

## COSO ERM Y LA GESTIÓN DE RIESGOS

### *COSO ERM AND RISK MANAGEMENT*

LILIANA RUTH SÁNCHEZ SÁNCHEZ\*

Unidad de Posgrado de la Facultad de Ciencias Contables

Universidad Nacional Mayor de San Marcos - UNMSM / Lima - Perú

[Recepción: Setiembre 2015 / Conformidad: Octubre 2015]



### RESUMEN

Considerando que cada entidad enfrenta una gran cantidad de riesgos que afectan las diferentes partes de la organización; la gerencia no solamente necesita manejar los riesgos individuales; sino también, comprender los impactos interrelacionados. Para ello, la metodología COSO ERM fue diseñada para identificar eventos potenciales que afectasen a una entidad, evaluar y responder a los riesgos detectados, para que estén dentro de los límites de nivel aceptables como parte de una buena administración.

La aplicación de esta metodología, ha permitido identificar los riesgos existentes en la empresa y evaluar la eficiencia y eficacia de los controles establecidos, a fin de que la entidad logre los objetivos trazados.

Las conclusiones de la investigación demostraron que la metodología COSO ERM identificó y administró riesgos a nivel de la entidad; alineó el nivel de riesgo aceptado con la estrategia de la empresa; mejoró las decisiones de respuesta al riesgo; minimizó sorpresas y pérdidas operativas; proveyó respuestas integradas a riesgos múltiples y sobre todo, aprovechó oportunidades.

### Palabras clave:

Control Interno; riesgos; COSO ERM.

### ABSTRACT

Considering that every entity faces various risks affecting different parts of the organization; management needs to not only handle individual risks but also understand the interrelated impacts. For this, the COSO ERM methodology was designed to identify potential events that affected an entity, evaluate and respond to identified risks, so that they are within the limits of acceptable level as part of a good management.

The application of this methodology, helped identify the risks in the company and assessed the efficiency and effectiveness of the controls, so that the entity achieved the objectives.

The research findings showed that the COSO ERM methodology identified and managed risks at the level of the entity; aligned the accepted risk level with the business' strategy; it improved the decisions on risk response; it minimized surprises and operating losses; it provided integrated responses to multiple risks and opportunities especially took advantage of opportunities.

### Keywords:

Internal control; risks; COSO ERM.

\* Maestría de Auditoría con mención en Auditoría de Gestión y Control Gubernamental - UNMSM. Contadora Pública Colegiada.  
Email: lilianaruthsanchezsanchez@hotmail.com

## INTRODUCCIÓN

Debido a la globalización de los mercados y a las nuevas estrategias competitivas y de expansión, las empresas se vieron en la necesidad de cambiar sus estructuras organizacionales, procesos, productos, consumidores e inversiones, hechos que ocasionaron riesgos inherentes normales y otros nuevos que se han ido considerando como parte del desarrollo y actualización de las empresas a los nuevos tiempos, tales como: los riesgos generados en la integridad de sus activos, el cumplimiento de leyes y regulaciones, los sistemas de información, la administración financiera, el talento humano y las operaciones. Por ello, algunas empresas entendieron que la administración de riesgos no es solamente el cumplimiento de los principios contables y legales, la diversidad de riesgos que aparecen todos los días requería que las empresas tuvieran un seguimiento más estricto en el manejo de los riesgos, viéndose en la necesidad de protegerse de irregularidades y fraudes con sistemas de control interno adecuados a la metodología COSO II ERM, con el propósito de efectuar una adecuada administración de riesgos que permitiera identificar, evaluar y responder adecuadamente a los riesgos presentados, de modo que se estuviese preparado para enfrentar situaciones que limiten el logro de los objetivos del negocio.

Al respecto, se han realizado y publicado importantes estudios e investigaciones relacionados a la implementación y evaluación de un adecuado marco de control interno, así, Vega Sepúlveda, Edilberto (2008) en su tesis denominada: “El sistema de control interno en la empresa moderna”, manifestó que un adecuado sistema de control interno es el elemento clave para llevar a cabo una adecuada gestión y que este no es el elemento perturbador de la gestión, sino todo lo contrario, es el elemento facilitador de la gestión óptima de las empresas modernas; asimismo, Ramón Ruffner, Jeri (2004) a través de su artículo “El control interno en las empresas privadas”, indicó que el control interno de las empresas privadas se ha convertido últimamente en uno de los pilares en las organizaciones empresariales, pues nos permite observar con claridad la eficiencia y la eficacia de

las operaciones y la confiabilidad de los registros y, el cumplimiento de las leyes, normas y regulaciones aplicables. Finalmente, Velezmore La Torre, Oscar (2010) en su investigación titulada “Modelo de gestión de riesgo operacional en una institución financiera peruana dentro de un enfoque integrado de gestión de riesgos”, desarrolló un modelo de Gestión de Riesgo Operacional bajo el enfoque de gestión integral de riesgos COSO ERM para prevenir y reducir niveles de pérdida que ocurran por este riesgo.

Basados en los aportes ya mencionados, el presente trabajo respondió a la necesidad de determinar el nivel de desarrollo de un Sistema de Control Interno aplicando la metodología COSO ERM, de modo que constituya una herramienta por la cual se pueda conocer con exactitud la situación actual de una entidad, en la medida que provee información a la gerencia y directorio con respecto a los riesgos más significativos y a la forma como los mismos están siendo administrados. El propósito principal fue identificar áreas de mayor riesgo y establecer planes de acción para mitigar los riesgos existentes; así como, contribuir a la consecución de objetivos establecidos por las principales áreas de cada empresa.

## METODOLOGÍA

El estudio tuvo un enfoque cuantitativo y es de carácter explicativo/correlacional porque estuvo dirigido a llegar al conocimiento y a la relación causa-efecto de los eventos. Asimismo, la investigación fue de tipo no experimental, porque no se tuvo control directo de las variables independientes debido a que sus manifestaciones ya habían ocurrido.

La metodología aplicada en la investigación fue el método inductivo-deductivo y se aplicaron técnicas de recolección de datos como: observación, entrevistas y encuestas al personal de la entidad que tomamos como base para realizar el estudio, en este caso, se tomó como muestra una empresa dedicada al otorgamiento y recuperación de créditos de consumo. Del mismo modo, se usaron técnicas específicas para el desarrollo del presente estudio como la investigación de campo con referencia documental y descriptiva.

## MARCO TEÓRICO

### Modelos de Control Interno

Como respuesta a los cambios constantes que atraviesan las empresas motivados por factores internos como externos, se desarrollaron métodos que permiten tener una visión global y estratégica de las organizaciones y de su entorno. Estos esfuerzos generaron diversos enfoques de control que impulsaron una nueva cultura administrativa en todo tipo de organizaciones y sirvió de plataforma para diversas definiciones y modelos de control a nivel internacional tales como: Cobit, Candbury, COCO, COSO I y COSO II, siendo este último lanzado el 29 de septiembre de 2004 como marco de control denominado COSO II, constituyéndose como un marco enfocado a la gestión de los riesgos mediante técnicas como la administración de un portafolio de riesgos.

### COSO ERM

COSO II o COSO ERM es un proceso continuo realizado por el personal de todos los niveles de la organización y no únicamente, por un departamento de riesgos o área similar – no es la mera conjunción de políticas, encuestas y formularios, sino que involucra gente de los distintos niveles de la organización y está diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre la consecución de objetivos.

Asimismo, el COSO ERM es un facilitador del proceso de la gestión de riesgos, este permite a los administradores de las empresas operar más eficazmente en un ámbito pleno de riesgo, aumentando la capacidad para:

- Alinear el nivel de riesgo aceptado con la estrategia.
- Unir crecimiento, riesgo y rendimiento.
- Mejorar las decisiones de respuesta al riesgo.
- Minimizar sorpresas y pérdidas operativas.
- Identificar y administrar riesgos a nivel de la entidad.
- Racionalizar el uso de recursos.

De acuerdo al marco definido en el informe COSO ERM, la gestión de riesgos corporativos está

conformada por ocho componentes relacionados entre sí, los cuales se describen brevemente a continuación:

- Ambiente interno: Abarca el entorno de una empresa, influye en cómo se establecen las estrategias y los objetivos y, cómo se estructuran las actividades del negocio.
- Establecimiento de objetivos: Las empresas deberán establecer los objetivos a fin de que se pueda identificar potenciales eventos que afecten a su consecución.
- Identificación de eventos: Está relacionado con la identificación de los eventos potenciales que de ocurrir podrían afectar a la organización, también, determina si representan oportunidades o si, podrían afectar negativamente la capacidad de la entidad para implementar la estrategia y lograr los objetivos con éxito.
- Evaluación de riesgos: Los riesgos deben ser analizados considerando su probabilidad e impacto como base para determinar cómo deben ser gestionados y se evalúan desde una doble perspectiva, inherente y residual. Para ello se deben considerar realizar autoevaluaciones, elaborar mapas de riesgo y distribuciones de severidad y probabilidad.
- Respuesta al riesgo: Una vez identificados los riesgos y establecido el nivel de significancia, la dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.
- Actividades de control: Son las políticas y procedimientos que se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente.
- Información y comunicación: La información relevante se identifica, capta y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación eficaz debe producirse en un sentido amplio, fluyendo en todas las direcciones dentro de la entidad.
- Supervisión: La totalidad de la gestión de riesgos se supervisa, realizando modificaciones oportunas cuando se necesiten. Esta supervisión se lleva a cabo mediante actividades permanentes de la

dirección, evaluaciones independientes o ambas actuaciones a la vez.

**HIPÓTESIS PRINCIPAL**

“Cuanto mayor sea el nivel de desarrollo del sistema de control interno basado en la metodología COSO ERM, este será más eficiente para identificar áreas de mayor riesgo y contribuirá a la consecución de objetivos de la entidad”.

**ANÁLISIS E INTERPRETACIÓN DE DATOS**

En primer lugar, establecimos la probabilidad y el impacto de cada riesgo. Para lograr este efecto, obtuvimos una respuesta consensuada entre los colaboradores de la empresa evaluada a través de una “lluvia de ideas” y consistió en tomar la lista o portafolio de riesgos identificados y distribuirla a todos los participantes acompañado de un cuestionario de preguntas por cada riesgo, que permitió establecer la

probabilidad de ocurrencia de un riesgo identificado y se basó en el número de veces que el riesgo podría materializarse en el año. Del mismo modo, se evaluó el impacto que no es más que la pérdida financiera estimada al hacerse efectivo el riesgo.

Al respecto, los participantes identificaron cuarenta riesgos en las áreas de créditos y cobranzas y, estos fueron evaluados en términos de probabilidad e impacto, los resultados de estos puntajes fueron transferidos a un mapa de riesgos que es una representación gráfica que traza en sus ejes estimaciones cuantitativas y cualitativas de la probabilidad e impacto de los riesgos identificados, luego, estos riesgos se presentaron desde los más significativos (mayor probabilidad e impacto) hasta los menos significativos (menor probabilidad e impacto); una vez identificados los riesgos, estos fueron clasificados en cuatro categorías: Bajo, medio, alto y crítico, para ello, el uso eficaz del mapa de riesgos permitió identificar las áreas que necesitaban mayor análisis y respuestas a riesgos específicos.

**Tabla N° 01**  
Valor del riesgo inherente de acuerdo a impacto x frecuencia

Impacto (en miles de US\$)	5.- Crítico	100	Moderado (20)	Moderado (33)	Crítico (100)	Crítico (200)	Crítico (1200)
	4.- Alto	80	Moderado (16)	Moderado (26.4)	Alto (80)	Crítico (160)	Crítico (960)
	3.- Relevante	35	Moderado (7)	Moderado (11.55)	Relevante (35)	Relevante (70)	Crítico (420)
	2.- Moderado	5	Bajo (1)	Bajo (1.65)	Moderado (5)	Moderado (10)	Relevante (60)
	1.- Bajo	1	Bajo (0.2)	Bajo (0.33)	Bajo (1)	Bajo (2)	Moderado (12)
			1.- Muy Raro (0.2)	2.- Raro (0.33)	3.- Eventual (1)	4.- Frecuente (2)	5.- Muy Frecuente (12)
			Frecuencia (anual)				

Fuente: Elaboración propia.

Una vez identificados y evaluados los riesgos, también evaluamos los controles que presentaban cada riesgo y que fueron implementados para minimizar dicho riesgo.

**Tabla N° 02**  
Evaluación de la efectividad de los controles

Impacto (en miles de US\$)	5.- Efectivo (5)	5 (Débil)	10 (Débil)	15 (Moderado)	20 (Fuerte)	25 (Fuerte)
	4.- Efectivo no formalizado (4)	4 (Débil)	8 (Débil)	12 (Moderado)	16 (Moderado)	20 (Fuerte)
	3.- Inefectivo Prueba (3)	3 (Débil)	6 (Débil)	9 (Débil)	12 (Moderado)	15 (Moderado)
	2.- Inefectivo en diseño (2)	2 (Débil)	4 (Débil)	6 (Débil)	8 (Débil)	10 (Débil)
	1.- Control no existente(1)	1 (Débil)	1 (Débil)	1 (Débil)	1 (Débil)	1 (Débil)
		1.- Muy Raro (1)   2.- Raro (2)   3.- Eventual (3)   4.- Frecuente (4)   5.- Muy Frecuente (5)				

**Frecuencia**

Fuente: Elaboración propia.

**Cálculo del Riesgo Residual**

Finalmente, evaluamos el riesgo resultante después de aplicar los controles, este riesgo se denomina riesgo residual. La fórmula para determinar el nivel de

exposición del riesgo es la división del nivel de riesgo entre el nivel de eficacia del control que se encuentra asociado al riesgo.

$$\text{Riesgo Residual} = \frac{\text{Nivel de Riesgo Inherente}}{\text{Control (eficacia)}}$$

**Tabla N° 03**  
Calificación del riesgo residual

Riesgo	Bajo	Moderado	Relevante	Alto	Crítico
Clasificación	Riesgo mínimo o tolerable	Riesgo desgastante o significativo	Riesgo medio	Riesgo intolerable	Riesgo de continuidad del negocio o catastrófico
Resultado del Producto	Entre 0.2 y 4.9	Entre 5 y 34.9	Entre 35 y 79.9	Entre 80. y 99.9	De 100 a más
Curso de acción requerido	No se requirió de ninguna acción adicional, el riesgo genera impactos bajos	Se requirieron acciones de corrección a mediano plazo, el riesgo fue aceptado	Se establecieron puntos de control que permitieran mitigar el riesgo	Se establecieron planes para tratar el riesgo	Se informó a la Alta Dirección, se requirieron acciones de corrección inmediatas

Fuente: Elaboración propia.

La siguiente tabla muestra los hallazgos en torno a las áreas de créditos y cobranzas, luego de aplicar la metodología COSO ERM.

**Tabla N° 04**  
Valoración de los riesgos y controles de los subprocesos de las áreas de la entidad

Valoración Componentes	Actividad con riesgo	Actividad con Control	Actividad sin control	Evaluación de acuerdo al Riesgo Inherente
Sub Procesos Área de Créditos				
Registro de solicitud	1	1		Moderado
Verificación de documentos	7	5	2	Moderado
Evaluación de la capacidad de pago	6	6		Moderado
Aprobación del crédito	4	4		Moderado
Desembolso del crédito	8	7	1	Relevante
Sub Procesos Área de Créditos				
Seguimiento	6	5	1	Relevante
Recuperación	8	6	2	Alto
TOTAL	40	34	6	

Fuente: Elaboración propia.

### Validación de hipótesis

Habiéndose aplicado la matriz de riesgos a las áreas de créditos y cobranzas, se determinaron 40 riesgos distribuidos en los subprocesos de estas áreas, estos riesgos se enfocaron, principalmente en cuanto afectarían a la consecución de los objetivos estratégicos y operativos de la empresa. Asimismo, se determinaron 34 controles establecidos en cada actividad y 6 actividades que no cuentan con controles, lo que nos indica que la aplicación de la metodología COSO ERM, nos permite obtener información que nos ayude a formular mejor la evaluación del control interno de la entidad, por cuanto al tenerse claramente identificados los procesos con mayores niveles de riesgos, las acciones y actividades se dirigirán hacia estos, con lo que los recursos humanos y materiales serán mejor administrados.

Asimismo, permitirá a la entidad establecer una adecuada gestión de riesgos en la que se involucre a todo el personal como parte de la filosofía de la empresa la misma que coadyuvará al logro de objetivos y mejoras en el trabajo de los colaboradores y los objetivos de la entidad.

### RESULTADOS

El análisis de los resultados se realizó en base a una reflexión sobre los resultados obtenidos del trabajo de campo y en función del problema de investigación, los objetivos del estudio, la hipótesis y el marco teórico. Para lograr nuestro objetivo, fue necesario tomar como objeto de estudio las áreas de créditos y cobranzas de una entidad dedicada a la colocación y recuperación de créditos de consumo; posteriormente, se depuró los datos e información y se describió los resultados, se analizó la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla y se estudió cada uno de los resultados, relacionándolos con el marco teórico. Los pasos a seguir fueron los siguientes:

- **Paso 1- Planificación del proceso de evaluación del control interno.**

Se reunió la información necesaria a fin de obtener un conocimiento amplio sobre los diversos asuntos relacionados con el control interno de las diversas áreas de la entidad evaluada. Para ello, se definió los objetivos y el alcance del trabajo, se estableció los controles que deberían ser aprobados y

documentados; se describió los procedimientos a ser ejecutados en la evaluación de controles; se organizaron el equipo y/o encargado responsable, el mismo que debió reunir habilidades, conocimientos y experiencias necesarias para desarrollar las tareas encomendadas.

• **Paso 2 - Identificación de controles internos.**

La identificación del proceso de evaluación descansó en dos niveles:

1. Controles en el nivel de la entidad: Comprendieron las actividades que generalmente operan en el nivel de la institución como son los controles relacionados con el ambiente de control y centralización del proceso y de los controles.
2. Controles en el nivel de procesos: Relacionados con los procesos del negocio y están diseñados para detectar y prevenir la ocurrencia de errores en la ejecución de dichos procesos. Un buen camino para confirmar la comprensión en el diseño de los controles fue realizar una prueba de recorrido apropiado sobre estos.

• **Paso 3 - Evaluación de la efectividad de controles internos e identificación de deficiencias.**

Para evaluar la efectividad de los controles internos en la entidad, se diseñaron las pruebas a ser usadas sobre los controles significativos; realizando las evaluaciones sobre los aspectos de diseño y operación de controles en los aspectos aplicables; evaluando los resultados obtenidos e identificando, si fuera el caso, las deficiencias (debilidades materiales y deficiencias significativas) en el control interno de la organización.

• **Paso 4 - Recomendación de mejoras en los controles internos e implementación.**

Las recomendaciones de las mejoras que resultaron de la evaluación de control interno se orientaron a corregir las debilidades materiales y deficiencias significativas identificadas, por este motivo, dichas mejoras debieron ser preparadas en términos concretos y ser factibles de implementar en corto tiempo. Para el diseño de las mejoras en los controles internos, el equipo responsable debió considerar las circunstancias que ayudaron

a la entidad a lograr la implementación de los criterios considerados como necesarios, teniendo en cuenta sus causas y consecuencias posibles, los beneficios de la aplicación de la mejora del control interno, el costo de implementación de la mejora en el control interno y las posibles consecuencias aplicables al control.

• **Paso 5 - Seguimiento de la implementación de mejoras en los controles.**

El seguimiento es la implementación de las recomendaciones para la mejora del control interno. Por lo tanto, la tarea realizada por el equipo responsable de la evaluación del control interno, no hubiera sido de utilidad si no se hubiesen logrado materializar las mejoras diseñadas y orientadas a incrementar la efectividad en las operaciones, la confiabilidad de la información financiera, la salvaguarda de activos y el cumplimiento de leyes y regulaciones aplicables.

**CONCLUSIONES**

1. Tal como apreciamos, la aplicación de una adecuada metodología como el COSO ERM en la evaluación del control interno nos permitió identificar y evaluar los riesgos en los diferentes procesos y áreas de una entidad, y proporcionar una evaluación sobre el desempeño de la misma, orientado a mejorar la eficacia y eficiencia en el uso de los recursos y la consecución de los objetivos institucionales.
2. La aplicación de la metodología, permitió contar con bases de datos que ayudaron a formular y mejorar los Planes de Control, por cuanto al tenerse claramente identificados los procesos con mayores niveles de riesgos, las acciones y actividades se dirigieron hacia estos, con lo que los recursos humanos y materiales fueron mejor administrados.

**RECOMENDACIONES**

1. Se recomienda que la metodología COSO ERM aplicada a lo largo de la investigación, sea considerada como base para la evaluación del control interno en las distintas entidades, debiendo tenerse en cuenta.

2. Es necesario que todos los colaboradores de la entidad deban cumplir con el rol de aseguramiento de éxito de la gestión de riesgo, ya que este no sería efectivo si su implementación y administración es realizada por personas con poca o ninguna comprensión de los factores de decisión que involucra la gestión de riesgos, por lo que se debe considerar su mayor efectividad si es conducido por personas que están cerca de las situaciones de riesgo en el negocio y comprenden con facilidad los factores que los rodean y sus consecuencias.

### REFERENCIAS BIBLIOGRÁFICAS

1. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (2013) Control Interno - Marco Integrado.
2. ESTUPIÑAN, R. (2006) Administración de riesgos E.R.M. y la auditoría interna. ECOE.
3. FONSECA, O. (2013) Sistemas de control interno para organizaciones.
4. RAMON, J. (2004) El Control interno en las empresas privadas. Revista Quipukamayoc, Vol 11 N° 22.
5. SLOSSE, C. (2000). Auditoría, un enfoque empresarial, Océano Centrum España.
6. VEGA, E. (2008) Tesis para optar el grado de Magíster en Administración: “ El Sistema de control interno en la empresa moderna”. Universidad San Martín de Porres.
7. VELEZMORO, O. (2010) Modelo de gestión de riesgo operacional en una institución financiera peruana dentro de un enfoque integrado de gestión de riesgos. Pontificia Universidad Católica del Perú.