



# Visión, estrategia y estructura

Optimizando  
los programas de  
Gobernabilidad,  
Riesgo y Cumplimiento



Las interrupciones empresariales, el ritmo rápido del cambio y un entorno regulatorio cada vez más estricto han avivado el debate sobre la unión e integración de las funciones de gobernabilidad, Riesgo y Cumplimiento. ¿El GRC integrado es imperativo o simplemente un buen programa que se debe tener? Para muchas organizaciones ha sido una tarea ardua y costosa, debido a un gran número de razones como la falta de una estrategia, falta de respaldo de la gerencia, implementaciones de tecnología fallidas, una gestión de cambio deficiente y una falta de relación entre el resultado del programa y las expectativas de los accionistas. Cualquiera que sea la causa, las organizaciones necesitan comprender que es posible desarrollar un programa de GRC altamente exitoso y que genere un retorno positivo de la inversión, siempre y cuando se adopten buenas prácticas. En este informe introductorio, se explica cómo podemos maximizar el valor de una inversión para GRC, enfocándonos en la importancia de establecer una estructura de visión, estrategia y estructura del programa de GRC.

**Es posible desarrollar un programa de GRC exitoso con un retorno positivo de la inversión, siempre y cuando se adopten ciertas buenas prácticas.**

## Ciclo de vida del proyecto GRC de KPMG:



### 1 Visión y Estrategia

- Visión y Estrategia de GRC
- Principios base
- Factores críticos para el éxito
- Compromiso de la gerencia
- Modelo de gobernabilidad
- Compromiso funcional
- Plan de trabajo

### 2 Elementos para el establecimiento y convergencia

- Elementos para el establecimiento. Comunicación entre las áreas funcionales de GRC y las áreas de aseguramiento
- Evaluar la madurez del área funcional de GRC
- Estado futuro del flujo de procesos
- Oportunidades de convergencia, unión de funcionalidades compartidas y los puntos de integración de la tecnología de GRC
- Definición de los requerimientos de negocio, funcionales y técnicos de alto nivel.

### 3 Gestión de programas

- Administración del proyecto
- Caso de negocios de GRC
- Planificación del proyecto, incluyendo planes detallados para cada fase de implementación
- Gestión de presupuesto
- Gestión de alcance
- Gestión de riesgo
- Seguimiento de debilidades
- Administración de recursos y gastos del proyecto
- Plan de monitoreo y entrega de informes del proyecto.

### 4 Gente y cambio

- Análisis de los accionistas
- Cargos y responsabilidades
- Plan de comunicaciones
- Aprendizaje, desarrollo y entrenamiento
- Adopción del plan de acción.

### 5 Selección del proveedor

- Desarrollo del caso de negocio de GRC
- Análisis de Compra vs Desarrollo (Buy vs. Build)
- Selección de herramientas
- Demostraciones de los proveedores, evaluación de conceptos y resultados de la solicitud de propuesta (RFP por sus siglas en inglés).

### 6 Habilitación de la tecnología

- Matriz de análisis de coincidencias y diferencias y/o de seguimiento. Determinar los requisitos tecnológicos de acuerdo con la complejidad específica
- Selección del enfoque de implementación y del plan detallado del proyecto
- Prueba del concepto
- Conversión de información
- Configuración del sistema
- Estrategia de evaluación, desempeño y aceptación del usuario
- Implementación de una lista de actividades pendientes.

# UNA VISIÓN PARA GRC

Un programa firme para la gestión de riesgo y cumplimiento requiere de una visión sobre qué conseguirá la organización con un nuevo diseño de programa de GRC; en otras palabras, cómo se determinará el éxito de dicho programa. Se debe responder a las necesidades del negocio y crear una alianza estratégica entre todos los objetivos generales de la organización.

Si los objetivos estratégicos de la organización y las metas del programa de GRC no se mueven a la par, éste no podrá generar los beneficios esperados y podría llevar a un impacto perjudicial en las capacidades de gestión de riesgo de la organización. La importancia de un programa de GRC efectivo recae sobre un enfoque integrado de control y riesgo junto con una línea de comunicación efectiva y oportuna de la información de riesgo para los encargados de la toma de decisiones. Existen muchos componentes clave para lograr que esto suceda, incluyendo taxonomías de negocio consistentes, administración del programa, procesos disciplinarios y que siempre se diseñen los programas teniendo el objetivo en mente.

La administración necesita comprender cuándo los límites de los riesgos son alcanzados, cuándo surgen nuevos riesgos y qué tanto riesgo es aceptable para alcanzar los objetivos. Esto requiere un enfoque integrado, en donde la administración de control y riesgo trabajen en conjunto compartiendo información y al mismo tiempo sigan cumpliendo sus instrucciones originales. Esto es un gran cambio para muchas organizaciones. Los departamentos de riesgo son más efectivos si comparten información y siguen un proceso consistente que les permita identificar los riesgos y oportunidades a la misma velocidad en la que ocurren los cambios en el mercado, y se crean las expectativas de los accionistas.

**La importancia de un programa de GRC no es evidente hasta que el negocio no impulse una visión de gestión de riesgos y cumplimiento compartida.**

Por lo tanto, para poder crear una visión se requiere que se identifiquen a los accionistas que se quiere que participen o contribuyan con el programa de GRC. ¿Cuáles son las expectativas, preocupaciones y necesidades de negocio que se necesita que sean consideradas? Si bien es cierto que la Junta Directiva tiene la responsabilidad de supervisar la gestión de riesgo de la empresa, existe un amplio rango de accionistas internos y externos que tienen un ávido interés en el desarrollo de este programa. Aunque no todos los accionistas se incorporaran foralmente al proceso, es de vital importancia que sus expectativas sean consideradas.

Convertir las necesidades de los accionistas en un plan de acción requiere de una visión que pueda ofrecer una dirección para el programa de GRC y que establezca el tono para la gestión de riesgo, y pueda guiar las actividades de cumplimiento a toda la empresa. La visión, en concordancia con los objetivos generales de la organización, debe ser entendible y asequible, y debe contener un conjunto de principios guía que se desarrollaran durante la ejecución del programa. Estos principios definirán cómo los departamentos de riesgo, cumplimiento y seguridad trabajarán en conjunto, rompiendo barreras para incrementar el valor de la empresa. Estos principios motivarán a los dueños de negocios para que busquen fuera de su esfera de control y se enfoquen para diseñar un programa de GRC estratégico y proactiva.

## Ejemplo de los principios de orientación



# Estrategia y Plan de trabajo



Una vez que la visión sea establecida y se les dé prioridad a las necesidades de los accionistas, entonces el equipo del proyecto desarrollará una **estrategia** para el programa de GRC que describirá los cambios que serán implementados y los efectos deseados para las operaciones de la organización.

Es de vital importancia cumplir con los principios de orientación establecidos con anterioridad en el programa. Como esta iniciativa atraviesa por varias de las funciones de los departamentos de control y riesgo, puede resultar desafiante llegar a un acuerdo entre las actividades necesarias para poder integrar satisfactoriamente la información de riesgo con los diferentes departamentos. Adicionalmente, se necesitará llegar a un acuerdo sobre la iniciativa; por lo tanto, es buena idea comenzar pronto.

Otro componente clave para la estrategia de un programa de GRC fuerte es el diseño y la creación de un plan de trabajo de alto nivel donde se muestre cómo alcanzar los objetivos planteados en la visión y la velocidad a la cual la empresa desea llegar. La escala de tiempo de un programa de GRC no es controlada sólo por la misma organización, también pueden existir impulsores regulatorios. Idealmente, el plan de trabajo de alto nivel debe ser manejado mediante un análisis de madurez de las funciones que van a ser habilitadas gracias a la tecnología GRC. Un factor crítico para el éxito es sólo habilitar los procesos completados.

Dichas funciones de control y riesgo que necesitan ser completadas serán puestas luego en el cronograma para permitir que tengan el tiempo para definir la operatividad a futuro.

También existen una cantidad de elementos fundacionales a los cuales se les debe dar prioridad y deben ser puestos al principio del cronograma. Por definición, estos son los elementos de la tecnología o de procesos comunes de los cuales todos los departamentos van a depender e incluyen la definición de una taxonomía común, bibliotecas comunes de control y riesgo, así como gestión de problemas. Adicionalmente, es frecuente que el proveedor de tecnología de GRC no haya sido seleccionado, por lo tanto la sincronización y las actividades relacionadas con la selección del proveedor tienen que estar incluidas en la planificación. Qué tan asertivamente la organización adopte e integre los cambios es la última consideración que se debe tener antes de culminar el diseño del plan de trabajo de alto nivel. Es por esto, que el plan de alto nivel debe establecer una visión, incorporar las expectativas de los accionistas y considerar el estado de las funciones que serán habilitadas, y la velocidad a la que se implementarán. Asimismo, se deben tomar en consideración los resultados rápidos (quick wins) para evidenciar el progreso y dar un impulso positivo. Esto no es una tarea fácil, pero es de vital importancia para poder permitir la accesibilidad al programar, facilitar la comunicación y presupuestar efectivamente.

## Ejemplo de un plan de trabajo de alto nivel de estrategia, visión y gobernabilidad

	Q2-2015	Q3-2015	Q4-2015	Q1-2016	Q2-2016	Q3-2016	Q4-2016
<b>Estrategia</b>	Crear/Aprobar/Socializar						
<b>Estrategia</b>	Definir/Crear y Confirmar						
<b>PMO</b>	Preparación	Apoyo continuo y Coordinación de PMO					
<b>Comunicaciones y Entrenamiento</b>	Preparación	Comunicación Continua (información actualizada) Diseño, Implementación y Resultados del Entrenamiento					
<b>Paso 1 IA&amp;SOX</b>	Futuro del Estado de la Funcionalidad	Preparación Entrenamiento	Prueba Extensión SOX				
	Futuro del Estado de la Funcionalidad		Preparación Entrenamiento	Prueba Extensión IA			
<b>Paso 2 ERM&amp;BCM</b>				Requerimientos del negocio Entrenamiento	Prueba Extensión ERM		
					Requerimientos del negocio Entrenamiento	Prueba Extensión BCM	
<b>Paso 3 ISC&amp;Cumplimiento Legal</b>						Requerimientos del negocio Entrenamiento	Prueba Extensión ICS
							Requerimientos del negocio Entrenamiento
							Prueba Extensión cumplimiento legal

# Estructura de la administración



**Una iniciativa de GRC debe ser vista como un programa y no un proyecto. Adicionalmente de crear una visión, una estrategia y un plan de trabajo de alto nivel, debe haber una estructura de gobernabilidad creada para el programa de GRC.**

Esto es esencial. Un alto ejecutivo, por ejemplo el Gerente de Riesgo, debe ser asignado para que supervise el programa y garantice que cumpla con la visión, permitiendo que el programa supere cualquier obstáculo significativo en el proceso hasta su culminación. En el tope de la pirámide organizativa debe estar un comité directivo conformado por los ejecutivos de alto nivel de todos los departamentos de control y riesgo que estén participando; y ellos se reunirán frecuentemente para formar un equipo que impulse el flujo de trabajo y genere productos y formatos de trabajo. Es importante incluir una variada representación por parte de la gerencia de los departamentos de riesgo y cumplimiento para poder implementar un programa de GRC exitoso, con la finalidad de ayudar a garantizar la eficiencia y ganancias máximas de dicho programa.

Crear un programa de GRC nuevo es un proceso complejo que involucra a muchas partes móviles y una amplia gama de departamentos corporativos. Un plan de proyecto es un componente crucial para la implementación; así como también, es necesario tener las funciones y responsabilidades claramente detallados para poder presentar una rendición de cuentas en todos los grupos de accionistas.

Adicionalmente, se considera que los programas de GRC son de transformación.

Una implementación efectiva normalmente incluye cambios significativos en la forma en que la gente realiza sus trabajos. Muchos accionistas estarán renuentes al cambio, por lo tanto un proceso de GRC exitoso empieza con la evaluación de las necesidades de los accionistas, seguido por el compromiso de los accionistas seleccionados y luego por una gestión de las expectativas de los accionistas. Este enfoque promueve un entendimiento general acerca de los cambios necesarios, de que los accionistas son una parte vital del proceso de cambio y de que estos pueden adoptar los cambios en su trabajo diario.

Un programa de GRC exitoso no sólo mejorará la forma en la que la organización gestiona sus departamentos de riesgo y cumplimiento, sino también las operaciones de negocio. Una organización con una buena cultura de riesgo y cumplimiento podrá resistir los impactos externos y prepararse ante las amenazas a sus operaciones y estrategias. Las oportunidades de negocios, riesgo y cumplimiento son tres facetas de una empresa sólida.



**Un programa de GRC exitoso no sólo mejorará la gerencia de riesgo y cumplimiento de la organización; también debería mejorar las operaciones del negocio.**

## Contáctenos

José O. Rodrigues  
Socio de servicios de Auditoría Interna  
y Cumplimiento Regulatorio  
T: +58 (212) 277 78 89  
E: jrodrigues@kpmg.com

Ivan A. Briceño  
Socio de servicios de Auditoría Interna,  
Cumplimiento Regulatorio y Servicios Forenses  
T: +58 (212) 277 41 39  
E: ibriceno@kpmg.com

 kpmgvenezuela@kpmg.com

 kpmg.com/ve

 @KPMG\_VE

 KPMG en Venezuela

 KPMGVenezuela

 KPMG Venezuela

### Caracas

Avenida Francisco de Miranda, Torre  
KPMG, Chacao, Caracas, estado  
Miranda, Venezuela.  
Telfs.: 58 (212) 277.78.11  
Fax: 58 (212) 263.63.50

### Puerto La Cruz

Centro Comercial Plaza Mayor,  
Edificio 6, nivel 2, Ofic. 6C-254  
Complejo Turístico El Morro,  
Municipio Urbaneja, Puerto La Cruz,  
estado Anzoátegui, Venezuela.  
Telfs.: 58 (281) 282.08.33 / 01.33

### Barquisimeto

Multicentro Empresarial Crystal Plaza,  
entre Av. Terepaima y prolongación  
Av. Los Leones vía Urbanización El  
Pedregal, PH-A,  
Barquisimeto, estado Lara, Venezuela.  
Telfs.: 58 (251) 267.65.66  
Fax: 58 (251) 267.55.74

### Puerto Ordaz

Centro Comercial Orinokia Mall,  
nivel Titanio. piso 1, Ofic. 1,  
Av. Guayana, Alta Vista, Puerto  
Ordaz, estado Bolívar, Venezuela.  
Telfs.: 58 (286) 962.42.87 / 7460  
Fax: 58 (286) 962.67.94

### Maracaibo

Torre Financiera BOD, piso 5,  
calle 77 / Av. 5 de Julio,  
entre Av. 3C y 3D, Maracaibo,  
estado Zulia, Venezuela.  
Telfs.: 58 (261) 793.47.80 / 49.33  
Fax: 58 (261) 793.45.75

### Valencia

Torre B.O.D., piso 5, Urbanización  
San José de Tarbes, Parroquia San  
José, Valencia,  
estado Carabobo, Venezuela.  
Telfs.: 58 (241) 823.50.25 / 74.60  
Fax: 58 (241) 823.95.35