

**DISEÑO DE UN SISTEMA DE CONTROL INTERNO EN UNA MULTINACIONAL  
DEL SECTOR DE HIDROCARBUROS, BASADOS EN LAS MEJORES  
PRÁCTICAS DE LA INDUSTRIA Y NORMATIVIDAD VIGENTE**

**CONSUELO BERNAL CAMARGO  
GEORGE MORALES SILVA**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE INGENIERIAS FISICOQUIMICAS  
ESCUELA DE INGENIERIA DE PETROLEOS  
ESPECIALIZACIÓN EN GERENCIA DE HIDROCARBUROS  
BUCARAMANGA  
2013**

**DISEÑO DE UN SISTEMA DE CONTROL INTERNO EN UNA MULTINACIONAL  
DEL SECTOR DE HIDROCARBUROS, BASADOS EN LAS MEJORES  
PRÁCTICAS DE LA INDUSTRIA Y NORMATIVIDAD VIGENTE**

CONSUELO BERNAL CAMARGO  
GEORGE MORALES SILVA

Trabajo de Grado para optar al título de  
Especialista en Gerencia de Hidrocarburos

**Directora:**  
ING. LAURA CRISTINA AMAYA RUEDA

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE INGENIERIAS FISICOQUIMICAS  
ESCUELA DE INGENIERIA DE PETROLEOS  
ESPECIALIZACIÓN EN GERENCIA DE HIDROCARBUROS  
BUCARAMANGA  
2013**

## CONTENIDO

Pág.

<b>INTRODUCCION.....</b>	<b>16</b>
<b>1. OBJETIVOS.....</b>	<b>17</b>
1.1 OBJETIVO GENERAL .....	17
1.2 OBJETIVOS ESPECIFICOS.....	17
<b>2. ANTECEDENTES.....</b>	<b>18</b>
2.1 CRECIMIENTO DEL SECTOR DE HIDROCARBUROS EN COLOMBIA .....	18
2.2 FRAUDE FINANCIERO .....	20
<b>3. MARCO DE REFERENCIA .....</b>	<b>21</b>
3.1 DEFINICION DE CONTROL.....	21
3.2 EVOLUCION DE LA CONCEPCION DE CONTROL INTERNO.....	22
3.3 COSO .....	23
3.4 COSO II – MARCO COSO ERM.....	26
3.5 ERM – ENTERPRISE RISK MANAGEMENT .....	27
3.6 SOX LEY SARBANES OXLEY .....	28
3.6.1 Organizaciones: .....	29
3.6.2 Sociedad: .....	29
<b>4. PROPUESTA MODELO DE SISTEMA DE CONTROL INTERNO .....</b>	<b>31</b>
4.1 DIAGNOSTICO SISTEMA DE CONTROL.....	32
4.1.1 Ambiente de Control: .....	33
4.1.2 Riesgos .....	34
4.1.3 Actividades de Control .....	35
4.1.4 Información y Comunicación.....	36
4.1.5 Monitoreo .....	36
4.1.6 Resultados del Diagnóstico:.....	37
4.2 EVALUACION DE RIESGOS CORPORATIVOS.....	37
4.3 IMPLEMENTAR FUNCION AUDITORIA INTERNA.....	44

4.3.1 Plan de Auditoria.....	44
4.3.2 Desarrollo del Plan.....	46
4.3.3 Seguimiento .....	48
4.4 CUMPLIMIENTO SOX.....	48
4.5 ESTRUCTURA DE AUDITORÍA INTERNA .....	52
4.5.1 Comité de Auditoría .....	52
4.5.2 Director De Auditoría Interna – DEA.....	52
<b>5. CONCLUSIONES .....</b>	<b>55</b>
<b>6. RECOMENDACIONES.....</b>	<b>56</b>
<b>BIBLIOGRAFIA .....</b>	<b>57</b>
ANEXO.....	58

## LISTA DE TABLAS

	Pág.
Tabla 1. Informe Estadístico Petrolero 2004 a 2012.....	18
Tabla 2. Riesgos Industria Hidrocarburos .....	40

## LISTA DE FIGURAS

	Pág.
Figura 1 Proceso de Control .....	22
Figura 2 Componentes de Control Interno COSO.....	24
Figura 3 Componentes de Control Interno COSO II.....	26
Figura 4 Modelo de Sistema de Control Interno.....	32
Figura 5 Ciclo Administración de Riesgos.....	38
Figura 6 Árbol de Riesgos.....	39
Figura 7 Matriz de Riesgos.....	41
Figura 8 Metodología Función de Auditoría Interna.....	44
Figura 9 Fases Desarrollo Plan de Auditoría.....	46
Figura 10 Etapas Implementación SOX.....	49
Figura 11 Flujograma .....	51
Figura 12 Matriz de Control.....	51

## ANEXOS

	Pág.
Anexo A Ejemplo de encuesta de Control Interno.....	58
Anexo B Ejemplo Informe de Resultados.....	60

## RESUMEN

**TITULO:** DISEÑO DE UN SISTEMA DE CONTROL INTERNO EN UNA MULTINACIONAL DEL SECTOR DE HIDROCARBUROS, BASADOS EN LAS MEJORES PRÁCTICAS DE LA INDUSTRIA Y NORMATIVIDAD VIGENTE.\*

**AUTORES:** CONSUELO BERNAL C. - GEORGE MORALES S.\*\*

**PALABRAS CLAVE:** Ambiente de Control, Gestión de Riesgos, Actividades de Control, Información y comunicación, Monitoreo, Operaciones, Reporte, Cumplimiento, SOX – Law Sarbanes Oxley, COSO - Committe of Sponsoring Organizations of the Treadway Commission, ERM – Enterprise Risk Management.

Basados en los escándalos financieros en la última década donde la alta dirección se vio involucrada y los riesgos propios de la región como el lavado de activos, y corrupción entre otros, es necesario que las compañías establezcan un modelo de control interno que sea robusto y flexible a la vez.

En Colombia, el sector petrolero ha sido dinámico y por esto llegaron compañías con capitales provenientes de países como Canadá, Francia, China, Rusia entre otros. Estas compañías han crecido de forma acelerada y requieren implementar un sistema de control interno que les permita una adecuada administración de los riesgos. Adicionalmente su sistema de control les debe permitir dar cumplimiento a las regulaciones locales, de las bolsas de valores y en general de todos los temas regulatorios.

En este trabajo se propone un modelo de sistema de control interno acorde con las necesidades de las compañías de hidrocarburos, que ayude a la administración al logro de los objetivos dentro de un marco de confiabilidad y el desarrollo del autocontrol.

La propuesta se enfoca en la implementación de un sistema de control interno, basado en las mejores prácticas internacionalmente aceptadas, que sea aplicable en cualquier país y que contempla cinco factores críticos:

- Implementar un Comité de Auditoría.
- Elaborar un diagnóstico del sistema de control de la compañía.
- Desarrollo de un sistema de administración de riesgos corporativos.
- Implementar la función de Auditoría Interna.
- Diseñar la metodología para el cumplimiento de la ley Sarbanes Oxley – SOX.

Todo este enfoque se propone para que el sistema de control sea flexible atendiendo las necesidades cambiantes del negocio y promueva la confianza de los accionistas.

\*Monografía de Grado

\*\* Facultad de Ingeniería Físicoquímicas. Escuela de Ingeniería de Petróleos. Director Ing. Laura Cristina Amaya

## ABSTRACT

**TITLE:** DESIGN OF A INTERNAL CONTROL SYSTEM FOR A MULTINATIONAL OIL & GAS COMPANY, BASED ON THE BEST PRACTICES AND REGULATIONS \*

**AUTHORS:** CONSUELO BERNAL C. – GEORGE MORALES S. \*\*

**KEY WORDS:** Control environment, Risk assessment, Control activities, Information & Communication, Monitoring activities, Operations, Reporting, Compliance, SOX – Law Sarbanes Oxley, COSO - Committe of sponsoring organizations of the treadway commission, ERM – Enterprise risk management.

According to the financial mismanagements that took place over the last decade, where the Senior Board was involved, along with all risks related to the region such as money laundering, corruption among others, it is necessary for Companies to establish an Internal Control Model robust and flexible enough.

In Colombia Oil & Gas Industry has been dynamic; therefore funded Companies came from different Countries such as Canada, France, China, Russia etc. These Companies have grown rapidly and required implementing an Internal Control System that allows them a suitable risk management. In addition to this, the Internal Control System must allow all Companies to perform in compliance to all local regulations of the stock exchange and all regulation issues in general.

This piece of work suggests and Internal Control Model according to Oil & Gas Company's needs, that leads the administration towards the achievement of goals, outlined within a reliable framework and self-control development.

The proposal is focus on the implementation of the Internal Control System, based on high standard and accepted international practices, applicable in any Country and considering five critical factors:

- Implementation of a Auditing Committee
- Development of an initial assessment of the Control System
- Development of a Management System of Corporate Risks
- Implementation of Internal Auditing function
- Design the methodology for compliance with Sarbanes – Oxley Act (SOX)

This approach is suggested in order to make the Control System flexible, addressing the dynamism of the market needs and promoting confidence in stakeholders.

\* Workdegree

\*\* Faculty of Physical Chemistry. School of Petroleum Engineering. Director Eng. Laura Cristina Amaya

## GLOSARIO

**AGENCIA NACIONAL DE HIDROCARBUROS - ANH:** Es la autoridad encargada de promover el aprovechamiento óptimo y sostenible de los recursos hidrocarburíferos del país.

**AUDITORIA INTERNA:** Actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

**CONTRATO DE EXPLORACIÓN Y PRODUCCIÓN E&P:** contrato que da derecho a una compañía a explorar un área contratada, y a producir los hidrocarburos de propiedad del Estado que se descubran dentro de dicha área.

**CONTRATO DE EVALUACIÓN TÉCNICA –TEA:** contrato cuyo objetivo principal es evaluar el potencial hidrocarburífero de un área e identificar prospectos para celebrar un eventual contrato de E&P sobre una porción ó la totalidad del área contratada.

**SOX: LEY SARBANES OXLEY:** ley federal de transparencia y control de Estados Unidos, que toma su nombre del senador Paul Sarbanes y el congresista Michael G. Oxley. La Ley se aplica a todas las empresas norteamericanas y extranjeras que cotizan en la bolsa de valores de Estados Unidos incluyendo a la Casa Matriz, sus subsidiarias y sus afiliadas.

**CEO: Chief Executive Officer:** persona que tiene a su cargo la máxima autoridad de la gestión y dirección administrativa en una empresa, organismo, asociación o institución.

**CFO: Chief Financial Officer:** funcionario responsable de la gestión financiera de la organización.

**COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION:** Comité conformado por la Asociación Americana de Contadores (AAA), Instituto Americano de Contadores Públicos Autorizados (AICPA), Instituto de Ejecutivos Financieros (FEI), Instituto de Auditores Internos (IIA) y el Instituto de Contadores Gerenciales (IMA); cuya función fue establecer una definición de control interno que fuera aceptada en todos los sectores y que fuera aplicable en cualquier tipo de organización.

**CONTROL:** Actividad preventiva o detectiva que adopta la administración para la oportuna detección o corrección de desviaciones, ineficiencias o incongruencias

con el propósito de procurar el cumplimiento de la normatividad que las rige y asegurar el logro del objetivo.

**FRAUDE:** acto en el cual una persona, una institución o una entidad actúan de manera ilegal o incorrecta según los parámetros establecidos, con el objetivo de obtener algún beneficio.

**RIESGO:** Es cualquier circunstancia, evento, amenaza, acto u omisión, que pueda en un momento dado impedir el logro de los objetivos estratégicos formulados por la alta dirección, o la exitosa implementación de las estrategias.

**SEGREGACIÓN DE FUNCIONES:** Su función es la de asegurar que ninguna persona o departamento maneje todos los aspectos o fases de un mismo proceso desde su autorización, pasando por la custodia de activos y el mantenimiento de los registros.

## INTRODUCCION

Teniendo en cuenta que a partir de 2003 los escándalos financieros han sacudido al mundo y han batido récord en cuanto a fallas sistémicas y de imagen tanto de corporaciones como de sus directivas, así como los riesgos que se generan propios de la región como el lavado de activos, se hace necesario que las compañías adopten un modelo de control interno robusto y que a la vez tenga la suficiente flexibilidad para responder al crecimiento de las mismas.

En Colombia específicamente en los últimos años en el sector petrolero se ha visto la llegada de compañías junior con capitales provenientes de países como Canadá, Francia, China, Rusia entre otros, que han tenido un crecimiento acelerado y que requieren que su sistema de control dé respuesta oportuna a sus necesidades.

Así mismo, algunas de estas compañías están obteniendo sus recursos a través de las bolsas de valores o mediante la emisión de bonos, lo que las obliga a ser vigiladas por entidades de control y por ende deben dar cumplimiento a temas regulatorios en cuanto a la emisión de información confiable.

De acuerdo con lo anterior, este trabajo busca desarrollar un modelo de sistema de control interno acorde con las necesidades de las compañías de hidrocarburos, que ayude a la administración en el logro de los objetivos dentro de un marco de confiabilidad y el desarrollo del autocontrol, propendiendo por el mejoramiento de la gestión a todo nivel el cual tendrá en cuenta los siguientes aspectos:

- Cumplimiento de los objetivos organizacionales.
- Mejor toma de decisiones.
- Mejores planes de acción.
- Mejoramiento continuo y adaptación a los cambios.
- Control sobre los riesgos.
- Aseguramiento de la información.
- Cumplimiento Legal.

Este diseño de sistema de Control Interno aportará a las empresas un conjunto integrado de procesos, que dirigido por la alta dirección y puesto en práctica por

los empleados, proporcionarán y darán una garantía razonable para el logro de los objetivos establecidos por la compañía.

# 1. OBJETIVOS

## 1.1 OBJETIVO GENERAL

Elaborar una propuesta para la implementación de un sistema de control interno para una compañía Multinacional del sector de hidrocarburos basados en las mejores prácticas de la industria.

## 1.2 OBJETIVOS ESPECIFICOS

- a. Proponer una metodología para el análisis de sistemas de control interno aplicados en empresas del sector de hidrocarburos, para determinar el nivel de madurez del sistema en la organización.
- b. Definir un modelo común de control interno con el cual las empresas multinacionales deberían operar en todas sus sedes o países.
- c. Proponer una estructura de la función de Auditoría Interna que garantice la independencia y optimice su gestión en cada una de los países donde tenga presencia y que sea aplicable según las necesidades y objetivos de cada una de las unidades de negocio.
- d. Diseñar un procedimiento para la planificación, ejecución y seguimiento de la Auditoría Interna que contemple la administración de riesgos, cumplimiento regulatorio y control interno.

## 2. ANTECEDENTES

### 2.1 CRECIMIENTO DEL SECTOR DE HIDROCARBUROS EN COLOMBIA

En la última década con la creación de la Agencia Nacional de Hidrocarburos ha ocurrido un crecimiento de las operaciones petroleras en Colombia. Esto originado por el cambio en la política petrolera y en el desarrollo de una intensa actividad de promoción entre inversionistas estratégicos y de evaluación del potencial geológico colombiano.

El nuevo contrato de Exploración y Producción E&P y la creación del contrato de evaluación técnica -TEA permitieron aumentar el número de contratos firmados, el área bajo exploración, los kilómetros de sísmica adquiridos, los pozos perforados y el conocimiento de las cuencas colombianas.

Entre 2004 y 2012 se observó un amplio incremento en las diferentes actividades propias del sector como la firma de 393 contratos de exploración y producción y de evaluación técnica llevando que a septiembre de 2012 existieran 449 contratos firmados vigentes. Así mismo, se observó el crecimiento de las actividades sísmicas donde en este periodo se adelantaron 156 mil kilómetros liderados por las empresas privadas con 121 mil kilómetros que equivalen al 77% del total.

Finalmente en este período se realizaron 687 pozos exploratorios (A3) de los cuales 262 pozos fueron productores lo que representa una tasa de 38% de éxito. El siguiente cuadro muestra la evolución anual:

Tabla 1. Informe Estadístico Petrolero 2004 a 2012

Año	Cantidad Contratos Firmados		Total contratos Vigentes*	Sísmica Miles KMS Equivalentes			Pozos A3
	E&P	TEA		Privadas	Ecopetrol y ANH	Ctd	
2004	21	7	227	5,87	0,90	6,77	21,00
2005	31	28	284	3,20	8,70	11,90	35,00
2006	32	12	257	16,50	9,99	26,49	56,00
2007	44	10	281	9,40	0,57	9,97	70,00
2008	43	16	289	12,48	3,80	16,29	99,00
2009	58	6	346	15,42	4,70	20,12	75,00
2010	7	1	363	23,45	2,51	25,96	112,00
2011	67	9	445	21,66	2,30	23,96	126,00
2012	1	0	449	13,92	0,64	14,56	93,00
<b>Total</b>	<b>304</b>	<b>89</b>	<b>449</b>	<b>121,89</b>	<b>34,12</b>	<b>156,01</b>	<b>687,00</b>

\* Incluye contratos asociación, concesiones, TEA y E&P

Fuente: Asociación Colombiana del Petróleo

Para llegar a los anteriores resultados, durante este periodo la inversión extranjera en el sector petrolero ascendió a USD\$24.002 millones. Entre los principales inversionistas aparecen grandes compañías con presencia a nivel mundial como: Shell, Ecopetrol, Petrobras, BHP Billiton Petroleum y Repsol y se crearon compañías junior como Petrominerales, Hupecol, Interoil Colombia Exploration and Production, Rancho Hermoso, Emerald EnergyPlc, Petro Caribbean, Resources, Pacific Rubiales Energy (Meta Petroleum, Pacific Stratus Energy), Nexen Petroleum, Omimex Oil & Gas Ltd., Talisman Colombia Oil & Gas Ltd., Cepsa, Petróleos Colombianos Limited, Cepcolsa, Pluspetrol Resources Corporation, Equión y Lewis Energy Colombia Inc., que han tenido una participación activa en el desarrollo del sector en Colombia y que les ha permitido buscar nuevas oportunidades a nivel regional en Centro y Suramérica.

El crecimiento acelerado de una organización y la adquisición de activos en otros países obliga a las compañías a invertir un alto nivel de esfuerzos en actividades para la atención de requerimientos legales, financieros y de gestión, necesarios para el desarrollo de las operaciones en el país local.

Generalmente esta situación hace que la administración se realice por silos (países o áreas) liderado por cada gerente local generando un rompimiento del sistema de control interno.

La necesidad de mostrar resultados por las Gerencias Locales, la existencia de operaciones y reportes manuales y el desconocimiento de la regulación local de la industria puede originar fraudes, sanciones, multas, llegando a una afectación de la imagen de la compañía, cancelación de licencias, escándalos financieros y quiebras.

Debido a lo anterior, se hace necesario que las organizaciones que tienen presencia en diversos países, implementen un modelo de Control Interno integral que les permita dar cumplimiento a todos los aspectos regulatorios asegurando la información de forma que la dirección y sus accionistas tomen decisiones adecuadas y protejan sus intereses.

## 2.2 FRAUDE FINANCIERO

Durante la última década se han presentado una serie de escándalos financieros que han generado altísimas pérdidas y la desconfianza del público en algunas operaciones de grandes empresas y en el mercado de valores en general.

El caso más representativo a nivel mundial es el de Enron, empresa distribuidora de energía con más de 21 mil empleados con sede en Houston en donde se ocultaron las pérdidas durante varios años con la complacencia de la firma auditora Arthur Andersen. Se calculó un pasivo de US63.000 millones y en el año 2002 ambas compañías desaparecieron.

Después de este caso aparecieron casos como el de Global Com con la falsificación de las cuentas de utilidades, Laboratorios Merck con ingresos elevados por la facturación con una subsidiaria, Parmalat ocultando su deuda de 14 mil millones de euros que era 8 veces mayor a la anunciada, entre otros.

Colombia no ha sido ajena a esto y es así que el caso más representativo es el de DMG Grupo Holding S.A. que fue acusada por lavado de activos y captación ilegal de dinero. En cuanto a la industria petrolera el caso más reciente es el de Alange Energy que en el año 2010 se ve envuelta en un escándalo de irregularidades en el área financiera en la compañía y la pérdida de confianza entre los accionistas por la presentación de reservas mayores a las reales.

Es así como se requiere que las compañías junior desarrollen un modelo de sistema de control interno acorde con las necesidades, que ayude a la administración en el logro de los objetivos dentro de un marco de confiabilidad. También se requiere que desarrollen su sistema de autocontrol, propendiendo por el mejoramiento de la gestión a todo nivel y que garanticen una adecuada información y ética en la organización.

### 3. MARCO DE REFERENCIA

#### 3.1 DEFINICION DE CONTROL

De acuerdo con el Instituto de Auditores Internos un sistema de control interno es el conjunto integrado de medidas que toma la dirección y todas las áreas de la compañía, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidas.

Los objetivos a que se hacen referencia se relacionan principalmente con:

- La efectividad y eficiencia de las operaciones.
- La confiabilidad en la información financiera y
- Cumplimiento de leyes y regulaciones.

La dirección planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable del cumplimiento de los objetivos trazados.

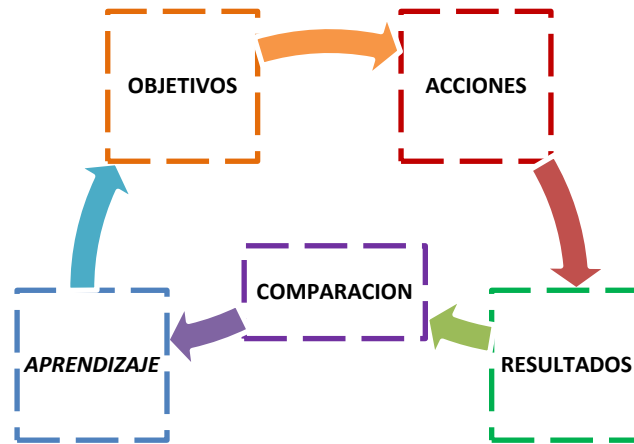
Las acciones tomadas por la Gerencia pueden ser preventivas para evitar que hechos no deseados ocurran, detectivas para identificar y corregir hechos no deseables que ya ocurrieron y directivas para causar o estimular la ocurrencia de un hecho deseado.

Es importante destacar que un sistema de control interno está conformado por personas que interactúan dentro de la organización permitiendo así que el proceso sea una articulación constante de elementos:

Tomado de: The Institute of Internal Auditors. "Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna", [www.theiia.org](http://www.theiia.org)

---

Figura 1. Proceso de Control



Fuente: Consuelo Bernal - George Morales

### 3.2 EVOLUCION DE LA CONCEPCION DE CONTROL INTERNO

Inicialmente el control interno comprendía una serie de actividades de aprobación y autorización de transacciones lo que implicaba que la dirección de la compañía centralizaba todas las decisiones y dejaba evidencia de sus autorizaciones. Las primeras funciones de auditoría interna concentraban su labor en la revisión y verificación de dichas aprobaciones previo a realizar cualquier transacción en la compañía.

Posteriormente éste se desplegó a hacer el seguimiento a la implementación de las estrategias impartidas por la alta dirección, lo que implicó que la función se enfocara a la revisión de la ejecución de varias actividades en las diferentes áreas de la compañía e informar a la alta dirección sobre el desarrollo de éstas.

Finalmente evolucionó a ser un sistema de control interno que implica que existan varias actividades de control dentro de una organización que estén coordinadas y que busquen el logro de los objetivos de la misma.

Surge así la necesidad de definir unos marcos regulatorios que orienten la función y que sean utilizados como referencia.

### 3.3 COSO

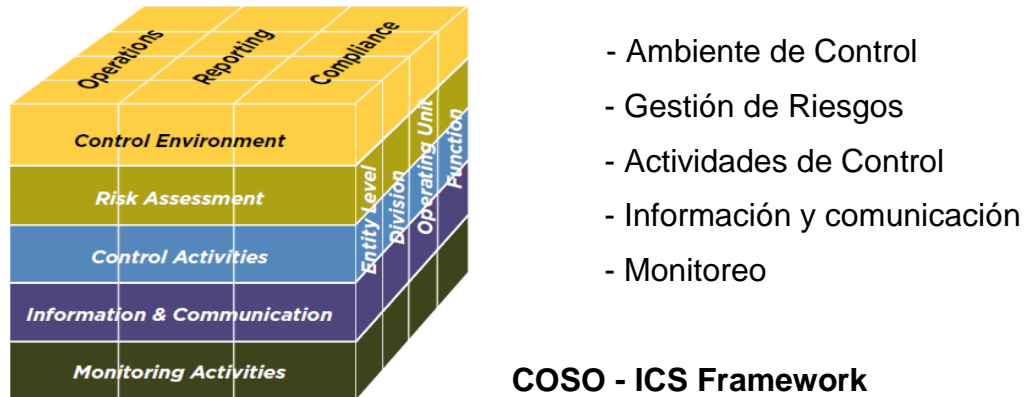
En Estados Unidos en el año 1992 se reunieron representantes de cinco organismos profesionales: la Asociación Americana de Contadores (AAA), Instituto Americano de Contadores Públicos Autorizados (AICPA), Instituto de Ejecutivos Financieros (FEI), Instituto de Auditores Internos (IIA) y el Instituto de Contadores Gerenciales (IMA); cuya función fue establecer una definición de control interno que fuera aceptada como un marco común que cumpliera las necesidades de todos los sectores y aportara una estructura de control interno que fuera aplicable en cualquier tipo de organización, surgiendo así el Informe “*COSO: COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION*”.

La incorporación de COSO condujo a diferenciar 3 aspectos:

- La naturaleza del control interno: efectuado por la administración principal y responsabilidad de ésta, definiciones-objetivos-componentes y temas relacionados.
- La consideración que respecto del control interno hace el auditor (independiente) para efecto de su auditoría de los estados financieros.
- El control interno en los diferentes componentes del ciclo contable.

De otro lado, el informe COSO definió el sistema de control interno en cinco componentes:

Figura 2. Componentes de Control Interno COSO



Fuente: Informe COSO - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

- a. **Ambiente de Control:** el ambiente de control marca la pauta del funcionamiento de una empresa e influye en la conciencia de sus empleados, dentro de los elementos que se debe tener en cuenta están:
- Integridad y valores éticos.
  - Incentivos y tentaciones.
  - Proporcionar y comunicar orientación ética.
  - Compromisos por la competencia.
  - Comité de auditoría.
- b. **Gestión de Riesgos:** se refiere a la identificación y evaluación de los riesgos de origen interno y externo ante los cuales se encuentra expuesto el negocio. En este punto se procede a identificar la categoría de los objetivos así:
- De operación.
  - De información financiera.
  - De cumplimiento

**c. Actividades de Control:** procedimientos, políticas y actividades que ayudan a asegurar los lineamientos y al cumplimiento de los objetivos.

- Revisiones de alto nivel.
- Actividades administrativas.
- Procesamiento de información.
- Controles físicos.
- Indicadores de desempeño.
- Segregación de responsabilidades

Es importante mencionar que las actividades de control deben contemplar también lo que se refiere a los sistemas de información:

- Generales: sobre operaciones del centro de datos, software del sistema, seguridad de acceso físico y lógico, desarrollo y mantenimiento.
- De aplicaciones en proceso.

**d. Información y Comunicación:** recopilar y comunicar información pertinente en forma y plazo que permitan la toma de decisiones. La calidad de la información depende de los siguientes aspectos:

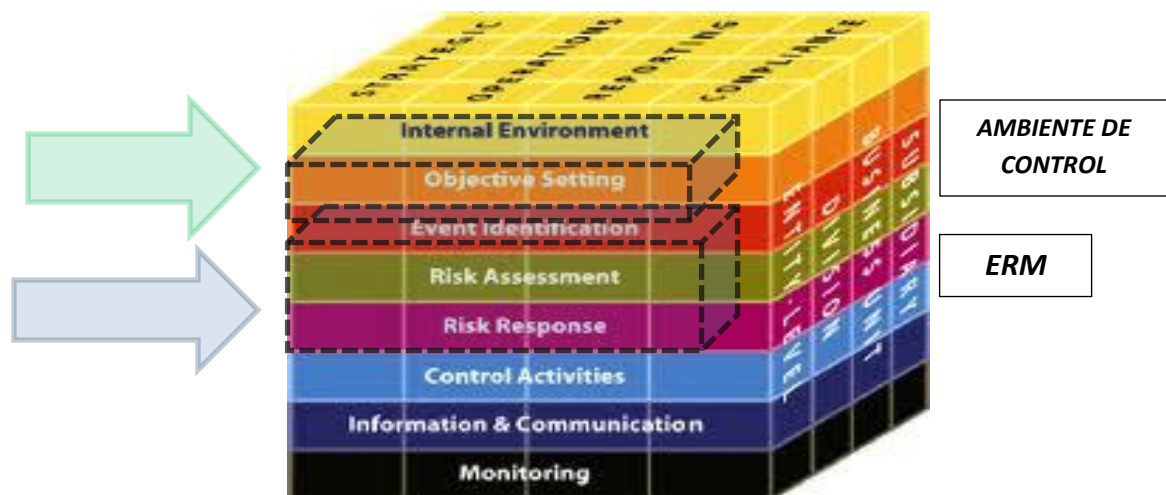
- Contenido apropiado (Se necesita ?).
- Información oportuna (Disponible cuando es requerida).
- Información actual (Es la más reciente).
- Información exacta (Los datos son correctos).
- Información accesible (Puede obtenerse fácilmente).

**e. Monitoreo:** actividades de supervisión, dirigidas a comprobar el funcionamiento del sistema de control interno a lo largo del tiempo

### 3.4 COSO II – MARCO COSO ERM

En septiembre de 2004 se introducen nuevos conceptos para COSO I, los cuales no contradicen lo que instituía sino que el nuevo marco establece una amplia visión del riesgo a hechos positivos y negativos, tolerancia al mismo, oportunidades y amenazas y manejo de los riesgos.

Figura 3. Componentes de Control Interno COSO II



Fuente: Informe COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Este despliegue de elementos en la gestión de riesgos permite que en la valoración de riesgos se identifique y analicen los hechos y eventos relevantes que impidan la consecución de los objetivos, con el propósito de determinar cómo se deben administrar los mismos.

Los riesgos se pueden originar de factores:

- Externos: desarrollos tecnológicos, expectativas cambiantes del cliente, competencia, legislación, fenómenos naturales, cambios económicos, entre otros.

- Internos: fallas proceso de sistemas, idoneidad del personal, políticas de entrenamiento y motivación, cambio en responsabilidades, acceso deficientemente controlado de empleados a activos, comité de auditoría.

### 3.5 ERM – ENTERPRISE RISK MANAGEMENT

ERM se puede entender como un enfoque basado en el riesgo a la gestión de una empresa, la integración de los conceptos de control interno, la Ley Sarbanes-Oxley y la planificación estratégica . Las organizaciones implementan sistemas de Enterprise Risk Management (ERM) basados regularmente en 3 factores de decisión principales:

#### a. Desempeño y valor:

- Alinear ERM a la planeación estratégica.
- Desarrollar un pensamiento crítico con la visión de administración de riesgos a la estrategia.
- Considerar un portafolio de riesgos que pueden impactar los objetivos estratégicos.
- Ayudar a las organizaciones a la obtención de sus objetivos.
- ERM debe ser parte de la cultura de la organización.
- Identificar la efectividad de la organización para responder a los riesgos.
- Ayudar a identificar oportunidades en riesgos para aumentar los retornos de las organizaciones.
- ERM ayuda a evitar problemas para anticiparse a los riesgos.

#### b. Regulación:

- Cumplir con la regulación local o internacional o de industria (energética, bancaria y de seguros).

- Cumplir con los requerimientos de Buen Gobierno Corporativo (p.e., Sarbanes-Oxley, Comités de Auditoría).
- c. Agencias de calificación y Bolsas de Valores:
- Cumplir con los requerimientos exigidos por las Bolsas de Valores con relación a responsabilidades de la Junta Directiva y de Buen Gobierno Corporativo.
  - Cumplir con la guía de las Agencias Calificadoras de Riesgos (p.e., Moody's and S&P), enfatizando la habilidad de las organizaciones para articular y ejecutar los requerimientos de información sobre estrategia, procesos y/o documentación solicitada.

### 3.6 SOX LEY SARBANES OXLEY

(Considerada la más profunda reforma a las prácticas de negocio desde 1934).

Es una ley de transparencia y control, emitida por el Gobierno de los Estados Unidos de América el 30 de julio del 2002, como resultado de una serie de escándalos corporativos que afectaron a ciertas empresas estadounidenses a finales del 2001, producto de quiebras, fraudes y otros manejos administrativos no apropiados.

La Ley se aplica a todas las empresas norteamericanas y extranjeras que cotizan en la bolsa de valores de Estados Unidos (empresas públicas), esto incluye a la Casa Matriz, sus subsidiarias y sus afiliadas.

Las empresas deberán cumplir con la Ley SarbanesOxley si cotizan en la bolsa de Estados Unidos y si son subsidiarias de empresas (Casa Matriz) que cotizan en la bolsa.

Los objetivos de SOX son principalmente:

- Fortalecer el gobierno corporativo.
- Lograr una mayor transparencia.
- Reforzar la responsabilidad de los directores de las compañías y en general en los profesionales que trabajan en ellas.
- Reforzar la independencia del auditor.
- Aumentar la supervisión y ampliar las sanciones por acciones indebidas.

Esta Ley trae consigo impactos directos tanto a las organizaciones como a la sociedad en cuanto a:

### 3.6.1 Organizaciones:

- Compañías públicas registradas en el SEC (Securities and Exchange Commission de Estados Unidos – Agencia federal encargada de la supervisión de los mercados financieros).
- Firmas de auditoría financiera.
- Securities and Exchange Commission de Estados Unidos.
- Aumenta las responsabilidades de los Chief Executive Officer y Chief Financial Officer y las penalidades por fraude.
- Impone nuevas normas de auditoría, más especificaciones sobre cómo elaborar los reportes y qué información se debe guardar.
- Nuevos estándares de contabilidad y penalidades criminales para la gerencia corporativa.
- Nuevos estándares para las Juntas Corporativas y Comités de Auditoría.
- Nuevos estándares de independencia para auditores externos.

### 3.6.2 Sociedad:

- Busca aumentar la confianza de la sociedad en las compañías públicas y de auditoría y así estabilizar el mercado de valores.
- Define nuevos delitos relacionados con el mercado de valores:
  - Destruir, alterar o falsificar récords con la intención de impedir / influenciar una investigación federal ó algún procedimiento de bancarrota.
  - No mantener toda la documentación de auditoría durante el período de retención mandatorio.

- Ejecutar un esquema de fraude contra los inversionistas relacionado a cualquier valor o acción.

Igualmente SOX contempla unas disposiciones especiales las cuáles deben cumplirse en lo que se refiere a:

- ✓ “Certificación” anual del CEO y del CFO.
- ✓ Comité de auditoría independiente y obligatorio para todas las empresas listadas.
- ✓ Devolución por el CEO y el CFO de su compensación (bonos, incentivos, ganancias de ventas de acciones) como resultado de la corrección de los estados financieros de la empresa.
- ✓ Prohibición de préstamos a ejecutivos y directores.
- ✓ Código de Ética obligatorio para altos ejecutivos.
- ✓ Nuevos estándares de conducta para los abogados y auditores que practican ante el SEC en representación de un emisor.
- ✓ Nuevo crimen, sujeto a prisión de hasta 20 años, en relación con la destrucción, alteración o falsificación de documentos con la intención de obstruir una investigación federal.

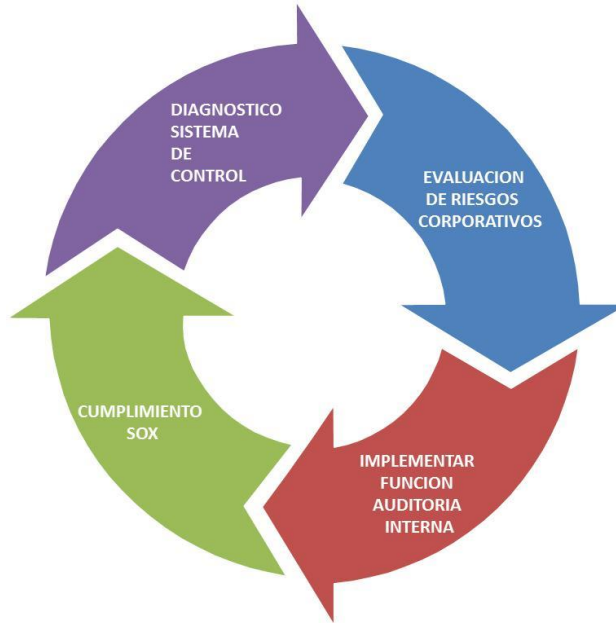
#### **4. PROPUESTA MODELO DE SISTEMA DE CONTROL INTERNO**

En este documento se propone un modelo de control interno con el cual las empresas junior multinacionales pueden operar en todas sus sedes o países y contempla las mejores prácticas definidas por el informe COSO y el Instituto de Auditores Internos (IIA).

El diseño de sistema de Control Interno aportará una metodología, estructura, esquema de planeación y gobierno del área de auditoría interna como también dará a las empresas un conjunto integrado de procesos de control, que dirigidos por la alta dirección y puestos en práctica por todas las áreas y empleados, proporcionarán una garantía razonable para el logro de los objetivos establecidos por la compañía, con una información veraz para sus accionistas y un alto grado de confianza de los socios y del mercado.

El modelo propuesto contempla un ciclo de cuatro elementos básicos que las empresas deben desarrollar una vez al año, los cuales se revisaran a continuación (Véase figura 4).

Figura4: Modelo de Sistema de Control Interno



Fuente: Consuelo Bernal – George Morales

#### 4.1 DIAGNOSTICO SISTEMA DE CONTROL

Para determinar las características del sistema de control interno de una empresa, debe realizarse una evaluación o análisis, a través del cual el área de auditoría interna podrá determinar un plan de acción que tenga un impacto real y que busque la mejora del sistema.

Este análisis debe estar basado en el informe COSO II, midiendo todos sus componentes: Ambiente de Control, que COSO II lo separó en Ambiente Interno y Establecimiento de Objetivos. Evaluación de Riesgos, que contempla los elementos de: Identificación de Riesgos, Evaluación de Riesgos y Respuesta a los Riesgos. Finalmente los componentes de Actividades de Control, Información y Comunicación y Monitoreo.

Para este análisis se sugiere que se adelanten entrevistas con la Junta o Consejo Directivo, Presidencia o Gerencia General, Vicepresidencias y Gerencias funcionales o dueños de proceso, con el fin de medir el nivel de madurez del sistema de control en la organización.

Para las entrevistas, se sugiere que se califique en escalas de 1 o de 1 a 5 donde uno es no se ha implementado y 5 es que se ha definido, comunicado, se está aplicando, se ha verificado y se han tomado correctivos.

Con una adecuada ponderación por cada tema se debe determinar una calificación general de cada componente de COSO y una calificación global del sistema de control interno de la compañía.

(Véase Anexo 1: Ejemplo de Encuesta de Control Interno.)

Los aspectos que se sugiere evaluar en cada componente son:

#### 4.1.1 Ambiente de Control:

Integridad, valores éticos, y comportamiento de los ejecutivos clave: se debe evaluar si la Junta o Consejo Directivo propende por la integridad y los valores éticos y si están formalizados en un código o política de ética.

Adicionalmente se debe determinar si la gerencia toma acciones disciplinarias apropiadas cuando ocurren violaciones a las políticas de ética.

Conciencia de control de la gerencia: se evalúa si la estructura de la gerencia es adecuada o está concentrada. Así mismo se debe evaluar la conciencia de la gerencia en cuanto a temas ambientales, litigios, dependencia de proveedores y en general de los factores externos que pueden impactar la compañía.

Adicionalmente, se debe determinar qué tan conservadora o no puede ser la gerencia con el reporte financiero y el uso de provisiones.

Competencia de la gerencia: se evalúa si la gerencia es competente si tiene las competencias y experiencia.

Participación de la junta directiva o el comité de auditoría: se evalúa si la estructura de la junta o consejo directivo es apropiada, su independencia, si existe una función de Auditoría Interna y si se hacen las reuniones periódicas y formales.

Estructura organizacional y asignación de autoridad y responsabilidades: Se revisa si es apropiada la estructura organizacional, si hay políticas de conflictos de interés, si hay prácticas de autorización y aprobación de transacciones por un nivel adecuado. Además se debe evaluar si es clara la asignación de responsabilidades y si las actividades incompatibles están debidamente segregadas.

Políticas y prácticas de talento humano: acá se verifica si existen normas y procedimientos para la contratación, capacitación, evaluación, promoción, remuneración, y terminación de personal. Así mismo si existe un proceso de selección de personal y si hay un proceso que busque atraer, mantener y retener el talento humano.

#### 4.1.2 Riesgos

En cuanto al proceso de Administración de Riesgos - ERM se debe evaluar:

Proceso Estratégico: se debe determinar si hay una planeación estratégica con sus objetivos claramente definidos que estén debidamente aprobados y comunicados a los Gerentes y Líderes de Procesos. Adicionalmente si se elabora el presupuesto de acuerdo con los objetivos estratégicos y si se hace seguimiento sobre su ejecución y si hay segregación de funciones entre las personas que elaboran, ejecutan y toman decisiones con respecto a cambios en el presupuesto.

De otro lado se debe verificar que el plan estratégico contemple las necesidades tecnológicas.

Identificación y Análisis de Riesgos se debe evaluar los mecanismos para anticipar, identificar y reaccionar a los cambios que pudieran tener un efecto dramático y dominante en la empresa y como la gerencia reporta a la junta directiva y/o el comité de auditoría los cambios significativos en la empresa. En este punto de revisar si existe un proceso para la identificación y valoración de

riesgos y si se han definido los mapas de riesgos y controles para cada objetivo estratégico.

Evaluación y Tratamiento de Riesgos: identificar si existe un proceso de evaluación de riesgos y si se cuenta con los planes para el tratamiento de los mismos.

#### 4.1.3 Actividades de Control

Políticas, normas, procesos y procedimientos: se debe determinar si existen formalmente y son aprobadas, difundidas y revisadas periódicamente las políticas, normas, procesos y procedimientos y los gerentes tiene responsabilidad sobre ellas. Además se debe verificar si se cuenta con una cadena de valor que identifique los procesos del core y los de apoyo

Planificación y presupuesto: verificar si se tienen objetivos claros en términos de presupuesto, utilidades, otras metas financieras y de operación. Adicionalmente si se han implantado sistemas de planificación y de reporte y como se reportan e investigan las variaciones. Así mismo cómo la gerencia revisa los indicadores clave de rendimiento y como se reporta e investiga.

Segregación de funciones: evaluar si hay una apropiada segregación de funciones en las actividades, estructura y en el sistema y como es el proceso de aprobación de accesos a las herramientas de TI para mantener la segregación.

Conciliaciones: determinar si existe un procedimiento para conciliar periódicamente activos, inventarios físicos y terceros como proveedores y clientes. Evaluar si las diferencias son investigadas y como se toman las acciones correctivas.

Documentación y registros: en este punto hay que evaluar cómo se custodian los archivos, documentos valores y la información electrónica y como es guardada y respaldada diariamente.

Actividades de control: incluye la evaluación de las revisiones periódicas a TI, si se cuenta con un ejecutivo de seguridad, un sistema de control para las transacciones críticas como contratación, JVA y manejo de proveedores, tesorería e inventario. Adicionalmente cómo se monitorea y responde a incidentes de intrusión maliciosa y como se divulgan y controla el cumplimiento de temas regulatorios críticos.

#### 4.1.4 Información y Comunicación

Información: evaluar si los sistemas de información proveen los reportes necesarios sobre el desempeño, y la junta o consejo reciben suficiente información oportuna que les permita tomar decisiones. Así mismo debe verificarse que los sistemas de información respondan al logro de los objetivos y como se destinan recursos humanos y financieros para desarrollarlos. De otro lado se verifica como es el proceso de back up y el plan de continuidad que incluya un plan de recuperación y si en la inducción de personal se capacita sobre políticas de manejo de información confidencial y estratégica.

Comunicación: se debe evaluar cómo se comunican los deberes y responsabilidades de control a los empleados, si hay canales para el reporte de situaciones impropias y si las líneas de autoridad y responsabilidad están definidas y comunicadas. Igualmente se debe determinar si existe un proceso de inducción apropiado, cómo la gerencia toma acciones sobre las comunicaciones recibidas de clientes, proveedores, reguladores u otras partes externas y si existe un proceso para comunicar la información crítica a toda la compañía. De otro lado, como los sistemas de información apoyan la comunicación y el establecimiento de metas y planes de seguimiento al recurso humano.

#### 4.1.5 Monitoreo

Monitoreo: determinar que se realicen evaluaciones periódicas del control interno, si se implementan las recomendaciones de auditoría interna y de reguladores y si se corrigen las deficiencias conocidas en forma oportuna. Además si se han definido metodologías de monitoreo, planes de mejoramiento, si hay mecanismos para hacer seguimiento al cumplimiento de estrategias y los indicadores corporativos.

Auditoría Interna: verificar si hay una función de auditoría interna independiente con personal debidamente capacitado y que dé cumplimiento a las normas del IIA en cuanto estatuto, alcance seguimiento al plan, autoridad, seguimiento a recomendaciones y evaluaciones de calidad a la función.

#### 4.1.6 Resultados del Diagnóstico:

Una vez se tenga el resultado de este diagnóstico, debe ser revisado con la alta gerencia y debe establecerse un plan de mejoramiento identificando actividades, responsables y fechas. Así mismo esta evaluación le servirá de base junto con la evaluación de riesgos para elaborar el plan de auditoría de forma que se enfoquen los esfuerzos de auditoría y que los entregables y recomendaciones aporten a la implementación de un sistema adecuado de control interno.

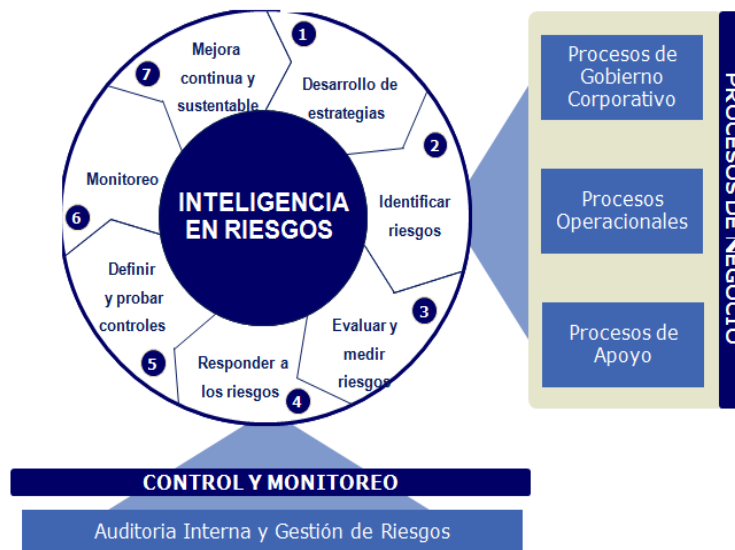
En el anexo 2 se presenta un ejemplo de informe de resultados de un diagnóstico, mostrando el ponderado por cada componente de COSO y los temas prioritarios para mejorar.

## 4.2 EVALUACION DE RIESGOS CORPORATIVOS

Riesgo de negocio: es el nivel de exposición a incertidumbres que la organización debe identificar y efectivamente administrar para alcanzar sus objetivos, ejecutar sus estrategias exitosamente y crear valor. Los riesgos de negocio surgen tanto de la amenaza de que algo MALO ocurra, como de la probabilidad de que algo BUENO no ocurra. El resultado balanceado, permite a la organización entender, anticipar y actuar sobre el riesgo, minimizando las amenazas y maximizando el reconocimiento de las oportunidades.

El análisis de riesgos consiste en separar los riesgos mayores de los menores y obtener datos que ayuden a evaluarlos y darles un tratamiento. El análisis debe considerar las causas, consecuencias y posibilidad de que ocurran. El riesgo debe ser analizado mediante la combinación de las medidas de control existentes. La identificación y calificación de riesgos es el primer paso para gestionar en forma adecuada los riesgos en la Empresa. Ver figura 2. Ciclo de Administración de Riesgos.

Figura 5. Ciclo Administración de Riesgos



Fuente: Deloitte Touche Tohmatsu Limited.

Un lenguaje común de riesgos permite una mejor comprensión de las vulnerabilidades y por lo tanto trazar planes de mitigación eficaces.

Ver ejemplo árbol de riesgos figura 6., donde se presentan los riesgos clasificados en Estratégicos, Financieros, Operacionales y Regulatorios que pueden afectar a la compañía.

Figura 6. Árbol de Riesgos

ESTRATÉGICO									
Gobierno Corporativo			Modelo de Negocios				Político y/o Económico		
Adherencia a las reglas	Comunicación y Divulgación	Relación con Accionista	Competencia Mercado	Estructura Organizacional	Fusión y Aquisiciones	Innovación Tecnológica	Industria		
Incentivos de Desempeño	Reputación e Imagen	Responsabilidad Social	Planeación y Presupuesto	Continuidad de Negocios	Gestión del Conocimiento	Satisfacción del Cliente	Entorno Económico y Político		
Sucesión	Conducta Anti-ética/ Fraude	Cultura Organizacional	Desarrollo de Productos / Servicios	Inversiones y proyectos	Marcas y Patentes	Indicadores de Desempeño y Riesgos	Terrorismo		
FINANCIERO			OPERACIONAL				REGULACION		
Crédito	Mercado	Liquidez	Proceso		RRHH	Información y Tecnología	Medio Ambiente	Regulación	
Concentración	Tasa de Cambio	Costo de Oportunidad	Canales de distribución	Obligaciones contractuales	Capacitación	Aceso y Confidencialidad	Residuos, vertimientos y emisiones	Contabilidad y Finanzas	
Garantía	Commodities	Disponibilidad de Capital	Capacidad Operacional	Tercerización	Concentración de personal	Confiability	Recursos Naturales	Legal	
Incumplimiento	Derivados	Flujo de caja	Eficacia y Eficiencia	Perdida y/o obsolescencia	Limite de Autoridad	Disponibilidad	HSEQ	Laboral	
	Tasa de interés		Falla de Producto / Servicio	Seguridad Patrimonial	Retención de Talentos	Integridad	Tributario / Fiscal		
	Participación	Suministro	Prácticas Comerciales					Civil	
									Ambiental

Fuente: Benchmark Deloitte ToucheTohmatsu Limited

A continuación se presenta un mapa de riesgos para la industria de hidrocarburos, los cuales fueron identificados mediante benchmark (Véase Tabla 2).

Tabla 2. Riesgos Industria Hidrocarburos

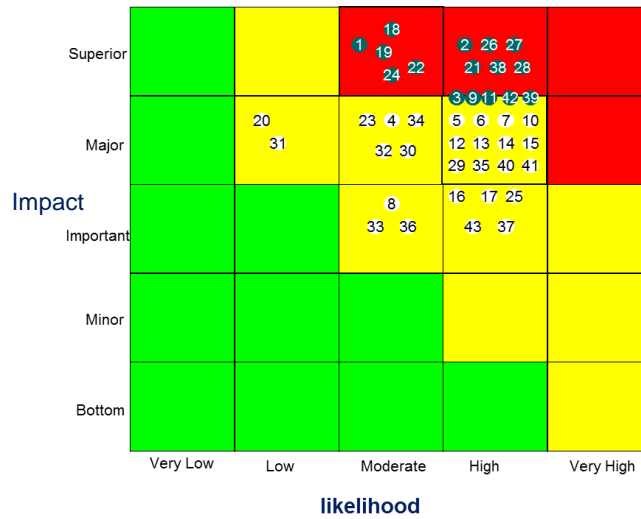
<b>ESTRATEGICOS</b>	<b>OPERACIONALES</b>	<b>CONTROL Y CUMPLIMIENTO</b>	<b>ENTORNO</b>
Reemplazo de reservas	HSEQ	Cumplimiento regulatorio	Socio político
Volatilidad del precio de Oil& Gas	Seguridad / Terrorismo	Fraude y corrupción	Oposición por parte de grupos de interés
Volatilidad de las Divisas	Retención y atracción del Talento Humano	Cambios legislativos	Licencia social para operar
Retrasos en proyectos	Continuidad del negocio	Inexactitud en los estimativos de reservas	Restricciones ambientales
Relación con socios	Medio Ambiente	Cambio climático, emisiones	Condiciones económicas globales

Fuente: Benchmark Deloitte Touche Tohmatsu Limited

Después de identificar los riesgos en reuniones conjuntas con las diferentes vicepresidencias o gerencias de la organización, se evalúan y jerarquizan con el fin de ubicarlos en una matriz de riesgos para definir los planes de acción, que permitan mitigar los riesgos, aceptarlos o transferirlos.

A continuación se muestra un ejemplo de matriz de riesgos clasificada de acuerdo con los resultados obtenidos tanto de probabilidad como de impacto (ver figura 7):

Figura 7. Matriz de Riesgos



Fuente: The Institute of Internal Auditors

El eje de análisis de Impacto indica la posibilidad de que la magnitud del riesgo antes de las acciones, afecte el cumplimiento de los objetivos o la eficacia de los mismos.

El eje de análisis de Probabilidad indica la posibilidad de que ocurra un evento que materialice los riesgos asociados a los objetivos.

Existen criterios de evaluación de Impacto y Probabilidad que deben ser evaluados y acordados por la organización y dependiendo de lo que la organización decida en cómo tratar los riesgos se puede generar una matriz de 5 x 5 o de 3 x 3 con el fin de poder ubicar los riesgos en la matriz y de esta manera saber su calificación.

Algunos criterios de evaluación de impacto pueden ser:

PUNTAJE	CATEGORIA	CRITERIO CUALITATIVO
5	Significativo	El riesgo impide de manera permanente y generalizada el logro de los objetivos del proceso y la utilización óptima de sus recursos para conseguirlos
4	Mayor	El riesgo impide de manera transitoria y/o parcial el logro de los objetivos del proceso y la utilización óptima de sus recursos para conseguirlos.
3	Moderado	El riesgo puede dificultar de manera esporádica y/o en áreas puntuales el logro de los objetivos y ocasionar la subutilización de recursos para conseguirlos.
2	Menor	El riesgo tendría un impacto mínimo en el logro de los objetivos del proceso y en la utilización de los recursos para su logro.
1	Insignificante	El riesgo no tendría un impacto en el logro de los objetivos del proceso y en la utilización de los recursos para su logro.

Algunos criterios de evaluación de probabilidad pueden ser:

PUNTAJE	CATEGORIA	CRITERIO CUALITATIVO
5	Muy Alta	Se presentó más de 5 veces en el año anterior y es muy posible que se repita en el año siguiente
4	Alta	Se presentó entre 3 y 5 veces en el año anterior y es posible que se repita el año siguiente.
3	Moderado	Se presentó entre 2 y 5 veces en el año anterior y es posible que se repita el año siguiente
2	Baja	Se presentó una vez en el año anterior y es posible que se repita el año siguiente
1	Muy Baja	Se ha presentado una vez en más de dos años o no se ha presentado

Los resultados de la matriz permitirán ver en una forma gráfica como están los riesgos dependiendo de su ubicación y del color en donde se encuentren siendo:

<b>Alto</b>	Los controles internos son inadecuados para mitigar los riesgos, proteger los activos o minimizar la exposición a las pérdidas.
<b>Medio</b>	Los controles internos son aceptables. Sin embargo, se identificaron un número de temas de riesgo medio que requieren atención de la gerencia.
<b>Bajo</b>	Los controles internos funcionan. La mayoría de temas de auditoría que se identificaron se evaluaron como bajos.

### 4.3 IMPLEMENTAR FUNCION AUDITORIA INTERNA

La Metodología de Auditoría Interna que proponemos se basa en el modelo COSO “Committee of Sponsoring Organizations of the Treadway Commission”, en las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna y comprende tres fases: plan de auditoría, ejecución del plan y seguimiento.

Figura 8. Metodología Función de Auditoría Interna



Fuente Consuelo Bernal – George Morales

#### 4.3.1 Plan de Auditoría

Para poderle dar un valor real a la compañía respondiendo a las necesidades, la elaboración del plan debe corresponder a un proceso juicioso, sistemático, con tiempo suficiente liderado por el Director de Auditoría Interna y con la participación del equipo de auditoría interna. No es una buena práctica que un plan de auditoría se haga con la simple percepción de la dirección de auditoría o de la empresa.

Para la elaboración del plan de auditoría se deben llevar a cabo las siguientes fases:

- Definir el Universo de Auditoría: el universo de auditoría corresponde a todos los macroprocesos y procesos del negocio, para esto se debe adelantar una revisión de la cadena de valor y del organigrama general de la organización. En este documento se deben identificar si los procesos son estratégicos, core o de soporte así como se deben determinar los subprocesos de los mismos.

- Asociar los riesgos estratégicos a los procesos: a los procesos definidos en el universo de auditoría se les debe asociar los riesgos estratégicos que los impacten. Es posible que varios riesgos afecten un solo proceso para lo cual se recomienda ponderar su calificación. Habitualmente son calificados con un semáforo: alto, medio y bajo siendo alto los de más alta probabilidad e impacto y bajo los de menor.
  
- Valorar Factores críticos: con el fin de tener un plan de auditoría interna que cumpla con las necesidades y de un impacto en la organización se deben tener en cuenta otros aspectos como:
  - Resultados de informes anteriores: dándole una mayor importancia a aquellos procesos que presentaron debilidades considerables. Igualmente el tiempo que ha transcurrido desde la última auditoría.
  - Plan de Auditoría Externa: busca coordinar las actividades para evitar la duplicación de esfuerzos o el complemento en los alcances definidos por cada función.
  - De interés de la Gerencia: con base en entrevistas a la alta dirección se deben identificar los procesos que ellos consideran de interés especial.
  - De interés de la auditoría: procesos en los cuales auditoría interna con base en su conocimiento considera de interés.
  - Cambios relevantes en el proceso: aquellos procesos en los cuales se presentaron o se prevé cambios importantes.
  - Auditorías de Cuenta Conjunta: es propio de la industria petrolera realizar auditorías a la ejecución de los contratos JVA (Joint Venture Agreement). Sus resultados deben ser tenidos en cuenta para la elaboración del plan de auditoría.
  - Resultados de otras auditorías: incluye resultados de las evaluaciones SOX (que se debe realizar por lo menos una vez al año, de acuerdo con la norma; sin embargo se recomienda que se hagan dos veces), auditorías de entes reguladores entre otros.

Para facilitar la decisión de los procesos a auditar se deben hacer calificaciones cuantitativas a cada elemento y su resultado final clasificarlo como ABC, siendo A

de interés para auditar a corto plazo, (6 meses), B para auditar a mediano plazo de 6 a 12 meses y para definir en el próximo plan.

- Cronograma y Recursos: de otro lado, con el fin de dar flexibilidad al plan de auditoria es recomendable incluir tiempos para proyectos que son de interés de la gerencia y que pueden surgir por situaciones puntuales que en el momento de la definición del plan se desconocen. Adicionalmente para el plan se debe tener en cuenta la participación del equipo de auditoria interna en actividades permanentes o periódicas tales como comités, inventarios y proyectos. Con el fin de mantener una adecuada gestión por parte del área se debe realizar la planeación de capacitación del equipo de auditoria.

Con base en lo anterior, se deben establecer los recursos necesarios y teniendo en cuenta la cantidad y la experiencia del equipo y definir un presupuesto en tiempo, gente y dinero. Este plan y presupuesto debe ser llevado al Comité de Auditoría para su aprobación.

#### 4.3.2 Desarrollo del Plan

El proceso de ejecución de la auditoria interna comprende las siguientes fases:

Figura 9. Fases Desarrollo Plan de Auditoria



Fuente: Consuelo Bernal – George Morales

Entendimiento del Proceso y Carta de Auditoria: el auditor debe llevar a cabo un análisis previo del proceso a auditar identificando los objetivos, cifras, actividades procedimientos y controles. Con base en esta información debe definir el objetivo y el alcance de la auditoria. Con el fin de coordinar las actividades y obtener el compromiso de la gerencia se debe elaborar una comunicación de auditoría que contenga el alcance, objetivos, cronograma y entregables.

Análisis de riesgos y controles: en esta fase el auditor junto con el dueño del proceso y su equipo debe llevar a cabo un taller de Identificación y valoración de los riesgos del proceso, la identificación y valoración de los controles y la determinación del riesgo residual.

Programa y Ejecución de Pruebas: el auditor con base en el entendimiento del proceso y el análisis de los riesgos elabora el programa de auditoria con el fin de evaluar el diseño de los controles, la ejecución y efectividad de los controles. Este programa describe la definición de las muestras y las pruebas a realizar paso a paso. El auditor debe dejar evidencia de las pruebas y sus resultados en los papeles de trabajo de acuerdo con las normas de auditoria. Los resultados de la auditoria deben ser revisados Bottom – Up. Esto garantiza un entendimiento claro por parte de cada actor en el proceso de las desviaciones encontradas y puede evitar errores en la apreciación por parte de los auditores. Así mismo es más fácil comprometer a cada actor para lograr la implementación de las acciones recomendadas.

Reporte de resultados y seguimientos: en esta fase se debe realizar el informe de auditoría que se recomienda se divida en dos cuerpos: resumen gerencial e informe detallado. El informe debe contener el objetivo, alcance, la justificación, información general para ubicar al lector, los hallazgos, riesgos, recomendaciones y compromisos. Como buena práctica, el informe gerencial no debe superar tres hojas, debe contener una calificación cualitativa general del proceso y se debe centrar en los aspectos críticos. El informe detallado debe ampliar la información y por cada tema evaluado debe tener una calificación cuantitativa (1 a 5) o cualitativa (semáforo). Así mismo debe detallar los compromisos definiendo claramente un responsable, acción y fecha.

En nuestra opinión básicamente podemos definir que el éxito de una auditoria es cuando las acciones correctivas se llevan a cabo. Es por esto que en nuestra opinión ***el auditor debe pasar de ser un gran identificador de problemas a un muy buen vendedor de ideas*** para solucionarlos. Es así que la fase de seguimiento es muy relevante para la gestión de auditoria interna; para esto se deben clasificar los informes según su calificación global así como los puntos de auditoria por su valoración. Para efectos de gestión se sugiere que para los temas calificados como altos deben hacerse pruebas intensas sobre muestras recientes, para temas calificados como medios pueden hacerse algunas pruebas para determinar las acciones correctivas y para los temas de tratamiento bajo se puede

solicitar una evidencia de la aplicación de la corrección en las fechas acordadas. Es posible que los compromisos cambien si como parte de la dinámica del negocio ya no apliquen y no se controlen los riesgos identificados.

#### 4.3.3 Seguimiento

El DEA debe informar al Comité de Auditoría periódicamente el trabajo ejecutado, haciendo un seguimiento interino bimestral o trimestral de acuerdo a lo que establezca el comité y como requerimiento debe emitir un informe anual donde se plasme lo realizado y en el cual debe hacer referencia a qué evaluaciones se han hecho sobre el control interno, cómo se ha supervisado, de qué manera se ha hecho la emisión de información financiera y no financiera en tiempo y forma. Para eso tendrá que declarar todo el trabajo que ha hecho y principalmente lo que debe hacer es suministrar información de que usó el sistema de evaluación gerencial, usó el sistema de revisión y alcance incluidos en el plan de auditoría interna y también la información que haya sido suministrada por el auditor externo.

#### 4.4 CUMPLIMIENTO SOX

Dando alcance al numeral 3.6 la Ley Sarbanes Oxley tiene dos perspectivas en la organización: un proyecto para lograr cumplimiento y un proyecto de valor agregado, pensando en el cumplimiento como una oportunidad para la implementación de mejoras de la calidad de la información financiera: transparencia, confianza, oportunidad y exactitud y de la efectividad operativa, organizacional, de procesos y tecnológica.

Es así como se debe tener en cuenta un enfoque “**Top-Down**” con el fin de definir estándares en lo que se refiere a:

- Definir un esquema de control interno.
- Definir las unidades legales/ de negocios relevantes.
- Definir los procesos relevantes.
- Definir requerimientos mínimos de control interno (controles claves).
- Definir proceso de auto-evaluación.

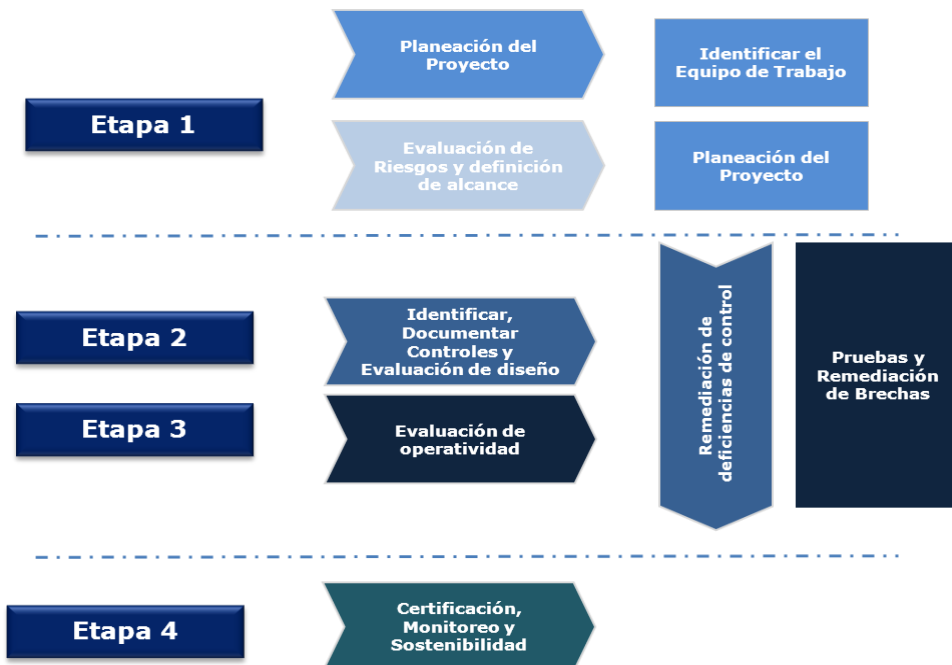
Igualmente, se debe tener en cuenta un enfoque “**Bottom-Up**” con el fin de tener en cuenta una Auto-evaluación en cuanto a:

- Consolidar los resultados de la auto-evaluación y reportar regularmente.
- Realizar la Auto-evaluación.
- Adaptar el concepto de control “top down” a los requerimientos específicos de las unidades de negocio/ entidades legales.

Se sugiere entonces una metodología para su implementación, la cual involucre Vicepresidentes, Gerentes, Directores, Dueños de procesos, responsables del control interno de la organización y facilitadores de procesos que pueden ser firmas de auditoría externas reconocidas.

La metodología comprende 4 etapas:

Figura 10. Etapas Implementación SOX

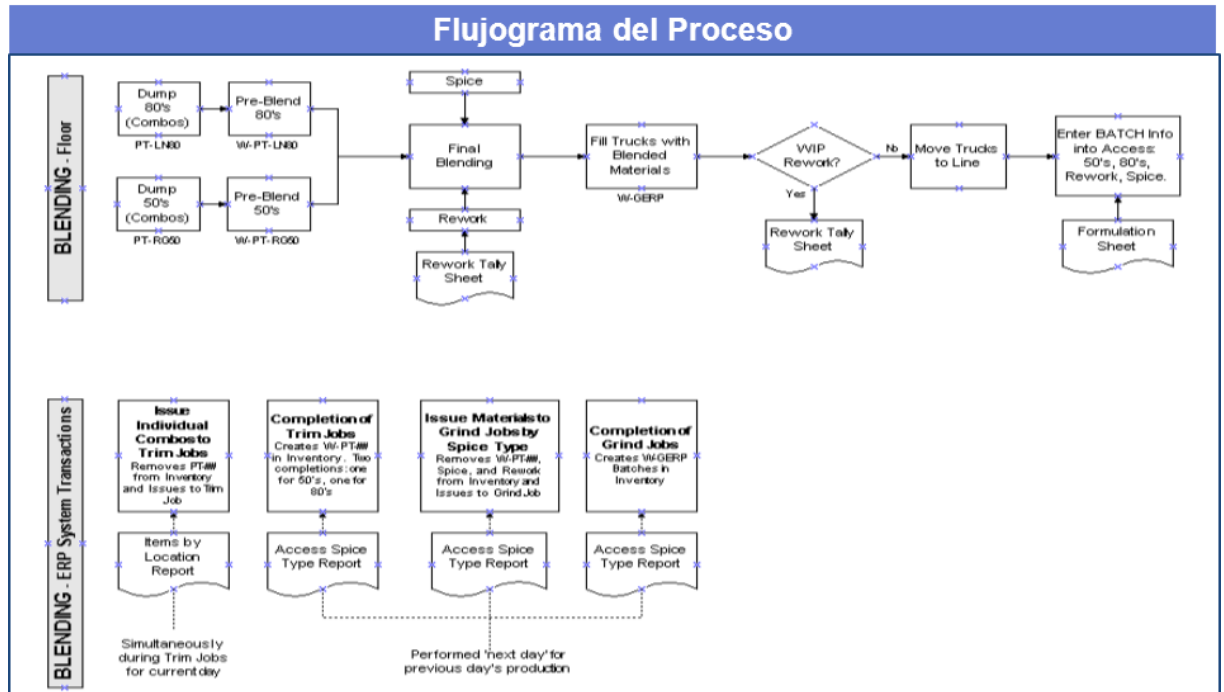


Fuente: Consuelo Bernal – George Morales

- Planeación y Enfoque: en esta etapa se establece el proceso de evaluación del control interno, se define el alcance, enfoque, eventos importantes, tiempos, y recursos del proyecto.
- Documentación: se debe documentar, el diseño de controles, evaluar el diseño del control interno sobre la generación de información financiera y documentar los resultados de la evaluación.
- Identificación de GAPS / transformación de control: identificar, acumular y evaluar las deficiencias del diseño de control, comunicar hallazgos.
- Plan de remediación / asistencia y cierre de GAPS (primer parte): se asesora en la elaboración de planes de remediación y se asiste a los dueños de proceso en la corrección de deficiencias de control.
- Evaluación efectividad operativa: se evalúa la efectividad operacional del control interno sobre la generación de información financiera y se documentan los resultados de la evaluación.
- Plan de remediación / asistencia y cierre de GAPS (segunda parte): se asesora en la elaboración de planes de remediación y se asiste a los dueños de proceso en la corrección de deficiencias de control.
- Interiorización de la Ley SOX: se prepara plan de comunicación y un esquema de asimilación del proyecto.

A continuación se muestra un modelo de los entregables de elaboración de matrices de SOX, narrativas de proceso y flujogramas:

Figura 11. Flujograma



Fuente: Deloitte Touche Tohmatsu Limited

Figura 12. Matriz de Control

Matrices de control						
Control Objective	Control Objective Group	Control Objective Category	Control Activity	Control Group	Control Category	Control Description
Amounts posted to A/P represent goods received			Goods received are matched on line with purchase order details and invoices. Long outstanding goods receipt notes, purchase orders and/or invoices are investigated timely and accrued as appropriate; documents are canceled once matched or on payment of the invoice to prevent reuse.			The Warehouse Receiving Clerk records goods received in the receiving module of the inventory system, producing "Receiving Reports". The Warehouse Supervisor reviews, approves and electronically transmits Receiving Reports to the A/P module of the GL. The A/P Clerk downloads all Receiving Reports and initiates automated reconciliation of the reports to related purchase orders and vendor invoices. A/P Supervisor reviews the reconciliation and approves the transactions for posting to the A/P sub-ledger. The A/P Clerk records, investigates and resolves discrepancies identified in the reconciliation in consultation with the vendor and/or the Warehouse Supervisor. The A/P Clerk records all transactions in the A/P sub-ledger.

Fuente: Deloitte Touche Tohmatsu Limited

## 4.5 Estructura de Auditoría Interna

### 4.5.1 Comité de Auditoría

En primer lugar, el valor más importante de la función de auditoría interna es su independencia y por esto debe depender directamente de la junta o del comité de auditoría bien sea el caso. La Junta o el Consejo Directivo es el ente responsable del control interno en la organización. Para hacer esta labor y dependiendo del tamaño de la organización es nombrado un Comité de Auditoría quien es el responsable de nombrar el Director de Auditoría Interna (DEA), el auditor externo o revisor fiscal, aprobar el plan de auditoría y hacer el seguimiento al desarrollo de las actividades propias de área.

Otras responsabilidades del comité son:

- Asistir a la Junta en la supervisión del proceso de reporte de información financiera y del sistema de control interno.
- Monitorear el cumplimiento de las leyes, regulaciones y el código de conducta.
- Monitorear el desempeño de auditoría interna y externa.
- Revisar el estatuto, planes, actividades, personal y estructura organizacional de la función de Auditoría Interna
- Revisar el alcance y enfoque de auditoría Externa y la coordinación de esfuerzos con la auditoría interna.
- Revisar la eficacia del sistema para vigilar el cumplimiento de las leyes y regulaciones y los resultados de las investigaciones y seguimiento efectuados por la dirección.

### 4.5.2 Director De Auditoría Interna – DEA

No hay un perfil predefinido del DEA, sin embargo en opinión nuestra, el comité de auditoría debe hacer una labor importante en la búsqueda y definición de este cargo. Dado que la función de auditoría interna no es del

core del negocio, es común observar que estos cargos en algunas compañías sean nombrados personas que no cumplen con las características necesarias y se pierda el aporte real de la función. Así mismo, es de considerable cuidado dado algunos DEA sin experiencia pueden aprovechar su condición emitiendo en forma inadecuada juicios y recomendaciones equivocadas.

En primer lugar como características generales el DEA debe ser un profesional especializado con experiencia en la dirección de la función de auditoría interna, habilidades en la dirección de equipos y el conocimiento suficiente de la empresa y de la industria. Igualmente, dentro de sus características técnicas debe tener estudios formales en auditoría o control interno y en lo posible ser certificado por el Instituto de Auditores Internos, lo que puede garantizar un entendimiento claro de la función y no dejar esto al simple olfato.

De otro lado debe ser una persona que cuente con la confianza de la dirección de la compañía con un alto grado de honestidad y liderazgo que debe ser reconocida en toda la organización y especialmente por el equipo de auditoría interna.

Es responsabilidad del DEA establecer el Estatuto de Auditoría Interna que es un documento formal que define el propósito, la autoridad, y la responsabilidad de la función de Auditoría Interna. El Estatuto debe establecer la posición de la Auditoría dentro de la organización, autorizar el acceso a los registros, al personal y a los bienes relevantes para el desempeño de los trabajos y definir el alcance de las actividades de la Auditoría Interna. El DEA debe evaluar periódicamente si el propósito, la autoridad y la responsabilidad, según se definen en el Estatuto, continúan siendo adecuados para permitir que la actividad de auditoría interna cumpla sus objetivos.

Otras funciones del DEA son:

- Suministrar una evaluación anual de la eficacia de los procesos de la organización para controlar sus actividades y gestionar sus riesgos.
- Informar problemas significativos relacionados con los procesos para controlar las actividades de la organización y sus afiliadas, incluyendo posibles mejoras y soluciones.

- Suministrar información periódicamente sobre el estado y los resultados del plan anual de auditoría y la suficiencia de los recursos del departamento.
- Coordinar y proporcionar vigilancia de otras funciones de control (gestión de riesgos, cumplimiento, seguridad, aspectos legales, ética, medio ambiente, auditoría externa).
- Tomar las medidas necesarias para garantizar la independencia de la AAI. Incluirá como parte de sus informes al comité de auditoría un informe regular sobre el personal de auditoría interna.
- Desarrollar un plan anual flexible de auditoría interna, utilizando metodología apropiada basada en el riesgo, incluyendo cualquier preocupación por riesgo o control identificada por la gerencia, y presentar ese plan al comité de auditoría para su revisión y aprobación.

Implementar el plan de auditoría anual de acuerdo con su aprobación incluyendo, si se estima apropiado, cualquier tarea o proyecto especial requerido por la gerencia y el comité de auditoría.

## 5. CONCLUSIONES

Las empresas deben implementar un sistema de control interno como respuesta bien sea por las condiciones de mercado o por los acontecimientos de fraude financieros que se han presentado en los últimos años, y para los cuales se han emitido nuevas normas, prácticas y leyes.

En general las empresas que tienen un sistema de control conocen oportunamente su situación real y pueden responder ante los cambios, implementando y adecuando controles internos, los cuales sean capaces de salvaguardar y preservar los bienes de la empresa.

La gestión del control interno debe ser responsabilidad de toda la organización, incluyendo la Junta Directiva, comités, dueños de procesos y en general todos los colaboradores quienes colectivamente contribuyen a proporcionar una seguridad razonable para el logro de los objetivos y su eficacia depende de alcanzar las metas en cuanto a la eficacia y eficiencia de operaciones, confiabilidad en la presentación de reportes financieros, cumplimiento de normas y obligaciones, salvaguarda de activos y el direccionamiento estratégico.

El modelo propuesto que contempla la evaluación periódica del sistema de control interno, la administración de riesgos, la implementación de una función de auditoría interna con una estructura que garantiza su independencia y el cumplimiento de la regulación SOX, ayudará a las organizaciones junior del sector de hidrocarburos al cumplimiento de los objetivos propuestos generando confianza a sus socios y accionistas con una información confiable.

## 6. RECOMENDACIONES

Implementar un sistema de control interno, basado en las mejores prácticas internacionalmente aceptadas y que le permite su aplicación en cualquier país.

Este sistema debe contemplar:

- Un diagnóstico del sistema de control actual que le permita entender su situación actual y proponer mejoras continuas.
- Un sistema de administración de riesgos corporativos que previene a la compañía sobre situaciones internas y externas que no permitan el logro de sus objetivos y que propone planes de tratamiento de los mismos.
- Implementar una función de Auditoría Interna garantizando su independencia, mediante la implementación de un Comité de Auditoría con un adecuado reporte y seguimiento. Así mismo debe realizarse un plan anual de auditoría incluyendo, si se estima apropiado, cualquier tarea o proyecto especial requerido por la gerencia y el Comité de Auditoría.
- Una metodología para el cumplimiento de la ley SOX que certifique transparencia de las operaciones de la organización y que tenga un sentido de valor para la empresa. “Simplemente cumplir con la regulación no es suficiente. Las compañías deben, hacer de este enfoque parte de su ADN; máxime si ven las nuevas normas como verdaderas oportunidades” (1).
- Para sostener el control en un ambiente de negocio cambiante, el sistema de control y los mismos controles de la organización no serán ni podrán ser estáticos. Mientras el negocio cambia, también lo deberán hacer sus controles con un enfoque orientado al mejoramiento del desempeño del negocio.

Finalmente, con el fin de mantener un adecuado sistema de control interno se requiere que a través del comité de auditoría se garanticen los recursos financieros para la ejecución del plan. Así mismo se deben destinar recursos para la adecuada capacitación de los funcionarios del área en buenas prácticas de auditoría interna, regulaciones, administración de riesgos, entre otros.

---

(1) Comentario”. Comentario William Donaldson SEC – Chairman Julio 30, 2003

## BIBLIOGRAFIA

---

- Orientaciones prácticas para la elaboración exitosa de trabajos de grado de ingeniería. Autores Martha Ilce Pérez y Zuly Calderon. Universidad Industrial de Santander. 2011.
- Ley Sarbanes Oxley, aportes realizados por Raúl Vásquez Erquicio, Gerente de División Auditoría Interna, Ferreyros S.A.A. Lima- Perú.
- Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna - The Institute Of Internal Auditors The IIA – 2004.
- Informe COSO - .
- El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial - The Institute of Internal Auditors The IIA – 2004.
- La Herramienta Clave del Buen Gobierno Corporativo: La Gestión del Riesgo de Negocio - Ernst & Young – 2003.
- Guía para los Comités de Auditoria – KPMG – 2005.

## ANEXOS

### ANEXO A. Ejemplo de Encuesta de Control Interno

<u>Elemento</u>	<u>PREGUNTA</u>	
<b>Proceso Estratégico</b>	Se lleva a cabo un proceso de planeación estratégica, hay objetivos estratégicos y se comunican a los Gerentes y Líderes de Procesos?	
	Periódicamente se revisan y actualizan los planes estratégicos de la empresa? El plan estratégico es revisado y aprobado por la junta directiva?	
	Establece la gerencia objetivos financieros y expectativas reales	
	Se elabora el presupuesto de acuerdo con objetivos estratégicos, existen métodos e informes de seguimiento y de control.	
	Existe segregación de funciones entre las personas que elaboran, ejecutan y toman decisiones con respecto a cambios en el presupuesto.	
	El plan estratégico incluye IT con las necesidades tecnológicas para cumplir con el plan estratégico?	
<b>Identificación y Análisis de Riesgos</b>	Existe un mecanismo adecuado que identifique riesgos de negocios?	
	La gerencia considera cuánto riesgo está dispuesto a aceptar y se esfuerza por mantener los riesgos dentro de esos niveles?	
	Existen mecanismos para anticipar, identificar y reaccionar a los cambios que pudieran tener un efecto dramático y dominante en la empresa o que pudiera afectar el logro de objetivos de la empresa o de niveles de procesos/aplicaciones.	
	Están bien controladas las adquisiciones y ventas disposiciones de negocios significativas y los activos	
	Se hacen revisiones periódicas o existen otros procedimientos para que, entre otras cosas, se anticipen e identifiquen eventos o actividades rutinarios que puedan afectar la capacidad de la empresa de cumplir con sus objetivos y tratarlos?	

<u>Elemento</u>	<u>PREGUNTA</u>	
	La gerencia reporta a la junta directiva y/o el comité de auditoría acerca de cambios que pudieran tener un efecto significativo en la empresa?	
	Existe un proceso metodológico establecido para la identificación y valoración de los riesgos divulgado a las áreas.	
	Se han definido mapas de riesgos y controles a nivel estratégico que contemple para cada objetivo riesgos generados por fuerzas internas, externas, mercados, clientes, productos y alianzas. Si se han definido se están actualizando constantemente.	
	Se diseñan mapas de riesgo y control a nivel de proceso, y se mantienen actualizado	
	Hay interés y compromiso por parte de la alta dirección en la identificación, manejo y monitoreo de los riesgos detectados.	
<b>Evaluación y Tratamiento de Riesgos</b>	Existe un proceso formal para la evaluación de los riesgos en el área o en la compañía.	
	Los riesgos identificados y evaluados se encuentran alineados con el plan estratégico del área y la compañía.	
	Existen planes de mitigación para los riesgos identificados, formalizados, aprobados y valorados.	
	Se responsabiliza a los Gerentes y a sus equipos por el monitoreo constante de riesgos.	

## Evaluación Control Interno

Se adelantó la evaluación para los componentes de control interno con el siguiente resultado.



### Prioridades

- ✓ Código de Ética
- ✓ Estructura Organizacional / Supervisión
- ✓ Políticas y Procedimientos
  
- ✓ Objetivos de la Organización y de las áreas
- ✓ Administración de Riesgos
  
- ✓ Responsabilidades
- ✓ Planeación y Presupuesto
- ✓ Revisiones TI
  
- ✓ Herramienta que soporte los procesos
  
- ✓ Indicadores
- ✓ Auditoría Interna