Estado. Normas de Control Interno. 2009.

requerimientos para el diseño, implantación, operación y fortalecimiento de los componentes del control interno de manera oportuna, sustentados en la normativa legal y técnica vigente y con el apoyo de la auditoría interna como ente asesor y de consulta, si es que esta existiera.

En las organizaciones: La máxima autoridad, los directivos y demás servidoras y servidores, según sus competencias, dispondrán y ejecutarán un proceso periódico, formal y oportuno de rendición de cuentas sobre el cumplimiento de la misión y de los objetivos institucionales y de los resultados esperados.

La rendición de cuentas es la obligación que tienen todas las servidoras y servidores de responder, reportar, explicar o justificar ante la autoridad, los directivos, la ciudadanía y/o accionistas, por los recursos recibidos y administrados y por el cumplimiento de las funciones asignadas. Es un proceso continuo que incluye la planificación, la asignación de recursos, el establecimiento de responsabilidades y un sistema de información y comunicación adecuado.

Se deben presentar informes periódicos de su gestión ante la alta dirección para la toma de decisiones, en los que se harán constar la relación entre lo planificado y lo ejecutado, la explicación de las variaciones significativas, sus causas y las responsabilidades por errores, irregularidades y omisiones.

**Tipos de control interno de TI**

De acuerdo al momento en que se realiza un control, estos se clasifican en:

1. Preventivo
2. Detectivo
3. Correctivo

**Preventivos**

Intentan evitar que ocurra el error. Se utilizan en las primeras etapas del flujo de datos de un sistema. Por ejemplo: el tener buenos formularios de entrada de datos ayuda a evitar que se produzcan errores en la captura, o un software de seguridad que impida los accesos no autorizados al sistema.

Son controles generales. Este hecho les hace inmunes a los cambios, pero posibilita la aparición de errores de muchas clases. Por ejemplo: la separación de tareas no cambia aunque las tareas se realicen de diferente manera, pero no garantiza que las tareas estén bien ejecutadas. El hecho de tener buenos formularios no impide que se cometan errores en la captura.

En resumen los controles preventivos tratan de evitar el hecho.

### Detectivos

Cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Identifican los errores después de que éstos ocurran. Tienden a ser controles específicos, utilizados en una fase posterior en el tiempo a los controles preventivos. El hecho de ser específicos hace que sean dependientes de los cambios. Ejemplo: programas de validación de entrada de datos, o el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

### Correctivos

Facilitan la puesta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad. Estos controles tratan de garantizar que se corrigen los errores detectados.

## 3. NORMAS DE CONTROL INTERNO PARA LA TECNOLOGÍA DE LA INFORMACIÓN

Como ya se mencionó, el control interno es fundamental en toda organización, éste ayuda a prevenir o corregir errores cometidos en los procesos de manejo de la información.

Para llevar a cabo un proceso de control interno, es necesario, que las situaciones a evaluar o controlar, sean comparadas con algo; este “algo” podría ser una norma, ley, reglamento, estatuto, disposición, resolución, etc., esto nos dará la medida para poder determinar el grado de cumplimiento de las tareas asignadas a un sistema de información.

En el concierto nacional e internacional han habido instituciones que se han preocupado por normar y estandarizar el uso de la tecnología de la información para llevar a cabo el proceso de datos en una organización, por ejemplo: ISACA (Information Systems Audit and Control Association) con la expedición de las Normas Cobit, ISO (International Estándar Organization) con la promulgación de las Normas ISO 177990, la CGE (Contraloría General de Estado) con las Normas de Control Interno para Tecnología de la Información.

A continuación daremos un vistazo a cada una de ellas, de tal manera que podamos tener una idea global de cómo es que estas organizaciones abordan los temas de control sobre la Gestión de Tecnologías de la información.

**Normas de la Contraloría General del Estado del Ecuador**

Este conjunto de normas, sirven como marco de referencia para las instituciones y organizaciones a nivel público, su aplicación son de carácter obligatorio en el caso del Ecuador, se encuentra categorizada en 5 componentes que definen una serie de criterios que se deben cumplir para salvaguardar los recursos de una organización.

El esquema general de las normas de control interno es:

100.- Normas generales

200.- Ambiente del Control

300.- Evaluación de Riesgos

400.- Actividades de Control

- 401.- Generales
- 402.- Administración Financiera – PRESUPUESTO
- 403.- Administración Financiera – TESORERÍA
- 404.- Administración Financiera – DEUDA PÚBLICA
- 405.- Administración Financiera – CONTABILIDAD GUBERNAMENTAL
- 406.- Administración Financiera – ADMINISTRACIÓN DE BIENES
- 407.- Administración del Talento Humano
- 408.- Administración de Proyectos
- 409.- Gestión Ambiental
- 410.- Tecnología de la información

500.- Información y comunicación

600.- Seguimiento

Como podemos observar, en el grupo 400, subgrupo 410 y en el grupo 500, se encuentran las normas para la evaluación del control interno para la Gestión de Tecnología de la Información.

Revisando el subgrupo 410 correspondiente a Tecnología de la Información, se describen 17 normas que permiten llevar a cabo el control de Tecnologías de la Información en las instituciones públicas del Ecuador; sin embargo, se considera también que para las instituciones privadas se convierte en un referente para normar su comportamiento en cuanto al manejo de la información.

Estas normas son:

410-01 Organización informática;

410-02 Segregación de funciones;

410-03 Plan informático estratégico de tecnología;
410-04 Políticas y procedimientos;
410-05 Modelo de información organizacional;
410-06 Administración de proyectos tecnológicos;
410-07 Desarrollo y adquisición de software aplicativo;
410-08 Adquisiciones de infraestructura tecnológica;
410-09 Mantenimiento y control de la infraestructura tecnológica;
410-10 Seguridad de tecnología de información;
410-11 Plan de contingencias;
410-12 Administración de soporte de tecnología de información;
410-13 Monitoreo y evaluación de los procesos y servicios;
410-14 Sitio web, servicios de internet e intranet;
410-15 Capacitación informática;
410-16 Comité informático, y
410-17 Firmas electrónicas.

**ISO 17799**

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de la información en una organización. Esta surgió de la norma británica BS 7799, la norma ISO 17799 como ya se dijo ofrece instrucciones y recomendaciones para la administración de la seguridad.

Existen multitud de estándares aplicables a diferentes niveles pero ISO 17799 como estándar internacional, es uno de los más extendidos y aceptados.

**Objetivo de la norma ISO 17799**

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

**Sistema de Gestión de la Seguridad de la Información (SGSI)**

En la actualidad las empresas son conscientes de la gran importancia que tiene para el desarrollo de sus actividades el hecho de proteger de forma adecuada la información que poseen y especialmente aquella que les sirve para realizar correctamente su actividad de negocio. El poder gestionar bien la seguridad de la información que manejan no sólo permitirá garantizar, de cara a la propia

organización, que sus recursos están protegidos -asegurando la confidencialidad, integridad y disponibilidad de los mismos- sino que de cara a los posibles clientes les aportará un grado de confianza superior al que puedan ofrecer sus competidores, convirtiéndose en un factor más de distinción en el competitivo mercado en el que comercia la empresa.

La norma ISO 17799 recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI), es un conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.

### Gestión de la Seguridad de Información con ISO

La norma ISO 17799:2005 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. **Políticas de seguridad:** el estándar define como obligatorias las políticas de seguridades documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.
2. **Aspectos organizativos:** establece el marco formal de seguridad que debe integrar una organización.
3. **Clasificación y control de activos:** el análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.
4. **Seguridad ligada al personal:** contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información. Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, o sea, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.
5. **Seguridad física y del entorno:** identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

6. **Gestión de comunicaciones y operaciones:** integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
7. **Control de accesos:** habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.
8. **Desarrollo y mantenimiento de sistemas:** la organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.
9. **Gestión de continuidad del negocio:** el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.
10. **Cumplimiento o conformidad de la legislación:** la organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

De estos diez dominios nombrados se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de inspecciones) y 127 o más controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). Ambos, se encuentran destinados a dotar y esparcir Seguridad a la Información en el “ambiente digital”, a través de numerosas auditorías, consultorías y/o paradigmas.

Cada una de las áreas constituye una serie de observaciones que serán seleccionadas dependiendo de las derivaciones obtenidas en los análisis de riesgos, conjuntamente, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle. Por eso, es aplicable a toda organización, independientemente, de su tamaño o sector de negocio; siendo un argumento fuerte y dinámico para los detractores de la norma

y un “conjunto de instrumentos” flexibles a cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la IT.

**COBIT**

Resulta imposible hablar de CobiT sin citar a ISACA (Information Systems Audit and Control Association), la entidad en cuyo seno vieron la luz los primeros “Objetivos de Control” (www.isaca.org/cobit), y a ITGI (IT Governance Institute), el organismo que hoy día se ocupa de su puesta al día (www.itgi.org/cobit).

La Asociación para el Control y la Auditoría de los Sistemas de Información (ISACA) es, actualmente, la organización profesional de referencia, a nivel mundial, en el ámbito del Control en la Gestión de Tecnologías de la Información, que agrupa a más de cincuenta mil miembros en ciento cuarenta países. Cuenta, asimismo, con una red de ciento setenta capítulos -tres de ellos en España: Madrid, Barcelona y Valencia-, uno en Ecuador en Quito.

Por su parte, el Instituto para el Gobierno de TI (ITGI) -apéndice de ISACA- es la entidad encargada de las actividades de investigación de la asociación. Nació tras la segunda edición de CobiT, en 1998, y desde ese momento, ha venido encargándose de su continua actualización y publicación.

La creciente complejidad de las Tecnologías de la Información, la dependencia de ellas por parte de las organizaciones y las expectativas que la alta dirección de estas últimas tiene respecto de las citadas tecnologías, conducen a la necesidad de contar con un marco genérico de control, gestión y gobierno de TI -independiente de la tecnología-, que garantice que se alcanzarán los objetivos de la organización; reduciendo los riesgos -derivados de las propias TI- y generando valor para la entidad.

En ese contexto, y con el fin de cubrir esa necesidad, aparece CobiT, pudiendo decirse de él que:

- Es un modelo de referencia para establecer controles sobre las Tecnologías de la Información y una guía para realizar auditorías de esos mismos controles.
- Es un código de buenas prácticas para la gestión de la seguridad de los activos de información.
- Y, sobre todo, es hoy en día, el modelo para implantar el Gobierno de TI, que ayuda a las organizaciones a alcanzar sus objetivos, facilitando la

comprensión y la gestión de los riesgos y del valor aportado por la información y sus tecnologías afines.

Más allá de esas definiciones, CobiT se materializa en una colección de referencias documentales, que tradicionalmente ha estado compuesta por los siguientes volúmenes:

- Resumen ejecutivo. Ofrece una sinopsis de los conceptos CobiT.
- Marco de referencia. Presenta la estructura CobiT de cuatro dominios de TI (PO -Planificación y Organización-; AI -Adquisición y Construcción/Implantación-; DS -Entrega y Soporte-; y ME -Supervisión y Evaluación-), junto con sus treinta y cuatro procesos de TI normalizados, asociados.
- Objetivos de control. Muestra los objetivos de controles detallados, correspondientes a cada uno de los procesos de TI u objetivos de control de alto nivel.
- Directrices de auditoría. Constituyen una referencia empleada para la revisión de los anteriores controles.
- Directrices de gestión. Desarrolladas para orientar a la Dirección en el Gobierno de TI, proporcionándole herramientas para evaluar y medir la capacidad de la entidad en cada uno de los procesos TI definidos por CobiT, dentro de un modelo de madurez de seis niveles.
- Herramientas de implantación. Incluyen una guía para la puesta en marcha de CobiT dentro de la organización.

La última edición de CobiT, aparecida hace unos meses, opta por un empaquetado distinto, en el que se ha reducido volumen, integrando y sintetizando, en un único documento, el resumen ejecutivo, el marco de referencia y los objetivos de control/directrices de gestión, que se han fusionado en un bloque común.

Puede decirse, de este modo, que CobiT 4.0 no ha sustituido a su antecesora, al menos a corto plazo, sino que ha supuesto una mera evolución de algunos de sus componentes básicos.

**Del control interno al Gobierno de TI**

Esa evolución a que se hacía referencia en el apartado anterior ha sido una característica de CobiT desde el primer momento y ha ido paralela a la propia

evolución de ISACA o, más concretamente, a la de su estrategia como organización.

La publicación de los “Objetivos de Control” originales, en 1992, y las posteriores ediciones de CobiT (primera, en 1996, y segunda, en 1998) marcaron una época en la que la orientación principal de la asociación era el Control Interno y la Auditoría de Sistemas, como tales, manteniendo una clara fidelidad a los orígenes de la entidad.

La edición tercera -la más consolidada en el tiempo, hasta la fecha-, publicada en 2000, vino acompañada, por vez primera, de las “Directrices de Gestión”, marcando un nuevo alcance, hacia la gestión de las TI.

Es propio de esta época, asimismo, el leve giro que, siguiendo la coyuntura, da la asociación hacia el “nuevo” campo de la seguridad. Como prueba de ello: la publicación de “Information Security Governance: Guidance for Boards of Directors and Executive Management” (2001); el establecimiento de la certificación CISM (2002) -Certified Information Security Manager: programa de certificación para responsables de la Gestión de la Seguridad de la Información, que cuenta ya con más de seis mil profesionales certificados desde su puesta en marcha en el año 2002, www.isaca.org/cism-; la aparición del producto derivado “CobiT Security Baseline” (2004); y el proyecto CobiT Mapping (2004-05), del que saldrían tres publicaciones en las que se compara CobiT con otras normas relativas a la Seguridad de la Información.

La actual edición 4.0 (2005) supone la culminación de la estrategia de ISACA -iniciada con la creación del ITGI, en 1998- de convertirse en el referente en Gobierno de TI, cuyo reflejo se materializa en la publicación de un elevado número de documentos, tales como: “IT Governance Executive Summary”, “IT Strategy Committee”, “Board Briefing on IT Governance” (2001, 2003), “IT Governance Implementation Guide” (2003), “IT Alignment: Who is in charge?” (2005), “Governance of Outsourcing” (2005), “The CEO’s Guide to IT Value at Risk” (2005) y toda la nueva familia Val IT, de productos complementarios a CobiT, creada en 2005.

Paralelamente, ha habido, en los últimos tiempos, una intención de simplificación y acercamiento de CobiT a los usuarios, mediante iniciativas como CobiT Quickstart, CobiT On-line, CobiT in Academia, etc., así como otros cursos y

material puestos a disposición por ISACA/ITGI para la difusión del modelo, entre los que destaca el inicio de las CobiT User Conventions.

Si algo se le ha criticado a CobiT, ha sido sus carencias en el ámbito del cumplimiento jurídico, debido a su carácter internacional.

**CONCLUSIÓN**

La Máxima autoridad tiene como responsabilidad en una organización el asegurar la implementación de un sistema de control interno, que permita que la gestión de tecnologías contribuya a la generación de información útil para la toma de decisiones. Es importante que toda organización tenga una política en que se defina un marco de referencia o normatividad que guie los procesos para el manejo adecuado de los datos e información y que brinde razonable seguridad tanto a usuarios internos como externos. La definición de Indicadores en cuanto a la gestión de tecnologías de la información, se vuelve una condición en la que todas las empresas tengan la capacidad de poder determinar el grado de eficacia y eficiencia con que los sistemas de información contribuyen al cumplimiento de los objetivos organizacional.

**BIBLIOGRAFÍA**


- Amaru Maximiano, A. C. (2009). Fundamentos de Administración: teoría general y proceso administrativo. Editorial: Pearson Educación.
- Bernal Torres, C. S., & Sierra Arango, H. D. (2008). Proceso Administrativo para las Organizaciones del Siglo XXI. Editorial: Pearson Educación.
- Bonilla Torres, E. M. (2012). Procesos Administrativos. Editorial: ESPOCH.
- Cabrera Silva, & Armando Augusto. (2009). Organización, Dirección y administración de centros de cómputo. UTPL.
- Contraloría General del Estado. (2009). Normas de Control Interno. Tecnologías de la Información. Recuperado de www.contraloria.gob.ec/normativividad_vigente.asp
- Daft Richard L., & Marcic Dorothy. (2010). Introducción a la Administración. Editorial: Cengage Learning.
- Ernst, & Young. (2010). Evaluación del Control Interno. Consideraciones para evaluar el control interno a nivel de Empresa. Revista: Assurance and Advisory Business Services.

- Hernández, & Rodríguez Sergio. (2012). Administración: Teoría, Proceso, Áreas Funcionales y Estrategias para la Competitividad. Tercera Edición. Editorial: McGraw-Hill.
- Information Security Inc. Education Center. (2006). Seguridad de la Información. Norma ISO 17799/ISO 27001. Implementación Práctica. Recuperado de www.i-sec.org
- Information technology Governance Institute. (2007). Cobit – Marco de Trabajo. Recuperado de www.itgi.org
- Information technology Governance Institute. (2007). Cobit – Objetivos de control. Recuperado de www.itgi.org
- Instituto Argentino de Normalización. (2002). Tecnología de la Información. Código de práctica para la administración de seguridad de la información. Norma IRAM-ISO IEC 17799. Documento de Estudio.
- Javier F. Kuong. Seguridad, Control y Auditoria de las Tecnologías de Información. Ed. MASP. 2008.
- Munch Galindo, L. (2010). Administración: Gestión Organizacional, enfoques y proceso administrativo. Editorial: Prentice Hall.
- Munch Galindo, L. (2007). Administración: Escuelas, Proceso Administrativo, Áreas Funcionales y Desarrollo Emprendedor. Editorial: Pearson Educación.
- RALPH, Stair. Principios de sistemas de información. 9na. Edición. 2011
- Ramírez Cardona, C. (2009). Fundamentos de Administración. Tercera Edición. Editorial: Ecoe Ediciones.
- Romero, M. (2004). El control como fase del proceso administrativo, Recuperado de www.tablero-decomando.com