19

Instituto Brasileño de Gobierno Corporativo

Cuadernos de Gobierno Corporativo

Gestión de Riesgos Corporativos

Evolución en Gobierno y Estrategia

IBGC | Instituto Brasileiro de Governança Corporativa

Gestión de Riesgos Corporativos

Evolución en Gobierno y Estrategia

IBGC | Instituto Brasileiro de Governança Corporativa

2020

2020 © IBGC

Instituto Brasileño de Gobierno Corporativo

Fundado el 27 de noviembre de 1995, el Instituto Brasileño de Gobierno Corporativo (IBGC), organización de la sociedad civil, es referencia nacional y una de las principales referencias en el mundo sobre gobierno corporativo. Su objetivo es generar y diseminar conocimiento al respecto de las mejores prácticas en gobierno corporativo e influenciar a los más diversos agentes en su adopción, contribuyendo para el desempeño sostenible de las organizaciones y, consecuentemente, para una mejor sociedad.

Junta Directiva

Presidente: Henrique Luz

Miembros de la junta: Armando de Azevedo Henriques, Carlos Eduardo Lessa Brandão, Claudia Elisa Soares, Gabriela Baumgart, Lêda Aparecida Patricio Novais, Israel Aron Zylberman, Leila Abraham Loria, Leonardo Wengrover

Alta Dirección

Directores: Pedro Melo, Adriane de Almeida, Reginaldo Ricioli, Valeria Café

Para mayores informaciones sobre el Instituto Brasileño de Gobierno Corporativo, visite la página web: www.ibgc.org.br. Para asociarse al IBGC llame al: +55 (11) 3185.4200.

Producción de la publicación traducida. Traducción: Carolina Osorio Agudelo; Corrección de estilo y pruebas: Camila Cristina da Silva; Soporte de back-office: William Barros A. de Melo; Producción editorial y portada: Kato Editorial; Costos de traducción: BID Invest.

Datos de catalogación de publicaciones internacionales (CIP) según ISBD

G393 Gestión de riesgos corporativos: evolución en gobierno corporativo y estrategia / organizado por Instituto Brasileiro de Governança Corporativa – IBGC ; traducido por Carolina Osorio Agudelo. – São Paulo, SP : Instituto Brasileiro de Governança Corporativa – IBGC, 2017.
66 p. ; 18cm x 25,5cm. – (Serie de Cuadernos de Gobierno Corporativo, 19).

ISBN: 978-65-86366-24-2

1. Gobierno Corporativo. 2. Junta Directiva. 3. Riesgo. 4. Gestión. I. Instituto Brasileiro de Governança Corporativa – IBGC. II. Agudelo, Carolina Osorio. III. Título. IV. Serie.

CDD 658.4
2020-2760 CDU 658.114

Preparado por Vagner Rodolfo da Silva – CRB-8/9410

Índice para el catálogo sistemático:
1. Gobierno corporativo 658.4
2. Gobierno corporativo 658.114

Créditos

Esta publicación es el resultado del proyecto desarrollado y ejecutado por la Comisión de Gestión de Riesgos Corporativos del IBGC. Su contenido no refleja, necesariamente, las opiniones individuales de aquellos que participaron de su elaboración, y si el entendimiento del instituto. Durante su elaboración, este documento pasó por un intenso proceso de debates internos y audiencia pública, recibiendo diversas contribuciones y sugerencias.

Coordinación General

Mercedes Marina Stinco.

Coordinación de los Grupos Redactores y de Revisión

Alex Lelis Buzato Borges, Érico Torres, Luciana Bacci, Ricardo Lemos y Roberto Lamb.

Miembros de la Comisión

Alberto Whitaker, Alberto Yamandú Messano Colucci, Alessandra Silva de Jesus Artifon, Alex Lelis Buzato Borges, André Coutinho, André Echeverria, André Vitoria, Antônio Cocurullo, Antonio Edson Maciel dos Santos, Antônio Lemos, Antonio M. F. Ribeiro, Arnaldo Bonoldi Dutra, Carlos Sá, Clara R. F. Biscar, Clovis Corrêa da Costa, Érico Torres, Erlon Lisboa de Jesus, Fábio Coimbra, Fábio Mendes, Fernando Nicolau Freitas Ferreira, Flavio Abrão, Francisco Carlos Fernandes, Frederico de Campos Ventriglia, Ivana Regina Galvão Leite, Ives Pereira Müller, João Francisco Arcoverde Lopez, Leandro Pavão, Leonardo Machado, Lucia Casasanta, Luciana Bacci, Marcelo Lerch Hoffmann, Marco Antonio Bueno, Marcos Lorençani, Marcus Lanzelotti, Maria Paula Aranha, Marilza Benevides, Mario Augusto Filipini, Mercedes Marina Stinco (coord.), Mirian Paula Ferreira Rodrigues, Paulo Baraldi, Pedro Antônio Maziero, Rainer Lutke, Ricardo Aparecido dos Santos, Ricardo Lemos, Ricardo Roschel, Roberto Lamb, Roberto Sobral Hollander, Sandra Cristina Bernardo, Silvio Valdrighi y Tatiana Leite.

Contribuciones y Agradecimientos Especiales

Al equipo del IBGC, por el apoyo a la comisión y por las contribuciones al documento.

A Lucas Legnare y Luciana Del Caro, por el soporte en el proceso de redacción del cuaderno.

A Carlos Eduardo Lessa Brandão, José Luiz Bichuetti y Sergio Moreno, por los comentarios y por la participación en banca que evaluó la publicación.

A Annibal Ribeiro Lima, Camila Sardenberg, Cida Hess, Clara Regina Ferrão Biscar, Edina Biava, José Martins, José Ricardo De Moraes Pinto, Leila de Oliveira Lopes Rega, Leonardo Viegas, Luiz Alberto de Castro Falleiros, Luiz Athayde, Maurício Loures Rodrigues, Roberta Simonetti, Tatiana de Oliveira Leite y Thomas Brull, por la participación en foro restringido que debatió el contenido del documento.

A Alexandre de Oliveira, Carlos Antonio Vergara Cammas, Diego Silveira Maciel, Felipe A. F. Gomes, Isabella Saboya, Sergio Mastrangelo Ferreira, Vladimir Barcellos Bidniuk y William Borges Lima, por las contribuciones enviadas a lo largo del proceso de audiencia pública.

A Francisco Fernandes, João Francisco Arcoverde Lopez, Maria Paula Aranha, Marilza Benevides y Silvio Valdrighi por las contribuciones generadas en la producción de los textos.

A Ricardo Lemos, por la consolidación y revisión de las diversas versiones generadas por los grupos redactores.

A Roberto Lamb, por la invaluable y relevante contribución a lo largo de todas las etapas de construcción del cuaderno, convirtiendo el texto lo más rico y actual posible.

ACERCA DE BID INVEST:

BID Invest, la institución del sector privado del Grupo Banco Interamericano de Desarrollo (BID), es un banco multilateral de desarrollo comprometido con los negocios de América Latina y el Caribe. BID Invest financia empresas y proyectos sostenibles para lograr resultados financieros que maximicen el desarrollo económico, social y medio ambiental de la región. BID Invest provee soluciones financieras innovadoras y servicios de asesoría que responden a las necesidades de sus clientes en una variedad de sectores. Para más información visite www.idbinvest.org.

Sumario

Presentación 07
Prefacio 09
Introducción 11

1. Definiciones y Bases 14
1.1 Conceptos de gestión de riesgos corporativos 14
1.2 Historia 16

2. Gobierno y Madurez de GRCorp 22
2.1 Gobierno corporativo y gestión de riesgos 22
2.1.1 Gobierno y cultura de GRCorp 23
2.2 Papeles y atribuciones del modelo de gobierno de GRCorp en las tres líneas de defensa 23
2.3 Agentes del modelo de gobierno de GRCorp 26
2.3.1 Órganos de gobierno 26
2.3.1.1 Junta Directiva 26
2.3.1.2 Consejo fiscal 27
2.3.1.3 Comité de auditoría 28
2.3.1.4 Comité ejecutivo de gestión de riesgos corporativos 28
2.3.1.5 Gerencia 30
2.3.2 Agentes de defensa 30
2.3.2.1 Primera línea de defensa – gestores de las unidades y responsables directos por los procesos 30
2.3.2.2 Segunda línea de defensa – GRCorp 31
2.3.2.3 Tercera línea de defensa – auditoría interna 31
2.3.3 Agentes externos 32
2.3.3.1 Auditoría independiente 32
2.3.3.2 Órganos reguladores 32
2.4 Nivel de madurez 33

2.4.1 Midiendo la madurez 33
2.4.2 Consolidando los resultados de la evaluación de madurez 37
2.4.3 Transformando los resultados de la evaluación de madurez en planes o proyectos 38

3. Modelo Conceptual de Implementación de GRCorp 40
3.1 Paso 1 – Identificar y clasificar los riesgos 41
3.2 Paso 2 – Evaluar los riesgos 42
3.3 Paso 3 – Implementar la función de gestión de riesgos y estructura de controles internos 44
3.4 Paso 4 – Monitorear 44
3.4.1 Definir medidas de desempeño 44
3.4.2 Preparar informes periódicos de riesgos y control 44
3.4.3 Registrar y cuantificar las pérdidas ocasionadas por la materialización de los eventos de riesgo 46

Consideraciones Finales 47

Referencias 49

Anexos
ANEXO 1 – Normas y regulaciones que envuelven gestión de riesgos 51
ANEXO 2 – Ejemplos de clasificación de riesgos 53
ANEXO 3 – Modelos de política y de normas internas de gestión de riesgos 57
3.1 Modelo de política de GRCorp 57
3.2 Modelo de norma interna de GRCorp 58
ANEXO 4 – Glosario 60

Presentación

Desde 1999, con el lanzamiento de la primera edición del Código de las Mejores Prácticas de Gobierno Corporativo, el IBGC pasó a publicar documentos específicos en el ámbito de las buenas prácticas de gobierno corporativo.

La presente publicación, **Gestión de Riesgos Corporativos: Evolución en Gobierno y Estrategia**, integran la serie de publicaciones denominada Cuadernos de Gobierno Corporativo, cuyo objetivo es traer al mercado información práctica que contribuya con el proceso del gobierno corporativo.

Los Cuadernos de Gobierno del IBGC son editados, de acuerdo con su contenido, en tres series: Documentos Legales de Gobierno, Documentos sobre Estructuras y Procesos de Gobierno y Temas Especiales de Gobierno. Traen contribuciones, sugerencias y recomendaciones elaboradas por los asociados del IBGC que integran sus diversas comisiones de trabajo.

Integra los Temas Especiales de Gobierno, este cuaderno habla sobre cómo los administradores, dando importancia a la junta directiva, pueden desarrollar un modelo eficiente de implementación de gestión de riesgos a partir de los principios del buen gobierno corporativo.

El cuaderno presenta de manera instructiva los papeles de los principales agentes de gobierno y algunas de las principales prácticas recomendadas, trayendo subsidios para la implementación de estructura de gestión de riesgos que dialogue con la estrategia de largo plazo establecida por la organización.

Con esta publicación, el IBGC espera contribuir para que las incertidumbres que acompañan los riesgos sean administradas de forma adecuada, garantizando que los administradores estén mejor preparados para tomar decisiones de forma reflexiva y equilibrada.

Prefacio

Esta obra propone traer reflexiones y orientaciones para los ejecutivos y, sobre todo, para las juntas directivas interesadas en implementar y perfeccionar el modelo de gestión de riesgos corporativos (GRCorp) de las organizaciones en las que trabajan. El documento tiene el propósito de servir a organizaciones en diferentes etapas de madurez de GRCorp.

Si el foco del primer cuaderno del IBGC sobre gestión de riesgos[1] era en la metodología del tratamiento de riesgos, esta publicación le brinda importancia al gobierno y la estrategia del GRCorp, o sea, a la estructura organizacional por medio de la cual la gestión de riesgos es concebida y operada. La finalidad del texto, por lo tanto, no es ser exhaustivo con relación a técnicas de gestión de riesgos. Muchos manuales que tratan de ese tema pueden ser encontrados en el mercado, y algunos son citados en las referencias bibliográficas al final de este material. Se optó, aquí, por presentar solo conceptos esenciales para que ejecutivos y miembros de la junta puedan comprender la importancia de su papel en la implementación y en la coordinación, supervisión y fiscalización de una estructura sólida y consistente de gestión de riesgos.

La gestión de riesgos ha ganado importancia en el día a día de las empresas no solo como una forma de reacción a fracasos corporativos que podrían haber sido evitados por una gestión adecuada, sino por su importancia estratégica. La información planteada por el GRCorp es parte integral del proceso de toma de decisiones empresariales, de la protección de activos y del proceso de creación de valor, lo que resalta la importancia de que esa estructura sea dotada de un gobierno adecuado.

El IBGC cree que las consideraciones y sugerencias aquí contenidas contribuirán para el perfeccionamiento del gobierno corporativo, ya que el GRCorp es un valioso instrumento de administración y gobierno y actúa en pro del desarrollo sustentable de las organizaciones, beneficiando a todas las partes interesadas.

Para concebir este cuaderno, fueron tomados en cuenta los debates y análisis hechos por la Comisión de Riesgos del IBGC a lo largo de los años, desde la primera edición del documento

1 *IBGC,* Guia de Orientação para Gerenciamento de Riscos Corporativos*, 2007. Cabe recordar que la Comisión de Riesgos del IBGC ya desarrolló otras publicaciones sobre el tema con la serie Estudios de Caso, a saber:* Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos*, 2008;* Gestão Integrada de Riscos: Banco Real e Brasil Telecom*, 2008; y* Gestão de Riscos como Instrumento para a Tomada de Decisão: Votorantim Celulose e Papel (VCP)*, 2008.*

(2007), las experiencias de proyectos y de la implementación de gestión de riesgos en empresas de diversos sectores y diferentes etapas de madurez en el proceso de gestión de riesgos. También fueron tomadas en cuenta las buenas prácticas de GRCorp diseminadas por organizaciones e institutos independientes, internacionales o nacionales, asociaciones de industria o profesionales, como organismos de regulación y entidades reguladoras.

En el momento de la conclusión de esta publicación, se encontraba en etapa de desarrollo la revisión de la norma ISO 31.000: *General Guidelines for Principles and Implementation of Risk Management*, así como el Coso ERM (*Enterprise Risk Management – Aligning Risk with Strategy and Performance*). Este último, específicamente, explora la forma como el GRCorp debe estar integrado a la planeación estratégica de las organizaciones, una vez que la estrategia influencia su desarrollo. Una empresa que integra GrCorp en su planificación estratégica le proporciona a la administración las informaciones de riesgos que necesitan ser consideradas en las alternativas estratégicas y en sus elecciones.

Así como el IBGC, esas organizaciones (ISO y Coso) percibieron la complejidad a la que las organizaciones están sujetas, los cambios ocurridos a lo largo del tiempo y el surgimiento de nuevos riesgos. Por lo tanto, se vuelve crucial el refuerzo y la consciencia de gestión de riesgos corporativos en las juntas directivas.

Con la expectativa de que el material sea útil y de buenos frutos, les deseamos una buena lectura.

Introducción

En la vida cotidiana de individuos y organizaciones, raramente se tiene en cuenta que casi todos los actos y actividades implican riesgos. La palabra riesgo proviene del latín risicum o riscum, cuya definición incluye el concepto de atreverse – a arriesgar. Así, cualquier acción o emprendimiento trae alguna dosis de riesgo. "Vivir es muy peligroso", decía el personaje Riobaldo en la obra Grande Sertão: Veredas, de Guimarães Rosa.

Las organizaciones se enfrentan cada vez más con temas como sustentabilidad, corrupción, fraude, abusos en los incentivos de corto plazo para ejecutivos e inversionistas, ética en los negocios y reputación. Cada uno de estos temas trae incluido en sí la noción de riesgo, cuya gestión es parte de lo que las organizaciones necesitan para obtener lucros, realizar objetivos importantes (sociales, ambientales, etc.), crear valor, y, principalmente, tener una existencia longeva.

Usualmente se entiende el riesgo como la posibilidad de que algo no salga bien. Pero su concepto actual en el mundo corporativo va más allá: incluye la cuantificación y la cualificación de la incertidumbre[2], tanto en lo que dice respecto a las pérdidas como las ganancias por individuos u organizaciones. Siendo el riesgo inherente a cualquier actividad e imposible de eliminar, su administración es un elemento clave para la supervivencia de las compañías y demás entidades.

Y es de esa forma que las actividades de gestión de riesgos corporativos (GRCorp) deben ser afrontadas. Ellas necesitan contribuir con la longevidad de la organización y para la consecución de sus objetivos estatutarios y estratégicos. Para que esto sea posible, es necesario que las organizaciones dispongan de una estructura de gestión de riesgo y de gobierno corporativo, aún en organizaciones menos maduras y de menor capacidad financiera. Esta publicación tiene el objeto de orientar a los miembros de la junta y ejecutivos tanto para la implementación de un modelo de GRCorp como para el fortalecimiento de los modelos existentes. Dadas las particularidades y las diferentes etapas de desarrollo de cada organización, las recomendaciones y sugerencias contenidas en este documento deben ser analizadas ante la realidad y el momento de cada una.

2 *Riesgo: evento futuro identificado, al cual es posible asociar una distribución de probabilidades de ocurrencia. Incertidumbre: evento futuro identificado, al cual no es posible asociar una distribución de probabilidades de ocurrencia. Ignorancia: eventos futuros que, en el momento del análisis, no podrán ni siquiera ser identificados, mucho menos cuantificados (ejemplo: acontecimientos derivados de sistemas complejos como el climático – las consecuencias del calentamiento global son impredecibles). M. Faber, R. Manstetten y J. Proops,* Ecological Economics: Concepts and Methods*, 1996, pp. 209-211.*

De acuerdo con la 5a edición del Código de las Mejores Prácticas de Gobierno Corporativo del IBGC: "los riesgos a los que la organización está sujeta, deben ser gestionados para subsidiar la toma de decisiones [...]. Los agentes de gobierno tienen la responsabilidad de asegurar que toda la organización esté en conformidad con sus principios y valores, reflejados en políticas, procedimientos y normas internas, y con las leyes y los dispositivos reguladores a los que esté sometida"[3].

El código del IBGC orienta que la junta directiva posea conocimiento sobre el tema, para que puedan identificar efectivamente, priorizar y garantizar la gestión eficaz de la exposición de la organización a los diversos riesgos relacionados a su negocio. La junta directiva debe adoptar una actitud proactiva, buscando información basada en el modelo de GRCorp. Esto será posible en la medida que la junta directiva logre evaluar los modelos, estructuras, procesos, herramientas e indicadores utilizados.

Este cuaderno se divide en tres capítulos. En el primero, son tratados los conceptos básicos sobre GRCorp, su importancia y como la gestión de riesgos se alinea a las estrategias empresariales. En el Capítulo 2, se centra en las atribuciones de varios agentes de gobierno corporativo, con énfasis en el papel de la junta directiva a partir de la óptica de los procesos decisorios, de las responsabilidades y de los inductores de riesgos. Para finalizar, el Capítulo 3 contiene ayudas para la implementación de una estructura de GRCorp adecuada al tamaño y la complejidad de la organización y que respete la etapa de madurez del negocio y la estrategia de largo plazo de su administración, presentando las principales prácticas recomendadas. El cuaderno contiene, además, anexos con información adicional.

3 *IBGC,* Código das Melhores Práticas de Governança Corporativa*, 2015, p. 91.*

1

Definiciones y Bases

1. Definiciones y Bases 14

1.1 Conceptos de gestión de riesgos corporativos 14

1.2 Historia 16

1. Definiciones y Bases

1.1 Conceptos de gestión de riesgos corporativos

Dado que el riesgo es inherente a cualquier actividad empresarial, les corresponde a las empresas gestionarlo con el objeto de asumir riesgos calculados, reducir la volatilidad de sus resultados y aumentar la previsibilidad de sus actividades y volverse más resilientes en escenarios extremos. La eficacia en su gestión puede afectar directamente los objetivos estratégicos y estatutarios establecidos por la administración y, en último análisis, impacta la longevidad de la organización.

La gestión de riesgos corporativos (GRCorp) puede ser entendida como un sistema intrínseco a la planificación estratégica de negocios, compuesto por procesos continuos y estructurados diseñados para identificar y responder a eventos que puedan afectar los objetivos de la organización y por una estructura de gobierno corporativo responsable por mantener ese sistema vivo y en funcionamiento. Por medio de esos procesos, la organización puede mapear oportunidades de ganancias y reducir la probabilidad del impacto de pérdidas. Se trata, por tanto, de un sistema integrado para conducir sus ganas de asumir riesgos en el ambiente de negocios, a fin de alcanzar los objetivos definidos.

Existen varias estructuras y modelos de GRCorp como los propuestos por el Committee of Sponsoring Organizations of the Treadway Commission (Coso II) y por la norma ISO 31.000[4]. El proceso de GRCorp generalmente se inicia con la identificación y clasificación de los riesgos, lo que puede ser realizado de acuerdo con la naturaleza, origen y conforme al segmento de actuación de la empresa, su cultura, entre otros criterios. Una metodología adoptada establece, por ejemplo, que existen riesgos internos (que surgen en la organización), externos (ajenos a la empresa) y estratégicos (relacionados a las informaciones utilizadas por la administración para la toma de decisiones). Unas de las herramientas generalmente aceptadas para clasificar o categorizar los riesgos es la matriz de riesgos, que considera el origen de los eventos (interno, externo o estratégico) y los divide en diversas clases. Los tipos de riesgos serán presentados de forma más detallada en el Anexo 2 de este cuaderno.

Las etapas posteriores del proceso de GRCorp son las evaluaciones, que buscan determinar el grado de exposición de la empresa al riesgo (dado por la probabilidad de ocurrencia e impacto del evento), la valoración (cuantificación de las estimativas de pérdidas) y el tratamiento dado a los riesgos. Esto implica la toma de una decisión básica por parte de la compañía: la de evitar o aceptar el riesgo. La opción de aceptarlos lleva a algunas alternativas, tales como retener, reducir, compartir o explorar el riesgo. Cuando decide retener el riesgo, la empresa lo asume en el nivel actual de severidad (impacto y probabilidad). Cuando decide reducir el grado de severidad, toma medidas para minimizar o mitigar su probabilidad de ocurrencia y su impacto. La acción de compartir se refiere a los casos en que El riesgo

4 Pudiendo integrarse aquí también, de forma auxiliar, las normas ISO 22.301, familia ISO 27.000 y NIST, ISO 38.500 y Cobit 5, y el draft de norma BS 65.000 del British Standard Institute (BSI), que tratan sobre gestión de riesgos con relación a los sistemas de información, gobierno de TI, continuidad de negocios y de la resiliencia organizacional.

es parcialmente transferido o dividido con terceros. La exploración significa, finalmente, el uso de las competencias de la organización para obtener resultados con la exposición en el nivel actual, o con aumento de la exposición, para aprovechar ventajas competitivas.

Otras etapas del proceso de GRCorp son el monitoreo y la comunicación de los riesgos. El primero incluye el constante acompañamiento, por parte de la junta directiva y de la gerencia, de la eficacia y adecuación del proceso. Y por otro lado, la comunicación contribuye para que el ambiente corporativo refleje los valores y la cultura de riesgos deseada por la organización.

Uno de los objetivos del GRCorp es encontrar un equilibrio de los niveles de retención, reducción, exploración y transferencia de riesgos, y que este sea adecuado al apetito al riesgo de la organización.

El apetito al riesgo está asociado al nivel de riesgo que la organización está dispuesta a aceptar en la búsqueda de la realización de su misión. El apetito debe ser establecido por la junta directiva (o por los socios, en caso de que la organización no posea junta directiva), teniendo en cuenta los intereses de la organización, y sirve como punto de referencia para fijar estrategias y para la elección de los objetivos relacionados a esas estrategias. A partir de este apetito, se configura el perfil de riesgo de la empresa. Haciendo una analogía con los inversionistas del mercado financiero, hay desde compañías más conservadoras hasta las más arrojadas cuando se trata de la propensión a correr riesgos y aceptar posibles pérdidas o ganancias. "La tolerancia al riesgo puede ser vista como la variación aceptable en torno a los límites establecidos. Dentro de los riesgos y exposiciones aceptables, los límites de tolerancia son 'detonantes' para la actuación de la junta directiva. Indicadores de riesgos e indicadores de la efectividad de los hedges deben ser supervisados por la junta directiva"[5].

Otro concepto importante es la estrategia de GRCorp. Ella debe incluir aspectos de expectativas, objetivos, metas, inversiones y desempeño con relación a las prácticas de GRCorp de la compañía. Tanto la definición de la estrategia de GRCorp como la determinación del perfil de riesgos son atribuciones de la junta directiva, que será detallado en el Capítulo 2 de este cuaderno.

La gestión eficaz de riesgos está dada por la calidad de la estructura de gobierno, de los recursos humanos, de las estrategias, de la cultura, por la percepción de los riesgos propios de la calidad del ambiente de negocios, de los procesos, de los controles y de la tecnología empleados. Ella es un diferencial de las empresas en las cuales las relaciones riesgo-retorno apoyan la toma de decisiones por parte de los administradores, con el objeto de alcanzar los objetivos de la organización. La relación riesgo-retorno sugiere que cuanto mayor es el retorno esperado de las inversiones, mayores serán los riesgos que se van a asumir, lo que exige la evaluación de la competencia para gestionarlos y controlarlos. Por lo tanto, la reflexión sobre la capacidad de gestionar los riesgos asumidos es fundamental para elecciones bien fundamentadas y conscientes.

La implementación del GRCorp trae varios beneficios para las compañías gestionan sus riesgos, ya sean operativos o relacionados al ambiente de negocios como un todo. Una vez que la

5 *S. A. Ross, R. W. Westerfield, J. Jaffe y R. Lamb,* Administração financeira*, 2015. p. 924. Mientras "apetito al riesgo" está asociado al nivel de riesgo que la organización puede aceptar en la búsqueda de la realización de su misión/visión (análisis ex ante), "tolerancia al riesgo" habla sobre el nivel aceptable de variabilidad en la realización de las metas y objetivos definidos (actividad más asociada a monitoreo, ex post).*

organización cuente con los procesos claros para identificar, medir, reportar, monitorear y mitigar los riesgos hay un mejoramiento de los controles internos, trayendo ganancias operativas, reduciendo la posibilidad de pérdidas y maximizando la eficiencia y la eficacia empresarial.

Otro beneficio de la gestión de riesgos es la profundización de los debates sobre aspectos clave del negocio, bien como la identificación de nuevas oportunidades. La información recolectada propicia una mejor base para la toma de decisiones, facilitando los procesos de elección de asignación de recursos.

El GRCorp promueve la transparencia, al aclarar los principales riesgos del negocio y la forma como ellos son tratados. Los inversionistas pasan a contar con más subsidios para evaluar si valdría la pena emplear el capital en aquella empresa (o cuál es el retorno esperado para eso). Otras partes interesadas, como la comunidad, el gobierno y los funcionarios, también se benefician directa o indirectamente de un sistema de GRCorp robusto y bien estructurado, en la medida en que la empresa genera valor por la asunción de riesgos, sus resultados son menos volátiles, y el sistema contribuye para la viabilidad de la organización, teniendo en cuenta las dimensiones económico-financiera, ambiental, social, reputacional y de conformidad.

Además, hay una mejoría en el gobierno corporativo en consecuencia de los procesos inherentes a la gestión de riesgos, como el aumento de la rendición de cuentas, de responsabilidad corporativa y de la participación de los diversos niveles de decisión de la organización, como la junta directiva. Todo eso converge, finalmente, para la longevidad de la compañía y para su valoración.

1.2 História

La gestión de riesgos es una práctica que hace parte de la rutina de cualesquiera empresarios desde tiempos muy remotos[6]. Sin embargo, el tema viene ganando relevancia creciente desde finales del siglo XX, dado el aumento de la complejidad de las compañías, instituciones financieras y organizaciones del tercer sector, además de una mayor interconexión entre los mercados (globalización). El inicio de la vasta literatura sobre el tema fue dedicado al área de seguros[7]. Más recientemente, el asunto se ha desarrollado como una metodología estructurada a partir de varias vertientes, entre las cuales se destacan las de finanzas, auditoría, estrategia y tecnología de la información.

En la industria financiera, el incentivo para implementar la gestión de riesgos surgió en la década de 1980, con la preocupación creciente del Bank of England y del Federal Reserve Board (EUA) con la exposición de los bancos a operaciones no registradas en equilibrio, combinadas con problemas de préstamos para los países entonces clasificados como del tercer mundo.

El Bank of International Settlements (BIS) dio continuidad a la iniciativa de las dos instituciones, por medio del envío de propuestas para los bancos y de peticiones para que estos hicieran comentarios y sugerencias. Los primeros resultados de ese proceso vinieron en el año 1988, con el primer Acuerdo de Basilea (Basilea I) y sus enmiendas subsecuentes a partir de 1996. El primer acuerdo, de 1988, tenía como punto principal la asignación de capital para hacer frente a riesgos de crédito.

6 *Ver P. Bernstein,* Desafio aos Deuses: A Fascinante História do Risco*, 1996*

7 *Ver, por ejemplo, E. J. Vaughan y C. M. Elliot,* Fundamentals of Risk and Insurance*, 2003.*

A partir de 1993, se introdujeron reglas para el riesgo de mercado, que tienen como referencia principal la publicación por JP Morgan del RiskMetrics[8] en octubre de 1994. El documento surgió en respuesta a los grandes desastres financieros de inicios de los años 1990 (casos conocidos como los de Procter & Gamble, Orange County, Barings, etc.) e introdujo el concepto de Value-at-Risk (VaR). El VaR mide la pérdida potencial máxima del valor de una cartera con determinado nivel de confianza en un intervalo de tiempo dado y en condiciones normales de funcionamiento del mercado.

Sin embargo, el proceso de identificación y tratamiento de riesgos no financieros se muestra más complejo. Mientras los riesgos financieros son fácilmente cuantificables por medio de herramientas como el VaR, la valoración de otros riesgos – como el operativo, el ambiental o el reputacional – implica mayor grado de subjetividad. Desde la publicación del RiskMetrics, se observa un intenso debate sobre cómo adaptar el concepto de VaR para los riesgos no financieros. No obstante, el único consenso alcanzado fue que el VaR no sería suficiente, siendo necesario combinar una serie de técnicas cuantitativas y cualitativas para la medición de los riesgos no financieros. Adicionalmente, es necesario recordar que en la definición de VaR se incluye el concepto de "ambiente normal de negocios", el que hace que, de antemano, modelos de VaR no funcionen en situación de crisis (para esos casos existen los modelos de "stress-test ").

En junio de 1999, el Basel Committee on Banking Supervision del BIS, el Comité de Basilea, propuso una nueva estructura para la adecuación del capital, el Basileia II, cuya publicación sustituyó el acuerdo de 1988. El comité de Basilea propuso una estructura apoyada en tres pilares: el primero trataba de la adecuación del capital regulatorio mínimo con base en los riesgos del mercado, de crédito y operativos; el segundo reforzaba la capacidad de los supervisores bancarios para evaluar y adaptar el capital regulador a las condiciones de cada institución financiera; y el tercero atribuía la transparencia y la divulgación de información un papel importante y relevante en el fomento de la disciplina de mercado.

Como resultado de la crisis financiera de 2007-2008, que reveló graves deficiencias en términos de regulación en el sistema financiero mundial, en el año 2010 el BIS volvió a proponer un nuevo acuerdo, el Basilea III, que pasó a promover el aumento de reserva de capital por parte de los bancos en busca de protección a eventuales crisis y la consecuente "estampida bancaria por incertidumbre".

En la misma línea del BIS, la Comisión Europea de Supervisión de los Seguros y Previsión (Ceiops – Commission for European Insurance and Occupational Pension Supervisors) elaboró en 2007 la directiva de enfoque para la Solvencia II[9]. Aplicada a la industria de seguros y de previsión, el régimen de Solvencia II tiene una estructura de tres pilares, en los que cada uno posee su enfoque y gobierna un aspecto diferente: i) cálculo de los requisitos de capital de solvencia y capital mínimo requerido, con base en el modelo estándar o interno; ii) principios generales que rigen la regulación de riesgos y controles internos; y iii) directrices sobre divulgación y transparencia de información al respecto de la solvencia y situación financiera.

8 *Ver <https://www.msci.com/documents/10199/5915b101-4206-4ba0-aee2-3449d5c7e95a>.*

9 *Solvency II o Solvencia II, en resúmen, y la supervisión basada en riesgo. Y el régimen creado por el Parlamento europeo (Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance [Solvency II]) para que las aseguradoras mejoraran sus prácticas de control y gestión de riesgos involucrando prácticas de gobierno.*

Paralelamente al desarrollo por la rama financiera, auditores, contadores y legisladores han dedicado una creciente atención a los controles internos. En las compañías no financieras, las directrices más utilizadas al respecto de gestión de riesgos tienen origen en las recomendaciones del Committe of Sponsoring Organizations of the Treadway Commission (Coso). Este comité emitió recomendaciones y estableció una metodología integrada para ayudar a las organizaciones a analizar y a mejorar sus sistemas de controles internos y sus procesos de gestión de riesgo empresarial (*ERM – Enterprise Risk Management*). Esa metodología, altamente difundida desde entonces, ha sido incorporada en las políticas, reglas y regulación por varias empresas para controlar mejor sus actividades, de forma que puedan alcanzar los objetivos establecidos.

El Financial Accounting Standards Board (Fasb) publicó guías fomentando la divulgación de estados financieros más completos, demostrando lo que se ha hecho para mitigar y gestionar los riesgos a partir del modelo de gobierno instaurado, entre otras iniciativas. Un grupo de reguladores y profesionales han publicado guías importantes relativas a los controles internos y a la gestión de riesgos. Entre los esfuerzos notables se incluyen, además del Informe Coso (1992), el Informe Cadbury (1992) y el Turnbull (1999).

Pero el siglo XXI se iniciaría con una nueva onda de escándalos corporativos (Enron, WorldCom, Adelphia, entre otros), que demandarían aún una mayor regulación. Como respuesta, fue creada en 2002 en los Estados Unidos la Ley Sarbanes-Oxley (SOX), que enfatizó el papel fundamental de los controles internos y transformó en exigencia legal en los EUA las buenas prácticas de gobierno corporativo. La SOX afectó a todas las empresas americanas y extranjeras con títulos y acciones negociados en bolsas americanas, además de sus subsidiarias. Y asimismo sirvió de base para regulaciones locales alrededor del mundo, poniendo en boga toda la metodología que venía siendo desarrollada para mejorar los controles internos. La SOX vino a exigir que gerentes, presidentes y gerentes financieros de empresas de capital abierto explícitamente certifiquen la precisión de los estados financieros publicados por medio de la estructuración de controles internos y de la gestión de riesgos corporativos, además de procedimientos de prevención y detección de fraudes. La ley estableció también castigos más rígidos (penales) para gerentes-presidentes y gerentes financieros y alteró la forma como las empresas son auditadas. En la misma línea de la SOX y en respuesta a la crisis del mercado financiero de 2007-2008, fue aprobada en los EUA la Ley Dodd-Frank, que aumentó la regulación y definió restricciones relevantes sobre la actividad financiera del país.

La UK Bribery Act de 2010 vino a reforzar y mejorar la ley anticorrupción americana (FCPA) establecida en 1977. Brasil formuló también su propia ley anticorrupción (Ley 12.846/2013), que entró en vigencia en el año 2014. Como consecuencia de esa ley, una serie de decretos y resoluciones contribuyeron con la regulación anticorrupción en Brasil. La ley busca responsabilizar empresas, sus controladores, controladas, consorciadas o vinculadas por prácticas que perjudican la administración pública. Las compañías pasaron a responder en las esferas administrativas y civil por actos de corrupción y fraude en licitaciones y contratos con el poder público.

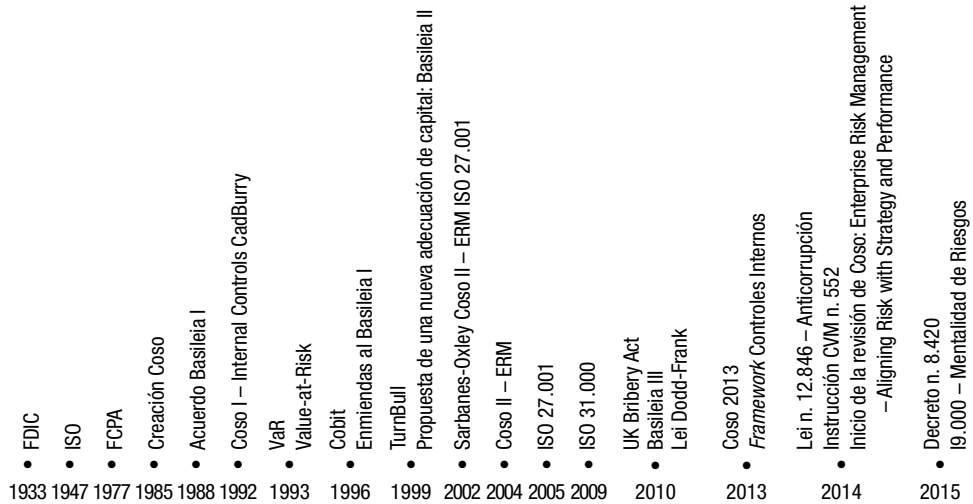
La regulación de la ley n. 12.846, dada por medio del Decreto Federal n. 8.420/2015, estableció los criterios para cálculo de multas, los parámetros para la validación de programas

de conformidad (compliance)[10], las reglas para la celebración de los acuerdos de indulgencia y disposiciones sobre el registro nacional de empresas sancionadas.

Específicamente sobre el programa de integridad (compliance), el decreto establece los mecanismos y procedimientos de integridad, auditoría, aplicación de códigos de ética o conducta e incentivos de denuncia de irregularidades que deben ser adoptados por la empresa y monitoreados por el Ministerio de Transparencia, Fiscalización y Control, antigua Contraloría General de la Unión. El programa de integridad debe ser estructurado, aplicado y actualizado de acuerdo con las características de riesgos actuales de las actividades de cada persona jurídica, que, a su vez, es responsable por el constante mejoramiento y adaptación del programa.

A pesar de todo ese reciente desarrollo, la búsqueda por estándares de GRCorp todavía continúa bastante activa en el Brasil y en el mundo. Los modelos alineados a las buenas prácticas están siendo desarrollados (algunos en respuesta a las crisis) con el objetivo de incorporar nuevos conceptos de evaluación de riesgos y de controles, adicionalmente de atender las exigencias del mercado y de órganos reguladores. La figura a continuación trae los principales eventos que van a contribuir con la evolución de las prácticas de GRCorp:

Figura 1. Evolución de la gestión de riesgos



Descripción:
FDIC – Federal Deposit Insurance Corporation
ISO – International Organization for Standardization
FCPA – Forreign Corrupt Practices Act
Coso – Committee of Sponsoring Organizations of the Treadway Commission Basileia
Basileia – Basel Committee on Banking Supervision
Cadbury – Committee on the Financial Aspects of Corporate Governance
Cobit – Control Objectives for Information and related Technology
Sarbanes-Oxley – Ley norteamericana formulada por Paul Sarbanes y Michael Oxley en 2002

10 *Los programas de conformidad, o compliance, tienen como objetivo asegurar el cumplimiento de las normas legales y reglamentarias. Además de eso, buscan garantizar la adecuación, el fortalecimiento y el funcionamiento de los controles internos de la organización.*

2

Gobierno y Madurez de GRCorp

2. Gobierno y madurez de GRCorp 22

2.1 Gobierno corporativo y gestión de riesgos 22

2.1.1 Gobierno y cultura de GRCorp 23

2.2 Papeles y atribuciones del modelo de gobierno de GRCorp en las tres líneas de defensa 23

2.3 Agentes del modelo de gobierno de GRCorp 26

2.3.1 Órganos de gobierno 26

2.3.2 Agentes de defensa 30

2.3.3 Agentes externos 32

2.4 Nivel de madurez 33

2.4.1 Midiendo la madurez 33

2.4.2 Consolidando los resultados de la evaluación de madurez 37

2.4.3 Transformando los resultados de la evaluación de madurez en planes o proyectos 38

2. Gobierno y madurez de GRCorp

2.1 Gobierno corporativo y gestión de riesgos

El IBGC, en su Código de las Mejores Prácticas de Gobierno Corporativo, define gobierno corporativo como "el sistema por el cual las empresas y demás organizaciones son dirigidas, monitoreadas e incentivadas, incluyendo las relaciones entre socios, junta directiva, gerencia, órganos de fiscalización y control y demás partes interesadas"[11].

La gestión de riesgos existe para ser asociada al proceso de toma de decisiones y al proceso de establecimiento de la estrategia, o sea, la gestión de riesgos y el proceso que debe ser integrado al proceso de decisión. Desde el punto de vista operacional, podemos decir que la gestión de riesgos integra el gobierno de una empresa, pues el riesgo necesita ser identificado, medido, tratado y monitoreado y esa información alimenta el proceso de toma de decisiones por parte de diferentes agentes, ya sean los socios, la junta directiva, la gerencia, así como las demás partes interesadas (por ejemplo, clientes, proveedores, comunidad, reguladores, gobierno, entre otros). De esta forma, el GRCorp trae ventajas en la estructura de gobierno de las organizaciones, como el aumento de la transparencia y de la rendición de cuentas, el fortalecimiento de los controles internos y mayor compromiso con la responsabilidad corporativa.

Para funcionar adecuadamente, el GRCorp necesita tener establecida y formalizada una estructura de gobierno clara. Esa estructura definirá atribuciones y responsabilidades de cada agente en los diferentes niveles y prácticas de GRCorp sobre lo que dice con relación a los riesgos, indicando, por ejemplo, quien identificará y evaluará los riesgos, quien tomará las decisiones sobre el tratamiento de los riesgos, quién va a monitorear los riesgos, y quién fiscalizará el proceso como un todo.

Las principales reflexiones que serán debatidas por la junta directiva y por la gerencia para la construcción del modelo de gobierno de GRCorp incluyen:

- ¿Qué puede comprometer el cumplimiento de las estrategias y metas?
- ¿Dónde están las mayores oportunidades, amenazas y dudas?
- ¿Cuáles son los principales riesgos?
- ¿Cuáles son los principales riesgos a explorar?
- ¿Cuál es la percepción de dichos riesgos?
- ¿Cuál es la exposición de esos riesgos? ¿Existe diferencia entre percepción y exposición de esos riesgos?
- ¿Cómo responde la organización a los riesgos?

11 *IBGC,* Código das Melhores Práticas de Governança Corporativa, op. cit., *p. 20.*

- ¿Existe información confiable para la toma de decisiones?
- ¿Qué se hace para garantizar que los riesgos estén en un nivel aceptable de acuerdo con el apetito a los riesgos que fue aprobado?
- ¿Los ejecutivos y gestores están conscientes de la importancia del proceso de gestión de riesgos?
- ¿La organización tiene las competencias necesarias para gestionar riesgos asumidos?
- ¿Quién identifica y monitorea activamente los riesgos de la organización?
- ¿Qué patrones, herramientas y metodologías son utilizadas?

Este cuaderno no profundizará en los temas relacionados a cada una de las preguntas, y ellas deben ser entendidas como un instrumento no exhaustivo para reflexión de las juntas directivas. Las respuestas a ellas servirán como base para la evaluación del modelo actual o para la creación del modelo de GRCorp más apropiado para la organización.

2.1.1 Gobierno y cultura de GRCorp

El gobierno y la cultura de GRCorp son la base de los demás componentes de gestión de riesgos. El gobierno define el tono, refuerza la importancia y establece las responsabilidades por el GRCorp. La cultura, a su vez, se refiere a los valores éticos, a los comportamientos deseados y al entendimiento de riesgo en la organización. La cultura está reflejada en el proceso de toma de decisiones y ampara el cumplimiento de la misión y de la visión de la organización. Una cultura de conciencia de los riesgos enfatiza la importancia del GRCorp e incentiva el flujo transparente de las informaciones de riesgos con una actitud de conocimiento, rendición de cuentas y mejoría continua.

La cultura de riesgos debe permear a toda la organización, y le corresponde a la junta directiva comprometerse para promover un amplio entendimiento de la importancia del tema para la longevidad de los negocios. La cultura de riesgos de una organización surge de su identidad y se refiere al conjunto de sus estándares éticos, valores, actitudes y comportamientos aceptados y practicados, y a la difusión de la gestión de riesgos como parte de los procesos de toma de decisiones en todos los niveles. Ella es establecida por el discurso y por el comportamiento de la junta directiva, de la gerencia y del apetito a los riesgos de la organización. La cultura de riesgos de una organización influencia la forma como ella identifica, acepta y hace la gestión de riesgos.

2.2 Papeles y funciones del modelo de gobierno de GRCorp en las tres líneas de defensa

El modelo de gobierno de GRCorp, representado por las funciones distribuidas en la estructura organizacional, auxilia la gestión de los riesgos en diferentes niveles de la organización.

Ese modelo tiene el objeto de asegurar que la información proveniente del proceso de gestión de riesgos sea adecuadamente comunicada y utilizada como base para la toma de decisiones y la responsabilidad en todos los niveles organizacionales aplicables. El modelo es más efectivo cuando

los objetivos de gestión de riesgos son integrados a las metas para la premiación de desempeño con el acompañamiento de indicadores clave que ponderan desempeño y riesgos asumidos.

Conforme al tópico anterior, la gestión y la consideración de los riesgos en el proceso decisivo deben ser integradas a la cultura de la organización, y varios agentes desempeñan papeles y responsabilidades en el GRCorp. Esas no pueden ser funciones de apenas un área o una persona, debe ser ejecutada por todas las áreas y personas dentro de la organización que tengan la responsabilidad de integrar y orientar los múltiples esfuerzos de gestión de riesgos, interactuando con la administración.

Los procesos involucrados en el GRCorp deben ser definidos e incorporados como parte integrante de la cultura y de la estructura organizacional, resultando en un sistema por medio del cual la responsabilidad de gestión de riesgos es claramente distribuida, las actividades son formalmente especificadas, y la comunicación es delineada para que todos los involucrados alcancen los objetivos organizacionales.

Las funciones del GRCorp deben ser descritas, formalizadas, aprobadas y divulgadas en la política del GRCorp de exhaustividad corporativa. Esta debe representar el conjunto de principios, acciones, papeles y responsabilidades necesarios para la identificación, evaluación, respuesta y monitoreo de los riesgos a los cuales la empresa está expuesta.

Tres documentos pueden constituir el marco para la comunicación de las prácticas de GRCorp:

1) *Política de gestión de riesgos, divulgada para el mercado (por ejemplo, de las revelaciones de la política de negociación de títulos mobiliarios, o de la política de transacciones con partes relacionadas);*
2) *Norma de gestión de riesgos (o documento equivalente), de divulgación interna que establece los procedimientos en la toma de riesgos, responsabilidades, inclusive de informe, rendición de cuentas, separación de funciones, fronteras de actuación, y el sistema general de gobierno de la gestión de riesgos; y*
3) *Código de conducta, de divulgación interna y externa, cuyo objetivo es promover principios éticos y reflejar la identidad y la cultura de la organización, complementando las obligaciones legales y de regulación*[12].

Los procesos y actividades que envuelven el GRCorp, bien como su monitoreo, deben ser ejercidos:

i. Por los diversos agentes de los órganos de gobierno, incluyendo la junta directiva, el comité de auditoría y demás comités de asesoramiento (como el comité de gestión de riesgos u otros que debatan temas técnicos específicos), la gerencia y el consejo fiscal, cuando sea aplicable. En caso de que la organización no posea una junta directiva, esa función será ejercida por él(los) socio(s).
ii. Por las tres líneas de defensa[13], como se detalla a continuación.

12 El Anexo 3 de este cuaderno trae un modelo de política y otro de normas de GRCorp para referencia. El IBGC pone a disposición en su página web su propio código de conducta (ver referencias bibliográficas), para que este pueda servir de inspiración para empresas, agentes de mercado y otros tipos de organizaciones.

13 Tres líneas de defensa o 3LOD es una estructura para el gobierno de la exposición al riesgo, también implícita en

1ª Línea de defensa – realizada por los gestores de las unidades y responsables directos por los procesos: contempla las funciones que gestionan y tienen la responsabilidad sobre los riesgos;

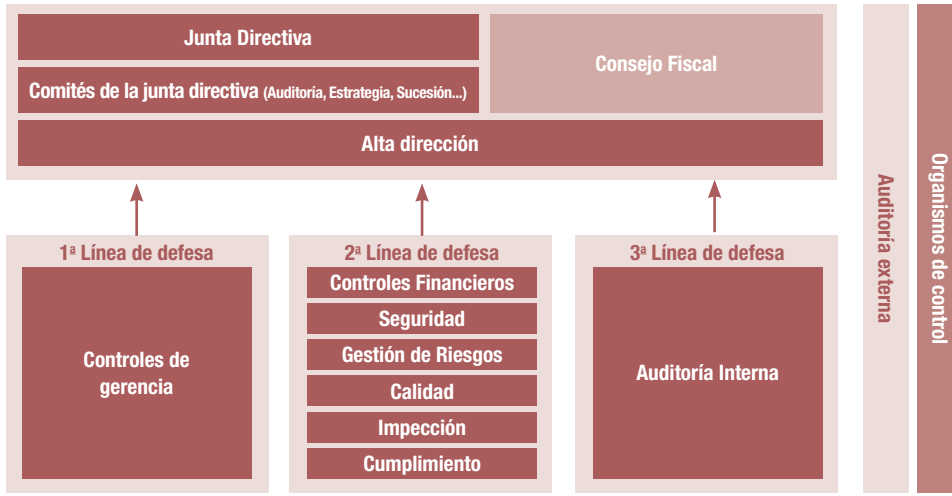
2ª Línea de defensa – realizada por los gestores corporativos de GRCorp, de conformidad o de otras prácticas de control, por ejemplo, el que contempla las funciones que monitorean la visión integrada de los riesgos;

3ª Línea de defensa – realizada por la auditoría interna: provee evaluaciones independientes por medio del acompañamiento de los controles internos.

El modelo de gobierno de GRCorp suponen la existencia de interacción entre todos los niveles de la organización, incluyendo la junta directiva y sus comités, el consejo fiscal, la gerencia y los agentes de la primera, segunda y tercera líneas de defensa.

En este modelo, cada una de esas tres líneas desempeña un papel distinto dentro de la estructura más amplia de gobierno de la organización.

Figura 2. Líneas de defensa de la función del GRCorp



Fonte: Adaptado de IIA, *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles*, 2013.

el cuadro de la referencia del ERM del Coso, amplia e internacionalmente usada por instituciones financieras, pero igualmente aplicable a cualesquiera organizaciones. Reúne diversas funciones y equipos corporativos, incluyendo estructuras y agentes de gobierno, permitiendo controlar riesgos-clave identificados. Existen enfoques orientados para cinco líneas de defensa o 5LOD, en el que la inclusión de dos líneas más determinan las responsabilidades relativas al gobierno de riesgos y al cumplimiento de regulaciones parte del tope de organización para la base involucrada (tone at the top), permite que las tres líneas de defensa funcionen adecuadamente de forma sistémica, siendo posibilitada entonces con la inclusión de la cuarta línea de defensa, conocida como "proveedores de garantía interna", y de la quinta línea de defensa, conocida como "consejo de supervisión de riesgos y gestión ejecutiva".

La gerencia incluye el gerente-presidente y los demás miembros que responden para la operación y por el desempeño de las diferentes unidades de negocio y de soporte. Los gerentes pueden tener diferentes responsabilidades y formas de rendición de cuentas en el modelo de las tres líneas de defensa, dependiendo de la organización en la que actúan. Por ejemplo, un gerente de tecnología puede ejercer el papel de segunda línea de defensa en una empresa del sector financiero, pero tal vez actúe en la primera línea de defensa en una compañía de tecnología.

Existen varias alternativas para la construcción del gobierno de GRCorp. Cada organización deberá adoptar aquella que sea más adecuada a su perfil según su nivel de madurez. De esa forma, las organizaciones en etapas iniciales deben reflejar a partir de los inductores antes mencionados, para que definan el mejor modelo que deberá ser adoptado

2.3 Agentes del modelo de gobierno de GRCorp

2.3.1 Órganos de Gobierno

2.3.1.1 Junta Directiva

La Junta directiva debe ser la responsable de determinar los objetivos estratégicos, los direccionamientos y el perfil de riesgos de la organización adaptado al apetito a riesgos de esta, relacionados a su cultura e identidad. Dichas responsabilidades se derivan de la idea del "*tone at the top*", o sea, los principios éticos de la organización deben provenir justamente de ese órgano.

Con relación a su papel en el GRCorp, la junta directiva debe monitorear el funcionamiento del proceso de gestión de riesgos y acompañar el perfil de riesgos de la organización y los planes de acción definidos en respuesta a los riesgos.

Corresponde a la junta directiva evaluar si el desempeño de la organización está de acuerdo con el apetito y la tolerancia a los riesgos establecidos. También es su tarea monitorear la eficiencia y la efectividad del sistema de control interno el cual debe sistémicamente evolucionar en capacidad conforme al avance de las modalidades de riesgos, inherentes a la evolución del desempeño corporativo y modelos de negocios, incluidos los cibernéticos.

Durante sus reuniones, la junta directiva debe dedicar tiempo para tratar de analizar la matriz de riesgos y del sistema de control interno, define los niveles adecuados de exposición y del acompañamiento periódico de las exposiciones al riesgo y de los respectivos planes de acción y mitigación.

La junta directiva tiene como misión proteger y evaluar el patrimonio de la organización. Debe tener pleno conocimiento de los valores de la empresa, propósitos y creencias de los accionistas, velando por su mejoramiento.

La junta directiva debe[14]:

- Procurar comprender los elementos-clave del éxito de la organización;
- Evaluar los riesgos estratégicos de la empresa;
- Definir su papel y el de los comités de asesoramiento en la supervisión de los riesgos;

14 Adaptado de NACD, Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward, 2009.

- Evaluar si el GRCorp de la empresa (incluyendo personas y procesos) es adecuado y tiene recursos suficientes;
- Debatir con la gerencia el nivel de efectividad del sistema de controles internos de la organización, así como suministrar orientaciones para su mejoramiento constante;
- Asegurar que la junta directiva implemente controles efectivos para mitigar los riesgos de interrupciones de negocios (continuidad de los negocios) y controles para mitigar los riesgos de pérdidas de la información o de accesos no autorizados (seguridad de la información);
- Definir, con los ejecutivos, los tipos, los formatos y la periodicidad de la información sobre riesgos y controles internos que necesita para el acompañamiento;
- Estimular el diálogo dinámico y constructivo sobre riesgos y controles entre la gestión y la junta directiva, incluyendo la disposición y la voluntad de los miembros de la junta de cuestionar presupuestos;
- Monitorear de forma continua los riesgos que pueden impactar los objetivos de la organización;
- Monitorear los alineamientos críticos: estrategia, riesgos, controles, conformidad (compliance), incentivos y personas;
- Evaluar periódicamente si los procesos de GRCorp permiten a la junta directiva alcanzar sus objetivos de supervisión de los riesgos;
- Ser el responsable formal por la orientación estratégica y por el monitoreo de las actividades de gestión de riesgos y del sistema de controles internos de la organización.

Adicionalmente, le corresponde a la junta directiva reflexionar sobre las etapas de madurez de GRCorp en el que se encuentra la compañía, en cada dimensión demostrada, y desarrollar, con la gerencia, una visión de futuro sobre la etapa en la que la organización deberá estar, y un plan de acciones necesarias para ello. La evaluación de la etapa de madurez será analizada más adelante, en el ítem 2.4.

2.3.1.2 Consejo fiscal

En calidad de agente de gobierno, el consejo fiscal tiene la responsabilidad de verificar si la organización está en conformidad con sus principios y valores, reflejados en políticas, procedimientos y normas internas, y con las leyes de los dispositivos de regulación.

En su trabajo de fiscalización, los consejeros fiscales deben abstenerse de orientar o direccionar cualquier actividad de la organización. Ellos pueden contribuir sobre temas de gestión de riesgos, haciendo constar en sus actas su parecer, conforme sea el caso, la información complementaria que consideren necesarias o útiles en el proceso de gestión de riesgos o la información de la asamblea general. La comprensión de la estrategia y de los riesgos a lo largo del ejercicio es parte fundamental del proceso de formación de la opinión del consejo fiscal sobre los resultados y el informe de la administración, que deberá presentarse a la asamblea general.

Algunas de las actividades principales relacionadas a la gestión de riesgos por el consejo fiscal son:

- Conocer los procesos, el mapa de riesgos, los indicadores-clave de riesgos y los responsables por el proceso de GRCorp y su alineamiento con los objetivos del negocio,

así como la estructura de controles internos, los riesgos monitoreados, los controles-clave, el sistema de monitoreo, y la adecuación de personal y presupuesto;

- Dialogar con los agentes con papel en la definición, supervisión y monitoreo de la gestión de riesgos: comité de auditoría, comité de gestión de riesgos, auditoría interna, áreas contables, jurídica, de conformidad, de ética y conducta, buscando reunir información sobre la gestión de riesgos para subsidiar la formación de su opinión sobre los actos de gestión;
- Definir, con los ejecutivos, tipos, formatos y periodicidad de la información sobre riesgos que el consejo fiscal necesita para su deber de fiscalización.

2.3.1.3 Comité de auditoría

Las organizaciones han tratado el comité de diversas formas. Son "órganos relevantes de asesoría a la junta directiva, para apoyarla en el control sobre la calidad de estados financieros y controles internos, con el objeto de ver la confiabilidad e integridad de la información para proteger la organización y todas las partes interesadas"[15].

El comité de auditoría tiene como objetivo:

- Supervisar la calidad y la integridad de los informes financieros;
- Supervisar la adherencia a las normas legales, estatutarias y regulatorias;
- Supervisar la adecuación de los procesos relativos a la gestión de riesgos y al sistema de controles internos, en línea con las directrices establecidas por la junta directiva;
- Supervisar las actividades de los auditores internos e independientes.

El comité de auditoría debe desarrollar papeles de supervisión de gestión de riesgos conforme hayan sido definidos por la junta directiva. La supervisión de la ejecución de las políticas, el cumplimento de las normas de gestión de riesgos, así como el acompañamiento de los indicadores-clave de riesgos deben ser objeto de informes para el consejo. Éstos, a su vez, deben incluir alertas y puntos de debate de temas relativos a los riesgos para deliberación de la junta directiva. Eso debe incluir evaluaciones periódicas de la cultura de riesgos que permea la organización.

2.3.1.4 Comité ejecutivo de gestión de riesgos corporativos[16]

Sobre la existencia de un comité ejecutivo específico de GRCorp, cabe destacar que no se trata de una exigencia regulatoria[17], pero está alineada a las mejores prácticas de gestión de riesgos

15 *IBGC,* Código das Melhores Práticas de Governança Corporativa, op. cit., *p. 79.*

16 *El IBGC entiende que los comités deben ser órganos de asesoría a la junta directiva formada por los miembros de la junta. Sin embargo, en el caso del comité ejecutivo de gestión de riesgos corporativos, fue adoptada la nomenclatura comúnmente utilizada en el mercado. Se trata, por lo tanto, de un órgano subordinado a la gerencia, con actividad diaria en la organización*

17 *Los órganos y entidades del Poder Ejecutivo Federal deben instituir un comité de gobierno, riesgos y controles. Las empresas estatales, federales deben implementar políticas de conformidad y gestión de riesgos adecuadas a su tamaño y consistentes con la naturaleza, complejidad y riesgo de las operaciones realizadas por ellas. Art. 23 brinda Instrucción Normativa Conjunta CGU/MP n. 001, de 10 de mayo de 2016.*

y controles internos. La existencia de ese comité está asociada al nivel de madurez de la organización con relación a las prácticas de gobierno corporativo y también a su madurez de GRCorp. El comité ejecutivo de gestión de riesgos es un órgano de evaluación colegiado de la gerencia, formado por los responsables directos, por los riesgos y demás ejecutivos y profesionales que puedan contribuir con el proceso decisorio de riesgos en la organización. Este comité puede ser constituido en el proceso de aprendizaje organizacional para la gestión de riesgos o en aquellas organizaciones que lidian diariamente con la adopción de riesgos y/o con operaciones de hedge. El órgano puede recomendar de forma colegiada aspectos de riesgos para ser decididos por la gerencia y proponer, en conjunto con otros órganos de gobierno, líneas de acción y directrices serán deliberadas y aprobadas por la junta directiva. El comité puede monitorear la ejecución de las políticas y el cumplimento de las normas de gestión de riesgos y hacer el acompañamiento de los indicadores-clave de riesgos, orientando decisiones cuando los indicadores presentan la necesidad de toma de decisiones. El comité puede también elaborar relatos e informes de acompañamiento para la junta directiva. cuando el proceso de gestión de riesgos de la organización esté maduro, las actividades del comité pueden ser asumidas como parte de la agenda de las reuniones de gerencia.

Se sugiere que el comité ejecutivo de riesgos sea coordinado por el gerente-presidente de la organización y tenga como miembros al gerente financiero, los gerentes operativos, la auditoría interna, asesores y otros responsables por las áreas relacionadas con los riesgos. Esa composición depende del nivel de complejidad de las operaciones de la organización, así como de la madurez de su proceso de gestión de riesgos, pero siempre debe contar con personas que posean competencias y cualidades adecuadas y que sean capaces de proporcionar supervisión independiente y objetiva, todo el tiempo. El comité puede, además, contratar profesionales calificados para actuar como especialistas.

Las principales responsabilidades del comité ejecutivo son:

- Aplicar y ejecutar las acciones relativas a los riesgos siguiendo los principios, políticas y estrategias de GRCorp de la organización;
- Evaluar el ámbito de la gestión, y sugerir alteraciones, cuando sea necesario, a la estrategia de GRCorp, para deliberación de la junta directiva;
- Monitorear y desarrollar acciones relativas a:
    a. Principales riesgos a los que la organización está expuesta (por tipo de riesgo y/o negocio) y el impacto de ellos en el perfil de riesgos de la organización;
    b. Desarrollar y perfeccionar indicadores-clave de riesgos y controles internos para monitorear la gestión de riesgos;
    c. Debatir y escoger estrategias de mitigación de riesgos evaluando alternativas recomendadas;
    d. Calcular impactos y probabilidades;
    e. Ayudar en el proceso decisivo de la gerencia, sobre todo en los casos más difíciles y complejos, integrando el proceso de análisis y cálculo de riesgos en las decisiones colegiadas o de las unidades.

2.3.1.5 Gerencia

La gerencia es directamente responsable por todas las actividades de una organización, inclusive por el GRCorp y por las actividades de control.

En cualquier empresa, el gerente-presidente es el depositario final de la responsabilidad por el modelo de GRCorp y por el sistema de controles internos. Uno de los aspectos más importantes de dicha responsabilidad es proveer los recursos necesarios para asegurar la efectividad del modelo de GRCorp. Más que cualquier otro individuo o función, es el gerente-presidente quien debe poner en práctica el tono y el nivel de madurez esperados por la junta directiva con relación al modelo de GRCorp, así como la efectividad del sistema de controles internos. Naturalmente, los gerentes de diferentes áreas tendrán diferentes responsabilidades en el GRCorp y en el sistema de controles internos. Esas responsabilidades pueden variar considerablemente, dependiendo de las características de la organización. Las responsabilidades del gerente-presidente incluye asegurarse de que todos los componentes del GRCorp estén implementados. El gerente-presidente generalmente cumple con sus responsabilidades:

- Suministrando liderazgo y direccionamiento a los altos ejecutivos. Junto a ellos, el gerente-presidente establece los valores, los principios y las principales políticas (aprobadas por la junta directiva) que constituyen la base del modelo de GRCorp y del sistema de controles internos que integra tal modelo;
- Reuniéndose periódicamente con los gerentes responsables por las principales áreas funcionales – ventas, marketing, producción, finanzas, recursos humanos – para revisar sus responsabilidades sobre la forma como administran riesgos. El director-presidente adquiere conocimientos de los riesgos inherentes a las operaciones, a las respuestas al riesgo y las mejoras en los controles necesarias, así como la condición de las iniciativas en marcha. Para poder desarrollar efectivamente su papel de liderazgo, el gerente-presidente deberá definir claramente la información que necesita, especialmente en la toma de riesgos estratégicos.

De poseer esa información, el gerente-presidente estará en condiciones de tomar decisiones con base en riesgos calculados y de monitorear las actividades y los riesgos con relación al apetito a riesgos de la empresa. En caso de alteración de las circunstancias, surgimiento de nuevos riesgos, implementación de estrategias o acciones anticipadas indiquen desalineación potencial con relación al perfil y al apetito a riesgos de la empresa, el gerente-presidente adoptará las medidas necesarias para restablecer los alineamientos y debatirá con la junta directiva las medidas que serán adoptadas, o también, si el perfil de riesgos de la empresa debe ser ajustado.

2.3.2 Agentes de defensa

2.3.2.1 Primera línea de defensa – gestores de las unidades y responsables directos por los procesos

Los gestores de las unidades y los responsables directos por los procesos son los encargados de la gestión de los riesgos relativos a los objetivos de sus unidades y/o de los procesos, así como por las actividades de control en ellos introducidos (ver Figura 2). Estas personas

entienden los objetivos estratégicos y alinean los objetivos operativos a los objetivos estratégicos. Además, orientan la aplicación de los componentes de GRCorp y de las actividades de control, en sus esferas de responsabilidad, asegurándose de que su aplicación sea consistente con el perfil y el apetito a los riesgos. En este sentido, la responsabilidad fluye en cascada, y cada ejecutivo efectivamente gerencia su área de actuación. Es importante destacar, por tanto, que la responsabilidad por el GRCorp debe ser atribuida a todos los niveles de la empresa, evitando que se convierta solo en responsabilidad de la junta directiva.

2.3.2.2 Segunda línea de defensa – GRCorp

Este grupo es responsable de fijar las políticas y metodologías – además de tener un papel importante de monitoreo del desempeño – del modelo de GRCorp. Los papeles y responsabilidades de este incluyen, entre otros:

- Ser el defensor "apoyador" de GCorp en la empresa (desde los niveles estratégicos hasta los operativos);
- Proveer política, estructura y metodología a las unidades de negocio para identificar, analizar y gerenciar efectivamente sus riesgos con el fin de dar cumplimiento a los objetivos;
- Facilitar el desafío y dirigir las actividades de GRCorp, sin que eso implique una posición de responsabilidad por el gerenciamiento corporativo de riesgos;
- Garantizar que las políticas y la estrategia de GRCorp definidas por la junta estén operando efectivamente para alcanzar los objetivos de la empresa;
- Identificar problemas actuales y emergentes;
- Identificar cambios en el apetito al riesgo implícitos de la organización;
- Auxiliar a la gerencia para desarrollar procesos y controles para gerenciar riesgos;
- Direccionar los problemas identificados a los responsables de resolverlos;
- Rendir cuentas a la junta directiva o a los comités de asesoría encargados de los temas de riesgos, si hay.

En algunas empresas, la responsabilidad de poner en operación las prácticas del sistema de control interno es compartida también con ese gestor.

2.3.2.3 Tercera línea de defensa – auditoría interna[18]

La auditoría interna desempeña un papel fundamental en la evaluación de la efectividad y determinación sobre las mejoras del GRCorp y del sistema de control interno. Además, hace parte de los sistemas de monitoreo de GRCorp y del control interno. La auditoría interna no tiene la responsabilidad primaria de establecer y mantener la estructura de GRCorp – esa tarea es responsabilidad del

18 *Definiciones extraídas del IIA, que realizó estudios, debatió con especialistas y definió el papel de los auditores internos con relación a los riesgos.*

gerente-presidente y de los profesionales que él designe –, pero es fundamental a la hora de verificar la efectividad de las políticas y normas establecidas.

Todas las actividades dentro de una empresa y no solo el control interno y el sistema de GRCorp están potencialmente dentro de la extensión de la responsabilidad de los auditores internos.

Le corresponde a la auditoría interna:

- Evaluar la fidelidad de la información, revisar la efectividad y la eficiencia de las operaciones, salvaguardar los activos asegurando el cumplimiento de las leyes, reglamentos y contratos;
- Examinar el sistema de control interno proporcionando alta dirección y una evaluación sobre su efectividad;
- Asesorar al gerente-presidente y la junta directiva, por medio del comité de auditoría, monitoreando, examinando, evaluando, informando y recomendando mejorías de adecuación en el ambiente interno y efectividad en el proceso de GRCorp.

Los auditores internos deben ser objetivos al respecto de las actividades que examinan. Esta objetividad está definida por la posición que ocupa dentro de la empresa, respondiendo directamente a la junta, reportándose al comité de auditoría y presentando informes al consejo fiscal. El ejecutivo principal de auditoría debe ser seleccionado y despedido con el consentimiento de la junta directiva o del comité auditor. El auditor interno cuenta con acceso a la gerencia, al comité de auditoría y al consejo fiscal. Los auditores internos también tienen un papel fundamental, ayudar a las áreas operativas a comprender los controles, las normas y las políticas establecidas.

2.3.3 Agentes externos

2.3.3.1 Auditoría independiente

Los auditores externos posibilitan a la gerencia y a la junta directiva, una visión singular, independiente y objetiva, que puede contribuir para que la organización logre sus objetivos de comunicación externa de información financiera.

Son responsables de emitir una opinión sobre los estados contables basados en la evaluación de conclusiones obtenidas de evidencias de auditoría y expresar esa opinión por medio de un informe escrito de acuerdo con las Normas Brasileñas de Contabilidad (ver NBC TA 700). Contribuyen en el cumplimiento de los objetivos de comunicación de información financiera de la empresa y para la gestión de riesgos, con información útil para que la administración cumpla con sus responsabilidades relativas al GRCorp y al sistema de control interno.

2.3.3.2 Órganos reguladores

Los órganos reguladores influyen directamente en la libertad económica y la esfera de actuación de la organización por la imposición de normas y conductas y por sanciones por el no cumplimiento de tales normas, o sea, regulan el ambiente de negocios con el cual la empresa está involucrada.

2.4 Nivel de madurez

Esta publicación propone los siguientes niveles de madurez con relación a la etapa de GRCorp de una organización: i) inicial, ii) fragmentado, iii) definido, iv) consolidado y v) optimizado. Existen distintas alternativas para la construcción del gobierno de GRCorp y para llegar al nivel de madurez deseado. Cada organización deberá diseñar la más adecuada a su perfil de negocio, cultura organizacional, modelo de gestión y nivel deseado de madurez con relación a sus prácticas de GRCorp.

De esa forma, podemos resaltar que el nivel de madurez en GRCorp en una organización es definido por los siguientes aspectos:

- Las acciones adoptadas para alcanzar sus metas y objetivos con relación al GRCorp y al sistema de control interno;
- El nivel de esfuerzo (tiempo e inversión) empleado para alcanzar esas metas y objetivos;
- Los resultados obtenidos, así como la eficacia y la eficiencia de las prácticas implementadas;
- El nivel de desarrollo de los profesionales con relación a esas prácticas;
- El nivel de entendimiento de madurez de la organización, así como de las oportunidades de mejora.

En última instancia, la madurez representa la comprensión de la posición actual de la empresa y debe determinar sus objetivos, además de los métodos y medios empleados para alcanzarlos.

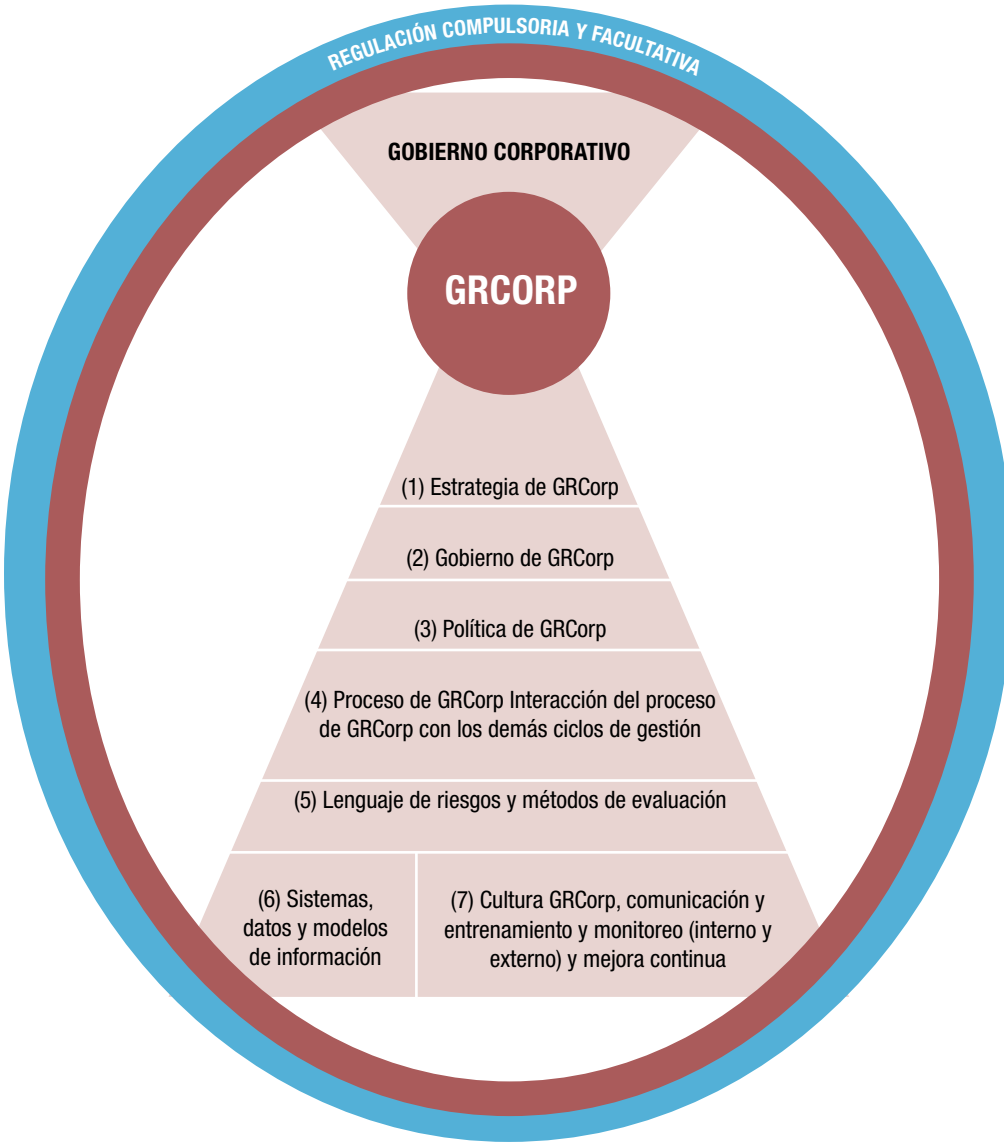
2.4.1 Midiendo la madurez

La medición de la etapa de madurez de GRCorp es una importante herramienta para que la organización pueda planificar, indicando donde está, donde desea llegar y qué acciones deberá tomar para alcanzar la etapa deseada de GRCorp.

Para esa medición, es necesario que las organizaciones evalúen capacidad actual con relación a las prácticas de GRCorp y que comprendan cómo y por qué deben perfeccionarlas. Esa evaluación permitirá que las organizaciones puedan documentar, comunicar y programar mejorías en su modelo.

La Figura 3 presenta una visión general de los componentes de GRCorp integrados al proceso de gobierno corporativo de la organización, considerando los principales elementos que deben existir para garantizar la implementación de GRCorp.

Figura 3 – Componentes de GRCorp



Por lo tanto, el nivel actual de madurez de una organización puede ser medido por medio de las respuestas encontradas para las siguientes reflexiones, relacionadas a los componentes de GRCcorp:

	COMPONENTE DE GRCORP	**REFLEXIONES**
(1)	Estrategia de GRCorp	• ¿Existen estrategias, objetivos y metas de GRCorp establecidos?
(2)	Gobierno de GRCorp*	• ¿Existe estructura organizacional con papeles y responsabilidades claramente definidos en las prácticas de GRCorp? • ¿La estructura considera el papel de la junta directiva y de la gerencia y de las tres líneas de defensas detalladas en el modelo de gobierno de GRCorp?
(3)	Política de GRCorp	• ¿Las preguntas antes mencionadas están regidas, aprobadas y divulgadas por medio de una política de GRCorp?
(4)	Proceso de GRCorp e interacción del proceso con los demás ciclos de gestión	• ¿Existe un proceso de GRCorp definido e implementado con actividades de identificación de riesgos, evaluación de riesgos (incluyendo escenarios), evaluación de las actividades de control, respuesta, monitoreo y comunicación? • ¿Existen normas de gestión de riesgos (o documento equivalente), de divulgación interna, que establezcan procedimientos, responsabilidades – inclusive de informe –, separación de funciones, fronteras de actuación y el sistema general de gobierno de la gestión de riesgos? • ¿Las prácticas de GRCorp están alineadas a las demás prácticas de control? • ¿Existe un modelo definido para la incorporación de GRCorp en los procesos decisivos y en los ciclos de gestión?
(5)	Lenguaje de riesgos y métodos de evaluación	• ¿Existe la taxonomía de riesgos (categorías) y métodos de evaluación definidos? • ¿La organización utiliza técnicas de medición?
(6)	Sistemas, dados y modelos de información	• ¿La información sobre la exposición de riesgos de la organización son compartidas con diferentes niveles de la organización y captadas de forma consistente?
(7)	Cultura de GRCorp, comunicación, entrenamiento y Monitoreo (interno y externo) y mejoría continua	• ¿El GRCorp está incluido en el proceso decisivo, en la cultura de la organización y en el día a día de la gestión del negocio? • ¿La organización evalúa la comprensión de los empleados con relación a la cultura, las prácticas de GRCorp y al sistema de control interno? • ¿Las acciones de comunicación y entrenamiento de la cultura de GRCorp son realizadas con los diferentes públicos de la organización? • ¿Los órganos de gobierno y las tres líneas de defensa monitorean permanentemente las prácticas de GRCorp? • ¿El GRCorp es realizado de forma continua?

* Hasta aquí el gobierno de GRCorp habla respecto a cómo el proceso general de gestión de riesgos, definido en la estrategia de GRCorp, es incorporado en el proceso general de gobierno de la organización, con el fin de garantizar que la estrategia de GRCorp sea efectiva y alineada con los objetivos estratégicos de la organización.

Al responder cada una de las reflexiones, la organización podrá autoevaluarse e identificar el nivel de madurez y la etapa en que se encuentra con relación a las prácticas de GRCorp, teniendo en cuenta las siete dimensiones de los componentes de GRCorp. La Figura 4 indica las características de las etapas de madurez propuestas en esta obra:

Figura 4. Medición de la madurez con relación a los componentes de GRCorp

	(1) Estrategia de GRcorp	(2) Gobierno de GRcorp	(3) Política de GRcorp	(4) Procesos de GRcorp e interacción de GRcorp del proceso de GRcorp con los demás ciclos de gestión	(5) Lenguaje de métodos y métodos de evaluación	(6) Sistema de datos y modelos de información	(7) Cultura, comunicación y entrenamiento, monitoreo y mejora continua
OPTIMIZADO	• Estrategia de gestión de riesgos claramente definida, implementada e integrada a los demás ciclos de gestión • Las metas de desempeño están alineadas con la estrategia y la gestión de riesgos	• Los objetivos están claramente definidos y alineados entre las diversas funciones de la 2ª línea de defensa con el fin de proveer valor a la organización • El modelo es referencia del sector	• Políticas y procedimientos son regularmente referenciados por terceros y por el sector. Las políticas tienen impacto sobre el ambiente de negocios externo	• Los procesos de identificación y evaluación de riesgos están bien integrados a los objetivos estratégicos • Actividades de monitoreo eficientes y coordinadas	• Utiliza enfoques estandarizados y consistentes para definir el apetito y la tolerancia a los riesgos • Escenarios futuros y pruebas de estrés son usados para explorar el análisis de los riesgos	• Tecnologías integradas habilitan a la organización a gestionar los riesgos y son consideradas altamente efectivas y reconocidas como prácticas líderes por el mercado	•La cultura de riesgos y controles es efectiva en todos los niveles de la organización • Programas de difusión son aplicados para la evolución continua de la gestión de riesgos
CONSOLIDADO	•Estrategia de gestión de riesgos claramente definida e implementada • Las metas de desempeño son monitoreadas	• Las funciones de la 2ª línea de defensa cubren de forma integral los riesgos de la organización • La estructura organizacional está bien definida y alineada a la estrategia y A los objetivos	• Políticas y procedimientos son bien desarrollados y aplicados consistentemente en toda la organización • Son continuamente actualizados de acuerdo con los cambios en la estrategia de negocios	• Los procesos de identificación y evaluación de riesgos están bien definidos, estructurados • Los gestores de negocio realizan monitoreo sistemáticamente los riesgos asociados a sus procesos	• Utiliza enfoques estandarizados y consistentes para definir el apetito y la tolerancia a los riesgos • Pruebas de estrés y análisis de escenarios son utilizados a nivel corporativo	• Tecnologías emergentes son aprovechadas para permitir que los objetivos de gestión de riesgos sean alcanzados a nivel corporativo	• La cultura de riesgos y control está incorporada en las actividades diarias de la organización y los riesgos son proactivamente tratados en los niveles de procesos y de funciones
DEFINIDO	• Estrategia de gestión de riesgos claramente definida e implementada • Las metas de desempeño son definidas	• Las funciones de la 2ª línea de defensa cubren los riesgos de negocio y generadores de valor, se pueden producir ciertos solapamientos • La estructura organizacional está definida	•Las políticas y procedimientos de GRCorp son formales y se comunican de forma consistente en toda la organización	• Un enfoque basado en riesgos es ejecutado de manera sistemática y consistentemente aplicado a nivel corporativo y por toda la organización	• Tienen un enfoque estandarizado para definir el nivel aceptable de riesgos. Aunque, no es utilizado por todas las funciones de manera consistente	• Los modelos de información y de informes están bien definidos y comprendidos. Los informes son elaborados con información correcta y completa	• Existen protocolos claros de comunicación y están abiertos para todos los empleados. La comunicación de dos vías con las partes interesadas es incentivada.
FRAGMENTADO	• La organización sabe por dónde comenzar, aunque no tenga claro a dónde quiere llegar • Las metas de desempeño existen	•Las funciones de la 2ª línea de defensa se centran en antecedentes en respuesta al cumplimiento de las obligaciones regulatorias	•Políticas y procedimientos son limitados a áreas generadoras-clave	• Los procesos de identificación, evaluación de riesgos son ejecutados como actividades distintas o separadas según la demanda	• No hay enfoques estandarizados para definir el nivel aceptable de riesgos • Son realizados análisis cualitativos y cuantitativos	• Modelos de información e informes son definidos por alta gerencia, pero no son comprendidos por la gestión o alineados en la organización	• Existe comunicación, pero no está formalmente definida. • Se realizan entrenamientos puntuales
INICIAL	•La organización no sabe cómo, quién, cuándo, dónde y por qué implementar gestión de riesgos • Las metas de desempeño existen	• Las funciones de la 2ª línea de defensa son realizadas individualmente, no están integradas a la visión estratégica.	• Políticas y procedimientos no están definidos y no hay un proceso consistente para su desarrollo y manutención	•Procesos y controles que dan apoyo a la gestión de riesgos son poco desarrollados • Se presentan mínimas actividades de monitoreo.	• No hay enfoques estandarizados para definir el nivel aceptable de riesgos • Se realizan análisis cualitativos y cuantitativos	• Modelos de información e informes son orientados por exigencias externas y no son suficientemente definidos	• No tienen un plan de divulgación implementado para formalizar las decisiones principales de la compañía con relación a las prácticas de riesgos

En este contexto, el modelo de madurez de GRCorp propuesto aquí se deriva de la función del modelo de gobierno corporativo de la organización.

Esta publicación propone la definición e implementación de todos los componentes escritos, considerando las particularidades de las organizaciones, con la participación decisiva de la junta directiva y de la gerencia en la definición y monitoreo de la estrategia de GRCorp, de gobierno de GRCorp y de la política de GRCorp.

Los agentes de la segunda línea de defensa deben racionalizar y también monitorear el funcionamiento de esos componentes que serán ejecutados por toda la organización, incluyendo la gerencia y la primera línea de defensa, representada por los gestores de las unidades y responsables directos de los procesos.

Considerando que cada organización está incluida en un contexto externo e interno determinado por su sector, nivel de actuación y regulación, además de sus intereses y modelo de negocio, para que se pueda posicionar y obtener el resultado de la medida de su madurez se recomienda que evalúe su etapa en cada dimensión y, entonces, realice la auto clasificación en los niveles de madurez propuestos.

Cabe destacar que, en general, las organizaciones presentan distintas etapas de madurez para cada dimensión analizada. Este hecho es parte del proceso. Corresponde a cada entidad evaluar su nivel de madurez en cada dimensión/etapa según su realidad y expectativas futuras con relación a las prácticas de GRCorp.

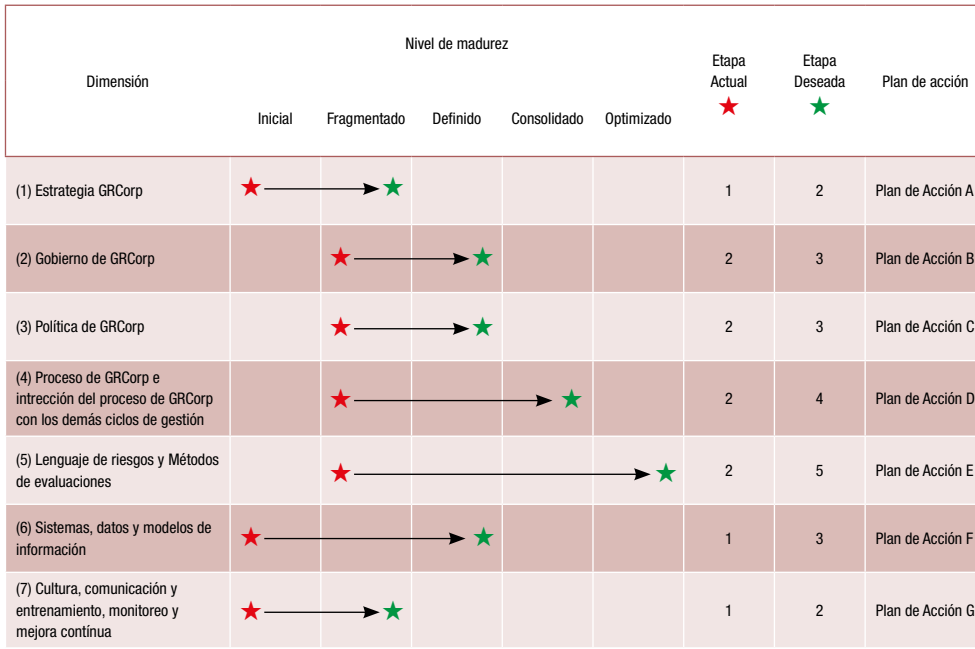
2.4.2 Consolidando los resultados de la evaluación de madurez

Una vez la organización haya realizado la evaluación del nivel de madurez de GRCorp en cada dimensión, la junta directiva debe reflejar en cual etapa debe estar la organización y, como consecuencia, la gerencia debe desarrollar las acciones necesarias y definir los plazos esperados para alcanzar las próximas etapas.

Es importante observar que el objetivo de la utilización del modelo de madurez es proveer a la organización una guía estructurada y detallada para facilitar la mejoría en aumento de la capacidad de gestión, permitiendo la definición en un enfoque realista de corto, medio y largo plazo para la estrategia de GRCorp. La evaluación del modelo de madurez permite que la organización pueda documentar, comunicar y programar mejoras en su modelo de GRCorp.

El producto final de dicha evaluación deberá incluir el análisis de la situación actual en cada dimensión, la definición de la etapa deseada y las acciones requeridas para alcanzarla, que deben ser objeto de planes de acción. También es recomendable realizar una búsqueda de estándares en la industria y comparar la organización con las empresas líderes en las prácticas de GRCorp. La Figura 5 presenta un ejemplo de consolidación de los resultados de madurez de GRCorp.

Figura 5. Ejemplo de consolidación de los resultados de madurez de GRCorp



2.4.3 Transformando los resultados de la evaluación de madurez en planes o proyectos

Una vez analizado el nivel de madurez actual y definido el nivel deseado, la organización necesita establecer las acciones necesarias para la evolución de las prácticas de GRCorp, debe designar un grupo de trabajo para actuar en cada uno de los frentes descritos, conforme se establece en el modelo de madurez. Una vez las acciones hayan sido implementadas, los planes de mejora deben ser estructurados y realizar nuevas evaluaciones.

En el proceso de evolución de las organizaciones, se deben hacer las siguientes preguntas:

- ¿Existe una persona o equipo responsable de la mejoría do GRCorp?
- ¿Existe un plan de mejora preparado para el progreso de las prácticas de GRCorp a partir del nivel actual de madurez para el próximo nivel en el modelo?
- ¿Antes de la implementación del plan de mejora, fueran medidos los beneficios que pueden obtenerse a partir del alcance del próximo nivel de madurez?

El plan de mejoría es gestionado en términos de proyecto con objetivos y recursos claros. Ese proceso de mejora continua debe ser revisado periódicamente a la luz de las expectativas y de la estrategia de GRCorp, del "tone at the top", de la identidad, de la cultura establecidas por la organización. Toda organización debe evaluar la relación costo/beneficio para determinar el nivel ideal que quiere alcanzar. En algunos casos, por ejemplo, No se puede justificar la búsqueda del nivel de madurez optimizado.

3

Modelo Conceptual de Implementación de GRCorp

3. Modelo Conceptual de Implementación de GRCorp 40

3.1 Paso 1 – Identificar y clasificar los riesgos 41

3.2 Paso 2 – Evaluar los riesgos 42

3.3 Paso 3 – Implementar la función de gestión de riesgos y estructura del control interno 44

3.4 Paso 4 – Monitorear 44

3.4.1 Definir medidas de desempeño 44

3.4.2 Preparar informes periódicos de riesgos y control 44

3.4.3 Registrar y cuantificar las pérdidas ocasionadas por la materialización de los eventos de riesgos 46

3. Modelo Conceptual de Implementación de GRCorp

A pesar de la tendencia de que las organizaciones indiquen un modelo específico de gestión de riesgos adoptado (como la ISO 31.000 y el Modelo ERM [Coso]), no existe una forma única de implementar el GRCorp, ni una única estructura adecuada para tal fin. El modelo escogido depende de la cultura de la empresa y de la complejidad y de la naturaleza del negocio.

De esta forma, es importante que las organizaciones, al considerar la implementación o construcción de un modelo de GRCorp, analicen el ambiente y el mercado en que actúan, así como su entendimiento sobre gestión de riesgos y su cultura organizacional. Ellas se pueden abordar los siguientes asuntos:

- Percepción de la propuesta de valor: La organización, por medio de la junta directiva, sobre todo, necesita asegurarse de que han comprendido la importancia de las prácticas de GRCorp para el fortalecimiento del gobierno corporativo y para alcanzar los objetivos estratégicos;
- Divulgación de cultura uniforme: La junta directiva, los gerentes y otros ejecutivos deben ejercer su liderazgo y autoridad para divulgar el GRCorp en todos los niveles de la empresa, establecer expectativas, definir responsabilidades, comprometer el público interno, provocar cambios y establecer una cultura de identificación y gestión de riesgos de forma coordinada e integrada;
- Análisis del contexto: La organización debe evaluar el contexto externo, en los aspectos culturales, socioeconómicos, políticos, legales, reglamentarios, financieros y tecnológicos. Debe evaluar también el contexto interno, considerando sus capacidades en recursos y conocimientos y las posibilidades de la aplicación práctica de los recursos y del conocimiento de la organización para la implementación de un modelo de GRCorp.

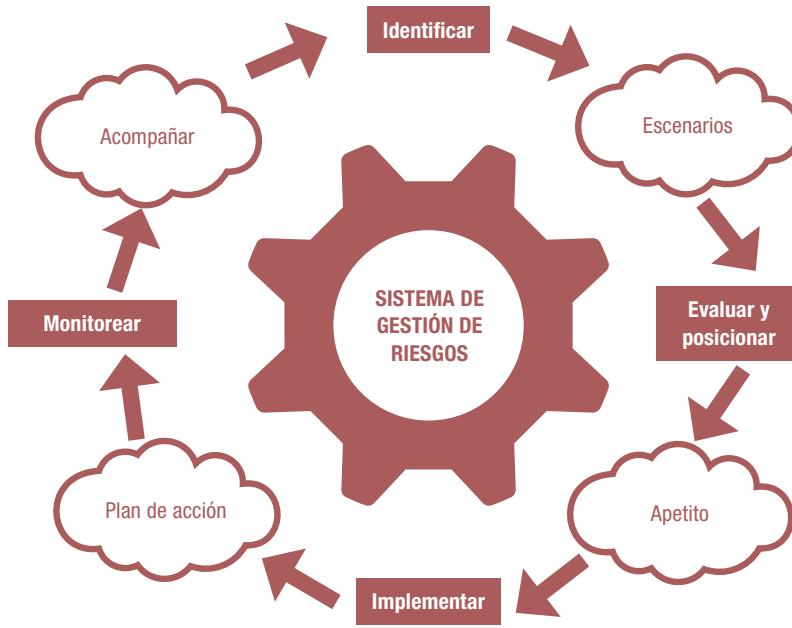
Las organizaciones tienen diferentes propósitos, valores, principios y estrategias, además de diversas estructuras organizacionales, filosofías operativas diversificadas y capacidades específicas de gestión riesgos a partir de sus perfiles. Pero, a pesar de esas singularidades, hay algo en común cuando se trata de GRCorp: lo importante es introducir en la organización la práctica de considerar los riesgos de forma estructurada en el proceso de decisión, así como de tratar los riesgos, identificando, evaluando y respondiendo de forma consistente con el modelo adoptado. La implementación del modelo de GRCorp es un proceso que debe ser continuamente mejorado y alineado al planeamiento estratégico y la identidad de la organización.

El gobierno de GRCorp está constituido por los procesos de toma de decisiones, de supervisión, de monitoreo y de garantías de funcionamiento efectivo de la estructura de gestión de riesgos. Esos procesos, unidos a los conocimientos de los gestores y directores sobre el negocio, viabilizan el desarrollo de mecanismos de toma de decisiones y del control de la exposición a riesgos.

En las empresas innovadoras, la toma de riesgos es incentivada. La creatividad, la flexibilidad y principalmente la rapidez de respuestas creativas generan la necesidad de una cultura de gestión de riesgos innovadora y un gobierno de GRCorp diferenciado y en consonancia con un ambiente altamente moderno. Esta puede ser una forma de tratamiento de los riesgos disruptivos – aquellos que amenazan tecnologías, productos o procesos existentes, por la destrucción de procesos graduales – por presentar soluciones de forma completamente revolucionaria.

Para la implementación del modelo propuesto en este cuaderno, a continuación, presentamos los principales pasos que una organización debe seguir.

Figura 6. Pasos para la implementación del GRCorp



3.1 Paso 1 – Identificar y clasificar los riesgos

Habla sobre la definición del conjunto de eventos, externos o internos, que pueden impactar (positiva o negativamente) los objetivos estratégicos de la organización, inclusive los relacionados a los activos intangibles. El proceso de identificación y análisis general de riesgos debe ser monitoreado y continuamente mejorado para identificar los riesgos eventualmente no conocidos, ya sea por ignorancia, o por la falta de funciones de probabilidad (incertidumbre), vulnerabilidad o velocidad. Este proceso debe ampliar el conocimiento de la exposición a los riesgos.

Los objetivos estratégicos orientan la manera en que la organización deberá trabajar para preservar y crear valor, lo que depende crucialmente del perfil de riesgos corporativos. La definición del perfil de riesgos es una función de la gerencia, la junta directiva debe evaluar dicho perfil (supervisar).

No hay un tipo de clasificación de riesgos que sea unánime, exhaustivo o definitivo y aplicable a todas las organizaciones; la clasificación debe ser desarrollada de acuerdo con las características de cada organización, contemplando las particularidades de su industria, mercado y campo de acción. Por ejemplo: las reservas de materiales de consumo son menos relevantes para un banco que para una industria, para la cual puede representar uno de los principales factores de riesgo. Análogamente, las variables relacionadas al "riesgo de mercado" son cruciales para un banco y pueden no ser tan relevantes para determinada organización manufacturera. Adicionalmente, el apetito y la disposición para aceptar riesgos tiene componentes subjetivos, lo que hace que las organizaciones de un mismo sector de la economía y en la misma área puedan tener perfiles y apetitos al riesgo diferentes. Sin embargo, el análisis de probabilidades e impactos de los riesgos que afectan una rama de negocios determinada puede ser general, el apetito y la disposición para aceptar riesgos tiene componentes subjetivos, lo que hace que las organizaciones de un mismo sector y en el mismo negocio presenten perfiles y apetitos al riesgo diferentes.

Una de las formas de clasificación de los riesgos consiste en diseñar una matriz que considere el origen de los eventos internos y externos a la organización y la naturaleza de los riesgos y su tipificación. Detalles adicionales sobre diversas categorías de riesgos pueden ser consultados en el Anexo 2 de este documento (Ejemplos de clasificación de riesgos).

3.2 Paso 2 – Evaluar los riesgos

Para definir qué tratamiento será dado a determinado riesgo, el primer paso consiste en determinar su efecto potencial, o sea, el grado de exposición de la organización al riesgo y la capacidad para administrarlo. Ese grado considera por lo menos tres aspectos: la probabilidad de incidencia, la vulnerabilidad de su impacto (en general medido por el impacto en el desempeño económico-financiero, en la imagen de la organización y en factores sociales, ambientales, de conformidad y estratégicos). Se debe incluir también el análisis del impacto intangible.

La cuantificación del grado de exposición no siempre es simple, puede haber interrelación entre los riesgos en dos niveles: i) los eventos pueden no ser independientes; ii) un evento determinado puede generar "múltiples impactos", o sea, efectos sobre diferentes tipos de riesgos, en diversas áreas. En ese caso, el grado de exposición dependerá del impacto financiero consolidado, de la probabilidad, de la velocidad o de la vulnerabilidad conjunta de todos los eventos y debe ser medido cuantitativamente de acuerdo con la metodología de cada empresa. Para el caso de eventos independientes que tengan efecto sobre una única área – como la mayor parte de los riesgos operativos –, el grado de exposición financiera será calculado con base técnica estudiada de manera que se adecue a los objetivos y apetitos al riesgo de cada organización.

La manera más usual de documentar el impacto, la probabilidad o la vulnerabilidad con relación a los riesgos identificados y por medio del mapa de riesgos. La Figura 7 es un ejemplo de mapa (la matriz) de riesgos. Las respuestas a los riscos deben ser desarrolladas comenzando con los riesgos encontrados en el cuadrante superior derecho (los riesgos-clave), que concentra eventos de gran probabilidad y gran impacto, o sea, de alta severidad. A medida que su grado de severidad disminuye

de intensidad, los riesgos pueden ser monitoreados y tratados en periodicidades más espaciadas, como se muestra. Pero, de ninguna forma, los llamados riesgos de severidad media (los de baja probabilidad y alto impacto, o alta probabilidad y bajo impacto) o baja deben ser ignorados, especialmente los primeros. Respetando las características de cada organización, los riesgos-clave deben ser monitoreados por la administración, y los riesgos secundarios deben ser monitoreados por los gestores de las capas inferiores de la organización. Es necesario tener en cuenta, incluso, la cantidad de riesgos en cuestión, de tal forma que su gestión no se vuelva demasiado costosa o difícil para la organización, con la debida atención a los efectos de la suma de un número grande de riesgos de bajo impacto o baja probabilidad. La organización necesita, basándose en su campo de acción y perfil, hacer una evaluación detallada de cómo gestionar esos riesgos, teniendo en cuenta su impacto para la organización y para la sociedad, estando permanentemente atenta a los efectos externos[19] generados por su actuación.

Figura 7. Matriz de riesgos

19 *Efectos de una transacción que inciden sobre terceros que no consintieron, o no participaron, no se ven reflejados completamente en los precios. Los efectos/factores externos pueden ser positivos o negativos.*

3.3 Passo 3 – Paso 3 – Implementar la función de gestión de riesgos y estructura de control interno

Para implementar el modelo y promover la cultura de GRCorp, se debe elaborar una estructura para facilitar la implementación del gobierno de GRCorp.

La gestión de los riesgos de un proceso determinado es una actividad delegada a los gestores de ese proceso, inclusive con la aplicación de modelos de mercado. A la gestión de GRCorp le corresponde integrar y orientar los esfuerzos varios, en consonancia con los objetivos establecidos por la administración, y evaluar la necesidad de establecer un comité ejecutivo de gestión de riesgos.

3.4 Paso 4 – Monitorear

3.4.1 Definir medidas de desempeño

El proceso de definición de medidas de desempeño debe incluir la gestión de riesgos y el análisis permanente de la efectividad de las medidas definidas en la medición de desempeño ajustado al riesgo y en la toma de riesgos ajustados al apetito.

El objetivo principal de la definición de medidas de desempeño y riesgo debe ser el de evaluar si los planes de acción y los respectivos controles implementados son efectivos para la evaluación del desempeño atendiendo los riesgos asumidos.

En caso de que se llegue a la conclusión de que los planes de acción y controles adoptados no son suficientes para el control de los riesgos asumidos en la búsqueda del desempeño o de la mitigación de los riesgos de la empresa, la propia gestión de los riesgos debe ser revisada. De la misma forma, es posible que la toma de riesgos sea demasiada para los objetivos esperados, conforme al apetito a riesgos definido en la estrategia, lo que también indica la necesidad de la revisión de la gestión de riesgos asociada a proceso decisorio.

Las cuestiones que deben ser consideradas en este paso son:

- Cómo se realiza la definición y gestión de los objetivos estratégicos y de las metas de desempeño;
- Cómo se realiza la gestión de los objetivos y de las metas estratégicas, orientando la identificación de los riesgos, sus respectivos controles y de los demás componentes de la estructura de riesgos;
- Cómo se realiza la gestión anticipada de cambios en el ambiente de negocios, en términos de objetivos, metas, riesgos y controles.

3.4.2 Preparar informes periódicos de riesgos y control

Debe ser enfatizada la importancia de combinar objetivos estratégicos con medidas de desempeño, factores críticos de éxito, riesgos y controles. Es importante también poner atención para que el número de indicadores sea limitado a los necesarios para la toma de decisión informada, de modo que no se perjudique su monitoreo.

Es de vital importancia la preparación de informes periódicos de riesgos, asegurando que los resultados reportados lleguen hasta la gerencia y la junta directiva. Su frecuencia depende del tipo de organización y del tipo de riesgo que está siendo reportado. Para una empresa financiera, puede ser fundamental que el informe sea diario y reportado a la administración. Para otra organización, en la cual el riesgo relevante es el contencioso o el estratégico de largo plazo, el informe periódico puede ser necesario solo cuando surjan nuevas informaciones que justifiquen su elaboración.

Los informes periódicos de riesgos y controles son piezas importantes en el modelo de GRCorp y pueden ser usados de diversas formas y finalidades, aquí enunciadas de forma no exhaustiva:

- Medir el progreso y monitorear metas-clave relativas a la contribución de las áreas para la realización de la estrategia organizacional;
- Emitir alertas cuando se hagan necesarias las acciones correctivas;
- Indicar para que la gerencia y la junta directiva evalúen el progreso referente a alcanzar las metas corporativas como un todo;
- Alertar a la gerencia y a la junta directiva de las áreas de riesgo que necesitan atención;
- Compartir mejores prácticas
- Alertar al departamento de auditoría interna al respecto de áreas de riesgo, que pueden necesitar una revisión de los controles internos.

Corresponde a la administración la evaluación continua de la adecuación y de la eficacia de su modelo de GRCorp. Este debe ser constantemente monitoreado, con el objetivo de asegurar la presencia y el funcionamiento de todos sus componentes a lo largo del tiempo. El monitoreo regular ocurre en el curso normal de las actividades de gestión. Ya que el alcance y la frecuencia de evaluaciones o revisiones específicas dependen, normalmente, de una evaluación del perfil de riesgos y de la eficacia de los procedimientos regulares de monitoreo

El monitoreo continuo realizado por el GRCorp debe incluir:

- La documentación formal relativa a los riesgos, los resultados de evaluaciones, análisis y pruebas realizados;
- El informe, la documentación interna y externa (cuando aplique) de deficiencias encontradas, así como el respectivo nivel de amenaza o exposición percibida, potencial o real, y oportunidades identificadas para exploración o refuerzo y revisión de los controles utilizados;
- El contenido de los informes relativos a los riesgos y los niveles de información estratégica: importancia de problemas o hechos anormales, principios de la cultura, implicaciones prácticas y comportamientos, información a los niveles superiores, laterales, gerencia, junta directiva, comité de auditoría, auditores y otras entidades externas.

Opcionalmente, la empresa podrá adoptar indicadores-clave de riesgos construidos a partir de intervalos de tolerancia a la pérdida. Toda vez que el indicador esté fuera del intervalo, una luz de alerta aparecerá en el panel de control de las áreas de monitoreo responsables en la segunda línea de defensa y/o auditoría interna, indicando la necesidad de algún tipo de intervención.

3.4.3 Registrar y cuantificar las pérdidas ocasionadas por la materialización de los eventos de riesgos

La gestión de GRCorp debe elaborar una base de conocimiento de pérdidas relacionadas a los negocios de forma que ayude en direccionamiento de las decisiones relacionadas a los riesgos. El proceso de constitución de la base de datos de pérdidas operativas abarque desde la implementación de controles de captura hasta la categorización y almacenamiento de las pérdidas, la modelización y el posterior reporte de las pérdidas operativas.

Las preguntas que deben ser consideradas en esta etapa son:

- ¿Cómo se realiza la definición de los controles de captura y la clasificación de los datos?
- ¿Cómo se realiza la implementación de la base de datos?
- ¿Cómo es realizado el proceso de evaluación continua?
- ¿Cómo se realiza la conciliación financiera/contable?
- Cómo debe estructurarse la base de datos de forma que proporcione información sistematizada, inclusive para soportar el tratamiento de eventos futuros aún no identificados?

Consideraciones Finales

La junta directiva debe ser la responsable de determinar los objetivos estratégicos y el perfil de riesgos de la organización. Definir su perfil consiste en identificar el grado del apetito a riesgos de la organización, así como los márgenes de tolerancia a desvíos con relación a los niveles de riesgos determinados como aceptables. La junta directiva debe establecer también la política de responsabilidad de la gerencia en: i) evaluar a cuáles riesgos puede estar expuesta la organización; ii) desarrollar procedimientos para administrarlos; y iii) evaluar, debatir y aprobar la política de riesgos propuesta por el comité ejecutivo de riesgos.

Es recomendable que los integrantes de la junta directiva tengan conocimientos sobre indicadores de desempeño para opinar sobre el asunto en cuestión, pues sin este conocimiento básico incluyendo finanzas corporativas, la gestión de riesgos corporativos no alcanzará los objetivos propuestos. Es recomendable también que la empresa tenga un programa para traer la cultura de gestión de riesgos para los nuevos miembros de la junta.

El papel fundamental de implementar una estructura sólida de gestión de riesgos el control es delegado a los gestores, con el comité de auditoría (el órgano subordinado que desempeña su función) ejerciendo la actividad de supervisión, auxiliado, cuando sea necesario, por las demás líneas de defensa.

Como punto de partida para análisis del modelo de GRCorp practicado por la organización, o para instituirlo, se sugiere que la junta directiva debata el tema con la gerencia, definiendo:

- Los riesgos que afectan el negocio y cómo están integrados a la planeación estratégica;
- Cómo son considerados y controlados los riesgos estratégicos en los procesos de decisión;

- Cómo los elementos de gestión de riesgos están articulados a las metas y a la remuneración de los ejecutivos;
- Cómo integra el GRCorp la agenda de la junta, de los comités y de los gestores;
- Quiénes son los gestores de riesgos de cada proceso y ante quien se reportan;
- Cómo es divulgada la cultura de gestión de riesgos;
- Cuáles son los informes relativos al GRCorp, quien los elabora y quien los recibe;
- Cuáles son los controles existentes para la identificación, el acompañamiento y la mitigación de los riesgos.

Los miembros de la junta directiva, a su vez, deben hacer una reflexión conjunta sobre cuál es el proceso relativo al GRCorp más adecuado para la organización, respondiendo las siguientes preguntas:

- ¿Cuáles riesgos deben ser llevados a la junta directiva y al comité de auditoría?
- ¿Cuáles temas merecen un debate profundo?
- ¿Es evaluada la relación entre riesgo y oportunidad?
- ¿Cuál debe ser el apetito a riesgos de la organización?
- ¿Cuáles son los márgenes de tolerancia para cada riesgo asumido y cómo la agrupación de riesgos afecta las tolerancias?
- ¿La junta directiva reflexiona explícitamente sobre los riesgos en sus procesos decisorios?
- ¿La junta directiva reflexiona periódicamente y recauda pruebas sobre la efectividad del ambiente y la cultura de integridad y conformidad en todos los niveles en la organización?

Esas reflexiones son necesarias para que los miembros de la junta directiva estén atentos a los riesgos que deben ser analizados por el órgano y para su papel dentro de la estructura de GRCorp de la organización. Las reflexiones ayudan a evitar penalidades y consecuencias nocivas a la organización y a sus propios miembros. La preocupación por los riesgos es fundamental para que la junta directiva cumpla “el papel de guardián de los principios, valores, objeto social y sistema de gobierno de la organización, siendo su principal componente, además de decidir los rumbos estratégicos del negocio”, de acuerdo con la 5ª edición del Código de las Mejores Prácticas de Gobierno Corporativo del IBGC en su ítem 2.1.

Referencias

ABNT (Asociación Brasileña de Normas Técnicas). *NBR ISO 31.000: 2009, Gestão de Riscos – Princípios e Diretrizes*.

Anbima (Asociación Brasileña de las Entidades de los Mercados Financieros y de Capitales). *Perspectivas: A Reforma Financeira Norte-Americana – A Lei Dodd/Frank*. Disponible en: <http://www.anbima.com.br/data/files/B2/24/B5/51/742D7510E7FCF875262C16A8/Perspectivas_20ANBIMA_20Reforma_20Americana_1_.pdf>. Consulta realizada el: 15 dic. 2016.

Baraldi, Paulo A. "Apetite e Tolerância aos Riscos". 2013. Disponible en: <www.riskatrisk.com.br/APETITE_E_TOLERANCIA_AOS_RISCOS1.pdf>. Consulta realizada el: 9 dic. 2016.

_____. "Como Alinhar Estratégias a Objetivos e Metas e ao Processo de Decisão". 2013. Disponible en: <www.riskatrisk.com.br/imagens-para-site/Alinhar.Estratégias.Metas.pdf>. Consulta realizada el: 9 dic. 2016.

_____. *Gerenciamento de Riscos Empresariais*. 2. ed. revisada y ampliada. Rio de Janeiro, Elsevier (Editora Campus), 2005.

Bernstein, P. *Desafio aos Deuses: A Fascinante História do Risco*. 3. ed. Campus, Rio de Janeiro, 1996.

BIS (Bank for International Settlements). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework (Basel II [Basileia II])*. 2005. Disponible en: <http://www.bis.org>.

Brealey, R. & Myers, S. *Financiamento e Gestão de Risco*. Porto Alegre, Bookman, 2005.

Brigham, E. F.; Gapenski, L. C. & Ehrardt, M. C. *Administração Financeira: Teoria e Prática*. São Paulo, Atlas, 2001.

Burnaby, Priscilla & Hass, Susan. "Ten Steps to Enterprise-wide Risk Management". *Corporate Governance*, vol 9, n. 5, 2009.

Coso. *Gerenciamento de Riscos Corporativos – Estrutura Integrada – Sumário Executivo Estrutura*. PriceWaterhouse-Coopers, São Paulo, 2007.

Coso Report. *Internal Control: Integrated Framework*. 1997. Disponible en: <http://www.coso.org>.

Coso II. *ERM – Enterprise Risk Management*, 2004. Disponible en: <erm.coso.org>.

Crouhy M.; Galai, D. & Mark, R. *Gerenciamento de Risco: Abordagem Conceitual e Prática – Uma Visão Integrada dos Riscos de Crédito e de Mercado*. Rio de Janeiro/São Paulo, Qualitymark/Serasa, 2004.

Doherty, Neil A. *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*. Nova York, McGraw-Hill, 2000.

Faber, M.; Manstetten, R. & Proops, J. *Ecological Economics: Concepts and Methods*. Cheltenham, Edward Elgar Publishing Ltd., 1996.

Galesne, A; Fensterseifer, J. E. & Lamb, R. *Decisões de Investimentos da Empresa*. São Paulo, Atlas, 1999.

Grinblat, M. & Titman, S. *Mercados Financeiros e Estratégia Corporativa*. Porto Alegre, Bookman, 2005.

IBGC (Instituto Brasileño de Gobierno Corporativo). *Código das Melhores Práticas de Governança Corporativa*. 5. ed. São Paulo, 2015. Disponible en: <http://www.ibgc.org.br/index.php/publicacoes/codigo-das- melhores-praticas>. Consulta realizada el: 9 dic. 2016.

_____. *Guia de Orientação para Gerenciamento de Riscos Corporativos*. São Paulo, IBGC, 2007 (Serie Cuadernos de Gobierno Corporativo, n. 3). Disponible en: <http://www.ibgc.org.br/index.php/publicacoescadernos- de-governanca>. Consulta realizada el: 9 dic. 2016.

_____. *Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos*. São Paulo, IBGC, 2008 (Serie Estudios de Caso, n. 1). Disponible en: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Consulta realizada el: 9 dic. 2016.

_____. *Gestão Integrada de Riscos: Banco Real e Brasil Telecom*. São Paulo, IBGC, 2008 (Serie Estudios de Caso, n. 2). Disponible en: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Consulta realizada el: 9 dic. 2016.

_____. *Gestão de Risco como Instrumento para a Tomada de Decisões: Votorantim Celulosa e Papel (VCP)*. São Paulo, IBGC, 2008 (Serie Estudios de Caso, n. 3). Disponible en: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Consulta realizada el: 9 dic. 2016.

_____. *Código de Conducta del IBGC*. São Paulo, IBGC, 2013. Disponible en: <http://www.ibgc.org.br/index.php/publicacoescodigo-de-conduta>. Consulta realizada el: 9 dic. 2016.

IIA (The Institute of Internal Auditors). *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles*. Ene. 2013. Disponible en: <http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf>. Consulta realizada el: 12 sep. 2016.

Jorion, P. *Value-at-Risk: A Nova Fonte de Referência para a Gestão do Risco Financeiro*. São Paulo, BM&F, 2003.

Kaplan, Robert S. & Mikes, A. "Gestão de Riscos: Um Novo Modelo". *Harvard Business Review*, jun. 2012.

NACD (National Association of Corporate Directors). *Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward*. Washington (DC), NACD, 2009.

Ross, S. A.; Westerfield, R. W.; Jaffe, J. & Lamb, R. *Administração Financeira*. Porto Alegre, Grupo AMGH, 2015.

Sarbanes-Oxley Act. *Public Company Accounting Reform and Investor Protection Act of 2002*, EUA, 2002.

Scott, H. *Risk Management and Insurance*. 2. ed. Boston, Mc Graw Hill, 2010.

Vaughan, E. J. & Elliot, C. M. *Fundamentals of Risk and Insurance*. 9. ed. Nova York, Wiley, 2003.

World Bank. *Governance and Development*. 1992.

Anexos

ANEXO 1 – Normas y regulaciones que involucran la gestión de riesgos

Debido a que sufren una evolución continua, las normas aquí citadas deben ser consultadas directamente en sus fuentes. Tampoco deben ser consideradas la única fuente para la toma de decisiones.

ISO 9.000:2015 – Instituye la mentalidad de riesgos en las empresas buscando la certificación de ISO, que deben garantizar que posean un proceso de GRCorp.

ISO 31.000:2009 – Esta ISO presenta principios, directrices, modelos y procesos para la gestión de riesgos.

ISO Guía 73:2009 – Complemento de ISO 31.000, presenta una colección de términos y definiciones relacionados a la gestión de riesgos.

Ver ambos (31.000:2009 y Guía 73:2009) en <http://www.iso.org/iso/iso31000>. Decreto Federal n. 8.420/2015 – reglamenta diversos aspectos de la Ley de Anticorrupción, tales como criterios para el cálculo de la multa, parámetros para evaluación de programas de conformidad, reglas para la celebración de los acuerdos de indulgencia y disposiciones sobre los registros nacionales de empresas sancionadas. Procedimientos que están bajo la responsabilidad de la antigua Contraloría-General de la Unión (CGU) ahora Ministerio de Transparencia, Fiscalización y Control.

Otros instrumentos normativos son:

- Ordenanza n. 909 CGU (evaluación de programas de integridad)
- Ordenanza n. 910 CGU (procedimiento para el proceso administrativo y acuerdo de indulgencia)
- Instrucciones Normativas CGU n. 01/2015 y 02/2015 (reglamenta el registro de información en el Registro Nacional de Empresas Inadecuadas y Suspendidas [Ceis] y en el Registro Nacional de Empresas Sancionadas [CNEP])
- Ordenanza Conjunta n. 2.279/2015 CGU y Secretaría de la Micro y Pequeña Empresa (reglas anticorrupción para micro y pequeñas empresas)
- Resolución CGPAR n. 18 de 10 de mayo de 2016
- Instrucción Normativa Conjunta MP/CGU n. 1 de 10 de mayo de 2016
- Ley n. 13.303 (Ley de las Estatales), de 30 de junio de 2016

ANEXO 2 – Ejemplos de clasificación de riesgos

En general, casi todos los riesgos son derivados de[20]:

- Fuentes externas (hechos ajenos a la empresa)
- Fuentes internas (originados en la organización)
- Estrategia o información para la toma de decisiones (en la búsqueda de su longevidad)

Fuentes externas

Riesgo externo o de ambiente surge cuando hay fuerzas externas que podrían alterar significativamente los pilares que sostienen los objetivos y estrategias de una organización y, en un caso extremo, sacarla de los negocios.

Se puede derivar de las fallas en la comprensión de las necesidades del cliente, del fracaso en anticiparse o reaccionar a acciones de competidores, del exceso de dependencia de proveedores o clientes, etc. Como la ventaja competitiva y la habilidad para sustentarla son cada vez más temporales, las premisas de la administración sobre el ambiente empresarial proveen un punto de partida crítico para formular y evaluar estrategias empresariales. Esas premisas incluyen el perfil estratégico de los principales competidores, tendencias demográficas y sociales, nuevas tecnologías que traen oportunidades para tener ventaja competitiva, desarrollos políticos, económicos y de regulaciones. Si la administración de una compañía no posee una comprensión uniforme de los riesgos del ambiente, sus objetivos estratégicos no tendrán foco. Las consecuencias pueden ser severas: pérdidas de parte del mercado y de ventajas competitivas. Frente a las graves consecuencias provenientes de errores estratégicos, la administración se tiene que asegurar de que las premisas del ambiente de negocios en las cuales su estrategia está basada tengan consistencia con la realidad.

Ejemplos:

- Riesgo de competitividad
- Riesgo de sostenimiento
- Riesgo de relaciones con accionistas

20 *Corresponde también destacar otro tipo de riesgo que podemos entender tiene naturalezas interna y externa, de crecimiento en escala mundial, muy ligado a conducta disruptiva generada por la nueva era de información masiva de poder colectivo generado, que viene cambiando radicalmente los modelos de negocios y empresas. El riesgo está en el llamado advenimiento y crecimiento por el mundo de las organizaciones exponenciales, detentoras de un propósito transformador masivo provocando cambios profundos, transformando e impactando industrias y economías, así como en el hecho de las organizaciones tradicionales y lineales, sus culturas, personas y dirigentes tuvieran visión y capacidad para entender y adoptar las prácticas de esa tendencia.*

- Riesgo de disponibilidad de capital
- Riesgo de desastre natural
- Riesgo político o de soberanía
- Riesgo legal y regulador
- Riesgo del mercado financiero
- Riesgo de recursos naturales
- Riesgo cibernético
- Riesgo disruptivo

Fuentes internas

El riesgo con origen en fuentes internas que normalmente inciden en el riesgo de los procesos de negocios empresariales:

- No sean claramente definidos;
- No estén adecuadamente alineados con estrategias empresariales;
- No sean ejecutados efectiva y eficazmente para satisfacer las necesidades de los clientes;
- No agreguen valor a la organización;
- Expongan recursos financieros, físicos e intelectuales significativos, a pérdidas inaceptables, apropiación indebida o mal uso.

Los riesgos del proceso incluyen:

- Riesgo operacional
- Riesgo de flujo de caja
- Riesgo de autoridad
- Riesgo de procesamiento de información/tecnología
- Riesgo de integridad
- Riesgo de satisfacción del cliente
- Riesgo de recursos humanos
- Riesgo de desarrollo de producto
- Riesgo de eficiencia y eficacia
- Riesgo de capacidad productiva
- Riesgo de desfase de desempeño
- Riesgo de ciclos
- Riesgo de fuentes de materias primas y suministros
- Riesgo de obsolescencia
- Riesgo de adherencia
- Riesgo de interrupción empresarial
- Riesgo de falla de producto/servicio
- Riesgo socio ambiental
- Riesgo de residuos vertidos y emisiones atmosféricas

- Riesgo de seguridad y salud
- Riesgo de deterioro de marca/patente

Dentro de los procesos organizacionales podemos detallar los riesgos financieros:

- Riesgo de precio
- Riesgo de derivados
- Riesgo de modelización
- Riesgo de tasa de intereses
- Riesgo de cambio
- Riesgo de commodities (materias primas)
- Riesgo de instrumentos financieros
- Riesgo de liquidez
- Riesgo de crédito
- Riesgo de concentración
- Riesgo de compensación
- Riesgo de garantía

El enfoque que ha sido considerado con mayor frecuencia está relacionado a los riesgos de comportamiento inesperado e indeseable de los funcionarios, así como las fallas de conformidad que llevan a consecuencias adversas de soborno, informes financieros fraudulentos y otros comportamientos ilegales y antiéticos.

El otro tema se refiere a la gestión de los riesgos de eventos externos incontrolables o en sistemas interconectados y complejos, con la identificación de riesgos que la empresa debe asegurar o proteger con un estimativo de la probabilidad y consecuencias de eventos súbitos y análisis de escenarios para anticipar y planear riesgos externos como los riesgos asociados a factores macroeconómicos o políticos globales.

Estrategia o información para la toma de decisiones

Riesgo de estrategia o riesgo de información para la toma de decisiones y el riesgo de que la información utilizada en el apoyo a decisiones estratégicas, operativas y financieras no sea pertinente o fidedigna.

Muchas de las decisiones son tomadas con base en medidas de desempeño o en resultados de análisis de la industria, de procesos empresariales o financieros. Si los indicadores de dichas medidas no están alineados con las estrategias empresariales o no fueran realistas, comprensibles y factibles, ellos no permitirán un enfoque adecuado y podrán incentivar decisiones que no sean compatibles con las estrategias. En ese contexto, procedimientos y tecnologías que permitan preservar las características conocidas como Cida (confidencialidad, integridad, disponibilidad y autenticidad de información y sistemas de información) son importantes.

Ejemplos:

- Riesgo de evaluación situacional
- Riesgo de actividades empresariales
- Riesgo de evaluación
- Riesgo de estructura de organización
- Riesgo de asignación de recursos
- Riesgo de planeación
- Riesgo de ciclo de vida
- Riesgo de planeación y presupuesto
- Riesgo de información contable
- Riesgo de evaluación de informes financieros
- Riesgo de evaluación de inversión
- Riesgo de informes regulados
- Riesgo de fijación de precios
- Riesgo de compromiso contractual
- Riesgo de alineamiento
- Riesgo de información reglamentada

ANEXO 3 – Modelos de política y de normas internas de gestión de riesgos

3.1 Modelo de política de GRCorp

Ítems que pueden constituir una política de GRCorp:

Objetivo

Alcance y directrices generales de la política de riesgos

Apetito a riesgos y límites aceptables para riesgos

Consideraciones sobre el alineamiento del perfil y del apetito a riesgos con las estrategias de la organización;
Consideraciones sobre los límites para riesgos y los responsables por su establecimiento y acompañamiento.

Riesgos y eventos objeto de la política de riesgos

Consideraciones sobre tipología de los riesgos que afectan la organización, de fuentes internas y externas;
Consideraciones sobre evaluaciones y tratamiento de riesgos realizados por la organización; Comentarios sobre riesgos priorizados por la organización.

Estructura organizacional para la gestión de riesgos e instancias de gobierno

Descripción concisa de la estructura organizacional de gestión de riscos;
Descripción concisa de los papeles atribuidos a las instancias de gobierno:

- Junta directiva
- Consejo fiscal
- Comité ejecutivo de gestión de riesgos
- Gerente designado como responsable general por la gestión de riesgos
- Gerencia
- Responsable por la gestión de riesgos
- Gestión de riesgos en las áreas
- Auditoría interna

Estructura de Monitoreo

Consideraciones sobre indicadores de riesgos, su acompañamiento y evaluación; Consideraciones sobre periodicidad de acompañamiento por el comité ejecutivo de gestión de riesgos, junta directiva y consejo fiscal.

Comunicación

Consideraciones sobre los procesos de comunicación y las directrices de comunicación y divulgación de información sobre riesgos en el ámbito de la organización.

3.2 Modelo de norma interna de GRCorp

OBJETIVOS DE LA NORMA INTERNA DE GESTIÓN DE RIESGOS

1. Objetivos
2. Exhaustividad
3. Autorizaciones
4. Responsables por la actualización
5. Responsables por la divulgación y distribución
6. Periodicidad de actualización
7. Público objetivo y responsabilidades
8. Cumplimiento y sanciones
9. Vigencia

ESTRATEGIA Y OBJETIVOS DE LA GESTIÓN DE RIESGOS CORPORATIVOS

1. Estrategia de la gestión de riesgos corporativos
2. Objetivos de la gestión de riesgos corporativos
3. Ciclo de vida de la gestión de riesgos corporativos

PRINCIPIOS DE LA GESTIÓN DE RIESGOS

1. Apetito a riesgo de la organización
2. Filosofías, principios, política, orientación y procedimientos
3. Modelo organizacional de la función de gestión de riesgos corporativos
4. Metodología de medición de riesgos
5. Perfil de riesgos
6. Ambiente de control
7. Límites y conformidad
8. Medida de desempeño del riesgo corporativo
9. Estructura de reporte
10. Sistema e infraestructura

MODELO DE GESTIÓN DE RIESGOS CORPORATIVOS

1. Definición de gestión de riesgos corporativos
2. Estableciendo el gobierno de gestión de riesgos corporativos
3. Modelo organizacional de la función de gestión de riesgos corporativos
4. Lenguaje común de riesgos
5. Proceso y procedimientos gestión de riesgos corporativos
6. Criterios de priorización
7. Ciclo de revisión periódica

HERRAMIENTAS UTILIZADAS EN GESTIÓN DE RIESGOS CORPORATIVOS

1. *Software*
2. Documentos complementarios

FORTALECIMIENTO DE LA CULTURA DE RIESGOS Y CONTROLES

1. Cultura de riesgos y controles
2. Plan de entrenamiento

GLOSARIO DE TÉRMINOS UTILIZADOS

1. Glosario de términos utilizados
2. Bibliografía

ANEXO 4 – Glosario

Agrupación de riesgos: Proceso en que se consideran los efectos conjuntos resultantes de diferentes riesgos o de los efectos del mismo riesgo en varios sistemas, varias áreas de negocio o diferentes procesos de la organización

Apetito a riesgos: Representa el nivel de riesgo que la organización puede aceptar, conforme es establecido por su visión y misión, indicando el grado de exposición aceptable en su búsqueda de valor.

Capacidad para el riesgo: Es definida por el impacto máximo de un riesgo que la organización puede soportar sin amenazar su continuidad.

Cultura de riesgos: La cultura de riesgos de una organización se refiere al conjunto de sus normas éticas, valores, actitudes y comportamientos aceptados y practicados, en la divulgación de la gestión de riesgos como parte del proceso de toma de decisiones en todos los niveles. Establecida por el discurso y por el comportamiento de la junta directiva y de la gerencia y del apetito a riesgos de la organización.

Dueño del riesgo: Es designado por la gerencia como el responsable por la identificación y gestión efectiva de riesgos de su área de actuación. Debe tener papeles y responsabilidades definidos para escoger y aplicar respuestas a esos riesgos y autoridad suficiente para priorizar acciones relativas a la gestión de riesgos de su área y estar integrado al proceso general de gobierno de riesgos de la organización.

Estrategia de GRCorp: La definición de expectativas, objetivos, metas, inversiones y desempeño con relación a las prácticas de GRCorp de la compañía. Ella define el punto al que la compañía quiere llegar cuando se trata de GRCorp y qué medios serán usados para alcanzar los objetivos.

Exposición al riesgo: Se refiere a la posibilidad de la organización de ser afectada por un determinado riesgo. Examinar se la exposición a determinado riesgo es importante porque puede ocurrir que una organización que actúe en determinado sector no tenga exposición a determinados riesgos que afectan otras empresas de ese sector.

IGobierno de GRCorp: Se refiere a los papeles y responsabilidad de cada uno de los agentes de gobierno corporativo de la empresa, desde los funcionarios involucrados en la gestión, que deben ser responsables por controlar riesgos directos de sus actividades, hasta los miembros de la junta directiva y de la gerencia. El flujo de información relativa al control de riesgos y a la transparencia de esos datos también es parte del gobierno de GRCorp de la compañía, que trata sobre cuáles son los foros de decisión, cuáles son los alcances de esos foros, cuáles son sus papeles y responsabilidades y cómo están compuestos. Orienta y debe estar incorporada en la política de riesgos y en la norma interna de gestión de riesgos.

Indicadores-clave de riesgos: Son los indicadores debatidos y definidos por la junta directiva y por la gerencia para la supervisión de las metas de desempeño asociadas al perfil de riesgos aceptado por la organización. Los indicadores-clave muestran niveles de alerta para actuación de la junta en la revisión de la estrategia.

Mapa (matriz) de riesgos: Herramienta que indica, gráficamente, cuáles son los riesgos de baja probabilidad e impacto, de baja probabilidad y alto impacto, de alta probabilidad y bajo impacto y, para finalizar, de alta probabilidad y alto impacto. Vea un ejemplo de mapa de riscos en el punto 3.2 de esta obra.

Madurez del modelo de gestión de riesgos: Refleja la comprensión de la etapa en que se encuentran los procesos de gestión y gobierno de riesgos de la organización. Para la evaluación de la madurez deben ser consideradas las acciones adoptadas para el alcance de metas y objetivos de GRCorp, el esfuerzo en tempo e inversión, la medición de la eficacia y eficiencia de las prácticas adoptadas, la participación de los profesionales, el entendimiento del proceso de gestión de riesgos como parte de la cultura, las estructuras organizacionales involucradas con GRCorp, la consideración de cómo los riesgos son integrados en el proceso decisivo en todos los niveles y el gobierno del proceso en su totalidad.

Norma interna de gestión de riesgos: es un documento de circulación interna de la organización que trae las orientaciones de la organización con relación al GRCorp, y que debe ser conocido por todos los funcionarios involucrados en procesos decisivos. La norma interna detalla la visión de la compañía sobre el apetito y el perfil de riesgos de la organización y establece las tolerancias para cada riesgo, con base en parámetros de indicadores-clave de riesgos. Debe tratar de los objetivos de GRCorp, traer orientaciones, el modelo organizacional de la función de GRCorp con la designación de los responsables directos por los riesgos, sus estructuras de reporte, y la integración del sistema de controles internos con el gobierno de GRCorp. La norma establece procedimientos, responsabilidades, segregación de funciones, fronteras de actuación, y operacionalización del sistema general de gobierno de la gestión de riesgos. El Anexo 3 de este cuaderno trae un modelo de norma interna de GRCorp.

Perfil de riesgos: Muestra el nivel de riesgos para un determinado desempeño y su tendencia de comportamiento cuando la organización avanza en la exploración de oportunidades o en la minimización de eventuales impactos.

Política de riesgos: Una declaración formal de la organización que describe al mercado sus principales entendimientos y su visión sobre riesgos, describiendo en líneas generales como ella hace la gestión de riesgos, con los objetivos y estrategias de la política de gestión de riscos. Trae consideraciones sobre el apetito y el perfil de riesgos de la organización, incluyendo, si es el caso, consideraciones generales sobre los riesgos para los cuales busca protección, los instrumentos utilizados para protección, la estructura organizacional de gestión de riesgos, la estructura organizacional de controles internos para la verificación de la efectividad de la política de gestión de riesgos y el proceso general de gobierno de riesgos. La política de riesgos es divulgada al mercado, así como las demás políticas declaradas por la organización y debe ser objeto de debate para conocimiento de todos los colaboradores de la organización. El Anexo 3 de esta obra trae un modelo de política de GRCorp.

Riesgo: La posibilidad de ocurrencia de eventos que afecten la capacidad de una organización de cumplir con sus objetivos.

Sensibilidad al riesgo: Habla respecto a cómo la organización es afectada por un determinado riesgo. Es determinada en función del tamaño del riesgo o de la relevancia de su impacto, de la posibilidad de su incidencia y de la capacidad y preparación de la organización para reaccionar y responder a ese riesgo.

Tolerancia al riesgo: Establece las variaciones aceptables en torno a los límites establecidos para los riesgos aceptados por una organización.

Tolerancia máxima al riesgo: Es establecida por el punto en que el perfil de riesgos encuentra la exposición aceptable determinada por el apetito a riesgos.

Patrocinio Master

Deloitte.

Deloitte ofrece servicios en las áreas de Auditoría, Consultoría Empresarial, Consultoría Tributaria, Consultoría en Gestión de Riesgos, Financial Advisory y Outsourcing para clientes de los más diversos sectores. Con una red global de firmas-miembro en más de 150 países, Deloitte reúne habilidades excepcionales y un profundo conocimiento local para ayudar a sus clientes a alcanzar el mejor desempeño, cualquiera que sea su segmento o región de actuación.

En Brasil, donde hace presencia desde 1911, Deloitte es una de las líderes del mercado y sus más de 5.500 profesionales son reconocidos por la integridad, competencia y habilidad de transformar sus conocimientos en soluciones para los clientes. Sus operaciones cubren todo el territorio nacional, con oficinas en São Paulo, Belo Horizonte, Brasília, Campinas, Curitiba, Fortaleza, Joinville, Porto Alegre, Rio de Janeiro, Recife, Ribeirão Preto y Salvador.

En el área de gestión de riesgos corporativos, Deloitte cuenta con la mayor estructura de profesionales dedicados exclusivamente a esa función en Brasil, ayudando a los clientes a dirigir todos los desafíos del género. Nuestra visión multidisciplinaria ha proporcionado también una posición diferenciada para contribuir con la mejora de la gestión corporativa en las empresas. acceda en nuestro website a una diversidad de contenidos y soluciones sobre gestión de riesgos y gobierno corporativo, entre muchos otros temas de negocios.

www.deloitte.com.br

Copatrocinio

Parker Randall Brasil

sabesp

Apoyo

- Carlos Sá
- CIP – Câmara Interbancária de Pagamentos
- Erlon Lisboa de Jesus
- Fernando Nicolau Freitas Ferreira
- Mario Filipini
- Mercedes Stinco
- Muller & Sinergy Consulting
- PFM Consultoria e Sistemas

Gestión de Riesgos Corporativos

Cuadernos de Gobierno Corporativo

Fundado el 27 de noviembre de 1995, el Instituto Brasileño de Gobierno Corporativo (IBGC), organización de la sociedad civil, es referencia nacional y una de las principales referencias en el mundo sobre gobierno corporativo. Su objetivo es generar y diseminar conocimiento al respecto de las mejores prácticas en gobierno corporativo e influenciar a los más diversos agentes en su adopción, contribuyendo para el desempeño sostenible de las organizaciones y, consecuentemente, para una mejor sociedad.

Patrocinio Master

Deloitte.

Copatrocinio

Parker Randall Brasil

sabesp

Colaboración

IDB | Invest

IBGC | Instituto Brasileiro de Governança Corporativa

Av. das Nações Unidas, 12.551
21º andar - Brooklin Novo
04578-903 - São Paulo - SP
Tel.: 55 11 3185.4200

ISBN: 978-65-86366-24-2
CBL
9 786586 366242