DESARROLLO DE UN MANUAL DE AUDITORÍA INFORMÁTICA APLICADO A COOPERATIVAS DE AHORRO Y CRÉDITO

Carlos Sarango Ontaneda

Departamento de Ciencias de la Computación; Escuela Politécnica del Ejército, Sangolquí, Ecuador
karlos_sarango@hotmail.com

Resumen: El presente artículo describe el desarrollo de un manual que sirva de referencia para auditar los principales procesos de tecnología de las Cooperativas de Ahorro y Crédito controladas por la Superintendencia de Bancos y Seguros del Ecuador. Dicho manual selecciona e integra los conceptos de los marcos de referencia, Cobit 4.1 (control de TI) y Magerit v2 (riesgos de TI) en los procesos de auditoría informática. Se inició con la identificación de las características del problema, la definición de los objetivos de proyecto y la planificación del mismo, lo cual se desarrolla en los capítulos de la tesis. Se realizó la investigación de las características del sistema cooperativo de ahorro y crédito nacional, su evolución en el tiempo y el marco legal aplicable; de esta forma se establecieron las obligaciones de la auditoría informática en dichas instituciones financieras. El desarrollo del marco teórico permitió definir la estructura conceptual de la investigación, se revisaron las normas de auditoría informática, marcos de buenas prácticas de control interno, gobierno de TI y gestión de riesgo tecnológico. A continuación, se desarrolló el manual de auditoría informática, mediante el análisis de las interrogantes del problema, se diseñaron y describieron los macro procesos de auditoría informática. Se delineó la estructura del manual, sus etapas y los entregables respectivos. Posteriormente se analizó la aplicación del manual generado mediante el desarrollo de un caso ficticio. Finalmente se detallaron las conclusiones y recomendaciones generadas a lo largo del proyecto.

Palabras Clave: Auditoría, Control, Riesgo, Informática, Cooperativas

Abstract: The enclosed article describes the development of a manual, which would serve as reference to evaluate the main technology processes of Cooperativas de Ahorro y Credito, overseen by the Superintendencia de Bancos y Seguros del Ecuador. The manual selects and integrates the concepts for frame of reference, Cobit 4.1(control de TI) and Magerit v2 (riesgos de TI), in the processes of informatic audit. It was initiated by identifying the characteristics of the problem, defining the objectives, and by planning the project. These topics are included in the chapters of the thesis.

The research was performed on the characteristics of the "sistema cooperativo de ahorro y credito nacional" (cooperative system of national savings and credit), as well as on its evolution throughout time and applicable legal implications. Though these findings, it was possible to establish the liabilities of the informatic audit in the above mentioned financial institutions. The development of the theoretical frame of reference enabled the definition of the conceptual structure of the investigation. Informatic audit norms were revised, as well as best practices for: internal control, governing practices of TI, and management of technological risks. Following, the manual of informatic audit was developed. Through the analysis of the problem's main questions, the macro processes of the informatic audit were designed and described. The structure of the manual, its phases and respective deliverables were delineated. Subesquently, the application of the generated manual was applied through the development of a fictitious

case. Finally, the conclusions and recommendations, generated throughout the project, were detailed.

Keywords: Audit, Control, Risk, Informatic, Cooperatives

I. Introducción

El desarrollo de un documento como el manual de auditoría informática, orientado hacia la evaluación de los procesos tecnológicos de las Cooperativas de Ahorro y Crédito, corresponde a una iniciativa enfocada en atender la necesidad de contar con un marco de referencia para el auditor informático en el cumplimiento de su trabajo. Se definió desarrollar un proceso de auditoría basada en riesgos, utilizando para dicha tarea varios de los conceptos establecidos por la metodología de análisis y gestión de riesgos de TI (Magerit). Adicionalmente, la definición de los procesos y los controles de TI se basó en el marco de buenas prácticas Cobit 4.1. Con estos insumos se definieron los macroprocesos principales de la gestión de auditoría informática interna, esto es la planificación anual y la ejecución de una revisión individual de auditoría informática.

El aporte principal corresponde a la definición de una herramienta que apoye el desarrollo de las evaluaciones de auditoría informática en las Cooperativas de Ahorro y Crédito, considerando los marcos de control y riesgos tal como lo exige la normativa de la Superintendencia de Bancos y Seguros del Ecuador. Se generó el manual con la definición de las actividades, documentos entregables y las consideraciones para implementación de los macroprocesos de auditoría informática.

Este artículo se ha estructurado en secciones cuyos temas de análisis corresponden a la definición del problema, estudio del ambiente de las Cooperativas de Ahorro y Crédito, profundización de los conceptos de auditoría y marcos teóricos de referencia, desarrollo del manual de auditoría informática y sus anexos; y, finalmente, las conclusiones y recomendaciones generadas por el proyecto.

II. Metodología

Se decidió trabajar en base a las normas de auditoría establecidas por la asociación mundial de auditores de sistemas de información (ISACA) y tomando como referencia los procesos de planificación anual y ejecución individual recomendados por el instituto de auditores internos (IAI). Para la definición de procesos y controles de TI, se consideró lo establecido en el marco de buenas prácticas Cobit versión 4.1, este hecho obedeció a la estrecha relación que existe entre dicho marco y los objetivos estratégicos de la organización.

Dado que los procesos de auditoría contaban con subprocesos enfocados en el análisis de riesgos, se definió para estas tareas adoptar el análisis de tipo cualitativo, motivado principalmente por su mayor sencillez al momento de aplicarlo. Se realizó una adaptación del método basado en activos, amenazas, riesgos y controles, propuesto por la metodología de análisis y gestión de riesgos de TI (Magerit) versión 2.0.

Adicionalmente, se trabajó con las escalas propuestas para dichas variables, las mismas se detallan en la metodología. En aquellos casos en donde se requirió acumular los valores de las variables (impacto, probabilidad, riesgo, valor, control) se utilizó la asignación de puntajes, los cuáles se trataron de forma aritmética para efectuar la selección de los procesos y controles. Con esta base se pudo establecer una priorización de los elementos a examinar por parte del auditor informático.

III. Evaluación de resultados y discusión

Los resultados obtenidos luego del desarrollo especificado en las secciones anteriores se detallan a continuación:

A. Proceso para la Planeación Anual de Auditoría

Con el fin de obtener los procesos a ser revisados por parte de la Auditoría Informática Interna, se requiere cumplir con varias actividades agrupadas en un macroproceso de Planeación Anual. El mencionado proceso incluye la evaluación de riesgos de la Cooperativa, de forma que se enfoque los esfuerzos de auditoría hacia lo que realmente le afecta a la institución en relación a su gestión tecnológica.

Las etapas de dicho proceso se pueden observar en la siguiente figura:

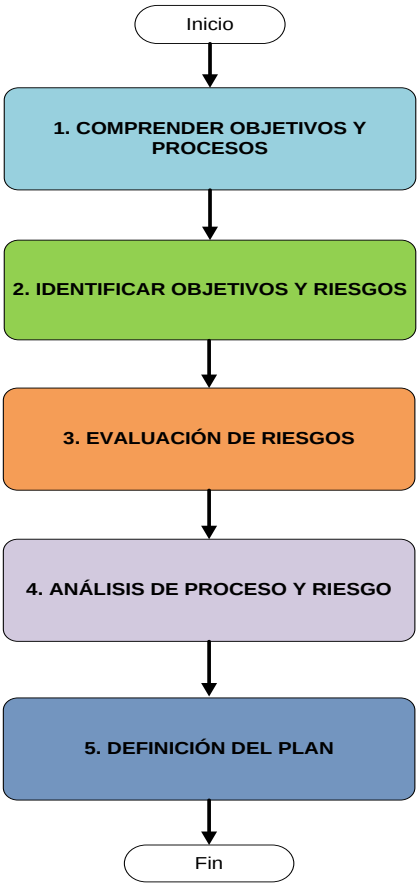

Figura 1. Proceso de Planeación Anual de Auditoría

- El proceso diseñado permite identificar las relaciones entre procesos de TI con los objetivos estratégicos de la Cooperativa.
- Se crea un enlace entre los objetivos de negocio y los objetivos de tecnología basados en como las aplicaciones apoyan a los primeros.
- La definición de los riesgos se toma del catálogo de elementos de Magerit, concentrándose en las amenazas que afectan a las aplicaciones.
- Se define los riesgos más relevantes y se identifica su relación con los procesos tecnológicos establecidos por el marco de buenas prácticas Cobit.

- Finalmente se establece la priorización para revisión de auditoría en base al nivel de riesgo de cada proceso Cobit. En este punto, la planificación de auditoría informática corresponde a los objetivos institucionales y considera revisar aquellos procesos tecnológicos que están originando la mayor exposición al riesgo.

B. Proceso para una Asignación Individual de Auditoría

Para la definición del macroproceso aplicable a una asignación individual de auditoría se ha tomado como referencia las etapas del proceso de auditoría con enfoque a riesgos propuesto por ISACA. El esquema desarrollado se muestra en la siguiente figura:

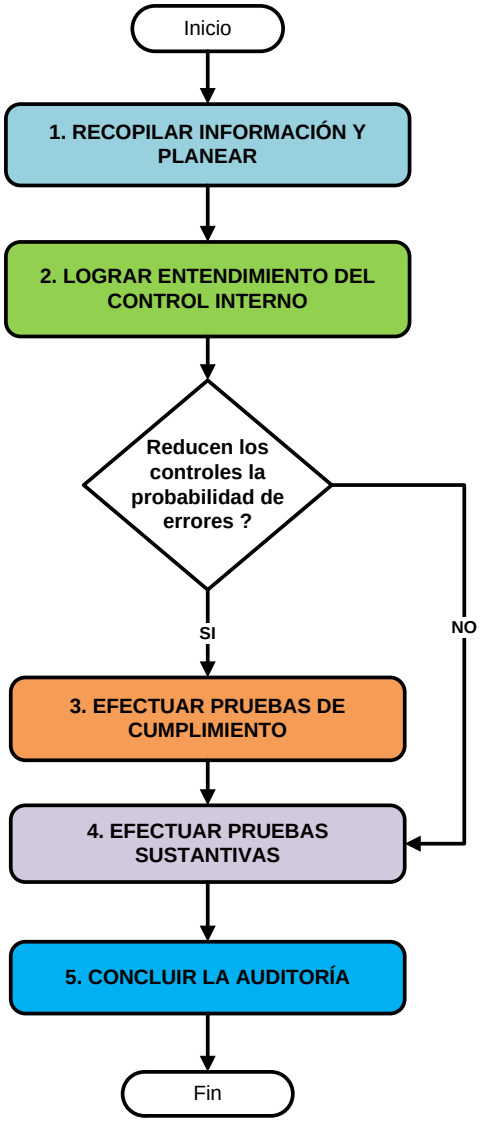

Figura 2. Proceso para una Asignación Individual de Auditoría

Los resultados obtenidos de la aplicación de dicho proceso fueron los siguientes:

- Se logró definir las actividades para auditar (desde el enfoque de auditoría interna) un proceso Cobit en una Cooperativa de ahorro y crédito.

- Se establecieron los controles a ser probados tomando en cuenta lo definido en Cobit 4.1, dependiendo del tamaño de la Cooperativa y el desarrollo de su nivel de control y administración de riesgos, se puede considerar el uso de Cobit Quickstart para la selección de los controles más relevantes por proceso.
- Se consiguió establecer el nivel de control que se tiene sobre el proceso, mediante la evaluación del riesgo de control.
- Se establecieron los valores para el riesgo de auditoría en base a la definición de componentes como: riesgo inherente, riesgo de control y riesgo de detección.
- Se definieron el tipo y la profundidad de las pruebas a desarrollar para evaluar los controles, esto basado en los resultados del riesgo de auditoría requerido para cada proceso de TI.
- Se consiguió detectar y comunicar los potenciales hallazgos de auditoría en base al desarrollo de las etapas del proceso, generando el informe de auditoría informática respectivo.
- Se desarrolló la auditoría informática basada en un análisis de riesgo tecnológico de la institución y considerando los objetivos de control establecidos por un marco de buenas prácticas de control como lo es Cobit 4.1.

En base a los resultados, se concluye que la propuesta posibilita contar con un manual de auditoría informática, constituido en un marco de referencia para efectuar la auditoría de los procesos tecnológicos. Dicho manual se basa en los riesgos tecnológicos y los objetivos estratégicos de la Cooperativa auditada.

IV. Trabajos relacionados

La Superintendencia de Bancos y Seguros conjuntamente con el Banco Interamericano de Desarrollo, ha desarrollado un documento denominado MUS (manual único de supervisión) el mismo es utilizado en el proceso de supervisión de instituciones financieras (entre ellas las Cooperativas de Ahorro y Crédito), bajo una metodología de trabajo con enfoque a riesgos. Sin embargo, el proceso descrito tiene una orientación hacia la evaluación integral de las instituciones financieras por lo que no corresponde a un enfoque especializado hacia la auditoría informática. Otra diferencia con el proceso propuesto por este proyecto es que si bien el MUS considera los dominios de Cobit, no cuenta con una referencia específica para la identificación de los riesgos tecnológicos, lo que aumenta el grado de subjetividad por parte del auditor al momento de la evaluación de los riesgos.

V. Conclusiones y trabajo futuro

En base a los resultados obtenidos, se concluye que la propuesta hace posible contar con un manual de auditoría informática que sirva de referencia para la evaluación de procesos de tecnología en las Cooperativas de Ahorro y Crédito. El documento describe los procesos de planificación y evaluación que toman como referencia el marco de buenas prácticas de Cobit 4.1 para el tema de controles, y la metodología Magerit v2 para el análisis de riesgos tecnológicos. Por lo expuesto, es posible asegurar que el mencionado manual es una herramienta importante para el trabajo de las unidades de auditoría interna de las Cooperativas de Ahorro y Crédito.

Es importante establecer que el manual de auditoría requiere el desarrollo de ciertas competencias para su uso y aprovechamiento, es importante que sea aplicado por profesionales con experiencia en el campo de la auditoría informática, esto debido a que

cada institución vive una realidad propia y es necesario contar con un criterio profesional entrenado para aplicar los conceptos y procesos descritos en el manual.

VI. Agradecimientos

Al ingeniero Paulo Bermeo, por la asesoría en el desarrollo del proyecto.
A la Asociación de Auditoría y Control de Sistemas de Información (ISACA) por la provisión del material bibliográfico.

VII. Referencias bibliográficas

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004).

Dirección Nacional de Estudios e Información de la Superintendencia de Bancos y Seguros del Ecuador. (2012). Comportamiento del Sistema de Cooperativas de Ahorro y Crédito a Marzo 2012. Quito

Enrique Hernández Hernández. (2006). Auditoría en Informática. México: Compañía Editorial Continental

Gestión de Riesgos Corporativos, Marco Integrado - USA

Isaca. (2009). Manual de Preparación para el Examen CISA. Illinois

Isaca. (2010). Manual de Preparación al Examen CISA – Illinois

IT Governance Institute. (2007). IT Assurance Guide Using Cobit. Illinois

IT Governance Institute. (2007). COBIT 4.1 Control Objectives for Information and Related Technology. Illinois

IT Governance Institute. (2007). Cobit Quickstart Second Edition. Illinois

Kirk Rehage, Steve Hunt, Fernando Nikitin. (2008). Developing the IT Audit Plan. Florida: IAI

Maestría de Evaluación y Auditoría de Sistemas Tecnológicos - ESPE (2010). Manuales, libros, folletos.

Ministerio de Administraciones Públicas de España. (2006). MAGERIT versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid

Superintendencia de Bancos y Seguros del Ecuador. (2009). Manual Único de Supervisión. Quito