Metodología Práctica para Auditoría de Sistemas Aplicando el Estándar de Mejores Prácticas Cobit 4.1

Practical Methodology for Systems Audit by Applying the Best Practice Standard 4.1 Cobit

Francisco Nicolás Javier Solarte Solarte
Grupo investigación GMETIS, Escuala de Ciencias Básicas, Tecnología e Ingeniería, Universidad Nacional abierta y a Distancia-UNAD, Pasto, Colombia
francisco.solarte@unad.edu.co

Recibido / Received: 31-07-2016 – Aceptado / Accepted: 30-03-2017

Resumen

El problema que se ha evidenciado es la aplicación de una metodología para realizar procesos de auditoría en las organizaciones, cada una de las normas y los autores describen de manera general cómo aplicar procesos de auditoría, cada uno con su propio estándar. Por lo tanto, la investigación tiene como objetivo proponer una metodología sencilla y clara para aplicar el proceso de auditoría informática y de sistemas. La metodología muestra cada una de las fases o etapas y las actividades que se deben llevar a cabo, partiendo de las metodologías planteadas por diversos autores que plantean tres etapas y brindan aspectos generales sobre los conceptos de auditoría y la metodología de auditoría informática y de sistemas en la práctica, pero aún no queda claro las actividades y cómo realizar cada una de ellas. Por lo tanto, se ha propuesto una nueva metodología de auditoría aplicada a la informática y los sistemas en empresas pequeñas que permita establecer las etapas y las actividades que se deban desarrollar en el proceso de auditoría y que pueda ser aplicada en distintos escenarios y ajustado a las normas vigentes. Esta metodología ya ha sido probada por estudiantes de pregrado y postgrado en la ciudad de Pasto y se ha obtenido buenos resultados, concluyendo que es una opción viable para que pueda ser aplicada teniendo los conocimientos básicos de auditoría y la norma que debe aplicarse.

Palabras clave: Auditoría de sistemas, Análisis de riesgos, Vulnerabilidad informática, Amenazas informáticas, Control interno informático.

Abstract

The problem has become evident is the application of a methodology for auditing processes in organizations, each of the standards and the authors describe generally how to apply auditing processes, each with its own standard. Therefore the research aims to propose a simple and clear methodology for implementing the IT

audit process and systems. The methodology shows each of the phases or stages and activities to be carried out, based on the methodologies raised by several authors who raise three stages and provide general aspects of audit concepts and methodology and computer audit systems in practice, but it remains unclear activities and how to perform each. Therefore it has proposed a new audit methodology applied to computing and systems in small companies in order to establish the stages and activities to be developed in the audit process and can be applied in different scenarios and adjusted to the regulations. This methodology has already been tested by undergraduate and graduate students in the city of Pasto and has archieved good results concluding that it is a viable so it can be applied to have the basic knowledge of auditing and the standard to be applied option.

Keywords: Systems audit, Risk analysis, Computer Vulnerability, Computer Threats, Internal control computer.

I. Introducción

El problema general que se evidencia en las distintas metodologías planteadas por diversos autores y en las normas, es la aplicación de una metodología práctica en los procesos de auditoría informática, de sistemas y aplicados a la seguridad informática y de la información, que ha llevado a que cada auditor plantee una metodología propia y un estándar específico sin importar los objetivos que se pretenda alcanzar en la auditoría. Por eso, se ha planteado la siguiente pregunta: ¿la metodología propuesta para llevar a cabo la auditoría informática y de sistemas, logrará describir las actividades prácticas en cada fase del proceso de auditoría?

La metodología está enfocada a describir cada una de las fases o etapas de desarrollo del proceso de auditoría, donde se incluye los conceptos de auditoría y aplicación de las técnicas e instrumentos de recolección de información, la metodología y el proceso de análisis de riesgos, el diseño y organización de los papeles de trabajo, el documento del plan de auditoría, el programa de auditoría, los formatos de resultados que surgen en cada etapa y la presentación de los resultados finales de la auditoría hasta llegar al informe final.

La importancia de este proyecto radica en que el proceso de auditoría podrá llevarse a cabo por los ingenieros de sistemas en cada una de las organizaciones o empresas pequeñas sin tener que contratar a personal especializado, puesto que la metodología describirá paso a paso cómo realizar cada una de las actividades en la práctica, las fases en el proceso de auditoría, el diseño de modelo de los formatos de auditoría, el proceso de análisis y evaluación de riesgos, las pruebas aplicadas, y los resultados mostrados en documentos como el dictamen y el informe final de auditoría. Esto logrará disminuir los costos y mejorar el funcionamiento de los sistemas y activos informáticos dentro de las organizaciones.

Según Echenique [1], la auditoría en informática es "la Revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones". Según Piattini Velthuis [2], la auditoría informática es "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos". De las anteriores definiciones, se deduce que la auditoría informática es la revisión, evaluación, verificación y confirmación de la existencia de políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos informáticos por parte del personal de una organización con el fin de lograr el uso eficiente, eficaz, efectivo y seguro de la información que sirva para una adecuada toma de decisiones.

La auditoría de sistemas de información, según Piattini [2], se define como "cualquier auditoría que abarca la revisión y evaluación de todos los aspectos de los sistemas automáticos de procesamiento de la información, incluidos los no automáticos relacionados con ellos y las interfaces correspondientes; también se puede decir que es el examen y evaluación de los procesos del área de Procesamiento Electrónico de Datos (PED) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas". De acuerdo con lo anterior, la auditoría de sistema puede aplicarse al área de informática, a los sistemas de información informáticos o alguno de ellos específicamente que sea el que presenta mayores dificultades.

Según Tamayo [3], el control "es un conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales". El control interno informático se encarga de examinar diariamente que todas las actividades de los sistemas de información se realicen cumpliendo con los procedimientos, estándares y normas fijados por la dirección de la organización y/o dirección informática para el cumplimiento de los requerimientos legales.

Según Pinilla [4], los papeles de trabajo se definen así: "comprende el conjunto de cédulas preparadas por el auditor y/o personal colaborador, con motivo del desarrollo del programa de auditoría para obtener evidencia comprobatoria suficiente y competente, que sirva como base objetiva para emitir una opinión independiente sobre el objeto auditado". Estas cédulas o formatos son registros que mantiene el auditor de los procedimientos aplicados, pruebas desarrolladas, información obtenida y conclusiones pertinentes a que se llegó en el trabajo.

Para realizar el proceso de auditoría informática y de sistemas, se requiere planear una serie ordenada de acciones y procedimientos específicos, que deben ser ejecutados de forma secuencial, cronológica y ordenada, teniendo en cuenta etapas, eventos y actividades que se requieran para su ejecución que serán establecidos de acuerdo con las necesidades de la organización.

La metodología general, según Muñoz [5], cubre tres etapas que son la base para adelantar estos procesos de auditoría, a su vez cada una de las etapas agrupa un conjunto de actividades para el cumplimiento de la misma; la primera etapa es la planeación o planificación de la auditoría; la segunda, es la ejecución de la auditoría; y la tercera, informe final de resultados de la auditoria.

El Estándar de Objetivos de Control para la información y las tecnologías relacionadas, denominado COBIT [6], se fundamenta en la filosofía de que todos los recursos de TI, deben ser administrados por un conjunto de procesos agrupados para proveer información oportuna y confiable que requiera la organización para el cumplimiento de los objetivos. La estructura del modelo COBIT permite un marco de acción para la evaluación de los criterios de información como la efectividad, la eficiencia, la confidencialidad, la integridad, la disponibilidad, el cumplimiento y la confiabilidad de la información. Además, COBIT permite auditar los recursos que comprenden la tecnología de información, como son los datos, las aplicaciones, la tecnología de información, las instalaciones, y el personal, entre otros. Los lineamientos conocidos como estándar COBIT se encuentran especificados bajo cuatro dominios que agrupan un conjunto de treinta y cuatro procesos, a cada proceso se le asocian objetivos de control general de alto nivel y varios objetivos de control específicos.

II. Metodología

El método de evaluación consiste en la aplicación de los conceptos teóricos de auditoría y las metodologías descritas por algunos autores [1], [2], [3], [4], [5], que se materializan y aplican en proyectos de auditoría reales que se llevan a cabo en las empresas

de la ciudad de Pasto. El método incluye la revisión de la documentación existente, el cumplimiento de las actividades en cada etapa y la organización de los papeles de trabajo.

TABLA 1. FASES Y ACTIVIDADES AUDITORÍA DE SISTEMAS

FASES O ETAPAS	ACTIVIDADES A DESARROLLAR
Fase de Conocimiento	1. Realizar visitas a la empresa u organización. 2. Realizar observaciones de cada uno de los procesos que se lleva a cabo. 3. Establecer los recursos de TI involucrados en el manejo de la información. 4. Determinar las entradas y salidas de la información. 5. Revisar la documentación existente. 6. Identificar las vulnerabilidades y amenazas a que está expuesta la organización. 7. Identificar los riesgos iniciales. 8. Hacer el análisis y evaluación de riesgos preliminar.
Fase de Planeación de la Auditoría	1. Identificar el origen de la auditoría. 2. Determinar el estándar que será aplicado para la auditoría. 3. Elaborar plan de auditoría: establecer los objetivos, alcances, metodología, recursos y cronograma de actividades de la auditoría. 4. Elaborar el programa de auditoría: grupo auditor, definir responsabilidades y actividades a desarrollar. 5. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría. 6. Diseñar los papeles de trabajo: entrevistas, listas de chequeo, cuestionarios, otros. 7. Elaborar el plan de pruebas de análisis y ejecución.
Fase de Ejecución de la Auditoría	1. Realizar las acciones programadas para la auditoría. 2. Aplicar los instrumentos diseñados para la auditoría. 3. Aplicar las pruebas diseñadas. 4. Aplicar el proceso de análisis y evaluación de riesgos aplicando una metodología. 5. Elaborar la matriz de riesgos. 6. Identificar los controles definidos para cada dominio y proceso. 7. Elaborar los formatos de hallazgos: identificar proceso, describir riesgos, identificar las causas, identificar los recursos afectados, identificar posibles soluciones en el contexto.
Fase de Resultados de la Auditoría	1. Definir tratamiento de los riesgos. 2. Determinar los controles y tipos de control: preventivos, detectivos, correctivos, recuperación. 3. Elaborar el Dictamen de la auditoría para cada dominio y procesos evaluado. 8. Elaborar el informe preliminar y presentarlo a discusión. 9. Elaborar el informe final de auditoría. 4. Integrar el legajo de papeles de trabajo de la auditoría. 5. Presentar el informe final de Auditoría y documentación.

Fuente: El autor, 2016

III. Resultados

Al aplicar los conceptos de auditoría en la práctica, se logra mayor claridad en cada una de las etapas en el proceso de auditoría integrando la teoría y la práctica.

En la metodología, se puede realizar el seguimiento de las actividades en cada etapa para el cumplimiento de los cronogramas previstos y el seguimiento continuo de los resultados.

En la metodología, se puede definir claramente las actividades individuales y en equipo para la medición del desempeño en el proyecto.

Esta metodología ha sido probada por los estudiantes de Ingeniería de sistemas desde hace algunos años, y comparándolos con grupos anteriores, se ha demostrado su efectividad como método para aplicar la auditoría informática y de sistemas en sus fases esenciales.

IV. Conclusiones

De la aplicación de la metodología se puede concluir, de acuerdo con las pruebas realizadas, que puede ser aplicada a cualquier tipo de organización y empresa no importando el tamaño, ya que las fases y actividades son genéricas para cualquier tipo de auditoría. También se concluye que, comparativamente con otros métodos, esta metodología es una forma nueva de llevar a la práctica los conceptos teóricos de auditoría y las normas de mejores prácticas con la rigurosidad y exigencia que el proceso amerita.

Referencias

[1] J. A. Echenique, Auditoría en Informática. México D.C., Editorial Mc Graw Híll, 2001, p. 158.

[2] M. G. Piattini, Auditoría informática. Un enfoque práctico, México, Alfamega-RA-MMA, 2001, p. 660.

[3] A. Tamayo Alzate, Sistemas de Información. Editorial Universidad Nacional, 1998.

[4] J. D. Pinilla Forero, Auditoría Informática. Un enfoque operacional. Editorial Ecoe 1992, p. 252.

[5] C. Muñoz Razo, Auditoría en sistemas computacionales. México D.C., Editorial Pearson, 2002, p. 818.

[6] Objetivos de Control para Tecnologías de la Información y Relacionadas COBIT 4.1, Asociación para la Auditoría y Control de Sistemas de Información ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 EE.UU, 2007, p. 209.