EVALUACIÓN TÉCNICA INFORMÁTICA DEL COMIL 10 ABDÓN CALDERÓN, UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT

John Narváez Mejía; Ing. Mario Ron Egas MSc.; Ing. Lourdes De La Cruz

Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, johnnarvaezm@gmail.com
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, mbron@espe.edu.ec
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, lrdelacruz@espe.edu.ec

RESUMEN

Utilizar herramientas y estándares no es lo más importante debido a que sirven para estructurar las ideas y tener una visión general, lo más importante del proceso son las personas involucradas y la capacidad de liderazgo que se aporte para su correcta aplicación.

Los procedimientos de la gestión tecnológica que aplica actualmente el Centro de Informática del Comil Nº 10, son seleccionados y adaptados a un modelo de gestión de TI, que dificulta la toma de decisiones, por esta razón se realizó la Evaluación Técnica Informática del Colegio Militar Nº 10 ABDÓN CALDERÓN utilizando el estándar internacional COBIT (Objetivos de Control para la Información y Tecnologías).

En este artículo se presenta un reporte condensado de dicha evaluación, se determinó el alcance con un análisis exhaustivo de todas las actividades que gestiona el Centro de Informática de la Institución, identificando los riesgos de TI mediante una Matriz de Riesgos, que permitió determinar los procesos y objetivos de control que fueron evaluados, posteriormente se elaboró el Plan de Investigación de Campo que ayudó a evaluar y medir el nivel de madurez de los procesos de negocio relacionados con los Sistemas de Información en base a evidencias y controles fundamentados en las directrices de auditoría planteadas por COBIT.

Se culminó con el Informe Final que está compuesto por un Informe Ejecutivo y un Informe Detallado que puntualizan los principales hallazgos encontrados en la evaluación, indicando las observaciones, recomendaciones y controles que deben efectuarse en el Departamento Informático.

Palabras Clave: Evaluación Técnica Informática, Auditoría, COBIT, Gestión tecnológica, Sistemas de Información.

ABSTRACT

Use tools and standards are not as important because they serve to structure ideas and take an overview, the most important of the process are the people involved and the leadership skills to be provided for proper application.

The procedures for managing technology currently applied by the Department of Information Technology of the Military School No. 10, are selected and adapted to a model of IT management difficult making decisions, for this reason was the Technical Evaluation of Military College Computing No. 10 Abdon Calderon using the international standard COBIT (Control Objectives for Information and Technology).

This article presents a condensed report of this evaluation, the scope was determined with a thorough analysis of all activities managed by the Computer Centre of the Institution, identifying IT risk using a risk matrix, which identified the processes and control objectives were evaluated , subsequently developed the Field Research Plan that helped to assess and measure the level of maturity of business processes related to information systems based on evidence and grounded in controls audit guidelines raised by COBIT.

It culminated in the Final Report consists of an Executive Summary and a Detailed Report to point out the main findings from the evaluation including observations, recommendations and checks to be conducted in the IT Department.

KeyWords: Computer Technical Evaluation, Audit, COBIT, Technology Management, Information Systems.

1. INTRODUCCIÓN

El desarrollo de las nuevas tecnologías de información y su implementación para agilizar procesos, innovar servicios y productos, implica cambio de paradigmas no sólo en el funcionamiento de las organizaciones, sino también en el quehacer de los profesionales de la información.

No se trata solamente de adquirir tecnologías, sino de administrarlas debidamente, la Informática está subsumida en la gestión integral de la organización, y por eso las normas y estándares propiamente informáticos deben estar sometidos a los generales de la misma. La Auditoría Informática existe para tener un acercamiento a otras disciplinas que de alguna manera apoyan y complementan a la toma de decisiones, debido a su importancia en el funcionamiento de la organización.

La meta a alcanzar por una organización que contrata la auditoria es asegurar que sus objetivos estratégicos y que los sistemas presten el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura. El Colegio Militar Nº 10 “Abdón Calderón” al ser una Institución educativa pública y de prestigio, cuenta con un Centro de Informática que gestiona las actividades de TI, administra la información, desarrolla sistemas requeridos por la Institución, brinda soporte técnico y ejecuta varios proyectos informáticos, debido a ello se ha considerado la necesidad de realizar una

Evaluación Técnica Informática Externa a los controles establecidos por la dirección de TI para determinar falencias actuales, bajo el estándar internacional como es COBIT.

El proceso de implementación del estándar de COBIT en el COMIL Nº 10, constituye una alternativa estratégica y operativa para medir la capacidad competitiva del departamento informático de la Institución, al desarrollar competencias que les permitan administrar de manera adecuada los riesgos de negocio, necesidades de control, procesos de evaluación, aspectos técnicos e indicadores claves de gestión que les faciliten la toma de decisiones para desarrollar estrategias relacionadas con las oportunidades y amenazas tecnológicas del entorno.

La Evaluación Técnica Informática del Sistema de Información del Colegio Militar Nº 10 "Abdón Calderón" utilizando el estándar internacional COBIT, se la realiza con el fin de evaluar la eficacia y eficiencia de la Institución al nivel de tecnologías de información. El producto final del trabajo del auditor constituye el informe final para la Gerencia y/o Dirección en el cual se presentan las observaciones y recomendaciones sobre los principales hallazgos.

2. METODOLOGÍA

La metodología que se utilizó en el proyecto, es la Auditoría en Base a Riesgos (ABR), normativa técnica que identifica los riesgos de TI, el cumplimiento de los requisitos técnicos y medios de verificación mediante la Matriz de Riesgos que se usará para determinar los puntos críticos a evaluar, los objetivos específicos de auditoría y los procedimientos o pruebas de auditoría.

Para la Evaluación Técnica Informática del Sistema de Información del COMIL Nº 10 se aplicará el estándar internacional COBIT (Objetivos de Control para la Información y Tecnologías). La estructura del proceso de auditoría informática, comprende las siguientes principales etapas de la Auditoría Informática:

- Planificación de la Auditoría.
- Análisis de riesgos y amenazas
- Evaluación de Controles.
- Informe de Auditoría.
- Seguimiento de Recomendaciones

2.1 Planificación de la Auditoría

Una planificación adecuada es el primer paso necesario para realizar auditorías informáticas eficaces. El auditor debe comprender el ambiente del negocio en el que se ha de realizar la auditoría así como los riesgos del negocio y control asociado. Se debe identificar cuáles son los procesos y plataformas que van a ser auditados, esto nos ayuda a centrarnos en los temas más relevantes, creando una estrategia de auditoría.

2.1.1 Marco de Trabajo

Para la evaluación técnica informática del Colegio Militar Nº 10 Abdón Calderón se adopto el marco de trabajo de COBIT que está enfocado: Al *management* puesto que provee a la administración de una base

de mejores prácticas con las cuales se pueden tomar decisiones de TI e inversión. A los *usuarios de TI* debido a la seguridad que les brinda para el control de objetivos y procesos. Y a *auditores* debido a que permite identificar problemas de control de TI dentro de la infraestructura de TI de la organización, como se muestra en la **Figura 1**.

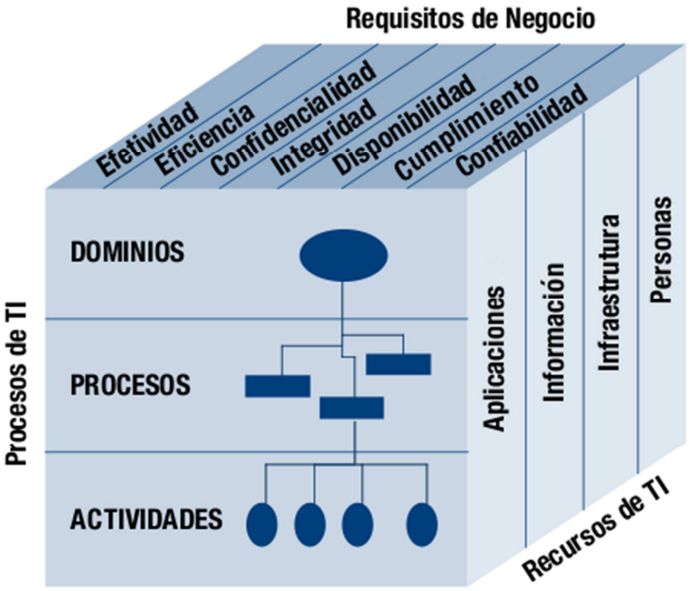

Figura 1 Modelo del marco de trabajo de COBIT

2.1.2 Alcance

En el proyecto se utilizó la versión 4.1 de COBIT, planteado por un organismo internacional de estandarización como es ISACA, a fin de identificar debilidades y emitir recomendaciones que permitan mitigar los riesgos del Centro de Informática de la Institución. El proyecto se desarrolló en el periodo comprendido de Enero 2012 hasta Julio 2012.

La evaluación fue realizada sobre los cuatro dominios del modelo COBIT:

- Planificación y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Monitoreo y Evaluación.

2.2 Análisis de Riesgos y Amenazas

Al determinar que áreas funcionales deben auditarse, el auditor debe evaluar los riesgos y determinar cuales de esas áreas de alto riesgo debe ser auditada.

Existen cuatro motivos por los que se utiliza la evaluación de riesgos, estos son:

1. Permitir que la gerencia asigne recursos necesarios para la auditoría.
2. Garantizar que se ha obtenido la información pertinente de todos los niveles gerenciales, y que las actividades de la función de auditoría se dirijan correctamente a las áreas de alto riesgo.

3. Constituir la base para la organización de la auditoría a fin de administrar eficazmente el departamento.
4. Proveer un resumen que describa como el tema individual de auditoría se relaciona con la organización global de la empresa así como los planes del negocio.

2.3 Evaluación de Controles

Se empleó una matriz de riesgos, que permite realizar el análisis de riesgos y en base a ese análisis priorizar los objetivos de control que fueron evaluados, fundamentándose en las directrices de auditoría planteadas por COBIT para el control interno, desempeño, y el nivel de madurez de los procesos del departamento informático de la institución. La información se recopiló en base a entrevistas y encuestas.

2.3.1 Planificación y Organización

Se estableció instrucciones para analizar el proceso de actualización de los planes de TI del Centro de Informática de la Institución. Se tiene definida las funciones a ser realizadas por parte del personal de TI pero no las que deben realizar los usuarios. Las políticas para soportar documentación son desarrolladas en base a necesidades individuales y no hay un marco de referencia global. Por ultimo la administración de riesgos se da por lo general en un alto nivel, actualmente no se ha realizado una evaluación de riesgos de TI y no se aplica a proyectos grandes solamente se aplica en fuerza mayor o como respuesta a problemas.

2.3.2 Adquisición e Implementación

La Institución cuenta con seis sistemas o programas, los mismos que son utilizados por el personal administrativo y usuarios del COMIL Nº 10, como se muestra en la siguiente **Tabla 1**:

Tabla 1 Sistemas manejados por la Institución

CATEGORÍA	SOFTWARE	OBSERVACIONES
EDUCACIÓN	Sistema Integrado Educativo: académico, de secretaría y de colecturía	Se tiene serias debilidades en cuanto al funcionamiento, lentitud general en todas las operaciones, no se realiza mantenimiento del sistema integrado y no se cuenta con reportes de fallas de seguridad y procedimientos formales de solución de problemas.
INSTITUCIONAL	Portal web de la Institución	Se han realizado actualizaciones importantes sin embargo no se sigue un proceso para el registro de los cambios.
ESTATAL	Sistema Integrado de Gestión documental, Sistema de Contratación Pública	Este sistema es nuevo actualmente su funcionamiento es administrado y supervisado por el estado, este sistema controla la gestión documental para docencia y empleados administrativos del COMIL Nº 10.

2.3.3 Entrega y Soporte

El Centro de Informática del Colegio Militar Nº 10 Abdón Calderón, maneja las áreas de administración de base de datos y software, administración de hardware y Help Desk (Soporte técnico a usuarios) y

administración de redes y servidores como se muestra en la **Figura 2**. Además al ser una institución militar sirve de enrutador teniendo conexiones con la dirección de la Comandancia, el Comando de Educación y Doctrina del Ejército entre otras entidades militares. La gestión de los servicios de terceros son revisados de forma periódica y satisfactoria debido a que es manejado por entidades del estado, sin embargo la Institución es la que decide con que proveedor laborar.

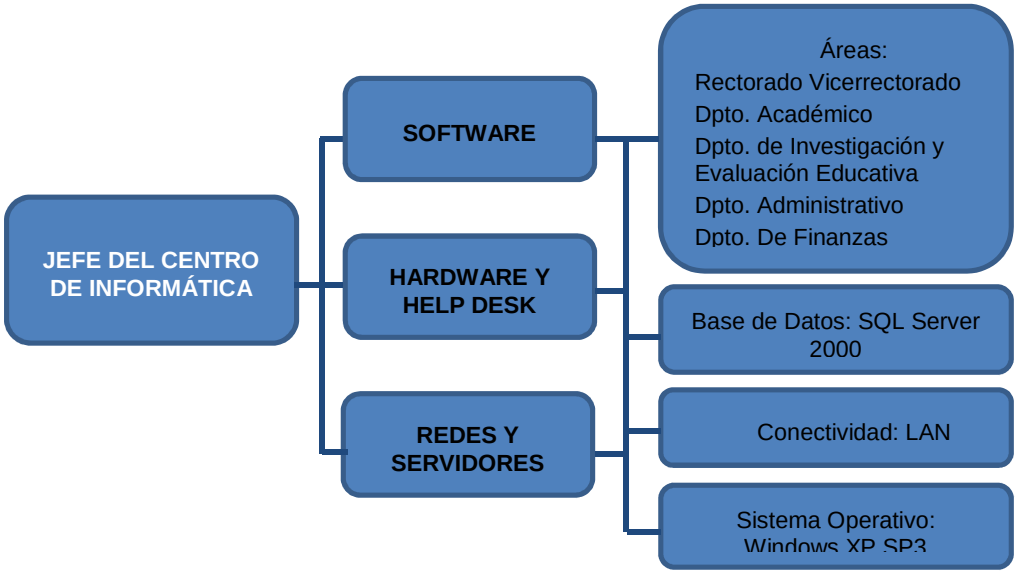

Figura 2 Procesos del Centro de Informática

2.3.4 Monitoreo y Evaluación

Los servicios son medidos por el Jefe del Centro de Informática quien monitorea el funcionamiento de sistemas, base de datos, proyectos de TI y por el administrador de hardware quien evalúa los pedidos de ayuda, esto es un proceso continuo pero no se tiene definido el proceso que permita medir el desempeño de TI en el Centro de Informática. Las acciones correctivas del proceso de monitoreo y evaluación del desempeño junto a las respuestas de gestión se da en base al instructivo del Comando de Educación y Doctrina del Ejército.

2.4 Informe de Auditoría

Los informes de auditoría son el producto final del trabajo del auditor informático, es utilizado para indicar las observaciones y recomendaciones a la Gerencia y se expone la opinión sobre lo adecuado o lo inadecuado de los controles o procedimientos revisados durante la auditoría, se tiene dos tipos de informes como resultado de la Evaluación Técnica Informática: el Informe Ejecutivo y el Informe Detallado, para exponer un informe de auditoría informática, generalmente tiene la siguiente estructura:

- Introducción al informe.
- Observaciones detalladas y recomendaciones de auditoría.
- Respuestas de la gerencia a las observaciones con respecto a las acciones correctivas.
- Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

2.5 Seguimiento de Recomendaciones

El trabajo de auditoría es un proceso continuo, se debe entender que no serviría de nada el trabajo de auditoría si no se comprueba que las acciones correctivas tomadas por la gerencia, se están realizando, para esto se debe tener un programa de seguimiento, la oportunidad de seguimiento dependerá del carácter crítico de las observaciones de auditoría. El nivel de revisión de seguimiento del auditor informático dependerá de diversos factores, en algunos casos el auditor tal vez solo necesite inquirir sobre la situación actual, en otros casos tendrá que hacer una revisión más técnica del sistema.

3. MATERIALES Y MÉTODOS

En la realización de la auditoría del presente trabajo, se empleó técnicas de recopilación de evidencias que se detallan a continuación:

- Revisión de las estructuras organizacionales de sistemas de información.
- Revisión de planes de TI, documentos que inician el desarrollo del sistema, historia de cambios a programas, manuales de usuario, especificaciones de bases de datos, listados de programas.
- Entrevistas con el personal apropiado, las cuales deben tener una naturaleza de descubrimiento no de acusatoria.
- Observación de operaciones y actuación de empleados.
- Auto documentación, el auditor prepara narrativas en base a su observación, cuestionarios de entrevistas realizados y aplicación de técnicas de muestreo pruebas (de cumplimiento o sustantivas).
- Checklist, en la conducción del caso de estudio para comprobar las tareas implementadas en el Centro de Informática.
- Matriz RACI, para delimitar las actividades y los responsables en la conducción del caso de estudio.
- Tabla de observación de tareas, para revisar las políticas y planes existentes de tecnología.
- Hallazgos encontrados, los resultados encontrados en el diagnostico de análisis de resultados.
- Matriz de Riesgos, es la herramienta que documenta los objetivos de control de los procesos evaluando los riesgos de TI.

4. DISEÑO E IMPLEMENTACIÓN

Para este estudio cualitativo se efectúa las siguientes etapas:

- **Elaboración del Marco Teórico:** se hace una revisión de la literatura bibliográfica con el beneficio de construir la perspectiva conceptual de nuestro trabajo.
- **Determinación de situación actual**: se efectúa un análisis de la estructura interna del Centro de Informática del COMIL Nº 10, con el propósito de comprender su organización institucional.

- **Diagnóstico de la Dirección Tecnológica:** se emplea los procesos de control a evaluar con el marco de referencia COBIT, que nos brinda las directrices para establecer su nivel de madurez.

Las fases mencionadas anteriormente presentan un enfoque descriptivo, debido a que se detallan los aspectos que se investiga. La responsabilidad de los controles de TI es una responsabilidad conjunta, entre el negocio y TI, pero la naturaleza de la responsabilidad cambia de la siguiente manera:

- La empresa es responsable de: Definir apropiadamente los requisitos funcionales y de control. Uso adecuado de los servicios automatizados.
- TI es responsable de: Automatizar e implementar los requisitos de las funciones de negocio y de control. Establecer controles para mantener la integridad de controles de aplicación.

Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, la responsabilidad de definir y el uso operativo es de la empresa.

5. RESULTADOS

a) Se ha cumplido con las expectativas de este proyecto por parte del Centro de Informática del Colegio Militar Nº 10 Abdón Calderón y se observó que la Institución ejecuta políticas militares empleando instructivos, teorías y ejecución de ideas generalizadas sin basarse en frameworks de gestión de TI.
b) Se requiere el involucramiento y el apoyo de la alta gerencia y de altos mandos para el éxito del Gobierno de TI, que asegure que las TI de la Institución estén alineadas y acorde a las estrategias y objetivos de la misma.
c) Se detectó una estructura deficiente en cuanto a gestión estratégica de tecnológica se refiere, por lo cual faltan políticas y estándares que ayuden a llevar un control activo de TI.
d) El marco de referencia COBIT, apoyó de manera eficiente el diagnostico a la dirección tecnológica del Centro de Informática del Colegio Militar Nº 10 Abdón Calderón, permitiendo la detección de fallas y la determinación de recomendaciones.
e) La Institución reconoce que el diagnostico del Centro de Informática era totalmente necesario, ya que permite conocer el estado de este, así como las deficiencias que posee en los controles de los procesos evaluados del marco de referencia COBIT, dando hitos para el inicio de una verdadera gestión de tecnología, inexistente en el Centro de Informática del COMIL Nº 10.

5.1 Contribuciones

En el presente trabajo se determinó el estado actual del Centro de Informática en el Colegio Militar Nº 10 Abdón Calderón, se verificaron los lineamientos de los objetivos de control que significa saber el nivel de madurez de los procesos evaluados.

Particularmente contribuyó a establecer un vínculo con los requerimientos de la Institución, organizando las actividades de TI en un modelo de procesos generalmente aceptado, ayudó a entender y administrar los riesgos de TI, además de identificar la forma en que la tecnología puede contribuir de la mejor manera al logro de los objetivos de la Institución en cuanto a una dirección tecnológica apropiada contribuyendo a tomar conciencia de la necesidad de implementar estándares internacionales.

6. CONCLUSIONES Y TRABAJO FUTURO

La importancia estratégica de la información, requiere que el Centro de Informática del Colegio Militar Nº 10 Abdón Calderón adopte un enfoque organizacional que permita enfrentar con éxito los desafíos y responder con efectividad y eficiencia a las demandas actuales y futuras de información.

El Centro de Informática a partir del modelo de COBIT propuesto por este proyecto contará con una herramienta de planeación estratégica y operativa para gestionar TI de manera integral. Se recomienda considerar todos los factores internos y externos establecidos en el informe final de la auditoría.

Fue muy enriquecedor e interesante para el autor de este artículo el análisis de cada objetivo de control presentado durante las diferentes etapas de la auditoría, se identificó los inconvenientes en un nivel estratégico alto, se sugiere verificar el cumplimiento de las recomendaciones del informe final como un trabajo posterior de modo que permita hacer una retroalimentación del proceso de control interno de TI de la Institución.

Cualquier tipo de empresa puede adoptar el estándar de COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos TI y consecuentemente sobre la posibilidad de evaluar el logro de los objetivos del negocio comprometido en procesos tecnológicos.

7. AGRADECIMIENTOS

Agradezco a mi Madre Teresa Mejía, quien me dio la vida y que con su amor y cariño me impulso a dar lo mejor de mí a lo largo de mi vida. A todos mis amigos y familiares que me brindaron su apoyo y paciencia en momentos difíciles.

Mi mas sincero agradecimiento al Ingeniero Mario Ron, por su acertada y desinteresada asesoría, durante la elaboración de este proyecto, por su comprensión y su gran profesionalismo que permitieron que concluya satisfactoriamente el presente trabajo.

8. REFERENCIAS BIBLIOGRÁFICAS

[1] COBIT 4.1 visitada 06/02/2012 Disponible en: www.cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

[2] Comité Directivo de COBIT y el IT Governance Institute (2000), Directrices de Auditoría, Tercera Edición.

[3] Procedimientos de Auditoría de Sistemas, visitada 09/04/2012

Disponible en: www.es.scribd.com/doc/26906140/Procedimientos-de-Auditoria-Se-Sistemas

[4] Cobit Sistema de Investigación visitada 12/03/2012

Disponible en: www.slideshare.net/Jasik/c-o-b-i-t-sistema-de-investigacin

[5] Técnicas y Herramientas TI, visitada 07/03/2012

Disponible en: www.netconsul.com/tecnicas/index.php?ver=cobit

[6] Auditoría Informática, William P. Leonard.