AUDITORIA DE RIESGOS INFORMATICOS A PYMES UTILIZANDO COBIT COMO MARCO DE REFERENCIA

JORGE GEOVANNI AUCANCELA SOLIZ

CAVES SA EMA - Tumbaco Sector Villa vega
www.caves-ghl.com.ec

RESUMEN

Un elemento crítico para el éxito y la supervivencia de las empresas, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada, considerados como los activos más valiosos.

Es necesario la implementación de un método de control o auditoria informática para tener una dimensión concreta del área de sistemas, de sus debilidades y fortalezas, y establecer medidas de control.

Se inicia con la definición de un procedimiento de selección de Procesos COBIT a ser Auditados, que garantice que estos están Alineados a los Objetivos del Negocio. Para seguidamente plantear una estrategia de auditoría definida para obtener resultados que permita identificar el Grado de Madurez de estos procesos, y de esta manera definir los Posibles Proyectos que deberían ser implementados para disminuir la brecha del nivel de madurez actual con el propuesto.

(Palabras clave: RIESGOS, MADUREZ, COBIT)

ABSTRACT

A critical element to the success and survival of companies, is effective management of information and information technology (IT) related, regarded as the most valuable assets.

You need to implement a method of control or audit information for a particular dimension of the area of systems, their weaknesses and strengths, and control measures.

It starts with the definition of a selection procedure COBIT processes to be audited, to ensure that these are aligned to business objectives. To then ask a defined audit strategy for results to identify the maturity assessments. of these processes, and thus define the possible projects that should be implemented to reduce the gap of current maturity level with the proposed.
(Key Words: Risk, Maturity, COBIT)

1. INTRODUCCION

Las PYMES, al igual que las grandes empresas, se ha vuelto cada vez más dependientes de la tecnología para manejar sus actividades de forma ágil y correcta, la disponibilidad de los sistemas informáticos se ha vuelto un aspecto crucial. Actualmente, se necesita un alto y continuo nivel de disponibilidad, ya que resultaría extremadamente difícil funcionar sin los recursos informáticos.

Estas son las razones entre otras por las que se hace muy necesario implementar un plan de auditoría en el área de sistemas de la empresa, con el fin de establecer lineamientos para que en el futuro puedan implementar y estandarizar procesos y procedimientos que no se los tenía antes, con el fin de mejorar el orden que se tiene al momento e incrementar la productividad y efectividad del área.

2. OBJETIVOS

2.1 Objetivo general

Evaluar la situación actual del Departamento de Sistemas de una PYME, utilizando COBIT como marco de referencia, y presentar alternativas de Proyectos Informáticos que deberán ser implementados, para minimizar los riesgos informáticos y conseguir incrementar la satisfacción de los usuarios de los sistemas automatizados.

2.2 Objetivos específicos

- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Presentar alternativas de Proyectos a corto mediano y largo plazo que permitirán asegurar una mayor integridad, confidencialidad y confiabilidad de la información
- Minimizar existencias de riesgos en el uso de Tecnología de información

3. MATERIALES Y METODOS.

3.1 MARCO DE REFERENCIA COBIT

COBIT : Objetivos de Control para la Información y Tecnologías Afines (Control Objetives for Information and related Technology).

COBIT: “ENFOCADO EN EL NEGOCIO, ORIENTADO A PROCESO, BASADO EN CONTROLES Y DIRIGIDO POR MEDIDAS.”

COBIT marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares.

Como se asegura la empresa que TI alcanza los objetivos y soporta el negocio?

- Definiendo objetivos de control que aseguren que:
  - Se alcancen los objetivos de negocio
  - Se prevengan o detecten y corrijan eventos indeseados
- Estableciendo y monitoreando los controles y niveles de funcionamiento de TI apropiados mediante:
  - Mediciones (Benchmarking) de capacidad de proceso de TI expresada como modelos de madurez.
  - Metas y Métricas de los procesos de TI para definir y medir sus resultados y funcionamiento (Balanced ScoreCard)

3. 2 PROCEDIMIENTO SELECCION DE PROCESOS COBIT A SER AUDITADOS

Selección de los procesos mediante la relación de procesos críticos del negocio y las metas del negocio propuesto por COBIT.

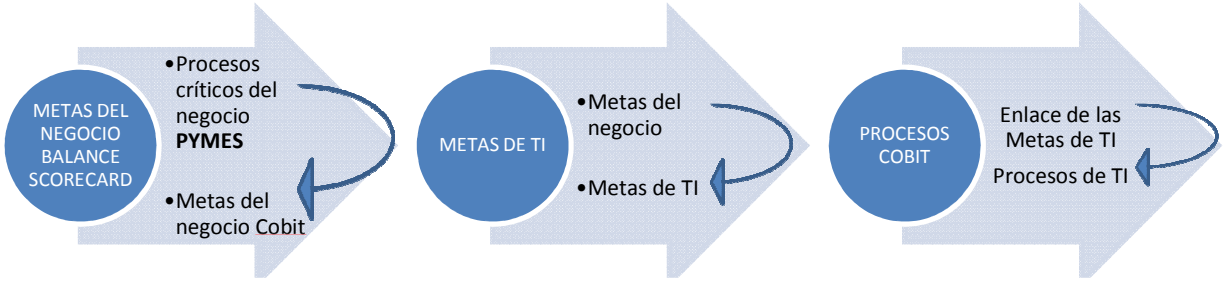

Figura 1. Procedimiento Selección de Procesos Cobit a ser Auditados

Como se muestra en la Figura 1, el procedimiento se inicia con la relación de los procesos críticos de una PYME y las Metas del Negocio Propuesto por Cobit, con el objetivo de seleccionar la Metas del Negocio en sus diferentes perspectivas, que se logren alinear con los procesos críticos del Negocio. Luego se obtiene las Metas de TI que están asociadas a las Metas del Negocio de Cobit, finalmente mediante el uso de la matriz de Procesos de TI con las Metas de TI, se realiza una ponderación para determinar los
Procesos COBIT a Auditar en la Empresa.

Como caso de estudio se realizó en la empresa CAVES SA EMA, se obtuvo los Procesos COBIT que deben ser Auditados:

DOMINIO: PLANEACION Y ORGANIZACION

PO9 Evaluación y Gestión de riesgos

DOMINIO: ENTREGA Y SOPORTE

DS5 Aseguramiento de la seguridad de los sistemas
DS8 Gestión de incidentes y de la mesa de soporte

3.3 ESTRATEGIA AUDITORIA DE PROCESOS COBIT SELECCIONADOS.

La Auditoria se realiza según los objetivos de control de COBIT mediante el cumplimiento de las Fase que se detallan a continuación:

- Obtención de entendimiento
- Evaluación de Controles COBIT
- Indicadores Claves de Rendimiento.
- Identificación del Nivel de Madurez Actual.
- Razones por Nivel de Madurez establecido.
- Definición de niveles de madurez e impacto en el negocio.
- Recomendaciones y Plan de Acción

4. RESULTADOS

4.1 DEFINICIÓN DE NIVELES DE MADUREZ E IMPACTO EN EL NEGOCIO.

Dominios y Procesos de Tecnología de Cobit 4.1			Nivel Actual	Causa	Nivel Objetivo	Causa	Brecha	Impacto		
								A	M	B
PLANEAR Y ORGANIZAR	PO9	*Evaluar y administrar los riesgos de TI*	0	No Existe una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera intuitiva	2	Definir una Metodología Formal para Administrar el Riesgo y al menos aplicar a los proyectos importantes . Los procesos de mitigación de riesgos deben ser implementados donde se identifiquen los riesgos.	2		X	
ENTREGAR Y DAR SOPORTE	DS5	*Garantizar la seguridad de los sistemas*	1	La empresa reconoce la necesidad de la seguridad de TI. La seguridad de TI se atiende de forma reactiva. La seguridad de TI no se mide. Las violaciones de seguridad de TI detectadas provocan respuestas de asignación de culpas dado que las responsabilidades no están claras.	3	Concientizar a gerencia. Definir la política de seguridad de TI, Establecer procedimientos de seguridad de TI alineados con la política de seguridad. Establecer responsabilidades de seguridad de TI. Definir un plan de seguridad de TI de acuerdo al análisis del riesgo. Establecer pruebas de seguridad ad hoc. Definir plan de capacitación en seguridad.	2		X	
	DS8	*Administrar la mesa de servicio y los incidentes*	1	No existe personal y herramientas automatizadas para responder a las consultas de los usuarios y para administrar la resolución de problemas. El proceso no está estandarizado y solo se proporciona soporte reactivo. No existe seguimiento a las consultas y problemas de los usuarios. No hay un proceso de jerarquización para garantizar que los problemas sean resueltos.	3	Implementación de una mesa de soporte y de un proceso de administración de incidentes. Los procedimientos deben ser estandarizados y documentados. Desarrollar una Base de datos con una lista de preguntas frecuentes (FAQs) y de directrices de usuario. Realizar Seguimiento a Las consultas y los incidentes. Los usuarios deben recibir instrucciones claras respecto a dónde y cómo informar acerca de los problemas e incidentes.	2	X		

Figura 2. Definición de Nivel de Madurez de la Empresa

5. CONCLUSIONES Y TRABAJO FUTURO.

La empresa CAVES SA EMA, objeto de la Auditoria de riesgos informáticos utilizando Cobit como marco de Referencia, obtuvo resultados que permitieron identificar el Nivel de Madurez que se encuentra los diferentes procesos COBIT seleccionados, permitiendo emitir recomendaciones para la implementación de diversos proyectos tecnológicos y de gestión que permitan disminuir la brecha existente entre el Nivel de madurez actual y el propuesto a alcanzar.

Se recomienda ejecutar los siguientes Proyectos de Inversión de Tecnología para los procesos Auditados con mayor impacto en la empresas para que mediante su la implementación disminuya la brecha de Nivel de Madurez identificada .

PROCESO		Nivel Actual	Nivel Objetivo	Se Requiere	Secuencia Proyecto a Ejecutar	PROYECTO PROPUESTO
PO9	*Evaluar y administrar los riesgos de TI*	**0**	**2**	Definir una Metodología Formal para Administrar el Riesgo . Los procesos de mitigación de riesgos deben ser implementados donde se identifiquen los riesgos.	**1**	IMPLEMENTACION DE MAGERIT COMO UNA SOLUCION PARA EL ANALISIS Y GESTION DE RIESGOS.
DS5	*Garantizar la seguridad de los sistemas*	**1**	**3**	Definir la política de seguridad de TI, Establecer procedimientos de seguridad de TI alineados con la política de seguridad. Establecer responsabilidades de seguridad de TI. Definir un plan de seguridad de TI de acuerdo al análisis del riesgo. Definir plan de capacitación en seguridad.	**2**	ELABORACIÓN DE UN PLAN DE GESTION DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 17799
DS8	*Administrar la mesa de servicio y los incidentes*	**1**	**3**	Implementación de una mesa de soporte y de un proceso de administración de incidentes. Los procedimientos deben ser estandarizados y documentados. Desarrollar una Base de datos con una lista de preguntas frecuentes (FAQs) y de directrices de usuario. Realizar Seguimiento a Las consultas y los incidentes.	**3**	IMPLEMENTACION DE SYSID COMO UNA SOLUCION DE MESA DE AYUDA BASADO EN LAS MEJORES PRÁCTICAS DE ITIL.

Figura 3. Proyectos Propuestos

La Figura 3 muestra los Procesos COBIT Auditados, con los niveles de madurez Actual y el Nivel Objetivo a alcanzar mediante la implementación del proyecto propuesto, adicionalmente se detalla la secuencia en que se debería ejecutar los Proyectos.

Estos Proyectos de Inversión propuesto contiene la siguiente información relevante: Objetivos, metodología a utilizar, se detalla los Recursos Humanos, Materiales, Actividades a ejecutarse, y la Gestión Económica del proyecto.

6. CITAS DENTRO DEL TEXTO.

La información, en todas sus formas (automatizada o no automatizada, formalizada o no formalizada, pública o reservada, etc.), es uno de los principales activos de cualquier Organización, necesario para el normal funcionamiento y la consecución de los objetivos que tenga marcados. [ISO27001.05] .

En el ámbito de los sistemas de información, el marco de referencia utilizado con mayor frecuencia en conjunción con COSO es COBIT [ISACA07].

7. AGRADECIMIENTOS: A CAVES SA EMA , en especial al personal del Departamento de Tecnología y Sistemas quienes contribuyeron con la investigación del presente artículo.

8. REFERENCIAS BIBLIOGRAFICAS.

- ISACA – Information Systems Audit and Control Association (http://www.isaca.org)
  [ISACA07] Control Objectives for Information and Related Technologies (COBIT), Versión 4.1, ITGI – Information Technology Governance Institute, ISACA, 2007.
- MAGERIT (http://publicaciones.administracion.es)
  [MAGE06] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, versión 2, F. López, M.A. Amutio, J. Candau y J.A. Mañas, Ministerio de Administraciones Públicas, 2006.
- [ISO27001.05] ISO/IEC 27001:2005, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).
- GUÍA DE LOS FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS (GUÍA DEL PMBOK®) Cuarta edición.