UNIVERSIDAD AUTONOMA METROPOLITANA AZCAPOTZALCO

DEPARTAMENTO DE ECONOMIA

AREA DE ECONOMIA INTERNACIONAL

REPORTE DE INVESTIGACION

«El MODELO DE GOBIERNO CORPORATIVO, RIESGO Y CUMPLIMIENTO"

NOVIEMBRE 2014

Por Fernando Velazquez Vadillo

INTRODUCCION

El objetivo de este artículo es presentar un desglose de la metodología aplicable a la implementación del Modelo GRC el cual consta de distintos ejes de análisis, y analizar la implementación de Gobierno corporativo en las empresas mexicanas, recalcando los controles a nivel de entidad, tanto de negocio como de tecnología de información, así como, la evaluación en la sustentabilidad y efectividad del control interno, incluyendo la Gestión de Riesgos, enfocándose exclusivamente en la administración y evaluación del riesgo operativo empresarial.

Los descalabros financieros que ocurrieron en Estados Unidos, como el caso de ENRON y la falta de compromiso, por parte de diversas empresas, sobre prácticas de gobierno corporativo, administración de riesgos y cumplimiento de regulación en transparencia de información financiera, motivan el análisis del cumplimiento de la normatividad aplicable a las empresas inmersas en el sistema financiero mexicano bajo un enfoque de GRC. En este se toma en cuenta la visión de la "Gestión del Desempeño" (Principled Performance, GD), un punto de vista hacia los negocios que ayuda a las organizaciones a alcanzar sus objetivos de manera confiable, mientras administran la incertidumbre (riesgos y retribuciones) actuando con integridad (en compromisos obligatorios y promesas voluntarias, www.oceg.org, noviembre 2012).

El logro de la GD exige una visión holística que aborda el Gobierno corporativo, el aseguramiento del desempeño, la gestión del riesgo y el cumplimiento.

I. Antecedentes del GRC.

En este apartado se exponen los principales antecedentes del GRC **(1)**, asi como los fundamentos del Marco Normativo **(2)** que sustentan su implementación en el caso de las empresas mexicanas.

1. Antecedentes del Gobierno Corporativo

Lamentablemente nuestro país fue catalogado con un elevado nivel de fraude (40%), en 2011, a pesar de que el gobierno mexicano ha estado implementado, en los últimos años, regulaciones, reglas y códigos de mejores prácticas corporativas.

En el ámbito económico o de negocios, el fraude y la corrupción hacen referencia a comportamientos no éticos. Las consecuencias para los grandes corporativos se pueden extender tanto a los accionistas, como a los clientes, proveedores, empleados, e incluso a los gobiernos locales (Tarantino, 2008).

El término Cumplimiento hace referencia al actuar de conformidad con las leyes, regulaciones, protocolos, normas y especificaciones establecidas. El punto crítico es el costo de no cumplir con tales regulaciones, ya que dicho incumplimiento deriva en temas civiles, criminales, de carencia de reputación, financieros y de mercado (Tarantino, 2008).

El Cumplimiento se refiere a las acciones organizacionales tomadas y ejecutadas para asegurar la adherencia a las leyes. (Pupke, 2008).

Con el propósito de combatir la corrupción y el fraude hacia y al interior de las empresas, sus agentes internos y externos, están demandando no solo un alto desempeño, sino también transparencia en la información contable/financiera.

Las formas más comunes de corrupción son: Administrativa o Burocrática, llevada a cabo por funcionarios públicos; Gran Corrupción, perpetrada por funcionarios de

estado y organizaciones políticas; Colusión, ejercida por funcionarios públicos o políticos junto con individuos u organizaciones privadas; Clientelismo, que se refiere al uso de una posición oficial para beneficiar y dar trato preferencial a individuos o entidades específicas.

Los sectores más afectados por fraude en México son: Comunicaciones en conjunto con Seguros (48%) y en menor escala las industrias Farmacéutica (23%) y Química (22%). PricewaterhouseCoopers, señala que el origen del fraude por personal interno a la organización representa (40% a 77%) en comparación con personal externo (23% a 60%).

Existe una lista extensa referente a normas, entes reguladores y leyes que las organizaciones, y más aún, las de presencia global, deben cumplir en el ámbito del sector en el que operan y con respecto a los productos y servicios que ofertan.

Pupke (2008), señala que los objetivos principales del Cumplimiento son: a) Asegurar el comportamiento ético y legal, identificando y monitoreando riesgos, b) Asegurar la calidad, c) Cumplimiento con normas y políticas internas, d) Apego a la regulación de órganos gubernamentales y, e) Mantener una cultura corporativa y de ética en todo el personal de la entidad.

Se identifican tres tipos de costos asociados al Cumplimiento: Costo de mantenimiento, que surge por implementar actividades asociadas al mismo; Costo de no cumplimiento, aquel que se eroga cuando una organización hace caso omiso de la normatividad impuesta por un ente regulador y; Costo de Gobierno Corporativo, aquel en el que se incurre para que la dirección de la organización ejecute y supervise el Cumplimiento con normas internas y externas.

Deloitte (2012), señala que en México a pesar de contar con normas y códigos corporativos de mejores prácticas (CMPC), aún falta mucho camino por recorrer.

Si bien es cierto que los grandes corporativos trasnacionales y nacionales cuentan con departamentos específicos orientados a cumplir la normatividad y regulación establecida, la falta de comunicación, coordinación e interrelación entre dichas

áreas, generan resultados parciales. Por estas razones, la práctica más importante que han adoptado las organizaciones a nivel internacional, es la institucionalización del Gobierno Corporativo, Riesgo y Cumplimiento (GRC), en efecto, el GRC permite esta unificación e integración de procesos, que deriva en la mejora de la eficiencia y efectividad de las funciones de control y riesgo en las compañías.

El antecedente inmediato del GRC fue la Ley Sarbanes-Oxley (SOX), enfocada a mantener un sistema de control interno confiable que permita que la información financiera de una compañía se reporte de manera oportuna y que cumpla con lineamientos de regulación tanto locales como internacionales. En particular ciertas secciones de SOX impactan en el tema del Gobierno Corporativo son: Sección 301, referente a quejas relacionadas a temas de contabilidad y auditoría; Sección 302, relacionada a la revelación de procedimientos y controles, incluyendo la certificación trimestral del CEO y el CFO; Sección 404, referente a la certificación anual del reporte financiero (ICOFR), evaluando el control interno bajo los lineamientos del Marco Integrado de Control Interno (también conocido como modelo COSO), asimismo, involucra la opinión de un auditor independiente que lleve a cabo una evaluación del referido control interno; y la Sección 409, que obliga a la rápida revelación de eventos importantes (Hightower, 2009).

SOX está basado en los principios fundamentales de buenos negocios, por lo que aquellas organizaciones que implementan SOX (estén obligados o no), obtienen como beneficio, el mantener una fuerte estructura de control interno que agrega valor a su negocio y que va más allá del cumplimiento mandatorio.

El Consejo de Supervisión sobre la Contabilidad de Compañías Públicas (Public Company Accounting Oversight Board, PCAOB) fue creado para dar cumplimiento a SOX, principalmente a la sección 404, que corresponde a los lineamientos a cubrir para una evaluación del control interno de una organización.

Otro antecedente importante es la Ley de Prácticas de Corrupción en el extranjero (Foreign Corrupt Practices Act, FCPA), la cual establece de manera concreta los

lineamientos a cumplir por las compañías oriundas de los Estados Unidos que cotizan en la bolsa de valores (incluye organizaciones extranjeras) y que tengan subsidiarias o representaciones en otros países, en dos temas principales: 1) Transparencia de provisiones contables y 2) Corrupción y pagos por sobornos a funcionarios de órganos gubernamentales.

En el caso de Latinoamérica, el Banco Mundial (BM), en un afán de mostrar el verdadero cumplimiento de las naciones que la integran, respecto al apego a leyes y controles de corrupción, diseñó indicadores de Gobierno Corporativo, definiendo a este último como las tradiciones e instituciones, por medio de las cuales, la autoridad en un país es ejercida e implementando los siguientes lineamientos:

Insertar: Dimensiones para el Gobierno Corporativo de acuerdo al BM

El primer tratado multilateral establecido contra la corrupción (2005) es UNCAC (United Nation Convention Against Corruption, Convención de la Naciones Unidas contra la Corrupción), que introduce un conjunto de normas, medidas y reglamentos para su aplicación en países que desean reforzar sus regímenes jurídicos destinados a la lucha contra la corrupción. Ademàs especifica la adopción de medidas preventivas y se tipifiquen los tipos de corrupción, tanto en el sector público, como en el privado, y exige a los Estados Miembros que devuelvan los bienes procedentes de la corrupción al país de donde fueron robados. Al cierre del año 2012, la Convención tiene un total de 165 Estados Miembro.

En los Estados Unidos, a nivel Federal, la SEC y las cortes judiciales, son los organismos encargados de reforzar las leyes federales y las regulaciones, por lo que el Gobierno corporativo hace referencia al método por el cual las compañías aseguran a inversionistas e interesados (clientes, proveedores, sociedad, reguladores, agencias de calificación) que utilizan los activos de la forma apropiada para fomentar la rentabilidad y el crecimiento (Tarantino, 2008).

El citado actor destaca que, Holly Gregory (autoridad experta en Gobierno corporativo), señala que en EU, existen cuatro características que delinean un marco de regulación corporativa efectiva, a saber:

Responsabilidades del Consejo. Es responsable del cumplimiento de las leyes y regulación aplicable, además de la supervisión sobre el funcionamiento del corporativo y de procesos relacionados como planeación estratégica, administración de riesgos, así como la publicación de información financiera.

Composición del Consejo. Se refiere a que la mayoría de los integrantes deben ser independientes.

Designación del CEO**.** Este proceso está sujeto a su publicación y al igual que los miembros del consejo, quien sea designado Director debe ser independiente y sin conflicto de intereses.

Independencia. Implica que los CEO deben ser capaces de ejercer juicios objetivos sobre el funcionamiento de la organización.

Debe mencionarse también a la SEC, Comisión de Valores (Securities and Exchange Commission, SEC), cuya misión es la protección de los inversionistas y el mantener mercados financieros justos, ordenados, eficientes además de facilitar la formación de capital, a partir de información financiera significativa.

2. Fundamentos del Gobierno Corporativo

Para el cabal funcionamiento del GRC, en donde las áreas de control reconocen su papel único mientras que comparten objetivos comunes los cuales se alcanzarán por medio del trabajo en equipo, las organizaciones, con el fin de alinear sus objetivos y estrategias y cumplir a cabalidad con la regulación, tanto local como internacional, analizan de manera integral sus funciones de riesgo y control, con el propósito de incrementar su eficiencia y efectividad, a través de identificar e integrar procesos que son rutinarios, como lo es la evaluación de riesgos.

Un ejemplo de lo anterior se observa al momento de lograr acuerdos sobre la definición e identificación de los riesgos más significativos que encara la organización y también al compartir los planes de trabajo, con lo que se evita la saturación de las áreas operativas con revisiones repetitivas y poco productivas. El GRC es un enfoque integrado a lo largo de toda la organización, cuyo principal objetivo es asegurar el firme cumplimiento de los códigos éticos de acuerdo a su apetito de riesgo, garantizando el cumplimiento de sus políticas internas y la regulación externa, mediante la alineación de sus estrategias, sus procesos, la tecnología y su personal.

Tarantino (2008) hace referencia a este marco por medio de brindar una descripción de cada una de sus partes, señalando que el término “Gobierno Corporativo” consiste en alinear los sistemas, los procesos y los controles de una organización para cumplir objetivos.

Broady y Roland (2008), hacen referencia al GRC citándolo como un proceso que ayuda a la organización a optimizar sus políticas y controles establecidos para alinearlos en el cumplimiento de sus obligaciones.

Algunas empresas que han implementado este enfoque y que han mejorado sus sistemas de reporte, de apego a la normatividad y cumplimiento con la regulación son: “Barrick Gold”, empresa minera, que implementó GRC para estandarizar sus procesos y reducir el riesgo al que se encuentra expuesta; “TCF Bank”, la cual administra riesgos y el cumplimiento regulatorio en toda su organización; “Danagas”, compañía de gas, implementó este enfoque para administrar temas de regulación. “The Royal Bank of Scotland”, mediante GRC, administra el riesgo operacional lo que le permitió detectar que las revisiones de control y auditoría internos son el mejor camino para dar seguimiento y validar los procedimientos. La aseguradora “Liberty Mutual”, mejoró el manejo de sus procesos, especialmente los de auditoría, riesgos y cumplimiento regulatorio. La compañía de servicios de minería GBF, ha logrado mantener una correcta documentación de su control interno, administración de incidentes, control de auditorías e inspecciones, administración de contratos y un adecuado reporte financiero (www.cmo-compliance.com, noviembre 2012).

La aplicación del GRC resulta entonces deseable en nuestro país, sin embargo una visión de su implementación como un costo en lugar de una inversión ha limitado su utilización.

La OCDE, define al gobierno corporativo como una serie de relaciones entre la administración de la compañía y sus directores, sus accionistas y otros interesados. Provee una estructura mediante la cual, los objetivos de la empresa son establecidos al igual que la forma en que serán monitoreados para su cumplimiento (OCDE, 2004).

El Gobierno corporativo se sustenta en una serie de principios, los cuales establecen un código de conducta para las empresas, un instrumento que ofrece normas no obligatorias y buenas prácticas, así como, una guía para su implementación, la cual puede ser adaptada a circunstancias específicas de entidades individuales o regionales. Los principios propuestos se dividen en dos partes: Principios de Gobierno corporativo (tabla 4) y Anotaciones a los principios

de Gobierno corporativo (comentarios para hacer más entendibles los razonamientos planteados en dichos principios).

Los principios 5 y 6 son de interés primordial para el GRC. En el caso del principio 5, la divulgación de datos incluye la publicación de información sobre los resultados financieros y operaciones de la compañía, los objetivos principales, transacciones con partes relacionadas, factores de riesgo probables y estructuras de gobierno. Además, se demanda que la revelación de información sea de conformidad con las normas establecidas y con los requerimientos de tipo financiero y no financiero que un auditor independiente solicita.

INSERTAR Principios de Gobierno Corporativo

El principio 6, atribuye varias funciones clave al Consejo de administración, tales como, la revisión de planes de negocio, presupuestos anuales y políticas de riesgo, el monitoreo del funcionamiento de la organización y las prácticas de gobierno corporativo con el fin de prevenir el indebido uso de activos.

Además, considera un punto trascendental a efecto de mantener un adecuado nivel de Gobierno Corporativo: Asegurar la integridad de la contabilidad y de los sistemas de reporte financiero de la compañía, incluyendo al auditor independiente y el aseguramiento de sistemas de control interno, de administración de riesgos y de supervisión operativo y financiero, así como, el cumplimiento con la regulación aplicable (Racz y Weippl, 2010).

Un enfoque que se es recomendable para cumplir con toda la mencionada regulación y que además, permite integrar y coordinar las distintas áreas de control y revisión (control interno, riesgos y cumplimiento, entre otros) es GRC, considerado como un enfoque integrado y aplicado en toda la organización y que asegura que ésta actúa de forma ética, que se apega a su apetito de riesgo y cumple con políticas internas y reglas externas, mediante la alineación de sus

estrategias, de sus procesos, de su tecnología y de su personal, que conlleven a la eficiencia y efectividad (Racz y Wieppl, 2010).

El marco GRC implica distintos componentes y el establecimiento de lineamientos ya definidos para su implementación. Dicho marco, se basa en las fases propuestas por la OCEG, donde señala los elementos y controles que las organizaciones deben diseñar y ejecutar.

El apego a un marco GRC, se logra integrando áreas e iniciativas, leyes y/o normas de órganos gubernamentales o del sector privado

II. Implementación del Gobierno Corporativo en el caso de las Empresas Mexicanas.

En esta sección analizaremos los procesos que permiten monitorear los objetivos de las empresas **(1),** asi como el modelo de Administración del Riesgo Operativo **(2).**

1. Modelos de Control aplicados a Gobierno Corporativo

Control se refiere a un conjunto de actividades empleadas en guiar, manejar y regular la administración de una organización. El control interno, se refiere a un programa de actividades establecidas para monitorear una potencial exposición que podría resultar en un error significativo, omisión, falla o fraude y que podría impactar de manera negativa en los estados financieros. El programa de control interno provee seguridad razonable (más no absoluta) en procesos que: Establecen parámetros para delegar poder o autoridad, para guiar y regular las

actividades económicas demandadas por entidades reguladoras, para probar y reportar el cumplimientos de esos parámetros establecidos, evaluar la efectividad y eficiencia operativa, evaluar la confiablidad del reporte financiero y reportar el cumplimiento con leyes aplicables. El control interno consiste en especificar una serie de políticas, procedimientos y actividades diseñadas para alinear la oportunidad, riesgo y la incertidumbre (Hightower, 2009).

El modelo COSO (Committee of Sponsoring Organizations, Comité de Organizaciones Patrocinadoras) de la Comisión Treadway) define al control interno como un proceso ejecutado por el personal, el comité ejecutivo y el consejo de administración de una organización, diseñado para proveer seguridad razonable respecto al logro de objetivos relacionados a las operaciones, el reporte financiero y el cumplimiento con la regulación (www.coso.org, marzo 2013).

Una forma de apoyar el cumplimiento de un gobierno corporativo adecuado, es mediante la evaluación del control interno sobre el reporte financiero (ICOFR) de una organización. Dicha evaluación, como lo sugiere la Comisión de Valores (Securities and Exchange Commission, SEC) y el Consejo de Supervisión sobre la Contabilidad de Compañías Públicas (Public Company Accounting Oversight Board, PCAOB) debe llevarse a cabo, bajo un enfoque basado en riesgo (top/down) iniciando al nivel de estados financieros, siguiendo con controles a nivel de entidad y continuando con riesgos en cuentas contables significativas, lo anterior permite tener un panorama completo sobre la posibilidad razonable de que existan errores materiales en los estados financieros y sus notas de revelación (www.pcaob.org, marzo 2013).

El Comité de Organizaciones Patrocinadoras (entidad que surge por la iniciativa de cinco organizaciones privadas -Asociación Americana de Contabilidad, Instituto Americano de Contadores Públicos Certificados, Asociación de Contadores y Profesionales Financieros en Negocios, Ejecutivos Financieros Internacionales y el Instituto de Auditores Internos- dedicadas a proveer tópicos de liderazgo y de cuestiones de gobierno corporativo, ética de negocios, control interno, administración de riesgos, fraude y reporte financiero) emitió en 1992 el Marco

Integrado de Control Interno, conocido como modelo COSO y en Mayo de 2013 publicó su última actualización considerando aspectos como: expectativas de supervisión de gobierno corporativo, globalización de mercados y operaciones, cambios y complejidad en los negocios, complejidad en leyes, reglas y normas, expectativas en competencias y niveles de responsabilidad, uso, desarrollo y confianza en sistemas de información y en la detección y prevención del fraude.

INSERTAR Integración del Modelo COSO

El modelo COSO ha sido reconocido como líder para el diseño, implementación, ejecución y evaluación de un sistema efectivo de control interno. Estableciendo tres grandes categorías de objetivos: de operación, de reporte y de cumplimiento. Estos objetivos se evalúan en cinco capas que penetran a la organización en su conjunto hasta alcanzar las funciones básicas de cada departamento.

La evaluación del control interno conforme al modelo COSO, se recopila en matrices de riesgos y controles que permiten acceder a un panorama completo y concreto de la manera en que el sistema de control de una organización se encuentra funcionando y las áreas en que es necesario implementar acciones correctivas.

Componente	Principios
Ambiente de Control Serie de normas, procesos y estructuras interesadas en el ámbito del Gobierno corporativo que provee las bases para cumplir con el control interno a través de la organización	o La organización demuestra un compromiso con la integridad y la ética o El consejo de administración demuestra independencia de la dirección de la organización para ejercer supervisión o Se establecen estructuras, líneas de

	reporte y apropiadas autoridades y responsabilidades o Existe compromiso para atraer, desarrollar y retener talento o Se tiene personal responsable para el cumplimiento del control interno
Evaluación de riesgos Involucra un proceso dinámico para identificar y evaluar riesgos para el logro de objetivos, para ello deben establecerse inicialmente objetivos relacionados a las operaciones, reporte y cumplimiento. También considera cambios en el ambiente externo y de manera interna	o Objetivos claros para identificar y evaluar riesgos o Se identifican los riesgos a través de toda la organización o Se considera el fraude en la evaluación de riesgos o Se identifican y evalúan que podrían impactar el sistema de control interno
Actividades de control Son acciones establecidas mediante políticas y procedimientos que aseguran a la organización a mitigar riesgos y alcanzar el cumplimiento de objetivos. Aplicables en toda la organización	o Controles para mitigar los riesgos y alcanzar los objetivos o Controles para los sistemas de información o Se despliegan controles para poner en acción las políticas y procedimientos establecidos
Información y comunicación La información es necesaria para cumplir con las responsabilidades del sistema de control interno, se obtiene de manera interna y externa. La comunicación es el continuo proceso de proveer, compartir y obtener información necesaria	o La organización obtiene o genera información de calidad para soportar el funcionamiento del control interno o La organización comunica internamente información, incluyendo objetivos y responsabilidades para el control interno o La organización se comunica con entidades externas respecto a temas que afectan la funcionalidad del sistema de control interno
Actividades de monitoreo Evaluaciones son ejecutadas para evaluar si el sistema de control está funcionando, las mismas se desarrollan en todos los niveles de la organización. Las deficiencias detectadas son evaluadas y comunicadas para su correcto seguimiento	o La organización selecciona, desarrolla y ejecuta evaluaciones a los componentes del control interno para evaluar su funcionamiento o Se evalúan y comunican las deficiencias de control interno de manera oportuna a los responsables respectivos y a los directivos

Componentes del Modelo COSO

2. Administración del Riesgo Operativo

El Riesgo típicamente hace referencia a la posibilidad de una pérdida o una falla originada por una actividad o una persona. La gestión de riesgos busca identificar, evaluar y medir el riesgo, en consecuencia, establece planes correctivos para minimizar, mitigar, transferir o evitar tal riesgo (Tarantino, 2008)

Hay diferentes tipos de riesgo que impactan una organización y varían dependiendo de la región, el tipo de industria, el nivel de globalización, algunos de ellos son: Por reputación, de liquidez, de mercado, financiero, de crédito y legal, entre otros. También se clasifican en internos y externos, sin embargo, hay un riesgo que impacta a toda organización: el riesgo operativo.

Riesgo	Descripción
Por Reputación	Relacionado a la confiabilidad en el negocio. El daño a la imagen de una organización puede resultar en la disminución de ingresos o en la destrucción del valor de los accionistas
De crédito	Se refiere al riesgo en que un prestatario caerá cuando incumple en el pago de una deuda en los plazos y condiciones establecidos
De mercado	Es la pérdida en posiciones por movimientos en los precios de mercado
De liquidez	Es el riesgo asignado a un bien bursátil o a un activo que no puede ser comercializado rápidamente en el mercado para prevenir una pérdida o para obtener la ganancia requerida
Operativo	Pérdidas resultantes de fallas en procesos internos, personas y sistemas, o como consecuencia de eventos externos

Tipos de Riesgo

El Comité de Basilea, órgano creado por el Banco de Compensaciones Internacionales (Bank for International Settlements, BIS) que supervisa en temas asociados al sector bancario a nivel mundial con el propósito de mejorar sus prácticas regulatorias, señala siete áreas de riesgo operativo: Fraude Interno, Administración de Procesos, Fraude Externo, Interrupción de Negocios, Prácticas de Contratación, Daños a Activos y Clientes, Productos y Negocios. Los aspectos a considerar para una adecuada administración del riesgo operacional (Operational Risk Management, ORM), se enfocan a distintas vertientes:

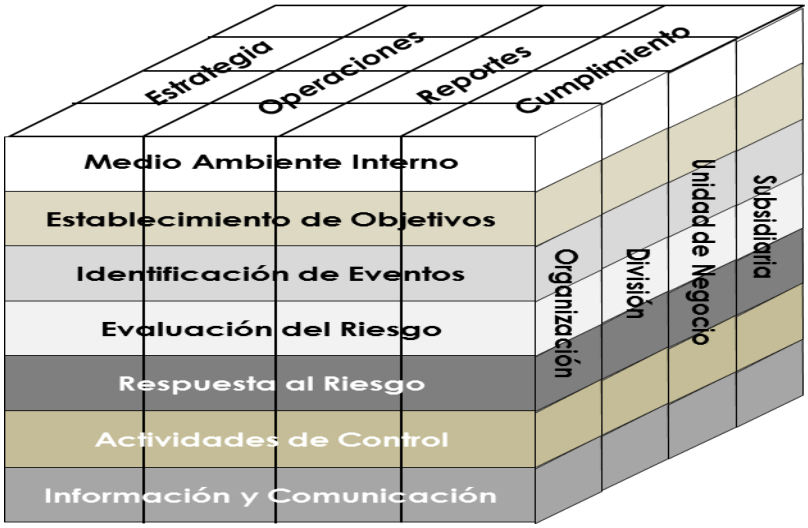
Vertiente	Descripción
Cultura corporativa	o Apoyo por el comité ejecutivo al ORM o Política de ORM o Establecimiento de un comité de ORM o Política de apetito de riesgo o Evaluación del riesgo operacional con base a escenarios o Designación de un Director de riesgos o Aplicación del marco de administración de riesgos ERM
Documentación	o Indicadores de desempeño (KPI) o Indicadores de riesgo (KRI) o Scorecards (tableros de seguimiento) o Plan de continuidad de negocios o Matrices de riesgos y controles (SOX-COSO) o Pruebas de stress y análisis de escenarios
Políticas y procedimientos	o Creación y establecimiento de procesos, políticas y procedimientos y difusión en toda la organización
Auditoría independiente	o Revisión independiente regular sobre los sistemas críticos y procedimientos que impactan el riesgo operacional
Plan de continuidad de negocios	o Plan de recuperación de procesos y de sistemas en caso de interrupciones por personas o eventos naturales, así como, una evaluación de los procesos críticos de la organización
Supervisión de la administración	o Ambiente de control mediante segregación de funciones y accesos a los sistemas o Actividades de monitoreo y seguimiento o Actividades de respaldo de información o Establecimiento de mecanismos de denuncias o Programas para investigaciones de comportamientos inadecuados o sospechosos o Implementación de una política de ética o Monitoreo sobre actividades que son y no son relacionadas al reporte financiero

Aspectos que Involucran la Administración del Riesgo Operativo (ORM)

En el año 2004, COSO publico ERM o COSO II, el cual establece un marco de administración de riesgos, que identifica y describe ocho componentes interrelacionados, necesarios para una adecuada administración del riesgo.

Se define al ERM como un proceso ejecutado por el comité ejecutivo de una organización, la administración general y otras personas, designadas a identificar potenciales eventos que puedan afectar a la entidad, gestionar el riesgo y proveer seguridad razonable de que los objetivos de la entidad se están cumpliendo.

El control interno se encuentra dentro del marco de ERM, y este a su vez, forma parte del Gobierno corporativo de una organización.



Componentes del Modelo ERM o COSO II

Por otra parte ERM, introduce dos nuevos conceptos referentes a la gestión de riesgos: a) Apetito de riesgo, referido al monto de riesgo que una organización está dispuesta a aceptar en el cumplimiento de sus valores y su misión y, b) Tolerancia al riesgo, el cual es el nivel aceptable de variación relativo al logro de objetivos.

La cuantificación del riesgo puede llevarse a cabo, mediante la aplicación de dos variables: impacto financiero y probabilidad de ocurrencia. Para esto, se recurre al uso de técnicas cuantitativas, por ejemplo, el análisis de riesgos de seguros, de crédito y de mercado, por lo regular utilizan herramientas estadísticas y de cuantificación de datos históricos. Los pasos sugeridos para evaluar y manejar el riesgo operacional son: a) identificar los procesos clave; b) identificar y evaluar el riesgo, identificando el origen de la falla, modelando y simulando el proceso de negocio; c) cuantificando el riesgo operacional y; d) monitorear y controlar el riesgo (Tarantino, 2008).

Pasos	Descripción
Definir	Se enfoca en el entendimiento del proceso, qué se hace, cómo se hace, quién lo hace y qué es lo que el cliente quiere, para efectos de cumplimiento, el cliente es la entidad reguladora.
Medir	Consiste en identificar los puntos críticos del proceso.
Analizar	Estudio profundo de los aspectos más importantes identificados en la fase de

Componente	Descripción
Ambiente de control	Considera la filosofía sobre el apetito de riesgo, ética y el ambiente en el que operan
Establecimiento de objetivos	Considera la identificación y priorización de objetivos
Identificación de eventos	Involucra la administración de evento internos y externos que afectan el logro de objetivos
Evaluación de riesgos	Cubre el análisis de riesgos, así como, su probabilidad e impacto financiero y la naturaleza de los controles necesarios para gestionar los riesgos
Respuesta al riesgo	Cubre la respuesta de la administración ante los riesgos existentes (aceptándolos, evitándolos, reduciéndolo o compartiéndolos). Un factor importante a evaluar es el costo-beneficio
Actividades de control	Son las políticas y procedimientos establecidos e implementados, para dar respuesta a los riesgos organizacionales
Información y comunicación	Comprende como la información es identificada, capturada y comunicada en tiempo y forma
Monitoreo	Comprende evaluaciones integrales y/o individuales sobre todo el marco ERM

Aspectos que Integran al Modelo ERM o COSO II

	medición, para tal efecto, se hace uso de herramientas de tipo descriptivas (histogramas y diagramas).
Mejorar	Implementación de planes creados, derivados de las deficiencias detectadas.
Controlar	Institucionalización de un sistema de seguimiento, que permita asegurar que el proceso mejorado cumple con los estándares establecidos.

CONCLUSIONES

El modelo GRC se integra por tres componentes principales: i) Gobierno corporativo, considerado como la alineación de procesos, sistemas y controles en beneficio del cumplimiento de los objetivos de la organización; ii) Riesgo, entendido como la posibilidad de una pérdida o una falla derivada de una actividad ejecutada o por una persona y; iii) Cumplimiento, definido como la forma de actuar de conformidad con las leyes, regulaciones, normas y especificaciones establecidas

(Tarantino, 2008). El apego a un marco GRC, se logra integrando áreas e iniciativas, leyes y/o normas de órganos gubernamentales o del sector privado, como sigue:

mplimiento	Consideraciones
ORM	Administración del Riesgo Operacional, uno de los riesgos que repercute en todos los procesos de una entidad, sin importar a giro a que se dedique. Los aspectos que considera son: cultura corporativa, documentación (procesos,

	riesgos, controles), políticas, auditorías, supervisión por pate de la administración
CMPC	Son prácticas corporativas que buscan ayudar a las sociedades en su proceso de institucionalización, en la transparencia de sus operaciones y en una adecuada revelación de información financiera
FCPA	Regulación a cumplir en dos aspectos fundamentales: provisiones contables y monitoreo de pagos a oficiales gubernamentales ilícitos (sobornos)
OCDE	Estableció principios de Gobierno corporativo, mediante un código de conducta que ofrece normas no obligatorias y buenas prácticas para organizaciones

Cumplimiento con GRC

BIBLIOGRAFÍA

CObIT, (2012), A Business Framework for the Governance and Management of Enterprise IT, Illinois. ISACA

Código de Mejores Prácticas Corporativas, (2010), México. CCE

COSO (2012), (Internal Control - Integrated Framework) USA. COSO

Mitchell, S., Stern, C., (2012), Red Book (El Libro Rojo), Arizona. OCEG

Naciri, A., (2008), Corporate Governance around the world, London. Rotledge

Principios de Gobierno Corporativo (2004), Paris. OCDE

Pupke, D., (2008), Compliance and Corporate Performance, Hamburgo. BoD

Racz, N., Weippl, E., (2010), A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC). Berlín. Springer

Tarantino, A., (2008), Governance, Risk and Compliance Handbook, New Jersey. Wiley

Vu Broady D., Roland H., (2008), SAP GRC, New Jersey. Wiley