BAKER TILLY

FUNDAMENTOS DE GRC

GRC: Gobierno, Riesgo y Cumplimiento

Ricardo Vasquez Bernal
Socio Líder de Servicios de GRC
Business Consulting
Latinoamérica

Créditos

Elaborado por:

Baker Tilly
Business Consulting
Colombia
Marzo, 2015

Para más información visite:
www.grcenespanol.com

Certifíquese como profesional de GRC. Participe de los Seminarios de formación en GRC.
Ingrese a **http://grcenespanol.com/seminarios-grc/** para más información.

Este documento es gratuito, para obtener una copia solo debe solicitarla atreves del sitio: **www.grcenespanol.com**

Queda prohibida la reproducción total o parcial de esta publicación, por cualquier medio o procedimiento, sin para ello contar con la autorización previa, expresa y por escrito de Baker Tilly. Toda forma de utilización no autorizada será perseguida con lo establecido en la ley del derecho de autor. Derechos Reservados Conforme a la ley, ©.

Todos los derechos reservados ®

2015

Contenido

Introducción.

La complejidad de implementar un elevado número de regulaciones, el incremento en la exposición a riesgos y la necesidad de encontrar eficiencias internas para hacer más efectivo el modelo de negocio, hace necesario entender la importancia, profundidad y alcance de un concepto como GRC, por cuanto es algo más que un acrónimo, que muchos identifican con las responsabilidades de cumplimiento, requerimientos de gobierno corporativo o la implementación de sistemas de riesgos.

GRC es, en verdad, una capacidad de la organización para potenciar el ahorro de costos, la optimización operativa, el mejoramiento continuo, la eficiente gestión de riesgo y controles, al igual que la gestión integrada del desempeño con fuertes niveles de aseguramiento. Es, en efecto, algo más que cumplir normas, implementar riesgos y emitir manuales y estatutos de gobierno, y no puede entenderse, tampoco, como una solución de tecnología, un programa de evaluación, y mucho menos una nueva norma o estándar para cumplir.

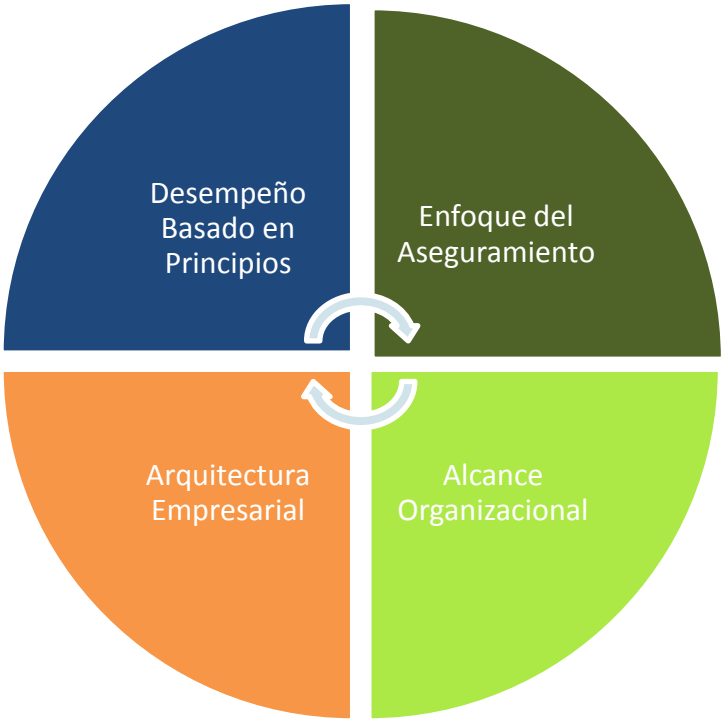
"GRC es una capacidad de la Organización para potenciar el ahorro de costos, la optimización operativa, el mejoramiento continuo y la eficiente gestión del riesgo y desempeño"

Conocer las potencialidades de GRC para el beneficio e impacto empresarial, en suma, requiere desarrollar y nivelar una base de común de conocimientos sobre los elementos que implica el acrónimo, las prácticas reconocidas de aplicación frente a problemas y desafíos contemporáneos, y el conocimiento de los elementos y componentes de un potencial marco estructurado.

Visto así, se presenta como una capacidad de mejoramiento continuo que apoya la optimización empresarial, que tiene distintos niveles de madurez que configuran su aplicación o implementación y, derivado de esto, cómo se pueden generar competencias

que apoyan la ejecución de proyectos de carácter integral con resultados multifuncionales.

Un GRC integrado y holístico se conforma por cuatro perspectivas: a. La perspectiva del desempeño basado en principios; b. La perspectiva de la Arquitectura Empresarial, c. La perspectiva del Enfoque del Aseguramiento y d) la perspectiva del alcance.



Con estas perspectivas, GRC cumple un importante derrotero establecer qué quiere lograr, cómo lo quiere lograr, cual nivel de madurez requiere y donde lo quiere lograr. El desempeño basado en principio define el marco de objetivos que la empresa quiere lograr, la identificación y gestión de los riesgos esperados y el cumplimiento de las normas internas y externas a los que la empresa deberá someterse. El enfoque de aseguramiento, implica establecer las intervenciones de gobierno, gestión y aseguramiento que serán requeridas para asegurar los derroteros del desempeño, riesgo y cumplimiento, en principio.

La arquitectura empresarial, por su parte representa los elementos y objetos requeridos para materializar los resultados y la operación del desempeño, riesgo y cumplimiento, como son los procesos, la estructura organizacional, la tecnología, la información y los recursos, al paso que el alcance organizacional se refiere a que esta implementación puede llevarse a cabo a nivel corporativo, de la entidad, de un proyecto o de una unidad o departamento.

Cada una de estas perspectivas será objeto de un análisis general e integral en las próximas líneas.

Perspectiva del Desempeño Basado en Principios.

2.1 Bases Conceptuales.

Concepto. El Desempeño basado en principios se refiere al logro de objetivos de una organización, de una manera confiable, abordando la incertidumbre y actuando con integridad.[1] Son varios sustantivos los que subyacen en la definición: el logro esperado de objetivos, en función del modelo de negocio, la incertidumbre que involucra el concepto de riesgo y control, y la integridad que va más allá del cumplimiento obligatorio de normas.

La construcción de este concepto, basado en el estudio de OCEG[2], involucra la necesidad de incorporar las variables de incertidumbre e integridad, atadas al desempeño. Es decir, que no basta con que una organización se constituya para generar rentabilidades y crecimientos patrimoniales, por cuanto, de manera recíproca su sostenibilidad en el largo plazo, depende de su responsabilidad y compromiso ante las partes interesadas, así como de la evaluación de los factores internos y externos que, en función del modelo de negocio, afectan su estrategia y operación.

[1] El Desempeño basado en principios es un concepto acuñado por OCEG, como base estructural del GRC. OCEG- Red Book. Modelo de Capacidad. Introducción al desempeño basado en principios. Pags.11 y 12.
[2] Curso de fundamento de GRC. OCEG. Open Compliance and Ethics Group. www.OCEG.org

La integridad, primero, ha jugado un rol fundamental en la sostenibilidad de las empresas en las últimas décadas. La profunda depresión, por ejemplo, del precio de las acciones de las empresas más grandes del mercado de valores en USA, a comienzos del siglo generado por los problemas de transparencia de información, malos manejos y reportes inexactos que llevaron a la quiebra a un sinnúmero de empresas estandarte del mercado de capitales, es un referente implacable de los efectos que produce en la sostenibilidad.

La incertidumbre, en igual sentido, ha representado efectos relevantes, como ocurrió a finales de la primera década, en tanto se materializó en una fuerte caída del precio de las acciones, como resultado de consideraciones y aspectos propios de la especulación del mercado, que no se explicó, propiamente, por caídas de las variables o indicadores fundamentales de las empresas sino por burbujas especulativas que generaron insuficientes e inexistentes garantías terminaron por quebrar la confianza en el sistema financiero y el mercado de valores a nivel global.

"Desempeño basado en Principios es el logro de objetivos confiables, abordando la incertidumbre y actuando con integridad"

El desempeño basado en principios impone condiciones. Estos son, en esencia, los mismos principios que deben acompañar el desempeño. Uno se refiere a la necesidad de que una organización defina objetivos razonables, alcanzables y medibles[3]. Es una falencia común en las empresas encontrar que los objetivos no se declaran y cuando lo hacen, o no se pueden medir porque no tienen mecanismos base de seguimiento, o no se pueden asegurar porque no se alinean con los procesos, operaciones o líneas de negocio. Este parece ser el sitio común de limitaciones en la definición de objetivos que niegan el principio del logro de objetivos confiables.

Además de este principio imperativo, se encuentra otro no menos importante que tampoco se aplica y es que los objetivos se deben ponderar en función de las

[3] OCEG. Curso de fundamentos y formación Profesional en GRC. www.OCEG.org

oportunidades y amenazas del negocio, es decir en un contexto de incertidumbre, aspectos estos que, si se consideran, no pasan de la identificación de factores externos o internos que pueden afectar el logro de los objetivos. Lejos de métricas, lejos de indicadores y, por supuesto, lejos de impactos.

Será preciso tener, en materia de la evaluación de la incertidumbre, la misma rigurosidad que se aplica para la definición y escalamiento de un objetivo estratégico en metas tácticas dentro del modelo de operación. La gestión integral del riesgo se resuelve, normalmente, por vía del examen de los riesgos financieros y no financieros, con fines regulatorios. Sin embargo, el principio de incorporación de la incertidumbre requiere una perspectiva de alcance estratégico, lejos de los requerimientos normativos.

Finalmente, la condición de integridad se refiere a que junto a los desafíos a alcanzar, están los compromisos voluntarios y obligatorios que se adquieren con las partes interesadas, y deben hacer parte integral del desempeño bajo principios. Este es un principio que, igual, va más allá de la verificación del cumplimiento de los marcos normativos obligatorios y se refiere a la actuación con integridad que implica comportamientos éticos y honorables, muchos de los cuales no se garantizan con la emisión de estatutos.

“El Desempeño basado en Principios no es un nuevo estándar. Es la integración y orquestación de las prácticas y estándares de Desempeño, Riesgo, Control y Cumplimiento”.

Alcance. Una organización, podría entender en principio, que aplicando las distintas prácticas y estándares inherentes para el desempeño, el riesgo, el control y el cumplimiento, como seguramente lo viene haciendo por las regulaciones en acción, cumpliría con las condiciones del Desempeño Basado en Principios. Sin embargo, el valor agregado de este importante concepto radica, justamente, en la aplicación integral e integrada de todas estas prácticas y estándares, para optimizar la eficiencia operacional.

Desempeño basado en principios requiere resolver los problemas de silos independientes causados por la aplicación individual de prácticas, que tratadas así, generan profundos costos e ineficiencias causados por duplicaciones de información, reprocesos, actividades de poco valor, procesos y protocolos no documentados, métodos y aplicativo de poco alcance, datos e información imprecisa, sobre-control, exposiciones en líneas o áreas críticas y desarrollos de tecnología subutilizados, solo por citar algunos temas que golpean con presión la efectividad del negocio.

El impacto esperado de la implementación del desempeño integral bajo principios debe significar un salto en la efectividad de los resultados de la empresa, un significativo ahorro en la eficiencia de los recursos y un notable avance en la eficiencia de las operaciones. Es potenciar la rentabilidad bajo el enfoque de optimizar los costos, procesos y métodos de operación.

La estructura del desempeño basado en principios incorpora, cuatro disciplinas, cada una de las cuales está soportada, en marcos de referencia propios, autónomos, con objetivos específicos, pero deben ser integrados. El desempeño con el derrotero central del logro de objetivos; el riesgo y control para la evaluación de la incertidumbre y la efectividad operacional, respectivamente, y el cumplimiento para desarrollar y garantizar el cumplimiento normativo.

Cuando se advierte que cada disciplina impone sus propios marco de referencia, modelos y niveles de madurez, se plantea, justamente uno de los problemas más serios que GRC debe resolver: la integración de prácticas de Desempeño, como puede ser el Balanced Sorecard o los modelos de planeación que potencian la estrategia, con los estándares de gestión de riesgos (ISO 31000 o Basilea). En igual sentido, la alineación de las prácticas o estándares de riesgo con los estándares de control y las prácticas de auditoría interna. Finalmente, la alineación de los requerimientos de cumplimiento normativo con las prácticas de control, gestión de riesgos y desempeño.

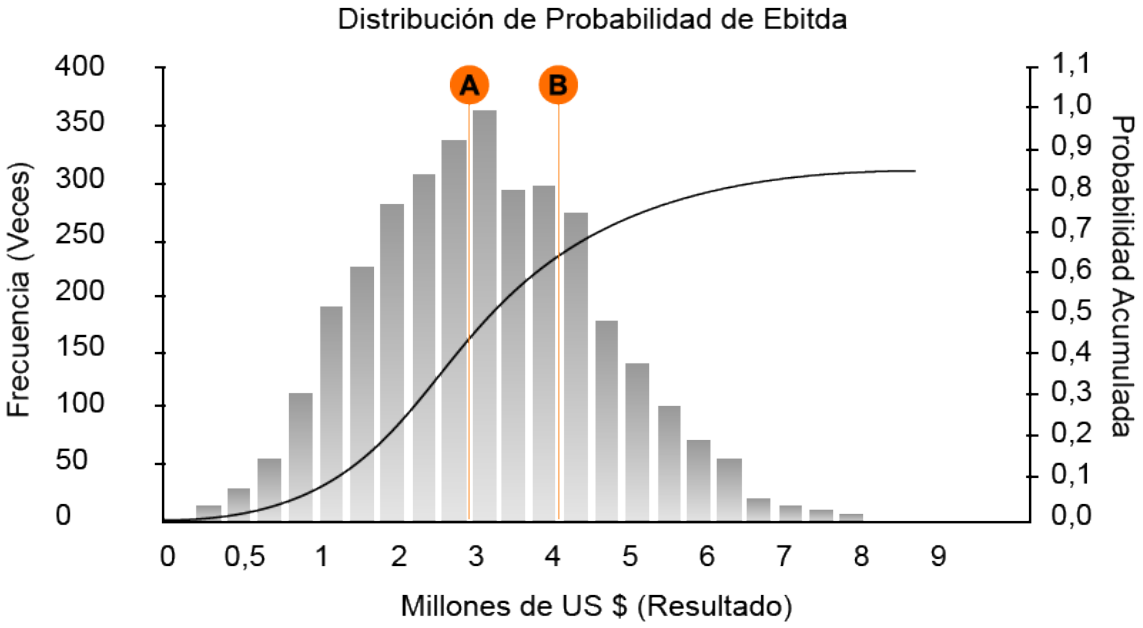
Fuente: WWW.OCEG.ORG – Curso de Fundamentos de GRC

Resolver este gran desafío se ha convertido en uno de los aspectos cruciales de la operación empresarial, por cuanto ha puesto en claro responsabilidades, funciones, información, organización, métodos y tecnologías comunes. Y es, a la postre, el principal desafío de GRC. La integración y orquestación del GRC requiere reconocer claramente el modelo de negocio, por cuanto en función de los derroteros y objetivos es que se pueden advertir los factores críticos y niveles de exposición que hacen posible la integración.

2.2 Desempeño: Logro de objetivos confiables.

Definición de objetivos estratégicos. Para comenzar por el desempeño, cualquier empresa establece sus objetivos aplicando algún indicador de valor, el cual se conforma a partir de las utilidades o ganancias generadas, tasas de crecimiento, nivel de costos operacionales, resultados por líneas de negocio, número de Ebitdas, indicadores compuestos de rentabilidad/financiamiento, o niveles de servicio, entre otros.

En todos los casos, es altamente probable que la organización disponga de la información base requerida para establecer los niveles alcanzables, las tolerancias y exposiciones del indicador de referencia, para construir una relación de probabilidad de riesgo/retorno donde debe establecer un resultado esperado en función de un nivel probabilístico de riesgo asumido, como el que se muestra a continuación.



En este caso, consideremos que una organización considera el Ebitda como su indicador de desempeño estratégico. Aplicando algunas técnicas de simulación sobre las variables base[4]: volumen de producción, costos variables, costos fijos y variables, la organización establece que con un nivel de probabilidad entre el 60% y el 80% se puede esperar un resultado que fluctúa entre el rango a-b, que implica resultados entre US $ 3 millones y US $ 4 millónes. Este será su rango de tolerancia.

"La gestión integral del Desempeño requiere la alineación e integración de los planes estratégicos con el modelo de operación."

Alineación de la estrategia con líneas y productos. El plan estratégico tendrá la función, en consecuencia, de segregar para cada línea de negocio y producto, los niveles de producción, operación y ventas requeridos. Este objetivo debe cumplir con las condiciones impuestas por el desempeño basado en principios; es decir, que es un objetivo intencional, medible y visible, y además de eso confiable, por cuanto, es razonable, veraz y verificable, en función de la dinámica

[4] Simulación de Montecarlo con variables objeto: Precio, Costo Variable, Costo Fijo, depreciación y volumen de producción. La variable resultado es la fórmula de cálculo del Ebitda. (Ganancia operacional más depreciación)

de la empresa y la capacidad productiva y operativa de sus procesos.

La identificación de este objetivo incorpora, necesariamente, el efecto de los factores externos e internos que introduce la incertidumbre, en un contexto particular. Los factores externos se refieren a condiciones de la industria, el mercado, las tecnologías, el ambiente normativo y fuerzas geopolíticas que pueden afectar la participación en el mercado, la competitividad y posicionamiento del producto, variables que, en la mayoría de los casos, están por fuera del control de la empresa. Así mismo, están los factores internos que, a diferencia de los anteriores, se subordinan y someten al control de la empresa. Estos tienen que ver con la estructura organizacional, los procesos de negocio, el capital humano, los recursos tecnológicos, financieros, físicos y de información que conforman la capacidad de operación de la entidad.

Pues bien, la alineación que requiere el desempeño, para intervenirse como una capacidad de GRC, es la necesidad de establecer como los factores internos considerados se incrustan en el modelo de operación, de manera que se tengan mecanismos accionables e inductores desde los procesos, la información, la cultura y el comportamiento, así como la tecnología y de los recursos disponibles.

Cualquiera sea la metodología aplicada – Balanced scorecard, Inteligencia de Negocios, Planeación estratégica-, la entidad debe alinear con las funciones y áreas de la estructura organizacional, los procesos misionales y operativos, la información y las tecnologías disponibles, la operación y capacidad de producción, ventas y financiación, de manera que metas operativas y tácticas respondan al objetivo estratégico establecido. Esto no será posible, si no se conocen y optimizan los procesos estratégicos y misionales. Así mismo, requiere métricas derivadas y alineadas con los procesos, la información y la tecnología basadas en variables objetivas y balanceadas, así como reportes objetivos que surgen de la operación.[5]

[5] The strategic Management Maturity Model. Balanced Scorecard Institute. Pags. 4 y 5. 2010.

2.2 Riesgo y Control: Evaluación de la Incertidumbre.

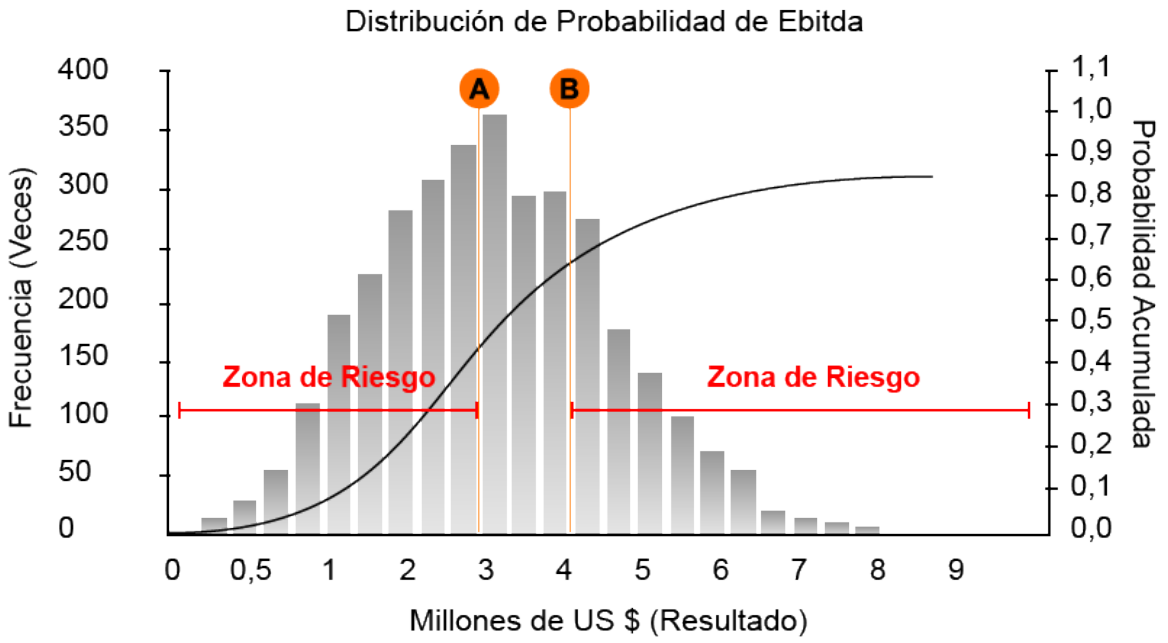
Identificación y alineación de los Riesgos estratégicos. La evaluación de la incertidumbre que enmarca el riesgo de las amenazas y el retorno de las oportunidades se desprende, justamente, de las variaciones que pueden presentarse, primero en el logro de los objetivos propuestos. Esto es el riesgo estratégico o del negocio que se refiere a una inadecuada estrategia de negocios para alcanzar o derivada de cambios adversos en los supuestos, parámetros, metas u otros aspectos que apoyan la estrategia. El riesgo estratégico es una función de los objetivos estratégicos, el desarrollo del modelo de negocio y los recursos desplegados para perseguirlos y alcanzarlos, y la calidad o eficiencia con la que se implementan tales recursos.[6]

"La gestión integral del riesgo requiere la determinación de los riesgos del negocio que se derivan de la estrategia y su alienación e integración con los riesgos operacionales y financieros de las líneas de negocios".

Para el caso del ejemplo, se estimaría la presencia de un riesgo estratégico cuando el Ebitda esperado, supera los niveles de probabilidad considerados entre el 60% y el 80%, de manera que la estrategia se empieza a separar del rango de tolerancia establecido, bien porque se disminuya a niveles no aceptables, a la izquierda de A, o a niveles inmanejables de ingresos, a la derecha de B.

En el primer caso, porque es evidente que se afecta la capacidad patrimonial por vía de los resultados operacionales, y en el segundo caso, porque se pueden estar generando circunstancias ajenas a los pronósticos relativos al máximo nivel de la capacidad de producción, a la disponibilidad de recurso humano, físico financiero para atender tal nivel de demanda, que afecte la sostenibilidad de largo plazo de la empresa.

[6] Operational RIsk – An Introduction. Tomada de www.fsiconnnet.org.



Los principios de evaluación de incertidumbre que refiere el concepto de desempeño basado en principios, incorpora las condiciones de una métrica holístico, es decir que debe incorporar circunstancias que pueden generar pérdidas o pueden generar beneficios, en tanto son desviaciones de resultados esperados. En este caso, por ejemplo, no sólo pueden ser malas las desviaciones adversas, sino también las desviaciones favorables que presionan el flujo ordinario, continuo y sostenible del negocio a excesos de la capacidad instalada.

Otro principio inherente a la evaluación de la incertidumbre es la proactividad, que significa buscar un resultado o beneficio esperado haciendo consciencia del riesgo asumido. En este caso, cuando la empresa estima alcanzar un rango de resultados esperados, admite un nivel probabilístico de confianza aceptable, y eso, al final del día, impone condiciones de capacidad productiva, financiera y de operación que la empresa debe sostener, generar y mantener.

Finalmente, la rigurosidad de la evaluación de la incertidumbre requiere establecer con absoluta precisión las causas y efectos para operar e inducir los resultados. Este principio confirma la necesidad de la alienación de la estrategia con los recursos y procesos del modelo de

operación, como bien se requiere para establecer el comportamiento del riesgo de negocio.

Es imperativo entonces, bajo GRC, la alineación de los objetivos estratégicos con los riesgos del negocio establecidos por las probabilidades de ocurrencia de factores internos y externos cuantificables y la severidad sobre los resultados esperados. Esta puede considerarse la primera alineación requerida.

Identificación y alineación con riesgos financieros y operacionales. No obstante, la efectividad del riesgo de negocio implicará operarse mediante un enfoque integral, de manera que debe alinearse con los procesos, funciones, líneas de negocios, roles y geografías, al igual que los objetivos, para que pueda integrarse con la misión y visión estratégica, mediante la evaluación del grado de exposición a la incertidumbre causada por potenciales desviaciones de los planes, presupuestos, recursos y operaciones.[7]

Se requiere, en consecuencia, una segunda alineación del riesgo del negocio estratégico, con otro tipo de riesgos financieros y no financieros que afectan la operación y sus resultados, y, en tal sentido, deben ser tomados en cuenta. Son riesgos financieros, el riesgo de liquidez y mercado, y riesgos no financieros, los riesgos operativos, en tanto se refieren a los procesos, recursos, tecnología e información del modelo de operación, para el cumplimiento de los objetivos.

Los riesgos financieros se ajustan a la situación de exposición de la tesorería, liquidez e inversiones financieras, al paso que los riesgos operativos se reconocen como los riesgos de pérdida que pueden resultar de fallas en los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos, en particular, incluyendo también las pérdidas que pueden resultar por incumplimientos, incorporadas bajo el riesgo legal.[8]

---

[7] Tomado de www.RIMS.org. Risk Maturity Model for Enterprise Risk Management.. Risk and Insurance Management Society. Pag.8

[8] El marco de Basilea, de aplicación para las entidades financieras, requiere los riesgos operativos se clasifiquen en categorías, como son el fraude interno, fraude externo, relaciones laborales, prácticas con clientes, productos y

Estos riesgos surgen del núcleo de la operación y sus factores son los procesos, la información, los recursos y la tecnología, en suma. Su estimación dependerá de información base para estimar probables pérdidas esperadas, a partir de modelos que tienen a ser más complejos, desde niveles cualitativos a bases cuantitativas que requieren la aplicación de bases de datos y modelos analíticos. En todo caso, desde el indicador más sencillo hasta el más complejo se hace precisa la categorización de los ingresos generados y, de manera particular, la clasificación de su origen por líneas de negocio: tipos de bancas, servicios y productos.

"La gestión del riesgo operacional requiere integración con las líneas de negocios, procesos, productos, información, tecnología y recursos involucrados."

La importancia de esta condición que impone el riesgo operacional, en el marco de GRC, es que hace imperativo nuevos requerimientos sobre la arquitectura de procesos, información, tecnología y recursos para objetivar y optimizar los resultados y la gestión del riesgo operacional, intención que debe acompañarse en los proyectos de optimización de procesos o de escalamiento de los objetivos estratégicos en el modelo de operación.

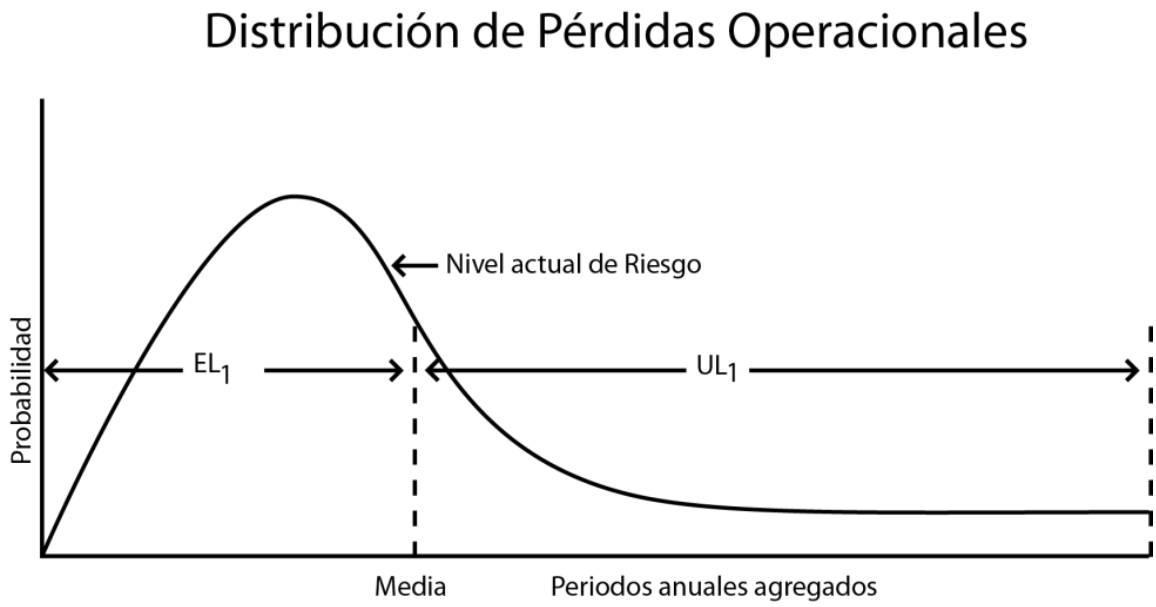
Los estándares de gestión de riesgo establecen, entonces, aspectos claves que el proceso debe considerar, entre los que se cita la necesidad de ser parte integral de la gestión, incorporarse en la cultura y las prácticas y adaptarse en los procesos de negocio de la empresa, para lo cual debe considerar fases de establecimiento de contexto, valoración y tratamiento del riesgo.[9] Esta valoración infiere la identificación, análisis y evaluación del riesgo. Las técnicas más comunes se refieren a la determinación de las fuentes, áreas y eventos de pérdida, así como sus causas y consecuencias, que permiten configurar probabilidades de

negocios, daños a activos materiales, incidencias en el negocio y fallos en los sistemas y ejecución de procesos. Comité de Basilea II. Operational Risk Management. BIS. Documento consultivo. (2001)

[9] ISO 31000 – Risk Management. Principles and guidelines. Numeral 5. Págs 16 a 17.

ocurrencia y niveles de severidad, en categorías y líneas de servicios y productos, como se comentó.

Evaluación de la efectividad del control. La gestión del riesgo implica advertir, en consecuencia, niveles de severidad y probabilidad de impactos de pérdidas esperadas, como se muestra en la gráfica siguiente.



La valoración permitirá identificar y establecer la probabilidad de ocurrencia de un evento de pérdida, dada todas las posibles frecuencias e impactos de severidad. Esto se hace posible mediante una matriz de probabilidades que pondera niveles de frecuencia o probabilidad de ocurrencia, con niveles de severidad o probabilidad de impacto. La curva explicaría que las pérdidas de alta frecuencia deben representar impactos de baja severidad y por contrario, las pérdidas de baja frecuencia son las que, seguramente, pueden potenciar impactos de gran severidad, en coherencia, justamente con la cola de la distribución.

La matriz, en suma, no es la estimación cualitativa de un evento posible individual, sino la estimación cuantitativa de un conjunto de eventos probables, y esto hace posible la generación de una curva con un nivel de pérdida esperada hasta la media relativa. En el caso de la curva de ejemplo es la línea identificada como EL1. Así mismo, hay un nivel de pérdidas que no sólo exceden el nivel máximo de una

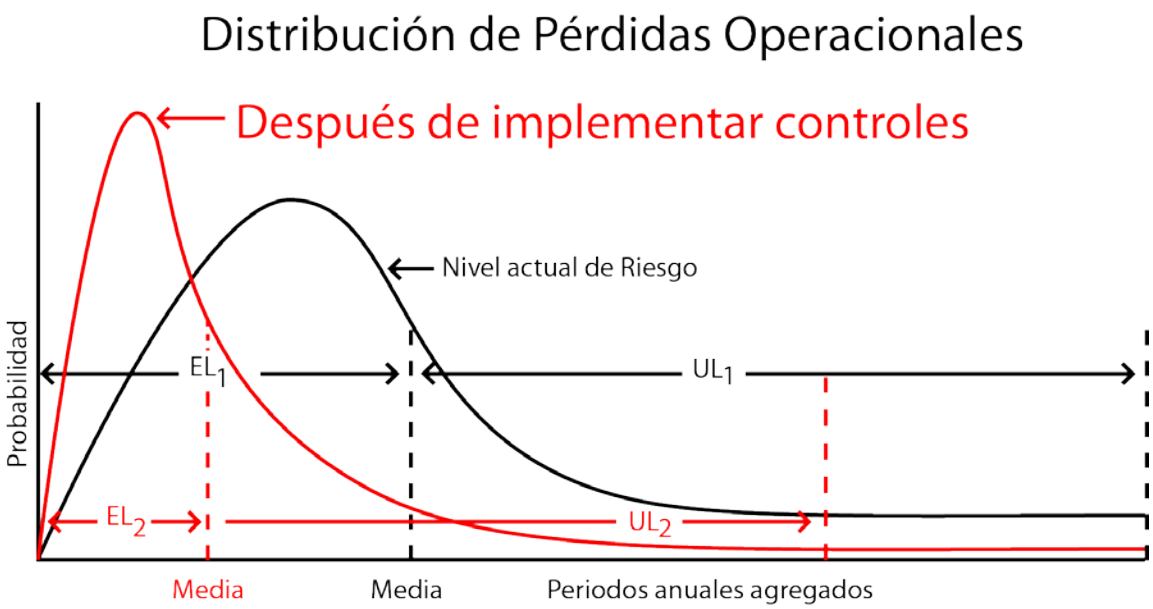
pérdida esperada, sino también representan pérdidas que exceden la tolerancia y la capacidad de sostenibilidad UL1.

La gestión de riesgos debe aportar elementos de tratamiento del riesgo en función de los niveles de pérdidas esperadas. Esto es, que en una línea de negocio si se exponen puntos de la curva que exceden los niveles de tolerancia, será preciso acudir a niveles de capitalización, seguros u operaciones de transferencia de riesgo con derivados. En todos estos casos, deben aplicarse planes de continuidad o contingencia operativa, por cuanto son riesgos generados por factores externos que están por fuera del control y la gestión corporativa. Así mismo, dentro de la curva de tolerancia, la entidad puede optar por la aplicación de controles que pueden representar una efectividad operacional, punto que se resolverá adelante, así como circunstancias donde no se hace preciso aplicar acciones de gestión.

La evaluación de la incertidumbre en el marco de GRC, como resumen, requerirá considerar, primero, si se trata de una desviación de los objetivos estratégicos que obedece a factores externos y puede ser tratada con algún mecanismo de cobertura o aseguramiento que requerirá de gestión. Si se trata de factores internos, debe contemplarse el efecto conjunto, a partir del análisis del riesgo operacional.

Las reflexiones en torno a las pérdidas esperadas del riesgo operacional, deben permitir, en igual sentido, establecer si hay riesgos que se generan por acontecimientos externos y pueden estar por fuera de la gestión organizacional, para tratarlos con planes de continuidad y coberturas. Si hay riesgos que se derivan por factores internos para la gestión de la empresa, la entidad tiene que establecer, primero, si los costos de la intervención de los controles reducen las pérdidas a niveles aceptables, en un contexto donde las pérdidas controladas exceden el costo de los controles.

Por último, si la entidad advierte que la intervención de los controles no reducen las pérdidas o éstas pueden ser inferiores a los controles, no resulta necesario ni pertinente aplicar control ninguno, distinto a mantener acciones de gestión de monitoreo e información. En el caso del ejemplo, la idea es que un control implementado tenga la capacidad de trasladar la curva de probabilidad a la izquierda, de manera que tiene la capacidad de reducir el nivel de pérdida esperada de EL1 a EL2.



Finalmente, lo que suele ocurrir en las empresas es que se aplican innumerables controles para preservar la disciplina, el comportamiento y la cultura directiva y operacional, pero la realidad es que técnicamente no deben llamarse controles sino acciones de gestión, por cuanto, nada tiene que ver, como se explicó con circunstancias de mitigación o reducción de riesgos. Esto es, justamente, una perspectiva del riesgo bajo un enfoque integrado de GRC.

Integración con el Control Interno. El control se entiende como "proceso" que debe aportar una garantía razonable sobre el logro de los objetivos relacionados con las operaciones, el reporte y el cumplimiento.[10] La razón por la cual se incorpora, en GRC, como un elemento de la dimensión del riesgo se explica porque el marco de control

[10] Control Interno – Marco Integrado. Committee of Sponsoring Organizations of the Treadway Commission. Resumen ejecutivo. Página 3. 2013.

establece que si bien el sistema es efectivo respecto a la consecución de los objetivos anotados, agrega que la efectividad se basa en reducir a un nivel aceptable el riego de no alcanzar un objetivo.[11]

"La efectividad del control interno se determina por su capacidad para reducir o mitigar los riegos operacionales".

Los objetivos de las operaciones hacen referencia a la efectividad y eficiencia de las operaciones, incluido sus objetivos de rentabilidad financiera y operacional, y la protección de los activos frente a las pérdidas.[12] Los riesgos inherentes a este objetivo deben ser valorados y gestionados por la dimensión del riesgo, incorporando los controles operativos necesarios. Así mismo, el objetivo de cumplimiento, como su nombre lo indica, se refiere a la garantía del cumplimiento de las normas. La premisa bajo GRC, en consecuencia, es si se advierten desviaciones de incumplimiento deben ser tratadas como riesgo legal y, en ese sentido, estarán, también, bajo la perspectiva de la dimensión del riesgo y control.

Así, los componentes de control que se componen por cinco componentes. El ambiente de control, la evaluación de riesgos y las actividades de control, son tres de los cinco componentes que se refiere al establecimiento de condiciones de gobierno para desarrollar el modelo de negocio y lograr los objetivos, se incorporan en la perspectiva del desempeño basada en principios. El componente de información se refiere, directamente a la perspectiva de la arquitectura de la información, que se relaciona en lo pertinente con los procesos, las aplicaciones y la tecnología, y en ese sentido deben ser objeto de evaluación de riesgos para establecer los controles efectivos.[13]

Finalmente, el componente de supervisión y monitoreo se relaciona con las dimensiones de aseguramiento que

[11] Control Interno - Marco Integrado. Resumen Ejecutivo. Página 8.
[12] Control Interno – Marco Integrado. COSO. Objetivos. Página 3. 2013.
[13] COSO. Control Interno. Marco Integrado. Componentes y Principios. Página 6.

establece la necesidad de considerar, además de la intervención del control, las evaluaciones independientes.

2.3 Cumplimiento: Actuación con Integridad.

Cumplimiento de normas obligatorias y de origen voluntario. El cumplimiento normativo se refiere a esa obligación de la empresa de garantizar el cumplimiento de las leyes y disposiciones externas, así como las políticas y directrices que una empresa adopta para el desarrollo de sus operaciones. Es esa una primera consideración. No obstante, también se incorpora la definición e implementación de códigos de comportamiento y ética, muchos de los cuales se potencian mediante bases, creencias y comportamientos culturales más que instructivos que se implementan en el modelo de operación.

"La gestión integral del cumplimiento requiere establecer niveles de conformidad de cumplimiento sobre normas obligatorias internas y externas, y alineación con el riesgo legal."

Bajo el cumplimiento deben incorporarse, en suma, todas las normas, políticas, directrices e instrucciones que una empresa decide adoptar, bien para operar, fortalecer el desempeño, gestionar el riesgo o aplicar protocolos de control.

El derrotero del cumplimiento se establece por niveles de conformidad y si bien, son obligaciones que se derivan de la certidumbre, no quiere decir que la organización no advierta potenciales incumplimientos que, de darse, se tratan como elementos probabilísticos del riesgo legal, y en tal caso se encaran como factores de riesgos: evaluación de la incertidumbre.

Alineación de Marcos de Referencia. El cumplimiento puede tener varios marcos de referencia que se refieren a la generación de reportes, trasparencia en relacionamientos con terceros, operaciones con vinculados y partes interesadas, regulaciones fiscales, comerciales y laborales.

De manera particular, el desempeño basado en principios establece, además del compromiso adquirido sobre los marcos obligatorios externos e internos, la necesidad de establecer mecanismos disciplinarios e intervenciones de gestión y control cuando un compromiso no es cumplido, por alguna razón.

El enfoque requiere que para cada marco normativo que debe ser objeto de cumplimiento se establezcan las dimensiones básicas y los atributos que deben ser cumplidos. Si se toma, por ejemplo, una norma como SOX que impone condiciones de reportes de las empresas que operan en USA, será preciso definir los tópicos claves que se deben perseguir, para encontrar que aspectos tales como las responsabilidades de la Junta de Directores, las revelaciones de la información, la operación e intervención de la Auditoría, las condiciones inherentes a la gestión del fraude y los conflictos de interés, son aspectos profundamente relevantes que deben hacer parte de una calificación de conformidad del cumplimiento.[14]

Estas responsabilidades y tareas de cumplimiento deben alinearse, también con elementos y dominios de la arquitectura como son los procesos de generación de reporte, las tecnologías de base transaccional, las funciones y responsabilidades inherentes a estos procesos de determinación y presentación de recursos y obligaciones, en función de las necesidades, objetivos y logros esperados.

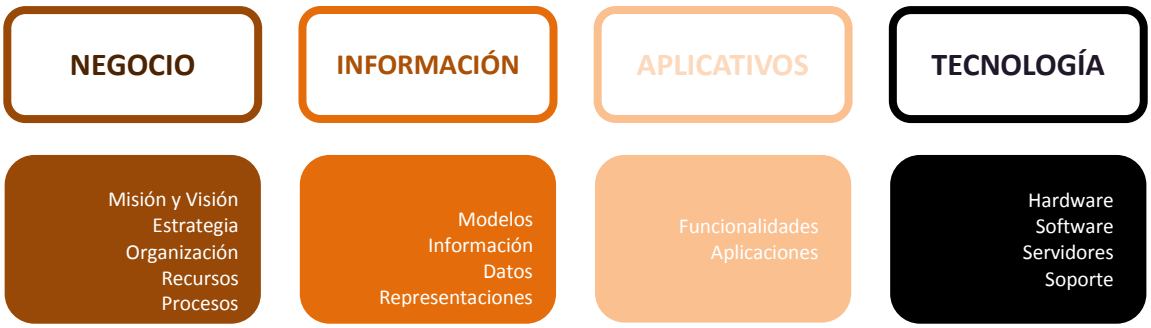
[14] Ley Sarbanex Oxley. Act of 2002. Estructura y Títulos.

Perspectiva de la Arquitectura Empresarial.

3.1 Bases Conceptuales.

Concepto. La arquitectura empresarial es otra perspectiva fundamental para GRC. La razón es que mientras las disciplinas: desempeño, riesgo y cumplimiento configuran el elemento abstracto del GRC, la arquitectura establece los objetos o elementos tangibles donde se materializan o implementan. Son varias las definiciones que pueden encontrarse sobre arquitectura empresarial; sin embargo, hay acuerdo en que representa el relacionamiento entre el conjunto de procesos, la organización, datos, sistemas informáticos, servicios, indicadores, y demás recursos empresariales, que se integran para hacer viable la operación del modelo de negocio. En otras palabras, la arquitectura empresarial hace posible la integración de la estrategia al modelo de operación.

El modelo de operación se reconoce como el nivel necesario de la integración y estandarización de los procesos de negocio para producir los bienes y servicios para los clientes. Un modelo de operación describe como una empresa desea prosperar y crecer mediante una perspectiva más estable y accionable que la estrategia, fundamentada en la ejecución.



Estos dominios, como se entienden en el leguaje de un estándar de arquitectura como TOGAF, se clasifican en cuatro tipos de arquitectura: la arquitectura de Negocio, la arquitectura de información y datos, la arquitectura de aplicaciones y la arquitectura de tecnología.

La arquitectura de Negocio incorpora la estrategia de negocio, la estructura organizacional y de gobierno y los procesos clave de la organización. La arquitectura de datos e información lo determinan la estructura de datos lógicos y físicos que posee una organización y sus recursos de gestión de datos. La arquitectura de aplicaciones se determina por las aplicaciones individuales, sus interacciones y relaciones con los procesos de negocio clave. Finalmente, la arquitectura de la tecnología son las capacidades de software y hardware que se requieren para apoyar la implementación de servicios de negocio, información y aplicaciones.[15]

Las arquitecturas son secuenciales, de manera que la arquitectura de negocio es un prerrequisito de los otros dominios de arquitectura. En igual sentido, la arquitectura de información es un paso fundamental para el desarrollo de las aplicaciones y de la tecnología.

3.2 Arquitectura del Negocio.

Alineación del desempeño basado en principios con la Arquitectura del negocio. Implementar los requerimientos del desempeño, como se mostró, para el logro de los objetivos, exige la precisión de la intención en objetivo, la configuración de la estructura organizacional y la alienación con los procesos para el establecimiento de metas tácticas en líneas de negocios, áreas, productos y geografías.

"La arquitectura empresarial representa el relacionamiento entre el conjunto de procesos, la organización, la información, las aplicaciones y tecnología que se integran para hacer viable el modelo de negocio"

Si bien la estrategia de negocio define que se debe lograr – los objetivos, las metas e indicadores, así como las métricas de logro y seguimiento, no está en capacidad de establecer cómo lograrlo, con la rigurosidad de un modelo de operación, y es ese, justamente, el rol de la arquitectura de negocio.

La arquitectura de negocio establece, en consecuencia, los requerimientos de funciones, asociadas con las actividades del negocio, la información que debe usada e

[15] TOGAF. Estándar The Open Group. Versión 9.1. Numeral 1.4. Página 24.

intercambiada entre actividades para responder a los requerimientos de los indicadores y metas, así como los aspectos de insumos, controles, resultados y recursos usados para la gestión del proceso.[16]

Se requerirá, entonces, de una gestión por procesos para que cumplan con su objetivo de transformación y de apoyo a la estrategia - BPM. La presión sobre los procesos en el marco de un enfoque integrado de GRC requiere, también, la incorporación de eventos de riesgo operacional, controles cuando se requiere, al igual que reglas o actividades para dar cumplimiento a instructivos normativos.

Se acoge así, en la base de procesos, consideraciones clave del desempeño, riesgo, control y cumplimiento, siendo esta la razón por la cual, la arquitectura de los procesos requiere de adecuados niveles de madurez en términos de su estructura, diseño, métricas, apoyo a la operación y alineación organizativa y funcional.[17]

[16] TOGAF. Framework. Numeral 8.2.3. Pag. 95.
[17] Niveles de madurez de procesos son el Process and Enterprise Maturity Model (PEMM™) de Michael Hammer y el de la Sofware Engineering Institute llamado Capability Maturity Model.

3.3 Arquitectura de información, Aplicaciones y Tecnología.

I**ntegración de la arquitectura de negocio con dominios de información, aplicaciones y tecnología.** Teniendo claro la arquitectura de negocios de manera que se conoce que áreas de la organización, líneas de negocio, funciones y procesos intervenir para el logro del desempeño basado en principios, así como la información y datos necesarios para perseguir las métricas y reportes necesarios, toma lugar la arquitectura de aplicaciones para identificar y definir lar principales aplicaciones que pueden ser requeridas para procesar los datos y soportar el modelo de negocios.[18]

El esfuerzo del dominio de arquitectura de aplicaciones no se relaciona con el diseño de las tecnologías, por cuanto no son propiamente sistemas computarizados sino funciones lógicas que resuelven requerimientos del negocio. Finalmente, la arquitectura de la tecnología busca mapear los componentes de las aplicaciones, representados en software o hardware para establecer que se debe adquirir o desarrollar en plataformas de tecnología, de suerte que define la realización física de soluciones funcionales.[19]

[18] The Open Group Architecture Forum. TOGAF. Framework. Numeral 11.1 Pag. 127.
[19] TOGAF. Framework. Numeral 12.1. Pag. 137.

Perspectiva del Enfoque de Aseguramiento.

4.1 Bases Conceptuales.

Concepto. El enfoque del aseguramiento resulta clave, en adición a las perspectivas vistas, para hacer posible que la alineación e integración requerida del desempeño basada en principios que se implementa en la arquitectura empresarial, cumpla las condiciones requeridas de separar las funciones de gobierno y gestión, y éstas a su vez, estén aseguradas bajo criterios de independencia.

4.2 Gobierno y Gestión.

Hablar de Gobierno no se limita al Gobierno Corporativo. En otras palabras, de una corporación - Conjunto de empresas controladas- es viable aplicar el término de control, pero el término de Gobierno se aplica también a sus partes, e incluso a todos y cada uno de los componentes de las perspectivas vistas. De otra forma, el gobierno corporativo que se conoce, a partir de varios principios y estándares[20], entre ellos los emitidos por OCDE, son, en efecto, intervenciones del Gobierno, pero no es la única presencia en la organización por cuanto bien se puede hablar del gobierno del riesgo, gobierno de los procesos o gobierno de la tecnología, como bien se incorpora en otras prácticas.

[20] Organización para la Cooperación y Desarrollo Económico- OCDE. Principios de Gobierno Corporativo.2004.

El Gobierno puede interpretarse como el acto de dirigir, controlar, evaluar y supervisar, de manera externa, una entidad, proceso, recurso, información o proyecto. Es una definición de carácter general que se aplica para aclarar que se trata de ese acto de orientar y supervisar pero no administra. De ahí, la reflexión de intervención externa.

"El Gobierno es una intervención externa de dirección, evaluación y control, al paso que la Gestión es una intervención interna y el Aseguramiento una intervención independiente".

Ahora bien, hablar de gobierno exige hablar de gestión. La gestión es la consecuencia de un acto de gobierno, por tanto se centrará en la ejecución y el logro de los objetivos trazados. La gestión se reconoce así, como el acto de dirigir, controlar, evaluar y supervisar, de manera interna, una entidad, proceso, recurso, información o proyecto. Esto quiere decir que el que gobierna traza la orientación, identifica y aprueba una directriz, asignando, de ser preciso, los recursos necesarios.

La gestión, por su parte, administra los recursos, cumple con los compromisos y rinde cuentas. La gestión tiene, en efecto, marcos de referencia independientes que establecen los principios, atributos y grados de madurez que se requiere para optimización y garantía de niveles de calidad[21].

Es fundamental en GRC, por decir lo menos, garantizar la separación de las funciones de gobierno y de gestión.

4.3 Aseguramiento.

La integridad del gobierno, la gestión y el control requiere de aseguramiento. Este aseguramiento es un acto de evaluación objetiva de un proceso, recurso, entidad, información o proyecto. El aseguramiento es una prenda de garantía para el acto de gobierno, de retroalimentación para el acto de gestión y de apoyo para el acto de control. Así, se reconoce como una evaluación objetiva e

[21] Norma ISO 9001.

independiente. El aseguramiento puede ser ejecutado por los auditores mediante evaluaciones independientes, pero se centra es en un pronunciamiento independiente sobre los resultados frente a criterios definidos, aplicado criterios y estándares objetivos.

El modelo de las tres líneas de defensa[22] es un elemento clave para distinguir como se integra el aseguramiento. La filosofía es que la empresa gobierna sus políticas mediante estrategias que se implementan y gestionan en la arquitectura empresarial – modelo de operación-, lo cual requiere considerar los riesgos asumidos y advertir los marcos normativos, internos y externos, que deben ser objeto de cumplimiento. Sin embargo, es importante definir, en este contexto, cómo se relacionan los actos de gestión y de control, de manera que no implique redundancias en las salvaguardas y más aún, como interviene la auditoría interna, de manera que agregue valor y no termine aplicando acciones ajenas a la integración requerida por GRC.

La primera línea de defensa se reconoce en este modelo como la gestión operativa, La gestión operativa, en un marco de GRC, es una parte de la función de gestión que se relaciona con la gestión del control y tiene que ver con la implementación de las políticas y procedimientos que sean

[22] IIA Declaración de Posición. Las Tres líneas de defensa para una efectiva gestión de riesgos y control. THEIIA. (2013)

requeridos, por efectividad como se vio, para detectar o mitigar los riesgos. Esto quiere significar que, en términos operativos tendrán el deben de establecer e informar también sobre exposiciones operativas de riesgo en los procesos, información y tecnología.

La segunda línea de defensa se refiere al gobierno y gestión –directiva- del riesgo, el cumplimiento y el control, para orientar y facilitar la implementación de prácticas efectivas por la operación. Bajo esta línea se potencia la administración de las políticas de riesgo, la definición de los roles y funciones requeridos, la efectividad de los controles y eficacia del cumplimiento normativo.

"La Auditoría Interna es la tercera línea de defensa que hace parte del aseguramiento."

La tercera línea de defensa se reconoce como la auditoría interna y, es una manifestación del aseguramiento independiente. La auditoría interna conforme con sus estándares debe cumplir con responsabilidades de la eficiencia y efectividad de las operaciones, salvaguarda de activos, confiabilidad de los procesos de reporte y cumplimiento de las normas.[23]

Cabe advertir que, en el marco de GRC, el aseguramiento también se brinda por los auditores externos, quienes tienen, por supuesto, claras responsabilidades reguladas para el aseguramiento de los reportes externos, tarea que en igualdad de condiciones funcionales aporta valor en materia del gobierno y la gestión de las transacciones, procesos y generación de reportes financieros.

[23] Estándares Internacionales de Auditoría Interna. Normas sobre Desempeño. Numeral 2100. Página 13. 2012

Perspectiva del Alcance Organizacional.

5.1 Bases Conceptuales.

Concepto. El alcance organizacional pretende precisar que un proyecto de GRC puede ser acometido desde la corporación, de suerte que se orienta al Gobierno, la gestión y aseguramiento de un grupo de empresas, pero también para una entidad, área departamento o proyecto, o para alguna de las dimensiones, componentes y perspectivas.

"El Alcance Organizacional implica que un Proyecto de GRC puede aplicarse a nivel de la Corporación, la Entidad, un Departamento, un Área, un proceso, o una Función: Desempeño, Riesgo, Control o Cumplimiento."

Esto quiere decir, que si el alcance es a nivel corporativo para atender requerimientos del gobierno "corporativo", se esperaría que los demás componentes del aseguramiento: gestión y aseguramiento, así como de los componentes de las perspectivas del desempeño basado en principios: desempeño, riesgo y cumplimiento, y de los componentes de la arquitectura empresarial: negocio, información, aplicaciones y tecnología, deben ser tratados, también a nivel corporativo.

5.2 Proyectos de GRC.

Desde la perspectiva práctica, el enfoque de un proyecto de GRC, puede ser acometido para:

a. Una entidad, área o departamento.
b. Una dimensión o componente de la perspectiva de arquitectura empresarial: la estrategia, los procesos, la información, aplicación o tecnología.
c. Una dimensión o componente de la perspectiva del desempeño basado en principios: desempeño, riesgo, control o cumplimiento.

d. Una dimensión o componente de la perspectiva del enfoque de aseguramiento: gobierno, gestión o aseguramiento.
e. Una combinación de dimensiones o componentes de varias perspectivas. Esto es: Gobierno del Riesgo; Gobierno de la Tecnología; Gestión del cumplimiento; Aseguramiento del desempeño; Gestión del control de los procesos; Gestión del cumplimiento de reportes e información.

La organización debe establecer niveles de madurez para establecer, desde el punto de vista crítico, cuáles y en qué orden pueden ejecutarse proyectos que tengan la capacidad de agregar valor, en condiciones de costo, beneficio e impacto.

Conclusiones.

GRC más que un acrónimo que significa Gobierno, Riesgo y Cumplimiento es la capacidad de una organización para gobernar, gestionar y asegurar el desempeño basado en principios, a partir de la optimización de los dominios de la arquitectura empresarial, ejecutada con base en circunstancias de mejoramiento continuo para el logro de adecuados niveles de madurez.

"GRC es la capacidad de gobernar, gestionar y asegurar el desempeño, riesgo, control y cumplimiento en los dominios de la arquitectura empresarial".

El desempeño basado en principios es un concepto que implica el logro de objetivos confiables, abordando la incertidumbre y actuando con integridad. Así mismo, los dominios de la arquitectura empresarial son el negocio: estrategia, organización y procesos, la información, aplicaciones y tecnología.

Bibliografía

OCEG. Open Compliance and ethics Group. Red Book. Modelo de Capacidad. www.OCEG. ORG. (2012)

BSCI. The Balanced Scorecard Institute. The strategic Management Maturity Model. (2010).

BIS. Bank for International Settlements. Financial Stability Institute. "An Operational RIsk – An Introduction. www.fsiconnnet.org. (2005).

RIMS. Risk and Insurance Management Society. Risk Maturity Model for Enterprise Risk Management. www.RIMS.org. (2014).

BIS. Bank for International Settlements. Operational Risk Management. Documento consultivo. (2001)

ISO. International Organization for Standardization. ISO 31000. Risk Management. Principles and guidelines. (2014).

ISO. International Organization for Standardization. Nueva ISO 9001. Gestión de Calidad. (2015).

COSO. Committee of Sponsoring Organizations of the Treadway Commission. Resumen ejecutivo. Marco Integrado. (2013).

Sarbanex Oxley. Act of 2002. Estructura y Títulos.

TOGAF. The Open Group Architecture Forum. Framework. Versión 9.1. (2009).

OCDE. Organización para la Cooperación y Desarrollo Económico- OCDE. Principios de Gobierno Corporativo. (2004).

THEIIA. Instituto Internacional de Auditores. A Declaración de Posición. Las Tres líneas de defensa para una efectiva gestión de riesgos y control. (2013)

THEIIA. Instituto Internacional de Auditores. Estándares Internacionales de Auditoría Interna. (2012).