PROPUESTA PARA DESARROLLAR LA EVALUACIÓN TÉCNICA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COSSFA, UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT

Eveline Estrella[1], Sara Alvear[2], Silvia Arévalo[3], Gabriel Chiriboga[4]

1 Escuela Politécnica del Ejército, Ecuador, eveline_ez@yahoo.com

2 Escuela Politécnica del Ejército, Ecuador, sary_870@hotmail.com

3 Escuela Politécnica del Ejército, Ecuador, smarevalo@espe.edu.ec

4 Escuela Politécnica del Ejército, Ecuador, gechiriboga@espe.edu.ec

RESUMEN

El proyecto realizado busca evaluar el correcto desempeño, y aplicar las buenas prácticas que deben establecerse en la gestión de TI, para esto se realizó una Auditoría Informática utilizando el marco de referencia COBIT, el mismo que permitió evaluar cómo se está desarrollando la administración de la tecnología en la Gerencia de TI del Comisariato de Servicio Social de las Fuerzas Armadas – COSSFA.

Se determinaron los procesos críticos que maneja el comisariato, lo que permitió determinar los riesgos que vulneran la Gerencia de TI, en base a estos se obtuvo una visión clara de lo que se debía auditar, lo que conllevó a la elaboración de una investigación de campo para evidenciar las debilidades de la Gerencia de TI.

A través del Marco de Referencia COBIT y los instrumentos utilizados para evaluar las diferentes áreas que componen la Gerencia de TI. Se emitieron recomendaciones basadas en el criterio de las mejores prácticas de TI que propone COBIT.

Se presentaron informes con el detalle de los hallazgos críticos que afectan la gestión de la gerencia de TI, y un resumen ejecutivo con los principales hallazgos de la evaluación realizada, el mismo que permitió tener una visión más clara de los problemas que se deben confrontar. Esta evaluación les va a permitir mejorar la administración de las tecnologías que gestiona la gerencia de TI del comisariato.

Palabras Clave: COBIT, TI.

ABSTRACT

This project seeks to assess the proper performance, and implement best practices in the management of IT, for this it was audited computing using COBIT framework, allowing it to assess how the administration is developing the technology in IT Management of “Comisariato de Servicio Social de las Fuerzas Armadas – COSSFA”.

We have determined the critical processes that the organization handle, which allowed us to determine the risks that make IT Management vulnerable, based on these we obtained a clear vision of what should be audited, which let us to demonstrate the weaknesses of IT Management.

Through COBIT Framework and the tools used to assess the different areas that make up the IT management. Recommendations were based on the criterion of best practices proposed by COBIT.

Reports were presented with details of critical findings that affect the IT management, and an executive summary with the main findings of the evaluation, which allowed COSSFA to have a clearer idea of the problems that must be confronted. This evaluation will allow to better managing the technologies of IT management commissary.

KeyWords: COBIT, TI.

1. INTRODUCCIÓN

Las empresas durante los últimos años han multiplicado esfuerzos para obtener información veraz, la cual le permita una mejor toma de decisiones, tanto para buscar nuevos mercados, como para proteger a la empresa de agentes externos que puedan vulnerar su estabilidad, motivo por el cual se caracteriza a la información como uno de los activos de la empresa, un recurso que se encuentra al mismo nivel que los recursos financieros, materiales y humanos, que hasta el momento habían constituido los ejes sobre los que había girado la gestión empresarial. “Si la teoría económica tradicional mantenía el capital, la tierra y el trabajo como elementos primarios de estudio, la información se ha convertido, ahora, en el cuarto recurso a gestionar”.

El conocimiento del entorno, en un mundo cada vez más complejo y cambiante, origina la necesidad de evaluar los sistemas tecnológicos, que es donde se genera la información que permite el correcto desarrollo de la empresa.

El Comisariato de Servicio Social de las Fuerzas Armadas, con el apoyo de la tecnología genera y administra grandes cantidades de información que son fundamentales para el correcto desempeño de la línea de negocio. Los responsables de informática día a día tienen que enfrentar grandes desafíos para mantener operativo el comisariato, por lo que es necesario realizar una evaluación informática, que permitirá evaluar y verificar políticas, controles, procedimientos y seguridad de los recursos dedicados al manejo de la información.

2. AUDITORÍA BASADA EN RIESGOS

Con la ejecución de la presente auditoría fundamentada en el estándar internacional COBIT, se realizaron los siguientes pasos:

- Planeación de la Auditoría.
- Desarrollo de la Auditoría (Recopilación de la Información).
- Emisión del Informe de Auditoría (Observaciones y Recomendaciones).

Para el desarrollo de este proyecto se utilizó una auditoría basada en riesgos la misma que permitió identificar, medir y priorizar las áreas más críticas con el fin de que el mayor esfuerzo sea realizado en las de mayor relevancia, como se muestra en la figura 1.

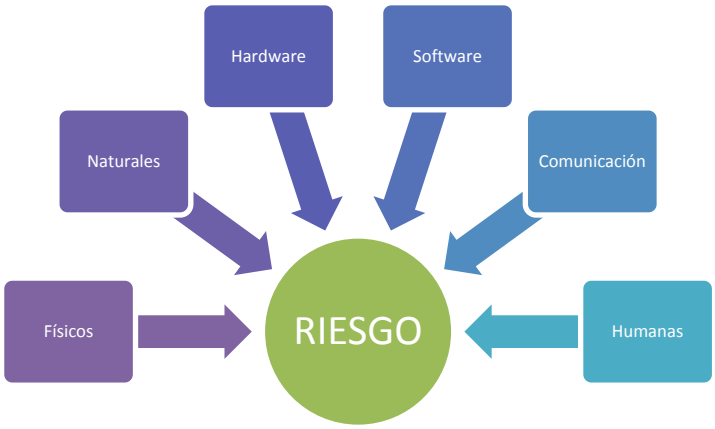

Figura 1: Áreas de Riesgo

Bajo la auditoría basada en riesgos, se realizó el análisis de la industria en la cual opera el comisariato, la estrategia de éste para lograr una ventaja competitiva sostenible en el contexto de su industria, los riesgos del negocio que amenazan el éxito de la estrategia y las respuestas del mismo a estos riesgos.

El análisis de riesgos permite el estudio de las diferentes estrategias de continuidad y el desarrollo de los respectivos procedimientos a emplearse ante la ocurrencia de un desastre (Inundaciones, Terremotos, Erupción Volcánica), el cual comprometa a las operaciones de la organización.

La principal aportación de este tipo de auditoría permite determinar las diferentes falencias y fortalezas que presentan en la actualidad los activos de la organización y se exponen las diferentes salvaguardas, estrategias y recomendaciones que permitirán la continua operación del negocio.

3. MARCO DE REFERENCIA COBIT

COBIT es un Marco de referencia de procesos y objetivos de control TI que pueden ser implementados para controlar, auditar y administrar la organización TI. Este Marco de referencia está basado en las mejores prácticas y sistemas de información de auditoría y control. Esto en particular aspira a ayudar a los líderes empresariales a entender y administrar los riesgos relacionados con la Tecnología de

la Información y la relación entre los procesos de administración, las preguntas técnicas, la necesidad de controles y los riesgos.

Está estructurado por 4 campos principales de administración, los cuales a su vez implican 34 procesos de administración asociados con la tecnología de la información. Cada proceso TI provee una descripción de los requerimientos del negocio e identifica los asuntos claves que deben ser llevados a cabo para administrar exitosamente estos procesos.

COBIT ofrece un conjunto de herramientas para administrar los procesos TI unificando los dos puntos de vista, el de la administración y el del auditor. Las Guías de Administración TI consideran los controles TI desde una perspectiva de la administración, mientras que las Guías de Auditoría proveen asistencia específica a los auditores en el diseño de programas adecuados de auditoría para cada dominio. COBIT también provee herramientas detalladas y personalizables de auto evaluación en forma de matrices y plantillas para asistir en la evaluación y medición de la organización comparada con los criterios de COBIT.

Para la definición de los requerimientos del negocio sobre la información, COBIT se basó en importantes estándares de calidad (Ej. Normas ISO), regulatorios (Ej. Informe COSO) y de seguridad (Ej. Systrust). De esta manera logra definir que las principales características que la organización debe esperar de la información son (7):

- Efectividad.- Información relevante y pertinente para el proceso del negocio, así como su entrega se debe realizar de manera oportuna, correcta, consistente y debe ser utilizable.
- Eficiencia.- Proveer la información a través de la utilización óptima (más productiva y económica) de recursos.
- Confidencialidad.- La información sensible debe ser protegida contra divulgación no autorizada.
- Integridad.- Precisión y suficiencia de la información, válida de acuerdo con los valores y expectativas del negocio.
- Disponibilidad.- De la información cuando ésta es requerida por el proceso de negocio en el presente y futuro. Salvaguardar de los recursos necesarios y capacidades asociadas.
- Cumplimiento.- De leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto.
- Confiabilidad.- Proveer de información apropiada a la administración, para operar la entidad y ejercer sus responsabilidades.

3.1 Relación de los Recursos TI

Para la administración exitosa de un ambiente informático se deberán tomar en cuenta los siguientes recursos:

- 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.

Para entender la combinación de los dos componentes anteriores (Requerimientos del Negocio y Recursos TI) se debe comprender que la información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI, como se muestra en la figura 2.

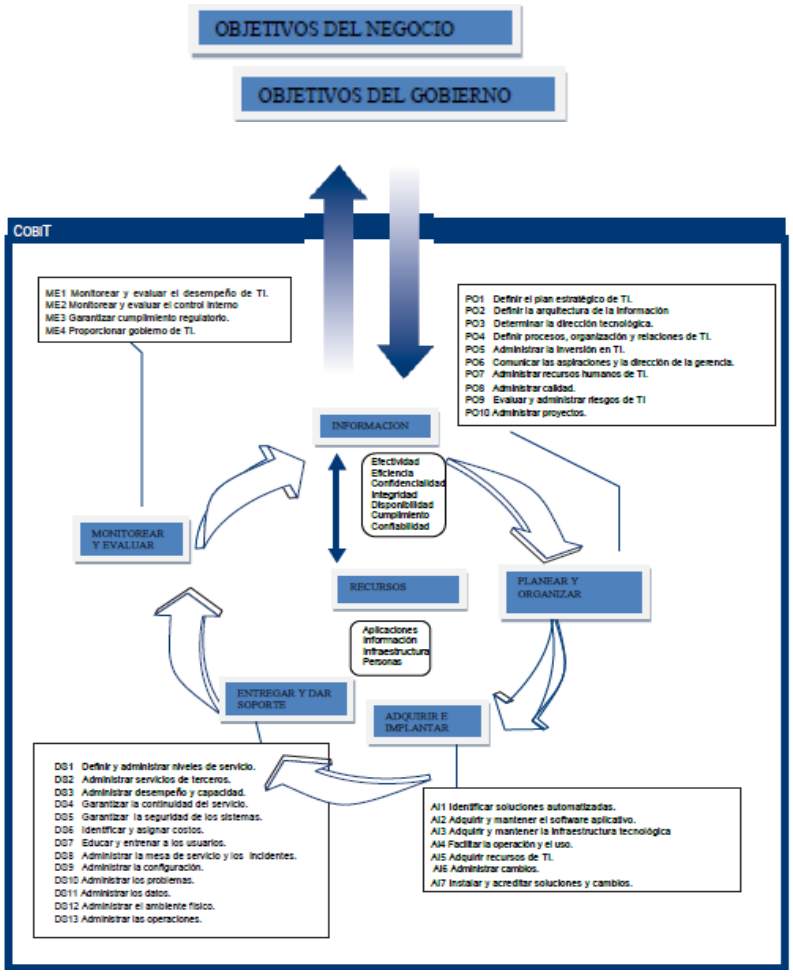

Figura 2: COBIT en Resumen[1]

[1] Tomado de Cobit 4.0 Español

Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se defina sus responsabilidades. Para gobernar TI efectivamente, es importante determinar las actividades y los riesgos que requieren ser administrados.

Normalmente se ordenan dentro de dominios de responsabilidad de planear, construir, ejecutar y monitorear.

- Planeación y Organización(PO).- Este dominio cubre la estrategia y las tácticas, se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.
- Adquisición e Implementación(AI).- Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio.
- Dar Soporte(DS).- En este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios.
- Monitorear y Evaluar(ME).- Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

4. RESULTADOS

Para el desarrollo del análisis de riesgos se ha utilizado la siguiente matriz de riesgos, presentadas en las tablas 1, 2, 3, 4, la misma que se desarrolló basado en los objetivos de control de COBIT enfocándose en los riesgos y procesos críticos de la organización.

Objetivos de Control	Auditado		Controles		Riesgo			Documentación	
	SI	NO	SI	NO	ALTO	MEDIO	BAJO	SI	NO
PLANEACIÓN y ORGANIZACIÓN									
PO1 Definir un plan estratégico para IT									
PO1.4 Plan Estratégico de TI	X		X		X				X
PO1.5 Planes Tácticos de TI	X		X		X				X
PO3 Determinar la Dirección Tecnológica									
PO3.1 Planeación de la Dirección Tecnológica	X		X		X				X
PO3.2 Plan de Infraestructura Tecnológica	X				X			X	

PO4 Definir los Procesos, Organización y Relaciones de TI									
PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento	X		X		X				X
PO5 Administrar la Inversión en TI									
PO5.2 Prioridades Dentro del Presupuesto de TI	X		X		X			X	
PO7 Administración de Recursos Humanos de TI									
PO7.2 Competencias del Personal	X		X		X			X	
PO8 Administrar la Calidad									
PO8.1 Sistema de Administración de Calidad	X		X		X				X
PO8.2 Estándares y Prácticas de Calidad	X		X		X				X
PO9 Evaluar y Administrar los Riesgos de TI									
PO9.1 Marco de Trabajo de Administración de Riesgos	X		X		X			X	
PO10 Administración de Proyectos									
PO10.2 Marco de Trabajo para la Administración de Proyectos	X		X		X			X	

Tabla 1: Planeación y Organización

ADQUISICIÓN e IMPLEMENTACIÓN									
AI1 Identificar Soluciones Automatizadas									
AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio			X		X			X	
AI1.2 Reporte de Análisis de Riesgos				X	X				X

AI2 Adquirir y Mantener Software Aplicativo									
AI2.3 Control y Posibilidad de Auditar las Aplicaciones			X		X			X	
AI2.8 Aseguramiento de la Calidad del Software			X		X			X	
AI2.10 Mantenimiento de Software Aplicativo			X		X			X	
AI3 Adquirir y Mantener Infraestructura Tecnológica									
AI3.1 Plan de Adquisición de Infraestructura Tecnológica			X		X			X	
AI3.3 Mantenimiento de la Infraestructura			X		X			X	
AI4 Facilitar la Operación y el Uso									
AI4.4 Transferencia de Conocimiento al Personal Operaciones y Soporte			X		X			X	
AI6 Administración de cambios									
AI6.3 Cambios de Emergencia			X		X			X	
AI6.4 Seguimiento y Reporte del Estatus de Cambio									X

Tabla 2: Adquisición e Implementación

ENTREGA DE SERVICIOS Y SOPORTE									
DS1 Definir y administrar los niveles de servicio									
DS1.3 Acuerdos de Niveles de Servicio			X		X			X	
DS1.5 Monitoreo y Reporte del Cumplimiento de los Niveles de Servicio			X		X			X	
DS4 Garantizar la continuidad del servicio									
DS4.1 Marco de Trabajo de Continuidad de TI			X		X			X	

DS4.3 Recursos Críticos de TI			X		X			X	
DS4.4 Mantenimiento del Plan de Continuidad de TI			X		X			X	
DS4.5 Pruebas del Plan de Continuidad de TI			X		X			X	
DS5 Garantizar la seguridad de los sistemas									
DS5.1 Administración de la Seguridad de TI			X		X			X	
DS8 Administrar la Mesa de Servicio y los Incidentes									
DS8.1 Mesa de Servicios			X		X			X	
DS10 Administrar los problemas									
DS10.1 Identificación y Clasificación de Problemas			X		X			X	
DS10.2 Rastreo y Resolución de Problemas			X		X			X	
DS12 Administrar el ambiente físico (Instalaciones)									
DS12.1 Selección y Diseño del Centro de Datos				X	X				X
DS12.2 Medidas de Seguridad Física			X		X			X	
DS13 Administrar las operaciones									
DS13.5 Mantenimiento Preventivo del Hardware			X		X			X	

Tabla 3: Entrega de Servicios y Soporte

Monitorear y Evaluar									
M1 Monitorear y Evaluar el Desempeño de TI									
ME1.4 Evaluación del Desempeño	X		X		X			X	
ME1.5 Reportes al Consejo Directivo y a Ejecutivos	X		X		X			X	

M2 Monitorear y Evaluar el Control Interno									
ME2.1 Monitoreo del Marco de Trabajo de Control Interno	X		X		X			X	

Tabla 4: Monitorear y Evaluar

5. CONCLUSIONES Y RECOMENDACIONES

Al culminar el proyecto de evaluación técnica e informática de los sistemas tecnológicos de información del Comisariato de Servicio Social de la Fuerzas Armadas, se ha cumplido con los objetivos propuestos al inicio del trabajo, por lo tanto se exponen a continuación las siguientes conclusiones y recomendaciones en torno a la realización del proyecto.

5.1 Conclusiones

- Para el desarrollo de una Evaluación Técnica Informática de los Sistemas de Información es de vital importancia contar con la guía de un marco de referencia. Para este proyecto se escogió el modelo COBIT, el cual a través de sus 4 dominios ofrece una serie de objetivos de control que permiten evaluar eficientemente el ambiente de control de una entidad, garantizando que TI esté alineada con el negocio y que los riesgos de TI se administren apropiadamente.
- Al alinear la Normativa respecto a Tecnologías de la Información y los objetivos de control propuestos por COBIT se logró identificar y valorar los riesgos dentro de la entidad para tomar las medidas pertinentes y minimizar la materialización de los riesgos identificados.
- Durante el análisis y evaluación del ambiente de control en la entidad aplicando los dominios propuestos por COBIT se logró identificar debilidades obteniendo observaciones y recomendaciones que fueron emitidas en el informe final. Para llevar a cabo el proceso de la Auditoria es de suma importancia contar con el compromiso y apertura a la Evaluación Técnica de los sistemas de información; de los principales involucrados como son las Autoridades superiores del COSSFA, el personal de la Gerencia de TI y el Departamento de Auditoría Interna.
- La Auditoria de TI en el COSSFA propone mejoras a los controles existentes, pues sabiendo que si los controles facilitan la rendición de cuentas mediante la evidencia; al mejorar los controles que están fallando se logrará mitigar los riesgos. La Administración debe identificarse y conocer plenamente los controles.

5.2 Recomendaciones

- Establecer un plan para la ejecución de las recomendaciones especificadas en el Informe Detallado de la Evaluación Técnica Informática, Matriz de Correlación de COBIT emitido por las evaluadoras.

- Se recomienda la certificación de estándares de calidad, para la mejora de los procesos dentro de la empresa.

6. AGRADECIMIENTOS

Especial agradecimiento al personal que conforma todas las áreas de la Gerencia de TI de COSSFA por el constante apoyo e información proporcionada concernientes a las áreas en las cuales colaboran prestando sus servicios profesionales. A la Ing. Silvia Arévalo Directora de Tesis, Ing. Gabriel Chiriboga Codirector de Tesis e Ing. Mario Ron por todo el apoyo y conocimiento brindado para que la ejecución de este proyecto.

7. REFERENCIAS BIBLIOGRÁFICAS

[1] Libro Auditoría, W. Messler, Julio 1996. Mc Graw-Hill.

[2] Riesgos Informáticos, http://audifinysis.blogspot.com/

[3] Control de Riesgos, http://www.slideshare.net/jaimeramos/gestin-de-riesgos-4567008

[4] Auditoria de Sistemas, http://html.rincondelvago.com/auditoria-de-los-sistemas-de-informacion.html

[5] Sistemas de Información, http://www.monografias.com/trabajos10/ausi/ausi.shtml

[6] Tipos de Auditoría, http://www.oocities.org/mx/acadentorno/aui1.pdf

[7] Control Interno, http://www.monografias.com/trabajos63/control-interno-auditoria/control-interno-auditoria2.shtml

[8] Elementos de una Auditoria Informática, http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

[9] Auditoría de Sistemas de Información, http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf

[10] Normas COBIT, http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml