AUDITORÍA BASADA EN COSO ERM A LA GESTIÓN DE RIESGO OPERATIVO PARA COOPERATIVAS DE AHORRO Y CRÉDITO

César Antonio Obando Changuán

RESUMEN: Las Cooperativas de Ahorro y Crédito en el Ecuador han asumido un rol protagónico en la trasformación e inclusión financiera con una buena aceptación en la población perteneciente al estrato de economía popular y solidaria, quienes manifiestan haber encontrado en las Cooperativas de Ahorro y Crédito la oportunidad de acceder a productos y servicios financieros de forma oportuna y eficaz, llegando a representar el 9,52% de las captaciones del sistema financiero Ecuatoriano, de ahí la importancia de utilizar un marco de de referencia para auditar los riesgos operativos con el fin mitigarlos antes de que se materialicen y contribuir de esta manera en la construcción de una economía equitativa, donde los socios estén informados de sus derechos y sean verdaderos protagonistas de su "buen vivir", por ello se realizó un examen de auditoría a los riesgos operativos enmarcados en el marco de referencia COSO ERM.
Se inició con el establecimiento de una propuesta de plan de auditoría, basado en COSO ERM que contempla principalmente los riesgos tecnológicos según las NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (capítulo incluido con resolución No JB-2005-834 de 20 de octubre del 2005), una vez ejecutada, elaborar un informe dirigido a la gerencia general, determinar el nivel de madurez en base a los 8 componentes de coso ERM aplicados en la auditoria y establecer las conclusiones y recomendaciones para la institución enmarcadas en COSO ERM.
Al final a través de los resultados se determina que la auditoría evidencia el cumplimiento de los objetivos planteados, mostrando los riesgos operativos más relevantes, expuestos en matrices y mapas de calor y expresando una opinión de auditoría sobre los resultados obtenidos.

(Palabras clave: COSO ERM, RIESGO, HALLAZGO)

ABBSTRACT: The Credit Unions in Ecuador have taken a leading role in financial inclusion and transformation with a good acceptance in the population belonging to the stratum of popular and solidarity economy , who claim to have found the Credit Unions the opportunity to access to financial products and services in a timely and effective manner , coming to represent 9.52% of deposits in the financial system , hence the importance of using a frame of reference to audit operational risks in order to mitigate them before materialize and thus contribute to build an equitable economy , where members are informed of their rights and are protagonists of their " good life" , so a review of audit was performed at the operational risks included under COSO ERM reference .
It began with the establishment of a proposed audit plan , based on COSO ERM mainly provides technological risks according to the GENERAL RULES FOR THE IMPLEMENTATION OF THE LAW OF FINANCIAL SYSTEM INSTITUTIONS TITLE X. - OF RISK MANAGEMENT AND ADMINISTRATION CHAPTER V. -

OPERATIONAL RISK MANAGEMENT (Chapter included with resolution No JB -2005-834 of October 20, 2005) , when executed, produce a report to senior management , determine the level of maturity based on 8 COSO ERM components applied in the audit and establish findings and recommendations for the institution framed in COSO ERM .
End through the results is determined that the compliance audit evidence of objectives, showing the most relevant operational risks outlined in matrices and maps heat and expressing an audit opinion on the results.

(Key words: COSO ERM, RISK, FIND)

I. INTRODUCCIÓN

El riesgo operativo está implícito en las pérdidas por fallas tecnológicas, errores de liquidación transaccional, inundaciones, fuego, robo terrorismo, fallas humanas, de procesos, además de eventos externos que pueden afectar a la cooperativa, por lo tanto la auditoria identifica como se está gestionando los riesgos corporativos que deben ser identificados cuantificados, monitoreados para mitigar las posibles pérdidas por el riesgo operativo.
El propósito de este trabajo es ejecutar la auditoría a la gestión del riesgo operativo utilizando como marco de referencia COSO ERM y la Resolución de la Junta Bancaria N. JB-2005-834 de 20 de octubre del 2005, en el capítulo V De la Gestión del Riesgo Operativo para una Cooperativa de Ahorro y Crédito, con énfasis en el riesgo tecnológico.
En la sección metodología se describe los pasos a seguir para auditar los riesgos operativos en base a tres fases: planeación, ejecución y emisión del informe de auditoría, se utilizan matrices para identificar los riesgos, evaluarlos y darles respuesta, se hace énfasis en la necesidad de emitir el dictamen del auditor.
Se realiza las conclusiones y se emite las recomendaciones con el fin de orientar a la institución en la importancia de utilizar un marco de referencia para auditar los riesgos, la opinión vertida muestra el estado en términos de madurez del proceso de gestión de riesgos de la institución.

II. METODOLOGÍA

La metodología proporciona la estructura conceptual y el camino a seguir para abordar la Auditoria basado en COSO ERM a los riesgos operativos de la Cooperativa con el fin de evidenciar el grado en el cual la institución posee una estructura de gobierno sustentada en la gestión integral de riesgo, con lo que cada entidad, independiente a su naturaleza de negocio, proporciona valor a sus distintos “grupos de interés”.

2.1 Fase I. Planeación de la auditoría

Se realiza un examen de los controles, procedimientos, sistemas informáticos, la utilización, eficiencia y seguridad, para recomendar programas, procesos y procedimientos alternativos para una utilización más eficiente y segura de los activos informáticos considerando cada uno de los componentes de COSO ERM, utilizando varios métodos de identificación, como lectura de documentos, encuestas, entrevistas y más.

2.2 Fase II: Ejecución de la auditoría

2.2.1 Ambiente interno

Se realiza la auditoría a la Gestión de Riesgos operativos y específicamente al riesgo tecnológico, considerando los siguientes objetivos de control.

- Identificar los procesos con los que cuenta la institución bajo los parámetros definidos en la norma de Riesgo Operativo
- Determinar la existencia de procedimientos para la administración de procesos
- Determinar la definición de procedimientos para la Administración del Capital Humano bajo los parámetros definidos en la norma de riesgo operativo.
- Definir un esquema formal para la administración del riesgo operativo acorde con la administración integral de riesgos, que permita: identificar, medir, controlar y monitorear las exposiciones al mencionado riesgo.

2.2.2 Identificación de Objetivos y Riesgos

Evaluar si la cooperativa posee procedimientos para facilitar la identificación de los riesgos de las fuentes que posee identificando si existen debilidades o amenazas en dichas fuentes. Los riesgos operativos están relacionados con la habilidad de la cooperativa para convertir la estrategia elegida en planes concretos, mediante la asignación eficaz de recursos, en el Gráfico 1, se expone dicho procedimiento.

Gráfico 1: Procedimiento de identificación de riesgos

Se evalúa los objetivos de control identificados en una matriz como se indica a continuación en la Tabla 1.

Condición:	
Criterio:	
Causa:	
Efecto:	

Tabla 1: Matriz de evaluación de riesgos

2.2.3 Evaluación del Riesgo

Riesgo Inherente y Residual

El riesgo inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto, es el que es parte del activo.
El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos, refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.
Pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

2.2.4 Probabilidad e Impacto

Mapa de Riesgos (Impacto - Probabilidad)

Al estimar la probabilidad e impacto de posibles eventos, ya sea sobre la base del efecto inherente o residual, se debe aplicar alguna forma de medición, como ejemplo, se establece cuatro tipos generales de medida: nominal, ordinal, de intervalo y de proporción.

	Riesgo	Sub-categoría	Significancia	Impacto	Probabilidad	Distribución de Control
1	Competencia	Riesgos de Ambiente Interno	1	2	1	1
2	Deseos de los Socios		1	1	1	1
3	Innovación Tecnológica		2	3	2	1
4	Sensibilidad		1	2	2	2
5	Relaciones con los Socios		1	2	2	2
6	Disponibilidad de Capital		1	1	2	1
7	Soberano / Político		2	2	1	2
8	Legal		1	2	2	2

9	Satisfacción al cliente	Riesgos de Procesos	4	2	2	2
10	Recursos Humanos		4	2	2	2
11	Desarrollo de Productos		4	2	2	2
12	Eficiencia		4	2	2	2
13	Capacidad		4	2	2	1
14	Alianzas		4	2	2	1
15	Cumplimiento		2	2	1	2
16	Interrupción		4	2	2	2
17	Eficiencia	Riesgo de Personas	4	2	2	2
18	Capacidad		4	2	2	2
19	Rotación		2	2	1	1
20	Permanencia		2	2	1	1
21	Desvinculación		4	2	2	2
22	Ética		4	2	2	1
23	Experiencia		2	2	1	2
24	Autoridad / Límite		2	1	2	1
25	Relevancia	Riesgos de Tecnología de Información	2	2	1	1
26	Integridad		6	3	2	1
27	Acceso		4	2	2	1
28	Disponibilidad		2	2	1	2
29	Infraestructura		4	2	2	1
30	Fraude de Empleados / Terceros		6	3	2	2
31	Actos Ilegales		2	1	2	2
32	Uso no Autorizado		6	3	2	1
33	Alineamiento		1	1	1	1
34	Servicios Públicos	Riesgos de Eventos externos	4	2	2	2
35	Desastres Naturales		2	2	1	1
36	Fraude externo		4	2	2	1
37	Monopolio de proveedores		6	2	3	3
38	Estructura Organizacional		4	2	2	1
39	Medición de Performance		4	2	2	1
40	Asignación de Recursos		2	2	1	2
41	Planeamiento		2	2	1	2
42	Ciclo de Vida		2	2	1	1

Tabla 2: Mapa de riesgos

2.2.5 Respuesta a los riesgos

Asignación de riesgos a los procesos de negocio

En este caso se asigna respuestas a los riesgos de tecnología identificados.

EVITAR	COMPARTIR
- Instalación de software no autorizado - Destrucción de información mal intencionada - Modificación no autorizada de software - Abuso de información privilegiada - Monopolio de la empresa de soporte y mantenimiento - Ataques externos a las redes - Manipulación de la configuración de Equipos - Cambio de prioridades de proyectos informáticos sin planificación	- Planificación estratégica de la tecnología de información, aprobada y respaldada por un procedimiento formal. - Plan operativo anual y presupuesto aprobados formalmente. - Procedimientos para la administración de incidentes y problemas incluyendo su registro, análisis y solución oportuna. - Documentación y establecimiento de procedimientos para las operaciones de tecnología de información.
REDUCIR	**ACEPTAR**
- Concentración de funciones - Robo de software institucional Deterioro de los respaldos de información -Instalación de hardware no autorizado en los equipos de computo. - Instalaciones donde se encuentran los backups vulnerables.	- Servicios de TI provistos por terceros se administran de acuerdo con las políticas institucionales de contratación de servicios. - Los contratos de servicios de TI provistos por terceros definen la propiedad de la información asi como las responsabilidades de cada parte. - La entidad ha identificado los requerimientos de seguridad relacionados con la tecnología de información y ha implementado los controles necesarios para minimizar el impacto de las vulnerabilidades e incidentes de seguridad. - La entidad cuenta con un sistema de administración de las seguridades de acceso a la información y niveles de autorización de accesos para ejecución de las funciones de procesamiento.

Tabla 3: Respuesta los riesgos

2.2.6 Información y comunicación

La difusión que se hace es una reunión entre el auditado y el auditor y se lee el borrador del informe se discute y luego envían el informe final, luego la Gerencia General da a conocer a los involucrados el cumplimiento elaborándose cronogramas de seguimiento en unas matrices.

2.3 Fase III: Informe

Se evidencia la existencia de una lectura preliminar de borrador con los dueños de los procesos auditados y al final se emite el informe definitivo a la gerencia general y este a su vez realiza la entrega del documento al responsable de la auditoría interna de la cooperativa para que se proceda a dar el seguimiento correspondiente

.

III. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

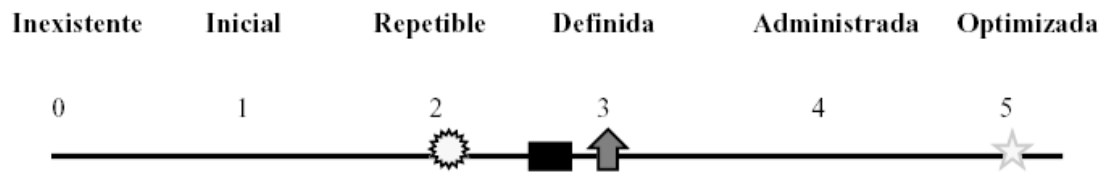
Modelo de madurez de los 8 componentes de coso ERM aplicados en la auditoria

Para emitir una opinión sobre la base de lo auditado contemplando los ocho componentes de COSO ERM nos basaremos en el enfoque del modelo de madurez para el control sobre los proceso de riesgo operativo que se reflejan en la tabla 4.

RESUMEN GERENCIAL DEL MODELO DE MADUREZ PARA LOS COMPONENTES DE COSO ERM EN LA AUDITORIAS

	Componente COSO ERM	Descripción	Inexistente	Inicial/Ad Hoc	Repetible pero intuitivo	Proceso definido	Administrable y medible	Optimizado
			0	1	2	3	4	5
1	**Ambiente Interno**	Filososfia de la gestion de Riesgo, cultura de riesgo, consejo de admonistración / direccion, valores eticos compromiso, estructura organizacional politicas y practicas de recursos humanos						
2	**Establecimiento de Objetivos**	Objetivos estratégicos, objetivos relacionados, riesgos aceptados, tolerancia al riesgo						
3	**Identificacion de eventos**	Eventos, eventos interdependientes, catagoria de eventos, riesgos y oportunidades						
4	**Evaluacion de Riesgos**	Riesgos inherentes y residuales, probabilidad e impacto, fuentes de datos, evaluación						
5	**Respuesta al Riesgo**	Evaluación de posibles respuestas, selección de respuestas						
6	**Actividad de control**	Integración de la respuesta al riesgo, tipos de actividades de control, políticas y procedimientos, controles de TI.						
7	**Información y comunicación**	Información y comunicación						
8	**Supervisión (Monitoreo)**	Actividades permanentes de supervisión - comunicación de deficiencias						

Tabla 4: Modelo de madurez



Este enfoque de Modelo de Madurez permitirá a la administración de la cooperativa ponerse en la escala y apreciar lo que está involucrado si necesita mejorar el desempeño.

3.1 Informe de la Auditoría

Los comentarios y sugerencias que se exponen en esta sección surgen de los procedimientos aplicados durante la revisión con la intención de ayudar en la toma de decisiones y en la optimización de controles de los recursos informáticos de la cooperativa.

3.2 Dictamen del auditor a la gerencia general

Una vez auditado el cumplimiento y sustanciación a la gestión de riesgos operativos con marco de referencia COSO ERM al cumplimiento y la sustanciación de la resolución No JB-2005-834 de 20 de octubre del 2005 con mayor énfasis en los riesgos tecnológicos. El auditor tiene la responsabilidad de expresar una opinión sobre la situación actual al corte; de la administración y gestión de riesgos operativos basados en el examen de auditoría.

IV. TRABAJOS RELACIONADOS

En términos de Riesgo Operativo, frente a otros países, nuestro país, está en una etapa inicial, ya que la normativa emitida por la Superintendencia tiene fechas de cumplimiento recientes, a diferencia de otros países donde dicha normativa data del 2006, por lo que ha sido mejorada e interiorizada por las organizaciones.

Existen varios tratados sobre auditorías y evaluación de Riesgos en las instituciones financieras y en especial de las Cooperativas de Ahorro y Crédito del país (Brito, 2009) en su tesis elaborada en la Escuela Politécnica del Litoral, hace una exposición amplia de la administración de riesgo operativo relacionado a la tecnología de la información orientado a las Cooperativas de Ahorro y Crédito.

(Ferreas Salegre, 2005) de la Unidad Central de Riesgos Operativos del BBVA el 13 de octubre de 2005 realiza una exposición de ciertas consideraciones relativas al uso avanzado de modelos de medición, donde expone los modelos de medición del riesgo operativo en España luego de la publicación en mayo de 2004 y que entra en vigencia en la Banca desde 2007 – 2008 donde se incluye una provisión de capital por riesgo operacional y considerando que cuando la gestión del riesgo sea mínima el nivel de gestión del riesgo será por un conocimiento bajo del conocimiento de la entidad.

El Magister Manuel Espinoza Cruz, realiza un tratado denominado “La Auditoria y sus Paradigmas”, donde plantea tres hipótesis orientadas a buscar evidencia de la gestión de una auditoria en el siglo XIX, auditorías del desempeño basadas en los riesgos del sistema operativo y por ultimo hace referencia que las auditorías son individuales a la naturaleza de cada institución.

Este trabajo presenta la metodología para auditar en base a COSO ERM a una cooperativa de ahorro y crédito, utilizando una serie de matrices y gráficos para evaluar los riesgos.

IV. CONCLUSIONES Y TRABAJO FUTURO

A través de los resultados obtenidos en el presente trabajo, se determina que la auditoría realizada demuestra el cumplimiento de los objetivos planteados, evidenciado los riesgos más relevantes, expuestos en matrices y mapas de calor COSO ERM, como marco de referencia de control interno hace énfasis en sus 8 componentes y sus objetivos permiten hacer un análisis profundo y de agregar valor si se implementa como metodología en cualquier institución financiera.

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos. Por esto agradezco a mi director de tesis, Ing. Paulo Bermeo, a mi oponente Eco. Gabriel Chiriboga, a mis profesores a quienes les debo gran parte de mis conocimientos, y un eterno agradecimiento a esta prestigiosa universidad la cual abrió y abre sus puertas a personas como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien.

REFERENCIAS BIBLIOGRÁFICAS

Coso. (09 de 2004). Recuperado el 28 de 01 de 2013, de http://www.coso.org/documents/coso_erm_executivesummary.pdf

Sistema Bibliotecario Matias. (2004). Recuperado el 21 de 01 de 2013, de http://webquery.ujmd.edu.sv/siab/bvirtual/Fulltext/ADCN0000558/Capitulo%201.pdf

(2011). *Agenda Política Económica del Buen Vivir.* Quito: Ministerio de la Coordinación de la Política Económica.

Dirección y Coordinación Técnica de Planificación. (06 de 2011). Recuperado el 28 de 01 de 2013, de http://www.fifomi.gob.mx/web/images/fifomi/documentos/normateca/mejorada/riegos/ma-dctyp-02.pdf

(2011). *Memoria COAC Alianza del Valle 2011.* Quito.

(2012). *Memoria COAC Alianza del Valle 2012.* Quito.

Net Consul.com. (2012). Recuperado el 28 de 01 de 2013, de http://www.netconsul.com/riesgos/cci.pdf

Registro Oficial No. 1061. (16 de 02 de 2012). *Reglamento a Ley Orgánica de Economía Popular y Solidaria*. Quito, Pichincha, Ecuador: Superintendencia de Economía Popular y Solidaria.

Universidad de la República de Uruguay, Control Interno. (12 de 10 de 2012). Recuperado el 29 de 01 de 2013, de http://www.ccee.edu.uy/ensenian/catcoint/material/control.PDF

Alfaro, N. (2008). *Universidad Autónoma Tomás Frias.* Recuperado el 28 de 01 de 2013, de ://www.uatf.edu.bo/web_descargas/manual_aud_interna.pdf

Báez, B. (2010). *Matriz de Riesgo Operacional.* Paraguay: DGRV.

Brito, J. (2009). Recuperado el 05 de 01 de 2013, de Escuela Politectica del litoral: http://www.dspace.espol.edu.ec/bitstream/123456789/5667/2/Tesis.doc

COSO. (2004). *Informe Coso.*

Ferreas Salegre, A. (octubre de 2005). Riesgo Operativo en España.

García, J. (6 de septiembre de 2010). *Pérdida de Riesgo Operacional*. Recuperado el 07 de 01 de 2013, de http://www.sbs.gob.pe/repositorioaps/0/0/jer/pres_doc_basilea/Bases_Datos_Eventos_Perdida_Riesgos_Operacionales%20.pdf

López, F. (2005). *La Gestión de riesgos en las Cooperativas de Ahorro y Crédito.* Recuperado el 21 de 01 de 2013, de http://www.aciamericas.coop/IMG/pdf/El_Riesgo_en_la_Gestin_Cooperativa.pdf

MIES. (2010-2013). *Agenda de la Revolución de la Economía Popular y Solidaria 2010-2013.*

Monografias.com. (s.f.). Recuperado el 27 de 01 de 2013, de http://www.monografias.com/trabajos12/coso/coso2.shtml

Ontoria Gonzalo, S. (2011). *Gobierno y Modelado de la Seguridad de la Información en las Organizaciones.* Madrid : Escuela Politécnica de Madrid.

Revista Seguridad. (2009). *Revista Seguridad*. Recuperado el 12 de 01 de 2013, de Resvista Seguridad: http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i]

Salnave, A., & Riaño, L. M. (2008). *Manual de Implementación.* Recuperado el 27 de 01 de 2013, de http://portal.dafp.gov.co/form/formularios