QUIPUKAMAYOC Revista de la Facultad de Ciencias Contables
Vol. 22 N.º 42 pp. 129-135 (2014) UNMSM, Lima - Perú
ISSN: 1560-9103 (versión impresa) / ISSN: 1609-8196 (versión electrónica)

COBIT: UN MARCO DE TRABAJO PARA EL DESARROLLO DE UNA AUDITORÍA EFICAZ

COBIT: A FRAME WORK FOR DEVELOPING AN EFFECTIVE AUDIT

Carlos Alberto Pastor Carrasco*
Docente Asociado de la Facultad de Ciencias Contables
Carmen Isabel Villanueva Ipanaqué**
Docente Auxiliar de la Facultad de Ciencias Contables
Universidad Nacional Mayor de San Marcos-UNMSM / Lima-Perú
Lucía Lorena de Santiago Gonzales***
Docente de la Universidad de Guadalajara / México

[Recepción: Setiembre de 2014/ Conformidad: Octubre 2014]

RESUMEN

El desarrollo de la tecnología es percibida en forma global, como un disparador de cambios permanentes en el ambiente de negocios. Sin embargo, existe una idea primordial que aparece inmóvil contra esta fuerza tecnológica que implica que las organizaciones que sobreviven, son aquellas que entregan más valor a sus clientes.

La función de la auditoría continúa proporcionándonos servicios de aseguramiento, tanto a clientes internos como externos. Dado que el empleo de la tecnología impacta la forma de hacer negocios, debe haber formas efectivas y sencillas para llevar a cabo la evaluación de los controles que deben existir para garantizar dicho servicio.

El objetivo principal de la investigación es *determinar qué metodología debería de emplearse para obtener un adecuado control de la tecnología de la información, riesgos y vulnerabilidades para el proceso de una auditoría eficaz.*

Nuestra hipótesis principal es: El COBIT desarrollado por ISACA es una metodología que debería de emplearse para obtener un adecuado control de la tecnología de la información, riesgos y vulnerabilidades para el proceso de una auditoría eficaz.

De la revisión e investigación realizadas, concluimos que con el COBIT, los auditores de tecnología de información contarán con una herramienta adecuada que les permitirá atender las nuevas necesidades de las organizaciones.

Palabras clave:
Auditoría; riesgos; vulnerabilidades; COBIT.

ABSTRACT

The development of technology is perceived globally as a trigger for permanent changes in the business environment. However, there is one overriding idea that appears immobile against this technological strength which implies that organizations that survive are those that provide more value to their customers.

The role of the audit continues to provide assurance services to both internal and external customers. Since the use of technology impacts the way we do business, there must be effective and simple ways to carry out the evaluation of the controls that must exist to ensure that service.

The main objective of the research is to determine which methodology should be used to achieve adequate control of information technology, risks and vulnerabilities for effective audit process.

Our main hypothesis is: The COBIT developed by ISACA is a methodology that should be used to achieve adequate control of information technology, risks and vulnerabilities for effective audit process.

From the review and research conducted, we conclude that the COBIT, auditors information technology will have a suitable tool that will allow them to meet the new needs of organizations.

Keywords:
Audit; risks; vulnerabilities; COBIT.

* Doctor en Ciencias Contables y Empresariales. Contador Público. Email: cpastorc@unmsm.edu.pe
** Magíster en Auditoría - UNMSM. Contadora Pública. Email: cvillanuevai@unmsm.edu.pe
*** Magíster en Impuestos. Licenciada en Contaduría Pública. Email: lucy_desantiago@hotmail.com

INTRODUCCIÓN

Las organizaciones que sobreviven, son aquellas que entregan más valor a sus clientes, el empleo de la tecnología impacta la forma de hacer negocios, y la función de auditoría continúa proporcionándonos servicios de aseguramiento, tanto a clientes internos como externos.

Existe un gran interés en el medio por identificar los estándares internacionales que serán utilizados en las empresas tanto públicas como privadas.

Los objetivos específicos serán:

- Verificar cómo podrían asegurarse las organizaciones que realicen una auditoría de sistemas, cubriendo adecuadamente las necesidades del cliente, en forma eficiente y oportuna, dentro del presupuesto contemplado.
- Determinar cómo ha evolucionado el enfoque en auditoría de tecnologías de Información, a fin de determinar riesgos y vulnerabilidades para el proceso de una auditoría eficaz.

La presente investigación, se justifica por el uso que deben emplear los auditores en el desarrollo de sus actividades de una auditoría de sistemas o auditoría de tecnología de información. Asimismo, la administración debe tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

EVOLUCIÓN DE LA AUDITORÍA

La auditoría se inicia desde el punto de vista de Finanzas y Contabilidad, revisando todas las operaciones financieras que ocurrían en la empresa. Posteriormente, se amplía el enfoque hacia la Economía, la eficiencia y la eficacia de las operaciones de la empresa, conocida como auditoría operativa o transaccional. En la actualidad, lo que la auditoría busca es la alineación con la visión y misión empresarial. Esto nos lleva hacia el concepto de la auditoría de sistemas o auditoria de las tecnologías de información.

La primera pregunta que realiza toda organización preocupada por su desarrollo empresarial es ¿Cómo implementar una Auditoría de TI que agregue valor a la organización? Las respuestas serían:

a) Realizar un cambio del enfoque tradicional al momento de realizar la auditoría.
b) La misión principal de la auditoria sería reportar los riesgos y los controles para mitigarlos.
c) Finalmente, la auditoría debe aplicar las mejores prácticas disponibles en el mercado.

Cambio del enfoque tradicional al realizar la auditoría

Auditoría tradicional

Después del establecimiento inicial de un acuerdo contractual entre el auditor y el auditado, un trabajo de auditoría generalmente procede con una evaluación de riesgos y la formulación de un plan de auditoría para delinear el alcance y los objetivos de la auditoría. Después de esto, los auditores recogen y analizan la evidencia de auditoría y se forman opiniones relativas a los controles internos; así como, la fiabilidad de la información proporcionada por la dirección. Al concluir, los auditores presentan un informe formal de opinión.

De hecho, este enfoque refleja la metodología del siglo XX por el que hay altos costos y demoras significativas asociadas con la recolección de información, procesamiento y presentación de informes. Sin embargo, estos costos históricos y los retrasos a menudo no son la norma hoy en día. Muy probablemente, en el mundo de los negocios actual, las transacciones se introducen a menudo y se agregan de manera que puedan ofrecer una respuesta inmediata acerca de las partes interesadas pertinentes. Por otra parte, los académicos y los profesionales reconocieron este cambio de información y desarrollaron numerosas soluciones que reflejaban adecuadamente el entorno empresarial actual.

Auditoría proactiva

Los procesos se efectúan en forma simultánea, empleado para ello, tecnologías disponibles, tales como:

- Internet/Conexiones Web
- Sistemas
- Databases & Apps
- Network Devices
- Non.IT devices

En este enfoque se incluye el análisis de riesgo en el negocio como punto importante en su revisión.

La auditoría debe tener como misión reportar los riesgos y los controles para mitigarlos

Para ello, debe confeccionar un plan estratégico que incluye una cuidadosa consideración acerca de los problemas de la resistencia al cambio, los costos que representa dicha tecnología y las utilidades que se lograrán, alcance del proyecto, y asegurarse que su formación debería dar lugar a resultados más favorables. Como mínimo, deber aplicarse las Técnicas de Auditoría asistida por el computador (Computer Assisted Audit Techniques - CAAT), que tienen el potencial de servir como un mecanismo de transición entre la auditoría manual y el final de la auditoría futura. Si se implementan y se utilizan según lo previsto, se realizarán beneficios significativos; de tal manera, que las empresas deben estar más abiertas a contemplar la idea de aventurarse más allá en el ámbito de la automatización.

El trabajo de auditoría debe incluir el análisis de riesgo durante el planeamiento. De acuerdo con el diccionario Aplicativo para Contadores, se define Riesgo como: "La posibilidad que el auditor pueda expresar una opinión financiera que esté distorcionada en aspectos materiales, o que los criterios técnicos del auditor hayan sido insuficientes o inapropiados".

Como sabemos, Basilea II incorporó el riesgo operacional a los riesgos ya evaluados por Basilea I (de crédito, de mercado y de tipo de cambio) y uno de los aspectos a evaluar del riesgo operacional es el factor de riesgo de tecnología de la información (TI).

¿Qué es el análisis de riesgo de TI?

Conocer los riesgos al que están sometidos los activos de TI es imprescindible para poder gestionarlos.

Dentro de los riesgos de la Tecnología de Información podemos mencionar a los siguientes:

- Información errónea o inoportuna.
- Tiempo laboral perdido por mal uso del e-mail e Internet.
- Alteración de datos.
- Insatisfacción del usuario.
- Acceso no autorizado.
- Ineficiente uso de los recursos tecnológicos.
- Robo de información.

El gran reto de este proyecto es enfrentar una problemática compleja dado que se interrelacionan diferentes tipos de activos, con lo cual si no se es metódico y riguroso, los resultados y conclusiones no son de fiar y difícilmente sean de valor para la Entidad.

Las acciones a desarrollar permitirán:

a. Incorporar a la matriz de riesgo operacional, el riesgo de TI asociado a cada proceso de negocio.
b. Concientizar a los responsables de las Gerencias de Tecnología y Sistemas de Información de la existencia de riesgos y brindar soluciones para su mitigación.
c. Ayudar a descubrir y planificar medidas oportunas para mantener los riesgos bajo control.
d. Preparar a la organización para procesos de evaluación, auditoría y cumplimiento, según corresponda.
e. Establecer los aspectos a tener en cuenta para la realización de planes de contingencias y continuidad del negocio y sistemas de gestión de seguridad informática.

En concreto, los avances en tecnología de la información en relación con los enfoques en tiempo real a la realización de negocios están desafiando la profesión de auditoría. Como tal, el objetivo principal de esta investigación es determinar qué metodología debería de emplearse para obtener un adecuado control de la tecnología de la información, riesgos y vulnerabilidades para el proceso de una Auditoría eficaz.

La auditoría debe aplicar las mejores prácticas disponibles en el mercado

En los sectores público y privado, se hacen uso de una serie de estándares que guían el desarrollo de proyectos de TI, entre ellos, se pueden mencionar:

- Directrices gerenciales de COBIT, desarrollado por la Information Systems Audit and Control Association (ISACA).
- The Management of the Control of data Information Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA).

- Administración de la inversión de tecnología de inversión: un marco para la evaluación y mejora del proceso de madurez, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO).
- Los estándares de administración de calidad y aseguramiento de calidad ISO 9000, desarrollados por la Organización Internacional de Estándares (ISO).
- SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA.
- El Modelo de Evolución de Capacidades de software (CMM), desarrollado por el Instituto de Ingeniería de Software (SEI).
- Administración de sistemas de información: Una herramienta de evaluación práctica, desarrollado por la Directiva de Recursos de Tecnología de Información.
- Guía para el cuerpo de conocimientos de administración de proyectos, desarrollado por el Comité de Estándares del Instituto de Administración de Proyectos.
- Ingeniería de seguridad de sistemas – Modelo de madurez de capacidades (SSE – CMM), desarrollado por la agencia de seguridad nacional (NSA) con el apoyo de la Universidad de Carnegie Mellon.
- Administración de seguridad de información: Aprendiendo de organizaciones líderes, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO).

El profesional de auditoría de Sistemas debe conocerlos y aplicarlos en su labor de revisión de las Tecnologías de Información que se emplea en cada entidad.

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:

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 –look and feel–", 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 traslada con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia.

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

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos claves que estos mismos

tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

Se comenzó el análisis a partir de los requerimientos de calidad, fiduciarios y de seguridad, 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.

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 identificarse/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 es 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.

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 sean satisfechos, deben definir, implementarse y monitorearse medidas de control adecuadas para estos recursos.

¿Cómo pueden entonces las empresas estar satisfechas respecto de la información obtenida de las características que necesitan? Es aquí donde se requiere un sano marco referencial de Objetivos de Control para TI.

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 las tareas necesarias para encontrar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras son consideradas más discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

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

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

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

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

Los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) fue desarrollado en respuesta a una necesidad percibida en un marco para el control interno del gobierno de TI. Fue construido en las mejores prácticas y se ha mantenido y actualizado para reflejar los cambios en tales prácticas. La documentación de COBIT se ha publicado en una serie de formas para satisfacer las necesidades de los diferentes miembros de una organización.

El producto final de la suite de COBIT es un conjunto de directrices de auditoría. Estas directrices proporcionan al profesional de auditoría de TI un marco con el que se lleve a cabo las auditorías. Las directrices subrayan la auditoría del proceso de TI:

- Obtener un entendimiento de las necesidades de negocio relacionadas con los riesgos y las medidas de control pertinentes
- La evaluación de la adecuación de los controles establecidos.
- La evaluación del cumplimiento por probar si los controles programados están trabajando como se lo recomendaron, de manera consistente y continua.
- Justificar si el riesgo de los objetivos de control no están cumpliendo con las técnicas analíticas o consultando fuentes alternativas.

CONCLUSIONES

1. COBIT, ITIL, ISO 17799 e ISO 27001 son el grupo más utilizado por las empresas en las metodologías respecto de la seguridad de TI y gestión de TI. Se utilizan en paralelo, lo que no debe sorprender, teniéndose en cuenta que representan mejores prácticas y experiencias que han sido aprobadas, desarrolladas y probadas en empresas de todo el mundo.
2. Las tendencias de estándares que van surgiendo, van paralelas con lo que aceleradamente ha sucedido en el sector privado, esto es, dado que se han gestado numerosos proyectos de sistemas de información que han fracasado, y la dura realidad del incumplimiento de los mismos con las necesidades propias de los clientes y del negocio en sí, hubo un incremento dramático en el número de organizaciones en el sector privado que están persiguiendo agresivamente el uso de estándares y mejores prácticas, como su estrategia primordial de supervivencia
3. La auditoría hizo grandes avances en la última década, pero aparentemente no ha seguido el ritmo de la economía en tiempo real. Algunos enfoques y técnicas de auditoría que fueron valiosas en el pasado aparecen ahora como obsoletas. Además, la

evolución de la auditoría ha llegado a un momento crítico por el que los auditores pueden llevar ya sea en la promoción y la adopción de la auditoría futura o seguir, para adherirse al paradigma más tradicional de alguna manera.

4. Los auditores reguladores y las entidades normativas requerirán estrategias de auditoría futuras para hacer ajustes significativos.

   Tales ajustes podrían incluir:

   - Cambios en el tiempo y la frecuencia de la auditoría.
   - Aumento de la educación en tecnología y métodos de análisis.
   - Adopción de un examen completo de la población en lugar de muestreo.
   - Un nuevo examen de conceptos tales como la materialidad y la independencia. Y
   - Ordenar la provisión del estándar de datos de auditoría.

5. Los auditores tendrán que poseer competencias técnicas y analíticas sustanciales, que en la actualidad no son componentes de los contenidos curriculares de la mayoría de los planes de estudios de la carrera de contabilidad.

REFERENCIAS BIBLIOGRÁFICAS

1. ABANTO, M., y otros (2012) Diccionario Aplicativo para contadores, 1ra ed., Editorial El Búho EIRL.
2. AICPA Assurance Services Executive Committee (June 2011) Audit Data Standards and Apps. University Presentation.
3. ALLES M., BRENNAN, G., and KOGAN, A. (2006) Continuous Monitoring of Business Process Controls: A Pilot Implementation of a Continuous Auditing System at Siemens. International Journal of Accounting Information Systems 7 (2): 137-161.
4. Association of Certified Fraud Examiners (2010) Report to the Nations on Occupational Fraud and Abuse.
5. BEST, P., RIKHARDSSON, P., and TOLEMAN, M. (2009) Continuous Fraud Detection in Enterprise Systems Through Audit Trial Analysis. Journal of Digital Forensics, Security, and Law 4 (1): 39-60.
6. CANGEMI, M., and SINGLETON, T. (2003) Managing the Audit Function: A Corporate Audit Department Procedures Guide, 3rd ed. John Wiley & Sons, Inc.
7. HERNANDEZ, S. (2014) Metodología de la Investigación, 3rd ed. Mexico.