AUDITORIA INFORMATICA BASADO EN EL ANALISIS DE RIESGOS DE LA EMPRESA TECNISEGUROS S.A.

Julio Cesar Calderón Carrasco; David Adolfo Ocaña Aldaz
jgato@hotmail.com; davidadolfo@hotmail.com

Universidad de las Fuerzas Armadas – ESPE
Maestría en Evaluación y Auditoría de Sistemas Tecnológicos
Sangolquí, Ecuador
Abril - 2014

RESUMEN: *La auditoría informática basada en riesgos es una técnica que permite enfocar los recursos de auditoría hacia los puntos de mayor importancia dentro de las organizaciones, esta técnica es preventiva ante situaciones o eventos no deseos. Este proyecto tiene como objetivo analizar la situación en la que se encuentra el Departamento de Tecnologías de Información de la empresa Tecniseguros S.A., mediante el desarrollo de una Auditoría Informática Basada en el análisis de riesgos, esta técnica es acompañada por una metodología y un marco de referencia. La metodología MAGERIT 3.0 permite identificar riesgos en los diferentes activos de la empresa. El marco de referencia COSO ERM apoya en el tratamiento de los riesgos identificados, administrándolos a lo largo de todo su ciclo de vida. Cuenta, por citar los más importantes: dominios especializados, desde el Ambiente de control, se revisan los Objetivos, los Riesgos, las actividades de control, llegan hasta la supervisión. La razón de iniciar esta auditoría es el desorden, identificado a nivel macro, en el área de desarrollo de la unidad de tecnología, misma que al momento, cuenta con 200 aplicaciones aproximadamente, entre ejecutables aislados y aplicaciones web, desarrollados en diferentes lenguajes y en bases de datos distribuidas no centralizadas. Al término de la auditoría, Tecniseguros S.A contará con un mapa de riesgos, mismo que permitirá priorizar los proyectos de tecnología y evidenciar las falencias relacionadas al manejo de riesgos en el departamento de tecnología, mejorando la postura de seguridad y funcionalidad.*

Palabras Clave: *Riesgo, auditoría, técnica.*

ABSTRACT: *The risk-based IT audit is a technique that focus the auditing resources to the greatest importance points in organizations, this technique is precautionary and allows to anticipate unwanted situations. The objective of this project is to analyze the actual situation of Information Technology Department of Tecniseguros S.A. Company is, through the development of an IT Audit Based on the risk analysis, the art is accompanied by a methodology and a framework. The MAGERIT 3.0 methodology is used to identify risks in different assets, it has the advantage of analyzing in detail the assets looking for risks. The COSO ERM framework supports the treatment of identified risks, managing them throughout their entire life cycle. It has, to name the most important specialized domains, starting with the Control Environment, Objectives, Risks, control activities and monitoring reach are reviewed. The reason for this audit is the disorder, identified at the macro level, in the development area of technology unit, at the same time, has approximately 200 isolated executable applications developed in different development languages and distributed databases and not centralized. At the end of the audit, Tecniseguros S.A. will have a risk map, which will allow them to prioritize technology projects and highlight the weaknesses related to risk management in the technology department, improving the security posture and functionality.*

KEYWORDS: *Risk, audit, technique.*

1. INTRODUCCIÓN.

Tecniseguros S.A. es una empresa del Grupo Futuro, los sistemas de Tecniseguros S.A. responden a los procesos organizacionales, por mencionar los principales tenemos: la parte financiera, registro de operaciones y la emisión de estados financieros. Debido a que la empresa cuenta con un desarrollo interno de software orientado a los procesos del negocio, se ha generado un desorden en los aplicativos resultantes, desarrollados en diferentes lenguajes de programación, bases de datos y dependencia hacia el personal de desarrollo.

El equipo trabaja con aproximadamente 200 aplicaciones, entre las que podemos citar, al sistema principal, mantenimiento de productos, reportería, gestión de renovaciones, cotizadores, entre otros. Estas aplicaciones se ejecutan como aplicaciones cliente servidor y aplicaciones web, con acceso a datos que se encuentran en un repositorio centralizado, constituido por varias bases de datos, distribuidas geográficamente en un motor MSQL 2008

No existe una normativa o estándar de desarrollo, formal o informal, dificultando el desarrollo de nuevas aplicaciones o el mantenimiento de las existentes. Al existir una única base de datos, sobre la que todas las aplicaciones tienen acceso, existe el riesgo de afectar dicha base al modificar un programa.

La empresa tiene alta dependencia a los desarrolladores, lo que trae complicaciones cuando estas personas se encuentran ausentes o se separan de la empresa, elevando los tiempos de respuesta o causando paralización del servicio de desarrollo y mantenimiento de aplicaciones.

El equipo de aseguramiento de la calidad tiene toda la responsabilidad de validar las aplicaciones, no existen ambientes homogéneos de desarrollo, pruebas y control de calidad, esto genera riesgo al momento de pasar a producción las nuevas aplicaciones o sus modificaciones, y en muchos casos, únicamente se valida el impacto del cambio en una aplicación y no en todas las aplicaciones, por lo que, este control llega a fallar.

No se ha realizado un modelamiento de la base de datos, por lo cual no se conoce las relaciones entre todas ellas.

Las aplicaciones son validadas y verificadas por el desarrollador y el asegurador de la calidad, todo esto en la misma máquina del desarrollador y las pruebas reales se hacen en producción, en donde los usuarios son quienes reportan los fallos.

Existe alto pedido de cambios en el funcionamiento de las aplicaciones, generalmente con tiempos cortos de desarrollo y pruebas, tampoco existe conciencia sobre las actividades de estabilización de las aplicaciones.

La auditoría basada en el Análisis de riesgos aplica dos metodologías, el marco de referencia COSO ERM para el manejo de riesgos y la metodología MAGERIT 3.0 para la identificación de amenazas.

El aporte de esta auditoría informática en la Empresa Tecniseguros S.A, es servir de herramienta base, mediante la cual, se identifican los riesgos del área de tecnología, se categorizan los riesgos de acuerdo a su probabilidad e impacto, sugiere una respuesta al riesgos y termina con un informe de auditoría en el que se destacan las principales observaciones para tener un diagnóstico de la situación actual y poder tomar medidas de acción.

2. METODOLOGÍA.

Esta investigación es de tipo inductiva, basada en el concepto global de llegar a lo específico, el cual inicia identificando cada una de las variables de la problemática establecida, de esta manera se establecerá la relación causa - efecto entre los elementos que componen la investigación, logrando una síntesis de la problemática.

Las técnicas y procedimientos utilizados para esta investigación son la observación (analizar el flujo de la información en todos los procesos) y la encuesta (realizada a los clientes o usuarios de los sistemas).
La información obtenida es tabulada y sometida a técnicas matemáticas de tipo estadístico y manejo de porcentajes, para lo cual se desarrollan tablas de resultados cuyos valores están representados en porcentajes, observados en la sección 3.7.2, tabla 7, página 7, de este artículo.
Este proyecto utiliza dos marcos de referencia, COSO ERM para tratar los riesgos y MAGERIT 3.0 para identificar amenazas en los activos. Estos marcos de referencia o metodologías permiten encontrar los valores de probabilidad e impacto de un evento, de esta manera, se multiplican los valores mencionados y se obtiene un valor entero, que es el riesgo.
COBIT 4.1 es utilizado para determinar el nivel de madurez de los procesos de TI.

3. EVALUACIÓN DE RESULTADOS

Aquí se presentan los resultados, de acuerdo al planteamiento de la evaluación.

3.1. Evaluación de Impacto

El impacto es un valor estimado, resultado de encontrar la afectación que puede tener un evento en Tecniseguros S.A. El resultado está clasificado en 5 niveles (Ver tabla 1.)

Impacto	
5	Alto
4	Crítico
3	Requiere Atención
2	Manejable
1	Nulo (Sin Riesgos)

Tabla 1. Evaluación de Impacto
Elaborado por: Los autores

El valor 1 (Nulo), equivale a que no se identifica ningún impacto. El valor 2 (Manejable), equivale a impactos manejables con un mínimo esfuerzo por parte del negocio. El valor 3 (Requiere atención), es utilizado si se requiere de acciones estructuradas por parte de la organización para remediar el incidente, sin embargo, Tecniseguros S.A. mantiene sus procesos en ejecución. El valor 4, (Crítico), se utiliza cuando librar el evento requiere de acciones específicas, conocidas y repetibles, la organización detiene parcialmente sus procesos y su operación. El nivel 5 (Alto), es utilizado cuando los procesos de la organización se detienen, existe perdida de servicio y el cliente final no puede ser atendido, requiere de acciones de emergencia para salvar el inconveniente.

3.2. Evaluación de Probabilidad

Esta evaluación se clasifica en una escala basada en la experiencia del negocio, es decir, se basa en el conocimiento de la probabilidad de una incidencia u ocurrencia de un evento, para lo cual se identificó 4 niveles. (Ver tabla 2).

Probabilidad	
1	Baja
2	Media Baja
3	Media Alta
4	Alta

Tabla 2. Evaluación de Probabilidad
Elaborado por: Los autores

El valor de probabilidad es un porcentaje calculado en base a la expectativa de ocurrencia al año, (Baja) equivale a menos del 25% y el valor (Alta), supera el 75% anual.

3.3. Evaluación de riesgos

El riesgo es un valor resultante, producto de la probabilidad y el impacto, sin embargo, la simple multiplicación no refleja completamente la realidad, para obtenerla colocamos los datos de probabilidad e impacto en una matriz, de modo que formamos 4 cuadrantes. (Ver tabla 3).

Impacto					
	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
	0	1	2	3	4
	Probabilidad				

Tabla 3. Tabla Medidas de Riesgo
Elaborado por: Los autores

Los riesgos en color verde, son aceptados y no tienen una respuesta mayor, salvo en casos excepcionales, son considerados pequeños.
Los riesgos en color amarillo del cuadrante superior son compartidos, es decir, aunque el impacto es alto la probabilidad es pequeña, por lo que, no es recomendable poner controles, pero los seguros y las pólizas pueden constituirse en elementos requeridos. Por otro lado, los riesgos en color naranja del cuadrante inferior son mitigados, es decir, la solución es aplicar controles que prevengan la ocurrencia, por ejemplo, colocar un control de accesos.
Los riesgos del color rojo son evitados ya que constituyen un riesgo no adecuado para el negocio, salvo excepciones, es decir, son acciones que no deben ejecutarse dentro de la empresa ya que constituyen un riesgo mayor a los posibles beneficios. (Ver tabla 3).

3.4. Respuesta al riesgo

La Tabla de medida de riesgo (Ver tabla 3), puede generalizarse y reutilizarse para otras evaluaciones de riesgos en otras compañías, negocios o instituciones.
Los 4 cuadrantes están enfocados en: aceptar, compartir, mitigar y evitar los riesgos. (Ver tabla 4).

Probabilidad/Impacto	Insignificante	Moderado Bajo	Moderado Medio	Alto
Probable	Compartir: Cuando la probabilidad es baja y el impacto es alto		Evitar: En el caso que la probabilidad y el impacto son altos.	
Posible Alta				
Posible Moderada	Aceptar: En el caso que la probabilidad y el impacto es bajo.		Mitigar: Cuando la probabilidad es alta y el impacto es bajo.	
Raro				

Tabla 4. Tabla Respuesta al Riesgo
Elaborado por: Los autores

3.5. Metodología MAGERIT para el Análisis de Riesgos.

MAGERIT ofrece un método sistemático para analizar riesgos y apoyar a determinar su ocurrencia, también apoya a planificar las medidas para mantenerlos bajo control. De esta forma se identifica riesgos por medio de los activos de cada proceso.
Esta metodología revisa 11 procesos, con el objetivo de obtener los riesgos que afectan a los activos y, en consecuencia, los riesgos por proceso, siendo este nuestro punto de partida para proceder a tratar y analizar el riesgo con el Marco de referencia COSO ERM.

Los procesos analizados son:

- Adquisiciones Garantías Equipo Electrónico (P11-01)
- Soporte Técnico (P11-02)
- Administración de Respaldos (P11-03)
- Administración Data Center (P11-04)
- Administración Redes LAN (P11-05)
- Administración Redes WAN (P11-06)
- Mantenimiento de Hardware (P11-07)
- Mantenimiento De Licencias (P11-08)
- Desarrollo y Mantenimiento de Aplicaciones (P11-09)
- Administración de Servidores (P11-10)
- Administración de usuarios (P11-11)

3.6. COSO ERM.

La metodología COSO ERM está orientada al manejo de riesgos de toda la organización en sus diferentes Unidades de Negocio como se puede ver en la parte lateral de la figura (Ver Figura 1), en este caso, usaremos como Unidad de Negocio el Área de Tecnología de Información, en la parte superior del cubo de la misma podemos observar los “Objetivos del Negocio”, del cual usaremos el objetivo de “Cumplimiento”.

De igual manera en la parte frontal se observa los componentes de evaluación (8), que inicia en ambiente de control y llega hasta el monitoreo, el resultado del análisis de cada dominio de evaluación es el punto de partida del siguiente.

Figura 1: El Cubo de COSO ERM

3.7.COBIT.

La metodología COBIT 4.1 es utilizada para determinar el nivel de madurez de los procesos evaluados, las auditorías informáticas tradicionales no contemplan la actividad de obtener el nivel de madurez de los procesos, esta es una tarea más relacionada a las consultorías, sin embargo, se utiliza con el objetivo de añadir valor a esta auditoría.

3.7.1. Modelo de madurez.

COBIT identifica el nivel de madurez y cumplimiento de los procesos de TI, los cuales han sido evaluados durante la ejecución de la auditoría informática. Para calcular el nivel de madurez de los procesos de TI se realiza la división del cien por ciento para los seis niveles de madurez descritos en la tabla 5.

Nivel	Descripción
0	No existente
1	Inicial
2	Repetible
3	Definido
4	Administrado
5	Optimizado

Tabla 5. Tabla Modelo de Madurez
Elaborado por: Los autores

3.7.2. Resumen de los niveles de Madurez por Dominio.

Los 11 procesos evaluados son específicos del Departamento de TI (Ver Párrafo 3.5), para determinar el nivel de madurez de cada proceso los cuales han sido relacionados con el Dominio que lo comprende (Ver Tabla 6).

Relación Dominios de COBIT 4 con Procesos			
Cobit 4	**Dominio**	**Código**	**Proceso**
AI3	Adquirir y Mantener Infraestructura Tecnológica	P11-01	Adquisiciones Garantías Equipo Electrónico
AI6	Administrar Cambio	P11-09	Desarrollo y Mantenimiento de Aplicaciones
DS4	Garantizar la Continuidad del servicio	P11-03	Administración de Respaldos
DS8	Administrar la Mesa de servicio y los incidentes	P11-02	Soporte Técnico
DS12	Administración del Ambiente Fisco	P11-04	Administración Data Center
		P11-05	Administración Redes LAN
		P11-06	Administración Redes WAN
		P11-07	Mantenimiento de Hardware
		P11-08	Mantenimiento De Licencias
		P11-10	Administración de Servidores
PO07	Administrar los Recursos Humanos de TI	P11-11	Administración de usuarios

Tabla 6. Relación Dominios COBIT con Procesos
Elaborado por: Los autores

La tabla 7 muestra el resultado del análisis de nivel de madurez efectuado, el detalle de los resultados están disponibles en el documento "Proyecto de titulación, Auditoría Informática Basada en el Análisis de Riesgos a la Empresa Tecniseguros S.A." en el capítulo 5, Establecimiento del modelo de madurez con COBIT, páginas 42 - 63.

Consolidado de niveles de Madurez por Dominio		
Dominio	**Nivel de madurez**	**Nivel de cumplimiento**
AI3 Adquirir y Mantener Infraestructura Tecnológica	3	62,5
AI6 Administrar Cambios	0	17
DS4 Dominio Garantizar la Continuidad del servicio	3	72,07
DS8 Dominio Administrar la Mesa de Servicio	3	64,71
Ds12 Administración del Ambiente Físico	3	72
Po07 Administrar Recursos Humanos De Ti	4	81,25

Tabla 7. Niveles de Madurez
Elaborado por: Los autores

4. Informe de Auditoría

El resultado final muestra 28 riesgos identificados, mismos que están clasificados de acuerdo a la tabla 3 (medidas de riesgo). Y mostrados en la tabla 8. La descripción de los 28 riesgos están disponibles en el documento "Proyecto de titulación, Auditoría Informática Basada en el Análisis de Riesgos a la Empresa Tecniseguros S.A." en el capítulo 4, Respuesta a los riesgos, Sección 4.8.1. Descripción de los riesgos, páginas 38 - 41.

Impacto					
	5		15, 17, 18	1, 3, 8, 12	9
	4		14, 16, 19, 27, 28	2, 7, 10, 11, 13, 25	
	3	24	6, 22, 23, 26	4, 5, 20, 21	
	2				
	1				
	0	1	2	3	4

	Probabilidad

Tabla 8. Clasificación de riesgos
Elaborado por: Los autores

No todos los riesgos generaron una observación, en algunos casos fue posible agruparlos, es por eso que, los 28 riesgos generaron 13 observaciones de auditoría, la descripción de las 13 Observaciones de Auditoría están disponibles en el documento "Proyecto de titulación, Auditoría Informática Basada en el Análisis de Riesgos a la Empresa Tecniseguros S.A." en el capítulo 6, Desarrollo del Proceso de Auditoría, Sección 6.1.1. Informe de Auditoria al área de Tecnología de Tecniseguros S.A. páginas 64 - 79.

5. Trabajos relacionados.

Las auditorías basadas en riesgos, generalmente, se basan en una normativa o marco de referencia, pero no realizan la fusión de algunas de ellas, es decir, siguen una metodología de inicio a fin. Actualmente no existen trabajos de tesis de postgrado en la Universidad de las Fuerzas Armadas relacionados con la auditoría basada en el análisis de riesgos de la empresa Tecniseguros S.A. ni de ningún otro centro educativo, siendo este el pionero y guía referencial para la empresa bróker de seguros.

6. Conclusiones y trabajo futuro.

La metodología COSO ERM está orientada a la administración de riesgos de toda la organización, se puede analizar unidades de negocio, sucursales, divisiones, etc. de manera independiente, y permite tener control total sobre los riesgos de una organización. En el caso de Tecniseguros S.A. COSO permitió identificar y darle tratamiento a los riesgos, aunque los valores de ponderación son elegidos por los auditores.
Las escalas de probabilidad e impacto, mostradas en este proyecto, fueron determinadas por la experiencia de los auditores y los expertos del negocio, los valores no tienen justificación matemática pero sí relevancia
Tecniseguros S.A. es una empresa que se encuentra en un momento de cambio, los procesos tecnológicos y del negocio no pueden manejarse como una empresa pequeña, posiblemente en el pasado sí fue suficiente, pero no ahora, el desadoren del desarrollo de los aplicativos es el primer ejemplo, sin embargo, existen otros como: control de cuentas privilegiadas, accesos, escaneo de vulnerabilidades, equipos de seguridad de la red perimetral, entre otros, que no han sido implementados.
La empresa muestra madurez en algunos procesos, exceptuando el de mantenimiento de aplicaciones, sin embargo, la ejecución de los procesos recae en personas y no en tecnología, es por eso que existe alta carga de trabajo hacia el personal de tecnología, permitiendo que se escapen detalles en el día a día.

7. Referencias Bibliográficas.

Carrillo, W. T. (12 de Agosto de 2007). *Auditoria y Seguridad de Sistemas*. Obtenido de http://walberto.bligoo.mx/

Comware. (15 de Marzo de 2013). *Comware S.A.* Obtenido de http://www.comware.com.ec/jsp/user/go.do?sectionCode=20

Duverge, C. A. (24 de Junio de 2004). *Auditoria registro y control del personal*. Obtenido de http://www.gestiopolis.com/recursos2/documentos/fulldocs/rrhh/audirrhh.htm

IT Governance Institute. (2007). *Cobit 4.1.* United States of America: IT Governance Institute.

Moyasevich, I. D. (10 de 04 de 2013). *Auditoría y Control de Sistemas e Informática.* Obtenido de http://perso.wanadoo.es/idmb/a_ing/temas/auditoria_informatica.htm

Perera, L. D. (20 de Enero de 2007). *La informatización en el proceso de Auditoría*. Obtenido de http://www.monografias.com/trabajos44/informatizacion-auditoria/informatizacion-auditoria.shtml

Wikipedia. (03 de Febrero de 2007). *Auditoría informática*. Obtenido de http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica