



Universidad de la República
Facultad de Ciencias Económicas y de Administración

Trabajo de Investigación Monográfico
para la obtención del Título de Contador Público
Plan 1990



**Análisis de alternativas
para la implementación
de un ERM exitoso en
las empresas uruguayas**

Cátedra de Control Interno
y Organización de Sistemas Contables

Integrantes: María Noel Ardao
Denis Rocha
Diego Thomasset

Tutor: Cr. Marcelo Jorge

Coordinador: Cr. Luis Sauleda

Mayo, 2009

INDICE GENERAL

<i>I</i>	<i>ADMINISTRANDO EL RIESGO</i>	<i>4</i>
<i>II</i>	<i>COMPONENTES DEL RIESGO DESDE LA PERSPECTIVA DEL ERM</i>	<i>16</i>
II.1	Identificación de eventos	16
II.2	Evaluación de Riesgo	29
II.3	Respuesta al Riesgo	49
<i>III</i>	<i>TENDENCIAS EN LA GESTIÓN DE RIESGOS</i>	<i>59</i>
<i>IV</i>	<i>TRABAJO DE CAMPO</i>	<i>63</i>
IV.1	Empresa A	63
IV.2	Empresa B	67
IV.3	Empresa C	76
<i>V</i>	<i>ANÁLISIS COMPARATIVO</i>	<i>81</i>
<i>VI</i>	<i>CONCLUSIONES</i>	<i>85</i>
<i>VII</i>	<i>ANEXO - CUESTIONARIO TRABAJO DE CAMPO</i>	<i>91</i>
<i>VIII</i>	<i>GLOSARIO</i>	<i>97</i>
<i>IX</i>	<i>BIBLIOGRAFÍA</i>	<i>102</i>

ABSTRACT

El presente trabajo está orientado al análisis de las técnicas de implementación del ERM (Enterprise Risk Management). Es así, que nuestra investigación se enfoca en precisar cuáles son las herramientas para la identificación y medición de factores de riesgo existentes, así como en las experiencias que, respecto a su uso, se pueden observar en Uruguay.

La justificación de nuestro trabajo está basada en que si bien los empresarios han tenido presente el concepto de gerenciamiento de riesgos corporativos y muchas organizaciones conocen el ERM, pocas tienen un panorama claro de cómo introducir una cultura del riesgo en la entidad, o cómo coordinar las funciones de control establecidas para mitigar dichos riesgos. En algunas empresas, se han realizado los esfuerzos por iniciar el proceso de ERM pero muchos de ellos han fracasado, o se han encontrado con dificultades a la hora de su implementación, lo que origina cierto escepticismo respecto a los beneficios esperados del ERM.

En nuestro trabajo monográfico investigamos a nivel teórico, cuáles son las medidas que aseguran la implementación de un ERM exitoso, cuáles son las herramientas con las que la Alta Dirección, la Auditoría Interna y demás integrantes de la organización deben contar, así como cuáles son los conocimientos teóricos sobre la administración de riesgos que debieran estar internalizados.

Por otro lado nuestra investigación práctica, se enfocó en tratar de establecer la metodología utilizada para la implementación de un ERM exitoso en las empresas de distinto porte y actividad radicadas en el Uruguay.

El enfoque dado al trabajo monográfico es entonces teórico - práctico, tratando de verificar la aplicación del marco teórico existente en nuestra realidad nacional.

CAPÍTULO

I



**ADMINISTRANDO
EL RIESGO**

I ADMINISTRANDO EL RIESGO

La premisa subyacente en la gestión de riesgos corporativos es que las entidades existen con el fin último de generar valor para sus grupos de interés. Todas se enfrentan a la incertidumbre, y el reto para la Dirección es determinar cuánta se puede aceptar mientras se esfuerzan en incrementar el valor para sus grupos de interés.

Todas las definiciones de riesgo presuponen que en una situación riesgosa existen varios elementos que es necesario analizar para poder llegar a controlarlo de manera razonable (probabilidad, incertidumbre, efectos), y si bien los riesgos pueden traer consecuencias negativas, no tomarlos en consideración, en algunas ocasiones, puede ser un riesgo en sí mismo, pues pueden perderse oportunidades que podrían aportar mayores beneficios.

Es importante diferenciar entre riesgo e incertidumbre. La incertidumbre existe siempre que no se conoce con seguridad qué ocurrirá en el futuro; el riesgo es la incertidumbre que afecta negativamente a la organización. La incertidumbre implica riesgos y oportunidades y posee el potencial de menoscabar o aumentar el valor. La gestión de riesgos corporativos permite a la Dirección tratar eficazmente la incertidumbre y sus riesgos y oportunidades asociados, mejorando así la capacidad de generar valor.

Se maximiza el valor cuando la Dirección establece la estrategia y los objetivos para encontrar un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad y los riesgos asociados, además de utilizar recursos eficaz y eficientemente a fin de lograr los objetivos de la entidad.

La gestión de riesgos corporativos incluye las siguientes capacidades:

Alinear el riesgo aceptado y la estrategia

En su evaluación de alternativas estratégicas, la Dirección considera el riesgo aceptado por la entidad, estableciendo los objetivos asociados y desarrollando mecanismos para gestionar los riesgos que ellos conllevan.

Mejorar las decisiones de respuesta a los riesgos

La gestión de riesgos corporativos proporciona rigor para identificar los riesgos y seleccionar entre las posibles alternativas de respuesta a ellos: evitar, reducir, compartir o aceptar.

Reducir las sorpresas y las pérdidas operativas

Las entidades consiguen mejorar su capacidad para identificar los eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costos o pérdidas asociados.

 *Identificar y gestionar la diversidad de riesgos para toda la entidad*

Cada entidad se enfrenta a múltiples riesgos que afectan a las distintas partes de la organización. La gestión de riesgos corporativos facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos.

 *Aprovechar las oportunidades*

Mediante la consideración de una amplia gama de potenciales eventos, la Dirección está en posición de identificar y aprovechar las oportunidades de modo proactivo.

 *Mejorar la dotación de capital*

La obtención de información sólida sobre el riesgo permite a la Dirección evaluar de manera eficaz las necesidades globales de capital y mejorar su asignación.

Estas capacidades, inherentes a la gestión de riesgos corporativos, ayudan a la Dirección a alcanzar los objetivos de rendimiento y rentabilidad de la entidad y a prevenir la pérdida de recursos. La gestión de riesgos corporativos permite asegurar una información eficaz y cumplir con las leyes y las normas, además de ayudar a evitar daños en la reputación de la entidad y sus consecuencias derivadas. En suma, la gestión de riesgos corporativos ayuda a una entidad a llegar al destino deseado, evitando escollos y sorpresas en el camino.

I.1.1 Eventos, Riesgos y Oportunidades

Los eventos pueden tener un impacto negativo, positivo o de ambos tipos a la vez. Los que tienen un impacto negativo representan riesgos que pueden impedir la creación de valor o erosionar el valor existente. Los eventos con impacto positivo pueden compensar los impactos negativos o representar oportunidades, que derivan de la posibilidad de que ocurra un acontecimiento que afecte positivamente al logro de los objetivos, ayudando a la creación de valor o a su conservación. La Dirección canaliza las oportunidades que surgen, para que éstas repercutan en la estrategia y en el proceso de definición de objetivos, y formula planes que permitan aprovecharlas.

I.1.2 Definición de la Gestión de Riesgos Corporativos

La gestión de riesgos corporativos se ocupa de los riesgos y oportunidades que afectan a la creación de valor o su preservación. Se define de la siguiente manera:

La gestión de riesgos corporativos es un proceso efectuado por el Consejo de Administración de una entidad, su Dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

Esta definición recoge los siguientes conceptos básicos de la gestión de riesgos corporativos:

- Es un proceso continuo que fluye por toda la entidad
- Es realizado por el personal en todos los niveles de la organización
- Se aplica en el establecimiento de la estrategia
- Se aplica en toda la entidad, en cada nivel y unidad, e incluye el adoptar una perspectiva de riesgo a nivel de la entidad
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del nivel de riesgo aceptado
- Es capaz de proporcionar una seguridad razonable al Consejo de Administración y a la Dirección de una entidad
- Está orientado al logro de objetivos dentro de categorías diferenciadas, aunque susceptibles de solaparse

La definición es amplia en sus fines y recoge los conceptos claves de la gestión de riesgos por parte de empresas y otras organizaciones, proporcionando una base para su aplicación en todas las entidades, industrias y sectores. Se centra en la consecución de los objetivos establecidos por una entidad determinada y proporciona una base para definir la eficacia de la gestión de riesgos corporativos.

En la medida que los líderes de negocios buscan nuevas formas de agregar valor a los accionistas, éstos han comenzado a interesarse en cómo la administración de riesgos está ligada a la creación del valor. Muchas industrias y organizaciones están reconociendo que los riesgos ya no son simplemente peligros que evitar, sino que en muchos casos son oportunidades que aprovechar. De hecho, muchos se están dando cuenta que el riesgo crea oportunidad, la oportunidad crea valor y, por último, el valor crea riqueza para los accionistas.

Según Suzanne Labarge, Jefe de Riesgos del Royal Bank of Canada, "el riesgo en sí mismo no es malo. Lo que sí es malo es que el riesgo esté mal administrado, mal interpretado, mal calculado o incomprendido". Una alta concentración de riesgo no necesariamente es perjudicial, todo depende de la predisposición que tenga la empresa para asumir esos riesgos.

I.1.3 Consecución de Objetivos

Dentro del contexto de misión y visión establecida en una entidad, su Dirección establece los objetivos estratégicos, selecciona la estrategia y fija objetivos alineados que fluyen en cascada en toda la entidad. La gestión de

riesgos corporativos está orientada a alcanzar los objetivos de la entidad, que se pueden clasificar en cuatro categorías:

-  *Estratégicos*: Objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo
-  *Operativos*: Objetivos vinculados al uso eficaz y eficiente de recursos
-  *Información*: Objetivos de fiabilidad de la información suministrada
-  *Cumplimiento*: Objetivos relativos al cumplimiento de leyes y normas aplicables

Esta clasificación de los objetivos de una entidad permite centrarse en aspectos diferenciados de la gestión de riesgos corporativos. Estas categorías distintas, aunque solapables (un objetivo individual puede incidir en más de una categoría) se dirigen a necesidades diferentes de la entidad y pueden ser de responsabilidad directa de diferentes ejecutivos. También permiten establecer diferencias entre lo que cabe esperar de cada una de ellas.

Dado que los objetivos relacionados con la fiabilidad de la información y el cumplimiento de leyes y normas están integrados en el control de la entidad, puede esperarse que la gestión de riesgos corporativos facilite una seguridad razonable de su consecución. El logro de los objetivos estratégicos y operativos, sin embargo, está sujeto a acontecimientos externos no siempre bajo control de la entidad; por tanto, respecto a ellos, la gestión de riesgos corporativos puede proporcionar una seguridad razonable de que la Dirección, y el Consejo de Administración en su papel de supervisión, estén siendo informados oportunamente del progreso de la entidad hacia su consecución.

I.1.4 Componentes de la Gestión de Riesgos Corporativos

La gestión de riesgos corporativos consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la Dirección conduce la empresa y cómo están integrados en el proceso de gestión. A continuación, se describen estos componentes:

Ambiente interno

Abarca el carácter de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía para su gestión, el riesgo aceptado, la integridad y valores éticos y el entorno en que se actúa.

Establecimiento de objetivos

Los objetivos deben existir antes de que la Dirección pueda identificar potenciales eventos que afecten a su consecución. La gestión de riesgos corporativos asegura que la Dirección ha establecido un proceso para fijar

objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

Identificación de eventos

Los acontecimientos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas repercuten en la estrategia de la Dirección o en los procesos para fijar objetivos.

Evaluación de riesgos

Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser gestionados y se evalúan desde una doble perspectiva, inherente y residual.

Respuesta al riesgo

La Dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.

Actividades de control

Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente.

Información y comunicación

La información relevante se identifica, capta y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación eficaz debe producirse en un sentido amplio, fluyendo en todas direcciones dentro de la entidad.

Monitoreo

La totalidad de la gestión de riesgos corporativos se supervisa, realizando modificaciones oportunas cuando se necesiten. Esta supervisión se lleva a cabo mediante actividades permanentes de la Dirección, evaluaciones independientes o ambas actuaciones a la vez.

La gestión de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro.

I.1.5 Relación entre Objetivos y Componentes

Existe una relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos, que representan lo que hace falta para lograr aquellos. La relación se representa con una matriz tridimensional, en forma de cubo.



Las cuatro categorías de objetivos; estratégicos, operativos, información y cumplimiento, están representadas por columnas verticales, los ocho componentes lo están por filas horizontales y las unidades de la entidad, por la tercera dimensión del cubo. Este gráfico refleja la capacidad de centrarse sobre la totalidad de la gestión de riesgos corporativos de una entidad o bien por categoría de objetivos, componente, unidad o cualquier subconjunto deseado.

1.1.6 Efectividad

La afirmación de que la gestión de riesgos corporativos de una entidad es eficaz, es un juicio resultante de la evaluación de si los ocho componentes están presentes y funcionan de modo eficaz. Así, estos componentes también son criterios para estimar la eficacia de dicha gestión. Para que estén presentes y funcionen de forma adecuada, no puede existir ninguna debilidad material y los riesgos necesitan estar dentro del nivel de riesgo aceptado por la entidad. Cuando se determine que la gestión de riesgos es eficaz en cada una de las cuatro categorías de objetivos, el Consejo de Administración y la Dirección tendrán la seguridad razonable de que conocen el grado de consecución de los objetivos estratégicos y operativos de la entidad, que su información es fiable y que se cumplen las leyes y las normas aplicables. Los ocho componentes no funcionan de modo idéntico en todas las entidades; su aplicación en las pequeñas y medianas empresas, por ejemplo, puede ser menos formal y estructurada. Sin embargo, estas entidades podrían poseer una gestión eficaz de riesgos corporativos, siempre que cada componente esté presente y funcione adecuadamente.

I.1.7 Contexto organizacional

Si bien nuestro trabajo de investigación se enfoca en analizar las herramientas prácticas para la implementación del ERM mediante el abordaje de tres de sus componentes; *Identificación de Eventos, Evaluación de Riesgos y Respuesta al Riesgo*, creemos necesario previamente, definir algunos aspectos del componente *Ambiente Interno* a fin de ubicarnos en el contexto de riesgo de la empresa. Nos centraremos en definir los conceptos de *Apetito* y *Tolerancia al Riesgo*.

Apetito de Riesgo

Es la cantidad de riesgo, expresado en términos cualitativos o cuantitativos, que una empresa está dispuesta a aceptar para generar valor y se considera en el establecimiento de la estrategia. Permite el alineamiento de la organización, las personas, los procesos y la infraestructura.

Tolerancia al Riesgo

Es el nivel aceptable de desviación en relación con el logro de los objetivos y se alinea con el apetito de riesgo. Al establecer las tolerancias al riesgo, la gerencia considera la importancia relativa de los objetivos relacionados.

Una organización determina su apetito de riesgo y su capacidad de tomar riesgos adicionales, de la misma manera que los inversionistas individuales equilibran su propia tolerancia ante varios riesgos contra sus ansias de mayores retornos y utilizan ese conocimiento para diversificar la cartera de acciones, bonos, y otros instrumentos financieros que posean.

Un aspecto crítico de la responsabilidad de la Administración es determinar qué riesgos y cuántos de ellos debe tomar la organización, y luego, reevaluar aquellas elecciones a medida que las circunstancias cambian. A diferencia de la Administración de Calidad Total (TQM, Total Quality Management), la que no acepta errores, el ERM sostiene que un número definido de errores puede ser tolerado, siempre y cuando el costo de protegerse de ellos sea superior que los riesgos que ellos suponen.

A modo de ejemplo, consideremos las perspectivas de un gobierno que compra chips de computadora para utilizarlos en misiles crucero y un fabricante de computadoras que compra los mismos chips para utilizarlos en computadoras personales. Ambas entidades poseen altos estándares para la calidad e integridad de los chips computacionales, pero difieren ampliamente en sus tolerancias ante fallas en ellos. El gobierno que fabrica de misiles crucero no puede tolerar ninguna falla en un chip. La probabilidad de dichas fallas puede ser baja, pero la magnitud de las consecuencias es demasiado alta para todos los stakeholders de la organización. De este modo, ese fabricante debe probar cada chip para asegurarse que cumpla completamente con los altos estándares que la organización ha establecido. Por otro lado, el fabricante de PC's no necesita probar todos sus chips porque puede, de hecho, tolerar algunas pocas fallas, ya que la magnitud de las consecuencias es considerablemente menor que la originada por las fallas de los chips en misiles crucero. Esta diferencia en el apetito de riesgo conducirá las

diferencias en las asignaciones de recursos y otras elecciones de la Administración.

I.1.8 Limitaciones

Aunque la gestión de riesgos corporativos proporciona ventajas importantes, también presenta limitaciones. Las limitaciones se derivan de hechos como que el juicio humano puede ser erróneo durante la toma de decisiones, que las decisiones sobre la respuesta al riesgo y el establecimiento de controles necesitan tener en cuenta los costos y beneficios relativos, que pueden darse fallas por error humano, que pueden eludirse los controles mediante conspiración de dos o más personas y que la Dirección puede hacer caso omiso a las decisiones relacionadas con la gestión de riesgos corporativos. Estas limitaciones impiden que el Consejo o la Dirección tengan seguridad absoluta de la consecución de los objetivos de la entidad.

I.1.9 Inclusión del Control Interno

El control interno constituye una parte integral de la gestión de riesgos corporativos, siendo una conceptualización y una herramienta más sólida para la Dirección. El control interno se define y describe en el documento *Control Interno Marco integrado*, el cual ha perdurado a lo largo del tiempo y es la base para las reglas, normas y leyes existentes. Aunque el ERM sólo recoge partes del documento, su estructura se incorpora en él a través de referencias.

I.1.10 Roles y Responsabilidades

Todas las personas que integran una entidad tienen alguna responsabilidad en la gestión de riesgos corporativos. El delegado por el Consejo es su responsable último y debería asumir su titularidad. Otros directivos apoyan la filosofía de gestión de riesgos de la entidad, promueven el cumplimiento del riesgo aceptado y gestionan los mismos dentro de sus áreas de responsabilidad en conformidad con la tolerancia establecida. El Director de riesgos, director financiero, auditor interno u otros, desempeñan responsabilidades claves de apoyo. El restante personal de la entidad es responsable de ejecutar la gestión de riesgos corporativos de acuerdo con las directrices y protocolos establecidos. El Consejo de Administración desarrolla una importante supervisión de la gestión de riesgos corporativos, es conciente del riesgo aceptado por la entidad y está de acuerdo con él. El CEO, con la colaboración del Directorio, debe definir la estrategia de gestión de riesgos de la empresa. Sin embargo, con frecuencia, esta estrategia se define involuntariamente, día a día, a través de diversas decisiones financieras y comerciales. Por ejemplo, es posible que un ejecutivo esté más dispuesto a asumir riesgos que otros o que tenga una opinión distinta respecto al nivel de riesgo que implica un proyecto dado. El resultado puede ser un perfil del riesgo con el que la compañía no se sienta cómoda o que no pueda ser manejado eficazmente. Por ello, es de vital importancia lograr consenso acerca de la estrategia.

La existencia de un área de gestión del riesgo corporativo, no exime a las unidades de negocio de la necesidad de asumir plena responsabilidad por los riesgos que deciden tomar. Las unidades de negocio comprenden mejor sus riesgos y representan la principal línea de defensa con la que cuenta una empresa para evitar asumir riesgos excesivos.

Las empresas deberían ofrecer educación y capacitación en gestión de riesgos, una materia bastante desconocida por los gerentes, y establecer incentivos eficaces que planteen las decisiones correctas sobre riesgo-retorno como una prioridad. Por ejemplo, si se analiza el desempeño de los jefes de unidades de negocio sólo por los resultados, esto podría alentar a tomar riesgos excesivos; por lo cual será necesario determinar también el desempeño ajustado por exposición al riesgo. Debería reconocerse y premiarse la conducta positiva del riesgo, e imponerse sanciones concretas a quienes no cumplan con los procesos y las políticas sobre riesgos.

Las empresas deben separar a aquellos empleados encargados de definir las políticas sobre riesgos y controlar su cumplimiento de quienes originan y administran el riesgo. El personal de ventas, por ejemplo, actúa en función de las transacciones, no siendo la mejor opción para determinar la predisposición al riesgo de una empresa y definir a qué clientes se les debe otorgar crédito.

I.1.11 Proceso de implantación

Previamente a la implantación, la Dirección debe plantearse cómo desplegar este proceso en la organización e involucrarla en él. El tamaño, complejidad, sector, cultura, estilo de gestión y otras características de una entidad afectarán al modo de implantar los conceptos y principios de la manera más eficaz y eficiente posible. Si bien se dispone de una gran variedad de opciones y enfoques, la experiencia muestra que existen determinados puntos en común a todas las organizaciones. A continuación, se proporciona una breve descripción de las principales etapas seguidas por aquellas empresas que han conseguido completar con éxito la implantación de la gestión de riesgos corporativos.

Grado de preparación del equipo líder

El establecimiento de un equipo líder, con representación de las unidades de negocio y funciones de soporte claves, incluyendo la planificación estratégica, constituye un importante primer paso. Este equipo se familiarizará a fondo con los componentes, conceptos y principios del ERM, de forma que desarrolle un conocimiento y lenguaje común, así como la base fundamental necesaria para diseñar e implantar un proceso de gestión de riesgos corporativos que aborde de manera eficaz las necesidades específicas de la entidad.

Apoyo de la Alta Dirección

Si bien la diagramación del calendario y la forma de instrumentar el apoyo varían según la organización, resulta importante que éste comience pronto y se consolide conforme avanza la implantación. El liderazgo a nivel de Dirección articula los beneficios de la gestión de riesgos corporativos y establece y comunica al resto de la organización el proyecto y las necesidades

de recursos para llevarlo a cabo. El apoyo de la Alta Dirección, cuando es directa y visible, conduce al éxito.

Desarrollo del plan de implantación

Se elabora un plan inicial para la ejecución de las siguientes etapas, estableciendo fases claves del proyecto e incluyendo la definición de flujos de trabajo, recursos y calendario. Se identifican las responsabilidades y se establece un sistema de gestión del proyecto como medio para la comunicación y coordinación del equipo. Sirve a su vez para comunicar y satisfacer las expectativas de las diversas unidades y personas, así como para gestionar adecuadamente el cambio que pueda afectar a la organización.

Diagnóstico de la situación actual

Incluye una evaluación de cómo se están aplicando actualmente las políticas y principios de gestión de riesgos corporativos en toda la organización, lo que implica determinar si existe una filosofía de dicha gestión, así como una comprensión homogénea del riesgo asumido. El equipo líder identifica también las políticas, procesos, prácticas y técnicas formales e informales aplicadas previo a la implantación, así como las capacidades existentes en la organización que permitan aplicar los principios y conceptos del ERM.

Visión de la Gestión de Riesgos corporativos

El equipo líder desarrolla un enfoque que establece el modo en que se va a aplicar la gestión de riesgos corporativos conforme su avance y cómo se integrará dentro de la organización para alcanzar los objetivos. Éste incluye la forma en que la entidad enfoca sus esfuerzos de gestión para situar en línea el riesgo aceptado con la estrategia, mejorar las decisiones de respuesta, identificar y gestionar riesgos en toda la empresa, aprovechar las oportunidades y optimizar la utilización del capital.

Desarrollo de capacidades

Este proceso proporciona, tanto la comprensión necesaria de las capacidades personales, tecnológicas y de proceso ya existentes, así como de las nuevas capacidades que habrá que desarrollar. Esto implica definir roles y responsabilidades, redefiniendo el modelo de organización.

Plan de implantación

Se actualiza y optimiza el plan inicial, se definen responsabilidades adicionales y el sistema de gestión del proyecto se modifica según sea necesario. El plan abarca habitualmente disciplinas generales de gestión de proyectos que forman parte de cualquier proceso de implantación.

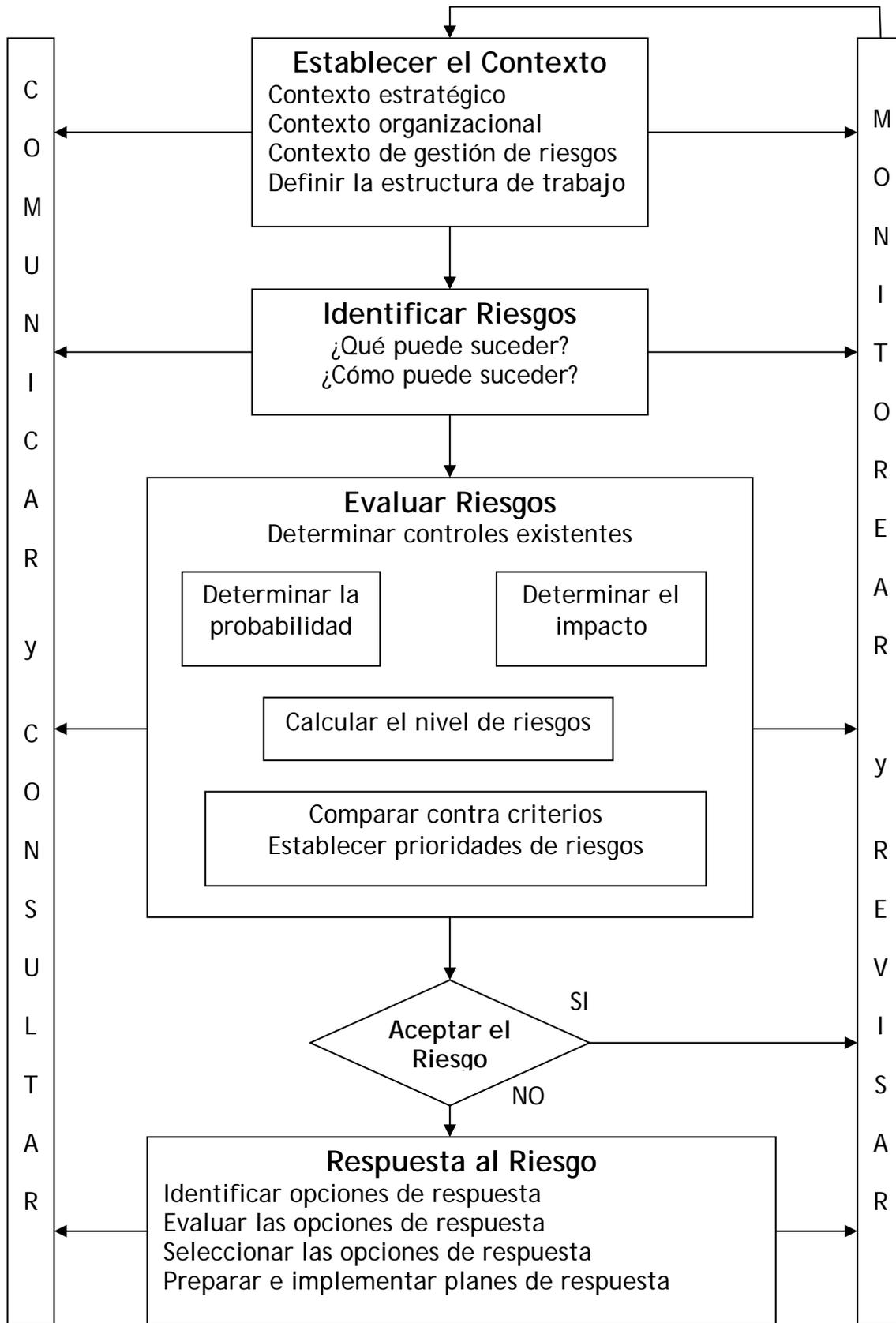
Desarrollo y puesta en marcha de la gestión del cambio

Se desarrollan acciones, según resulte necesario, para implantar y sustentar el enfoque y las capacidades de gestión de riesgos corporativos, incluyendo planes de puesta en marcha, programas de capacitación, formas de motivación y seguimiento del resto del proceso de implantación.

📌 Seguimiento

La Dirección revisa y refuerza continuamente las capacidades de gestión de riesgos como parte de su proceso continuo de gestión.

A fin de visualizar gráficamente el ciclo de la Administración del Riesgo se presenta el siguiente esquema:



CAPÍTULO II



**COMPONENTES
DEL RIESGO**

II COMPONENTES DEL RIESGO DESDE LA PERSPECTIVA DEL ERM

II.1 *Identificación de eventos*

II.1.1 Definición de Eventos

Un evento es un incidente o acontecimiento, derivado de fuentes internas o externas, que afecta a la implantación de la estrategia o a la consecución de los objetivos. Los eventos pueden tener un impacto positivo, negativo o ambos a la vez.

Al identificar eventos, la Dirección reconoce que existen incertidumbres, por lo que no sabe si el evento ocurrirá, cuándo o su impacto preciso. La Dirección considera al inicio una gama de eventos potenciales, derivados de fuentes internas o externas, sin tener por qué centrarse sobre si su impacto es positivo o negativo. De esta forma, la Dirección identifica no sólo los eventos potenciales negativos, sino también aquellos que representan oportunidades a aprovechar.

Para evitar una consideración excesiva de eventos relevantes, se realiza de forma separada la identificación y la evaluación de su probabilidad de ocurrencia e impacto, aspecto este último que corresponde a la *Evaluación de Riesgos*. Pero incluso los eventos con una probabilidad de ocurrencia relativamente baja no deberían ignorarse si es grande su impacto sobre la consecución de un objetivo importante.

II.1.2 Factores Influyentes

Miles de factores externos e internos provocan eventos que afectan a la implantación de la estrategia y a la consecución de los objetivos. Como parte de la administración de riesgos corporativos, la Dirección reconoce la importancia de entender dichos factores y el tipo de evento que puede derivarse de ellos. Los factores externos, junto con ejemplos de eventos relacionados y sus implicaciones, incluyen:

 **Económicos:** Eventos tales como los cambios de precios, la disponibilidad de capital o menores barreras a la entrada de la competencia, que generan mayores o menores costos de capital y competidores nuevos.

 **Medioambientales:** Incluyen las inundaciones e incendios, que provocan daños a las instalaciones o edificios, un acceso restringido a las materias primas o la pérdida de capital humano.

- 🖨️ *Políticos:* Incluyen la elección de los gobiernos con nuevos programas políticos, leyes y normas, que provocan, por ejemplo, nuevas restricciones o aperturas en el acceso a mercados extranjeros o impuestos mayores o menores.
- 🖨️ *Sociales:* Relacionados con los cambios demográficos, costumbres sociales, estructuras familiares, prioridades trabajo/ocio, que tienen como resultado cambios en la demanda de productos y servicios, nuevos puntos de venta, aspectos relacionados con recursos humanos y paros en la producción.
- 🖨️ *Tecnológicos:* Relativos a los nuevos medios de comercio electrónico, que generan una mayor disponibilidad de datos, reducciones de costos de infraestructura y un mayor aumento en la demanda de servicios basados en la tecnología.

Los eventos también pueden derivarse de las decisiones de la Dirección respecto a cómo se producirán. La aptitud y capacidad de una entidad para reflejar las decisiones previas, influyen en los acontecimientos futuros y afectan a las decisiones de la Dirección. Los factores internos, junto con ejemplos de eventos relacionados y sus implicaciones incluyen:

- 🖨️ *Infraestructura:* Eventos como el incremento de asignación de capital para mantenimiento preventivo y el apoyo a los centros de atención a clientes, reducen el tiempo de inactividad del equipo y mejoran la satisfacción del cliente.
 - 🖨️ *Personal:* Eventos como los accidentes laborales, las actividades fraudulentas y el vencimiento de convenios colectivos, causan pérdidas de personal disponible, daños reputacionales o monetarios y paros en la producción.
 - 🖨️ *Procesos:* Eventos como la modificación de procesos sin adecuados protocolos para la gestión de los cambios, los errores en su ejecución y la tercerización de entregas al cliente con un control insuficiente, provocan pérdidas de cuota de mercado, ineficiencias, insatisfacción del cliente y pérdida de negocios recurrentes.
 - 🖨️ *Tecnología:* Eventos como los fallos de seguridad y la potencial caída de los sistemas, dan lugar a atrasos en la producción, transacciones fraudulentas e incapacidad para continuar con las operaciones del negocio.
-

Factores externos	Factores internos
<i>Económicos</i>	<i>Infraestructura</i>
- Disponibilidad del Capital	- Disponibilidad de Activos
- Emisión de Deuda, no pago	- Capacidad de los Activos
- Concentración	- Acceso al Capital
- Liquidez	- Complejidad
- Mercados Financieros	<i>Personal</i>
- Desempleo	- Capacidad del Personal
- Competencia	- Actividad Fraudulenta
- Fusiones / Adquisiciones	- Salud y Seguridad
<i>Medioambientales</i>	<i>Procesos</i>
- Emisiones y Residuos	- Capacidad
- Energía	- Diseño
- Catástrofes Naturales	- Ejecución
- Desarrollo Sostenible	- Proveedores / Subordinados
<i>Políticos</i>	<i>Tecnología</i>
- Cambios de Gobierno	- Integridad de Datos
- Legislación	- Disponibilidad de Datos y Sistemas
- Políticas Públicas	- Selección de Sistemas
- Normas	- Desarrollo
<i>Sociales</i>	- Producción
- Demografía	- Mantenimiento
- Comportamiento del Consumidor	
- Responsabilidad Social Corporativa	
<i>Tecnológicos</i>	
- Interrupciones	
- Comercio Electrónico	
- Datos Externos	
- Tecnología Emergente	

La siguiente figura ilustra un esquema utilizado para comparar los mecanismos continuos de identificación de eventos, en relación con los factores externos e internos que los pueden originar, para ayudar a determinar si existe la necesidad de emprender acciones adicionales.

Mecanismo – Procedencia de la información	Factores externos					Factores internos			
	Económicos	Medioambiental	Político	Sociales	Tecnológicos	Infraestructura	Personal	Procesos	Tecnología
Conferencias sectoriales/técnicas	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sitios Web de empresas afines y campañas publicitarias	✓				✓				
Grupos de presión política			✓						
Encuentros sobre gestión de riesgos internos						✓	✓	✓	✓
Resultados de benchmarking	✓				✓	✓	✓	✓	✓
Procesos legales de competidores	✓			✓	✓				
Índices externos clave	✓	✓	✓	✓	✓				
Índices internos clave / Medidas de riesgo y rendimiento / Cuadros de mando						✓	✓	✓	✓
Nuevas decisiones legales	✓		✓	✓					
Informes en los medios	✓	✓	✓	✓	✓				
Informes mensuales de la dirección						✓	✓	✓	✓
Informes de analistas	✓		✓	✓					
Tablones de anuncios electrónicos y servicios de notificaciones	✓	✓	✓	✓	✓				
Publicaciones sectoriales, comerciales y profesionales	✓	✓	✓	✓	✓				
Calendario del lanzamiento de nuevos productos frente al de la competencia	✓						✓	✓	✓
Perfil de las llamadas al servicio a clientes	✓				✓			✓	
Información en tiempo real sobre la actividad de los mercados financieros	✓								

La identificación de factores internos y externos que impactan en los eventos es útil, a su vez, para la identificación efectiva del evento. Una vez que se han identificado los principales factores contribuyentes, la Dirección puede considerar su relevancia y centrarse en los eventos que puedan afectar el logro de los objetivos.

La identificación de eventos debe hacerse en forma preventiva, documentando aquellos que potencialmente pueden ocurrir, de darse determinadas circunstancias durante la consecución de las metas y objetivos institucionales. El proceso preventivo de la identificación de eventos debe ser permanente, estar integrado y ser inherente al proceso de planeación corporativo, así como al proceso de planeación particular al interior de las unidades de negocio, respondiendo a las preguntas de qué, cómo, y en qué circunstancia se pueden originar hechos que influirán en la obtención de resultados en esos dos ámbitos.

La identificación correctiva ocurre cuando se dan determinadas circunstancias no previstas originalmente, que por razones obvias no requieren de análisis para su identificación, pero sí de la valoración respectiva. Los riesgos identificados en el transcurso del ejercicio, quedarán también incorporados al plan estratégico institucional, o bien al programa anual de la unidad de negocio responsable.

II.1.3 Técnicas de Identificación de Eventos

La metodología de identificación de eventos de una entidad puede comprender una combinación de técnicas junto con herramientas de apoyo. Por ejemplo, la Dirección puede usar talleres interactivos de trabajo con un facilitador que emplee alguna herramienta tecnológica para ayudar a los participantes.

Las técnicas de identificación de eventos se aplican tanto al pasado como al futuro. Aquellas centradas en eventos y tendencias pasadas consideran temas tales como historiales de falta de pagos, cambios en los precios de los bienes y accidentes que provocan pérdidas de tiempo. Las técnicas que se centran en los riesgos futuros consideran temas tales como cambios demográficos, nuevas condiciones de mercado y acciones de los competidores.

Las técnicas varían ampliamente en su nivel de sofisticación. Aunque muchas de las más sofisticadas corresponden a sectores específicos de la industria, la mayoría se derivan de un enfoque común. Por ejemplo, tanto los servicios financieros como los del sector de la salud, utilizan técnicas de rastreo e identificación de eventos que generan pérdidas. Estas técnicas empiezan con un enfoque sobre los eventos históricos comunes. Los enfoques más básicos estudian acontecimientos derivados de percepciones del personal, mientras que las técnicas más avanzadas se basan en fuentes reales de eventos observables y luego, se introducen los datos en modelos de previsión más sofisticados. Las empresas más avanzadas en la administración de riesgos corporativos aplican una combinación de técnicas que contemplan tanto eventos pasados como potenciales futuros.

Las técnicas también varían según donde se estén aplicando dentro de una entidad. Algunas se centran en el análisis detallado de datos y crean una perspectiva ascendente de eventos, mientras que otras lo enfocan al contrario.

Los siguientes son ejemplos de algunas de las técnicas utilizadas en la Identificación de Eventos:

-  **Inventarios de eventos:** son listados detallados de acontecimientos potenciales, comunes a empresas de un sector determinado o a un proceso o actividad específica. Los Directorios utilizan listados de eventos posibles, los cuales se elaboran por el personal de la entidad o bien son listas externas genéricas y se utilizan, por ejemplo, con relación a un proyecto, proceso o actividad determinada, pudiendo resultar útiles a la hora de asegurar una visión coherente con otras actividades similares de la organización.
 -  **Análisis interno:** puede llevarse a cabo como parte de un proceso rutinario del ciclo de planificación empresarial, mediante reuniones del personal de la unidad de negocio. El análisis interno utiliza a veces la información procedente de grupos de interés de dicha unidad (clientes, proveedores y otras unidades de negocio) o de expertos en el tema ajenos a ella (expertos funcionales internos o externos a la Auditoría
-

Interna). Por ejemplo, una empresa que esté considerando introducir un nuevo producto, usa su propia experiencia histórica, junto con investigación externa de mercado que identifique eventos que hayan afectado al éxito de productos de los competidores.

- 📌 **Dispositivos de escala o umbral:** estos dispositivos alertan a la Dirección respecto a áreas con problemas, comparando transacciones o eventos actuales con criterios predefinidos. Una vez que suena la alarma, es posible que un evento exija una evaluación o una respuesta inmediata. Por ejemplo, la Dirección de una empresa hace un seguimiento del volumen de ventas en mercados seleccionados, con vista a nuevos programas de marketing o de publicidad y reorienta los recursos según los resultados. La Dirección de otra empresa sigue las estructuras de precios de los competidores y contempla los cambios en sus propios precios cuando se franquea un determinado umbral.
- 📌 **Talleres de trabajo y entrevistas:** estas técnicas identifican los eventos, aprovechando el conocimiento y la experiencia acumulada de la Dirección, el personal y los grupos de interés, a través de discusiones estructuradas. Un facilitador lidera una discusión sobre los eventos que pueden afectar a la consecución de los objetivos de la entidad o alguna de sus unidades. Por ejemplo, un controller financiero dirige un taller de trabajo con miembros del equipo contable, para identificar eventos que puedan afectar a los objetivos de informe financiero externo. Al combinar los conocimientos y la experiencia de los miembros del equipo, se identifican eventos importantes que de otro modo podrían haberse olvidado.

Para la realización de Talleres de trabajo se recomienda que se cumplan las siguientes etapas:

Previo a su desarrollo

- 📌 Identificar un moderador experimentado que dirija la sesión, gestione la dinámica de grupo y planifique el mejor modo de captar las ideas generadas
- 📌 Establecer normas básicas y llegar a acuerdos sobre ellas al inicio del taller
- 📌 Reconocer los diferentes estilos y personalidades de los participantes y considerar el modo de optimizar su contribución
- 📌 Identificar los objetivos, categorías de objetivos y categorías de acontecimientos hacia los que se desea enfocar la sesión
- 📌 Invitar a un número apropiado de participantes al taller, con un máximo de 15 personas
- 📌 Establecer de antemano expectativas realistas con respecto a los logros a los que aspira el taller

Orden del día

1. Introducción

- 📌 Explicar los antecedentes del taller y los motivos por los que ha sido invitado cada participante
- 📌 Explicar sus normas básicas

2. Explicación del proceso del taller

- Se han de considerar los acontecimientos en relación con los objetivos corporativos
- Para cada objetivo, el moderador estimulará la discusión sobre acontecimientos que surgen de los siguientes factores, así como sobre sus efectos relacionados:

Externos

Económicos
Medioambientales
Políticos
Sociales
Tecnológicos

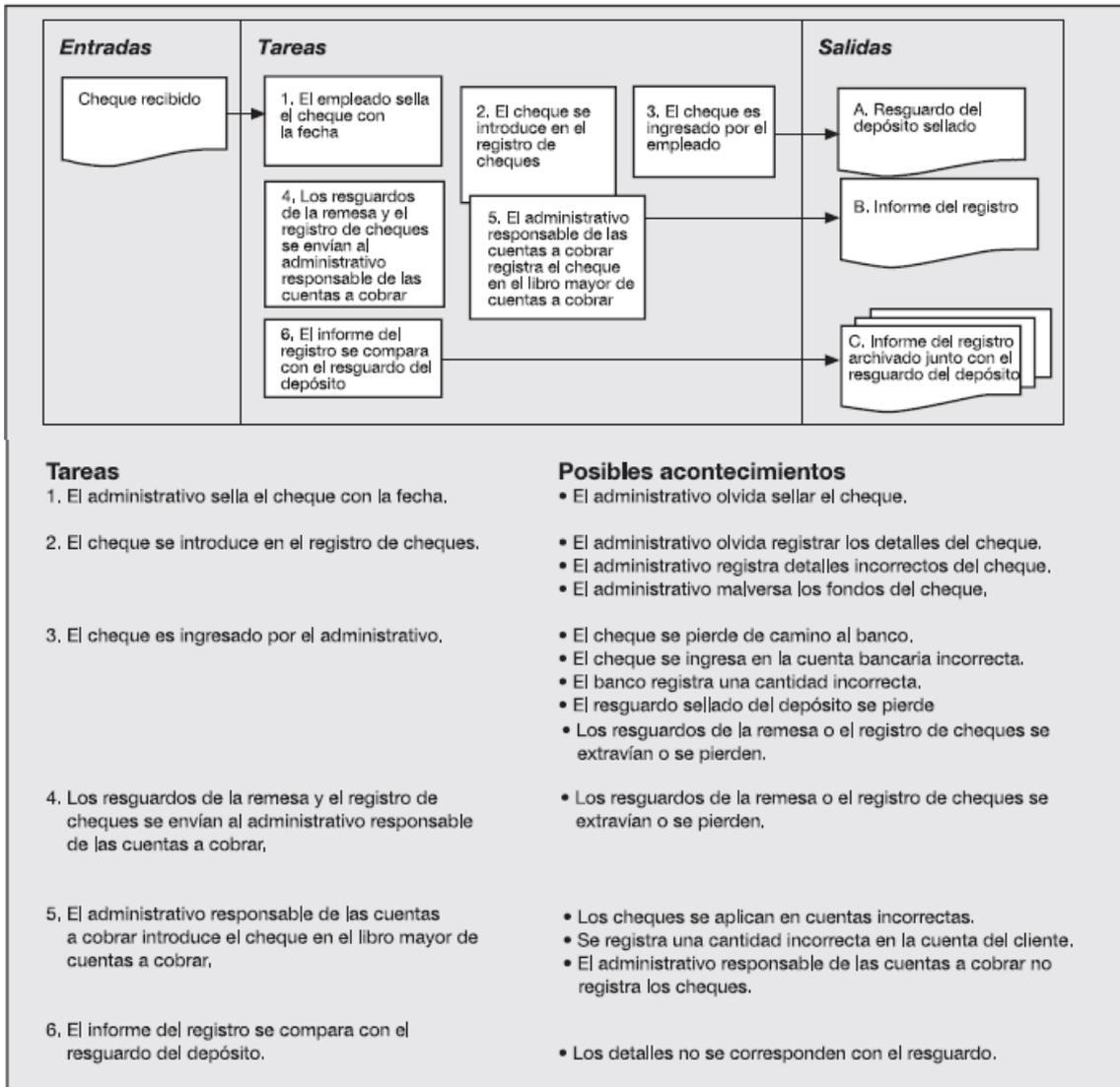
Internos

Infraestructura
Personal
Procesos
Tecnología

- Describir cómo y cuándo se emplearán las distintas modalidades de voto y las aportaciones verbales
 - Explicar el modo de documentar las ideas y conclusiones
3. Exploración de objetivos
- Identificar cada objetivo, su unidad de medida y sus respectivas metas establecidas
 - Obtener un consenso sobre la tolerancia al riesgo
 - Discutir los factores internos y externos que actúan sobre los posibles acontecimientos relacionados con dicho objetivo
 - Determinar qué hechos representan riesgos con respecto al logro del objetivo y cuáles representan oportunidades
 - Considerar de qué modo se relacionan entre sí los múltiples riesgos que afectan a un objetivo
4. Sigüientes pasos y cierre
- Distribuir los resultados del taller a todos sus participantes en un plazo de 48 horas, junto con un plan para los próximos pasos

■ **Análisis del flujo del proceso:** esta técnica considera entradas, tareas, responsabilidades y salidas que se combinan para formar un proceso. Al considerar los factores internos y externos que afectan las entradas o las actividades dentro de un proceso, una entidad identifica los eventos que podrían afectar a la consecución de los objetivos. Por ejemplo, un laboratorio médico elabora mapas de los procesos de recepción y análisis de muestras de sangre. Utilizando los mapas de proceso, considera la gama de factores que podrían afectar entradas, tareas y responsabilidades, identificando así riesgos relativos al etiquetado de muestras, trasferencias en el proceso y cambios de turno del personal.

El siguiente esquema, muestra un ejemplo del modo en que una empresa representa su proceso de cobro como base para identificar riesgos relacionados con el objetivo de depositar y registrar todos los cobros de un modo preciso y oportuno.



 **Indicadores de eventos importantes:** monitoreando datos correlacionados con los eventos, las entidades identifican la existencia de condiciones que podrían dar lugar a un acontecimiento. Por ejemplo, las instituciones financieras, reconocen desde hace mucho tiempo la correlación entre la demora en el pago de préstamos y su eventual cesación futura de pago, así como el efecto positivo de una intervención anticipada. El monitoreo de los hábitos de pago proporciona el potencial natural para que sean mitigadas por acciones oportunas.

La siguiente figura proporciona ejemplos de indicadores de eventos importantes y su respectiva alarma.

Descripción del objetivo de la unidad de negocio	Medición	Objetivo y tolerancia	Evento posible	Principal indicador	Indicadores de alarma para la unidad de negocio
Desarrollar una campaña promocional del producto en una cadena de supermercados de la región.	Número de unidades vendidas al mes por establecimiento	<i>Objetivo:</i> 1.000 unidades de producto nuevo vendidas al mes por establecimiento durante la campaña promocional. <i>Tolerancia:</i> 900 – 1.250 unidades vendidas al mes por establecimiento.	La confianza del consumidor disminuye, provocando reducciones en las compras de productos de la empresa.	Indicadores de confianza del consumidor.	El nivel de confianza del consumidor descende más de un 5%.
Crear y mantener un nivel de seguridad elevado contra intrusiones externas en los sistemas.	Número de intrusiones realizadas con éxito.	<i>Objetivo:</i> 0 por mes. <i>Tolerancia:</i> 0 por mes.	Acceso de individuos no autorizados a los sistemas de la empresa a través de puertos de Internet.	El proveedor o un tercero publican vulnerabilidades en los sistemas operativos centrales de la empresa; número de intentos no autorizados.	Nuevas vulnerabilidades críticas identificadas por terceros.
Cumplir los estándares que regulan los movimientos de material peligroso.	Volumen de derrames de materiales peligrosos transportados por el personal de la empresa.	<i>Objetivo:</i> <100 litros por año. <i>Tolerancia:</i> 0-125 litros.	La corrosión de los barriles provoca fugas de material desde los camiones durante el transporte.	Edad de los barriles empleados para transportar material peligroso.	Barriles utilizados durante más del 85% de su vida útil estimada.
Mantener un personal estable y altamente cualificado.	Rotación de los considerados mejores empleados.	<i>Objetivo:</i> Rotación de los mejores empleados <10%. <i>Tolerancia:</i> 2% - 12%.	Los mejores empleados abandonan su puesto.	Moral de los mejores empleados.	Respuestas de insatisfacción “alta” o “moderada” por parte de los mejores empleados en la encuesta anual realizada a ellos.

 **Seguimiento de datos para eventos con pérdidas:** los registros de datos sobre eventos individuales con pérdidas en el pasado son una fuente útil de información para identificar las tendencias y causas principales. Una vez que se identifica una causa, la Dirección puede averiguar qué es más efectivo, si evaluarla y tratarla o afrontar los

eventos individuales. Por ejemplo, una empresa que opera una gran flota de automóviles mantiene una base de datos de los reclamos por accidentes y, mediante su análisis, averigua que un porcentaje desproporcionado de accidentes, tanto en número como en valor monetario, se vincula a conductores del equipo en ciertas unidades, localizaciones geográficas y franjas de edad. Este análisis otorga a la Dirección las herramientas para identificar las causas principales de los eventos y tomar acciones.

La Dirección selecciona técnicas que encajen con su filosofía de administración de riesgos, las cuales aseguran que la entidad desarrolle las capacidades necesarias de identificación de eventos y que estén operativas las herramientas de apoyo. Por encima de todo, la identificación de eventos necesita ser sólida, ya que forma la base de los componentes de la evaluación de riesgos y la respuesta a ellos.

II.1.4 Interdependencia de Eventos

En general, los eventos no ocurren de forma aislada; un acontecimiento puede hacer que se desencadene otro, por lo que pueden ocurrir de forma concurrente. En la identificación de eventos, la Dirección debería entender cómo éstos se relacionan entre sí. Evaluando estas relaciones, se puede determinar dónde mejor deberían aplicarse los esfuerzos en la administración de riesgos.

Como ejemplos se pueden citar los siguientes:

- Un cambio en el tipo de interés de un banco central afecta los tipos de cambio de moneda extranjera, relevantes para las ganancias y pérdidas en las transacciones de una entidad.
- Una decisión para ampliar la formación en marketing puede mejorar las capacidades de venta y la calidad del servicio, lo que dará lugar a un aumento de la frecuencia y volumen de los pedidos recurrentes de clientes.
- Una decisión para entrar en una nueva línea de negocio, con incentivos de rendimiento importantes, puede incrementar los riesgos de error en la aplicación de principios contables y de que se genere una información fraudulenta.

II.1.5 Categorías de Eventos

Puede ser útil agrupar los eventos potenciales en categorías. Al agregarlos horizontalmente en toda la entidad y verticalmente dentro de las unidades operativas, la Dirección desarrolla un entendimiento de las relaciones entre eventos, obteniendo una mejor información como base para la evaluación del riesgo. Mediante esta agregación de eventos similares, la Dirección puede determinar mejor las oportunidades y riesgos.

La clasificación de eventos por categorías también permite a la Dirección considerar la totalidad de los esfuerzos aplicados a su identificación. Por ejemplo, una empresa puede haber clasificado los eventos relacionados con los cobros de deudores en una única categoría denominada "no pago de

créditos". Si la Dirección estudia los eventos relacionados con esta categoría, puede evaluar si se han identificado todos los posibles eventos significativos relacionados con dicho no pago.

Algunas empresas desarrollan categorías de eventos basadas en la clasificación de sus objetivos por categorías, usando una jerarquía que empieza con los objetivos de alto nivel y luego, baja en cascada hasta los objetivos relevantes para las unidades organizacionales, funciones o procesos de negocio.

II.1.6 Distinción entre Riesgos y Oportunidades

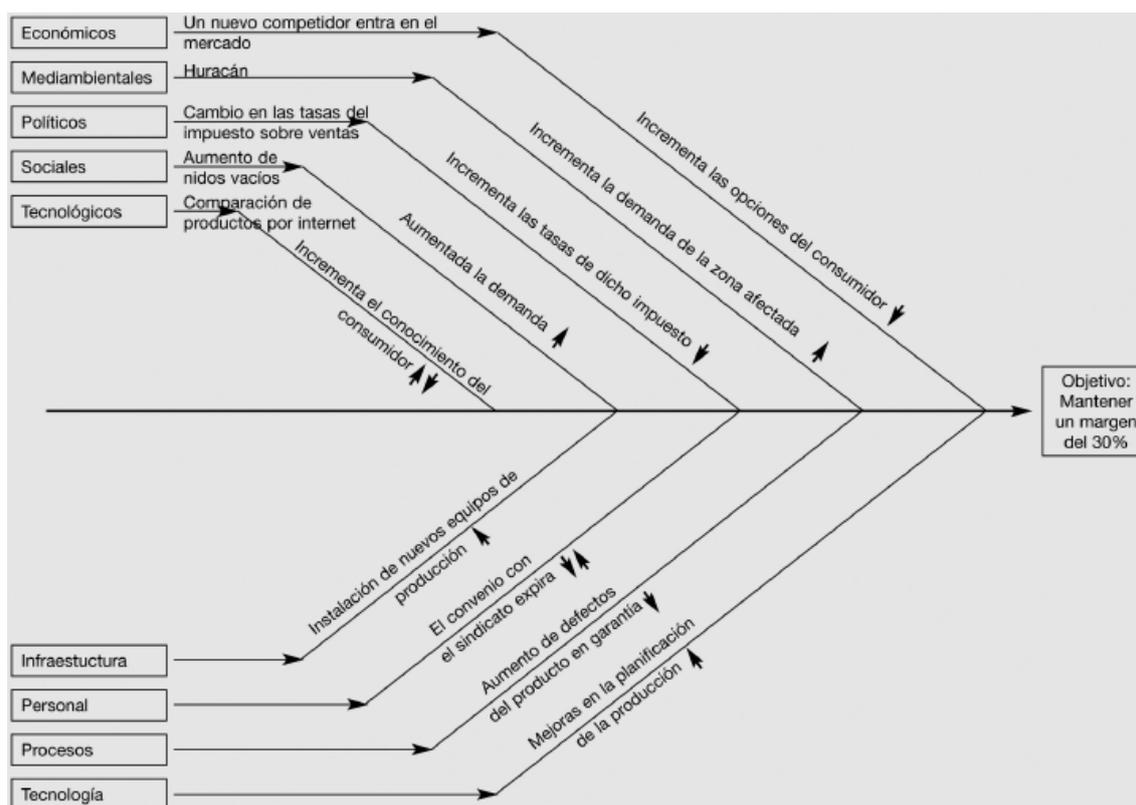
Los eventos, si ocurren, tienen un impacto negativo, positivo o de ambos tipos a la vez. Los de signo negativo representan riesgos que requieren la evaluación y respuesta de la Dirección. Por tanto, un riesgo es la posibilidad de que ocurra un evento que afecte de modo adverso a la consecución de objetivos.

Los eventos de signo positivo representan oportunidades. Una oportunidad es la posibilidad de que ocurra un evento que afecte positivamente a la consecución de objetivos y a la creación de valor. Los eventos que implican oportunidades son canalizados hacia los procesos de la Dirección en que se establecen la estrategia y los objetivos de la entidad, de forma que puedan formularse acciones para aprovechar las oportunidades. Los eventos que compensen el impacto negativo de los riesgos deben tenerse en cuenta por parte de la Dirección al evaluar los riesgos y darle respuesta.

Ejemplo:

Objetivo: Lograr un margen del 30% en los productos.

Para ello es necesario determinar qué factores y acontecimientos afectan la demanda del producto y su costo de producción, ya que ambos podrían afectar el logro del objetivo.



II.1.7 Puntos a evaluar

Para la autoevaluación por parte de la administración o la evaluación independiente de la calidad de los elementos de esta etapa, se deben considerar como mínimo los siguientes puntos:

- El compromiso de la Dirección en apoyo a las acciones para la determinación de factores de riesgo externos e internos
- La idoneidad de los mecanismos para identificar eventos de riesgos internos y externos
- La identificación de todos los riesgos importantes que pueden impactar sobre cada objetivo relevante establecido para las distintas actividades
- La documentación de las acciones efectuadas para conocer los factores de riesgo
- El grado de participación de los funcionarios y empleados clave en la determinación de los factores de riesgo
- El uso dado a los resultados y el grado de coherencia con las decisiones adoptadas
- El grado de comunicación de los estudios realizados
- La existencia de mecanismos dentro de la organización para identificar acontecimientos o eventos relacionados con sus objetivos
- La confiabilidad de la metodología utilizada para identificar eventos que puedan afectar el logro de los objetivos
- Los mecanismos de actualización e investigación de nuevos acontecimientos

II.1.8 Caso de estudio

Como ejemplo práctico de un análisis integral de gestión de riesgos, tomamos el estudio realizado por el departamento de Auditoría Interna de una empresa estatal de servicios, a los efectos de observar su implementación en relación a los tres componentes estudiados, y respecto a la Matriz de Riesgos utilizada por la misma.

En cuanto al componente desarrollado en este capítulo, las etapas que se llevan a cabo son las siguientes:

-  Se determinan los recursos del proceso
-  Se seleccionan amenazas críticas
-  Se establecen escenarios de riesgo
-  Se seleccionan factores de vulnerabilidad, (humano, ambiental, económico, operacional, de imagen, de mercado e de información)

En los siguientes capítulos se realizarán las consideraciones sobre este caso vinculadas a cada componente.

II.2 Evaluación de Riesgo

II.2.1 Contexto de la Evaluación de Riesgos

Los factores externos e internos determinan qué eventos pueden ocurrir y hasta qué punto afectarán a los objetivos de una entidad. Aunque algunos factores son comunes a empresas de un mismo sector, los eventos resultantes son a menudo únicos para una entidad determinada, debido a sus objetivos establecidos y a sus decisiones anteriores. En la administración de riesgos, la Dirección tiene en cuenta la mezcla de potenciales eventos futuros relevantes para la entidad y sus actividades, dentro del contexto de los aspectos que conforman el perfil de riesgo de la entidad, como son su dimensión, la complejidad de sus operaciones y el grado de regulación de sus actividades.

Al evaluar los riesgos, la Dirección considera los eventos esperados e inesperados. Muchos de éstos son rutinarios y recurrentes y ya se contemplan en los programas de gestión y presupuestos operativos, pero otros son inesperados. La Dirección evalúa el riesgo de los eventos potenciales inesperados y, si todavía no lo ha hecho, los eventos esperados que puedan tener un impacto significativo en la entidad.

El término “evaluación de riesgos”, no sólo se aplica en relación a una actividad puntual, sino que cuando se analiza dicho componente en el contexto de la administración de riesgos, éste constituye una continua e iterativa interacción de acciones que tienen lugar a través de la entidad.

II.2.2 Clasificación de Riesgos

El riesgo se presenta de cuatro formas principales; riesgo de mercado; de crédito, operacional y de volumen de negocio.

- El riesgo de mercado adopta la forma de una exposición a los movimientos adversos de los precios, tales como el valor de las acciones, los tipos de cambios de las divisas, las tasas de interés o los spreads y los precios de los commodities. A modo de ejemplo, Ford se vio afectada por el riesgo de mercado en el año 2002 cuando los precios del paladio se desplomaron y tuvo que asumir una importante depreciación en sus existencias.
 - El riesgo de crédito es la exposición a la posibilidad de que un deudor o una contraparte no cumpla sus obligaciones contractuales. Por ejemplo, en el año 2002, el Banco de Nueva York anunció que incrementaría su provisión de créditos vencidos en 185 millones de dólares, hasta un total de 225 millones para el tercer trimestre del año, debido principalmente, a los
-

préstamos que había concedido a empresas de telecomunicaciones.

- El riesgo operacional es la exposición a pérdidas debido a procesos y sistemas internos no adecuados y/o eventos externos. Así por ejemplo, Allfirst, una filial con sede en Baltimore de Allied Irish Banks, perdió 691 millones de dólares a causa de un solo intermediario cuyas prácticas delictivas pasaron desapercibidas durante 5 años, hasta su detección en el 2002.
- El riesgo de volumen de negocio es la exposición a la volatilidad de los ingresos, que surge como consecuencia de cambios en la demanda, en la oferta, o en la competencia. Así por ejemplo, la compañía aérea líder en los EEUU, United Airlines, solicitó en el 2003 amparo bajo el capítulo 11 del código estadounidense de quiebras, después de que el descenso de la demanda afectara sus ingresos.

Los cuatro tipos de riesgo afectan a cada industria de forma diferente, por lo tanto, cada empresa debería desarrollar una taxonomía construida sobre estas categorías de riesgo. Así por ejemplo, en el caso de la industria farmacéutica, una empresa puede enfrentar riesgo de volumen de negocio si alguno de sus rivales introdujera en el mercado una medicina superior, y riesgo operacional si la inesperada retirada del mercado de alguno de sus productos redujera sus ingresos. Además, las empresas deberían considerar cómo clasificar y evaluar el riesgo asociado a investigación y desarrollo de productos, a fin de identificar los riesgos asociados al eventual hecho de que una nueva medicina no fuera aprobada por la autoridad sanitaria o no lograra los requisitos de seguridad durante la realización de pruebas clínicas.

Las empresas no sólo deben comprender los tipos de riesgo que asumen, sino que también deben saber el monto de capital en juego. A su vez deberían comprender la forma en que los riesgos asumidos por las distintas unidades de negocios podrían estar vinculados entre sí y el efecto sobre el nivel general de riesgo. Dicho en otras palabras, las empresas necesitan una visión de conjunto. Por ejemplo, si la industria aérea se desplomara repentinamente, podría darse el caso de que American Express quedara, como resultado de ello, expuesta a tres tipos de riesgos: riesgo de volumen de negocio en sus servicios relacionados a viajes, riesgo de crédito asociado a su negocio de tarjetas (el riesgo de tener que reembolsar tickets pagados pero no usados) y por último, el riesgo de mercado de las inversiones efectuadas en bonos de aerolíneas o en contrato de arriendo de aviones por su propia división de seguros.

II.2.3 Riesgo Inherente y Riesgo Residual

De acuerdo al ERM los riesgos se pueden clasificar en: riesgo inherente y riesgo residual. El primero es aquél al que se enfrenta una entidad en ausencia de acciones de la Dirección para modificar su probabilidad o impacto. El riesgo residual es el que permanece después de que desarrolla sus

respuestas a los riesgos. Por lo tanto, la Dirección considera a la vez ambos conceptos de riesgo. La evaluación de riesgos es aplicada primero a los riesgos inherentes, y una vez que la respuesta a los riesgos ha sido incorporada, la Dirección considera el riesgo residual.

II.2.4 Estimación de Probabilidad e Impacto

La incertidumbre de los eventos potenciales se evalúa desde dos perspectivas; probabilidad e impacto. La primera representa la posibilidad de que ocurra un evento determinado, mientras que la segunda refleja su efecto. Ambos términos pueden encontrarse también como frecuencia, severidad, seriedad o consecuencia.

Es una tarea difícil y llena de retos la determinación de cuánta atención hay que prestar a la evaluación de la gama de riesgos a los que se enfrenta una organización. La Dirección reconoce, que por lo general, no merece ulterior consideración un riesgo con poca probabilidad de ocurrencia y escaso impacto potencial. Por otro lado, exige una atención considerable un riesgo con alta probabilidad de ocurrencia y significativo impacto potencial. Las circunstancias entre ambos extremos requieren juicios difíciles. Es importante que el análisis sea racional y cuidadoso.

El horizonte de tiempo usado para evaluar los riesgos debería ser consecuente con el horizonte de tiempo de la estrategia y objetivos correspondientes. Como estos dos conceptos apuntan en muchas empresas a horizontes de tiempo entre el corto y medio plazo, la Dirección se centra en los riesgos asociados con estos plazos de tiempo. Sin embargo, algunos aspectos de la orientación y objetivos estratégicos se extienden hasta el largo plazo. Como resultado, la Dirección necesita ser conciente de las franjas de tiempo más largas y no ignorar los riesgos que pueden aparecer.

Por ejemplo, una empresa dedicada a la producción de lácteos, puede tener en cuenta el riesgo de interrupción de sus operaciones a causa de una severa sequía. Sin un horizonte de tiempo específico para la evaluación de riesgos, la probabilidad de que una sequía supere los seis meses es alta. Sin embargo, la probabilidad de que una sequía de tal intensidad suceda dentro de dos años es sustancialmente menor. Al establecer un horizonte de tiempo, la empresa entiende mejor la importancia relativa del riesgo y mejora su capacidad para comparar riesgos múltiples.

La Dirección usa medidas de desempeño para determinar el grado de consecución de objetivos, aplicando la misma unidad de medida, u otra congruente, que la utilizada para considerar el impacto potencial de un riesgo sobre la consecución de un objetivo concreto. Por ejemplo, una empresa que tiene establecido el objetivo de mantener un nivel determinado de servicio al cliente, habrá diseñado un coeficiente para dicho objetivo, tal como el índice de satisfacción del cliente, el número de reclamaciones o el volumen de negocio por cliente. Por lo tanto, al evaluar el impacto de un riesgo que podría afectar el servicio al cliente, tal como la posibilidad de que la web de

la empresa pueda estar no disponible durante un período, éste se determina mejor usando los mismos coeficientes.

En el siguiente ejemplo, la Dirección evalúa el riesgo inherente a las variaciones en los tipos de cambio de divisas extranjeras, en función de su efecto en los ingresos generados por las operaciones de la empresa en el extranjero. En este caso, la Dirección consideró la cobertura ante el tipo de cambio como una respuesta al riesgo y volvió a evaluar el índice de riesgo remanente tras los efectos de esta cobertura.

Objetivo de operaciones	Ingresos de explotación en operaciones en el extranjero de 100 millones				
Unidad de medición	Variación en los ingresos de explotación en operaciones en el extranjero.				
Riesgo	La fluctuación en el tipo de cambio afecta de manera adversa a los ingresos de explotación en operaciones en el extranjero.				
Tolerancia al riesgo	La variación aceptable es de +/- 10.000.000.				
Riesgo	Evaluación de riesgos inherentes		Respuesta al riesgo	Evaluación de riesgos residuales	
	Probabilidad	Impacto		Probabilidad	Impacto
El tipo de cambio sube un punto porcentual en 90 días	10%	5.000.000	No se pone en marcha ninguna acción	10%	5.000.000
El tipo de cambio sube 1,5 puntos porcentuales en 90 días	4%	10.000.000	Obtener instrumentos de cobertura frente a variaciones en el tipo de cambio para limitar el impacto	4%	5.000.000
El tipo de cambio sube 3 puntos porcentuales en 90 días	1%	20.000.000		1%	8.000.000

II.2.5 Fuentes de Datos

A menudo, las estimaciones de la probabilidad del riesgo y su impacto se determinan usando datos procedentes de eventos anteriores observables, que proporcionan una base más objetiva que las estimaciones totalmente subjetivas. Los datos autogenerados a partir de la experiencia propia de la entidad pueden reflejar un menor sesgo subjetivo personal y proporcionan mejores resultados que los datos procedentes de fuentes externas. Sin embargo, incluso cuando los datos generados internamente sean una entrada

primaria, los datos externos pueden resultar útiles como punto de contraste o para mejorar el análisis. Por ejemplo, la Dirección de una empresa que evalúa el riesgo de paradas en la producción por fallas de los equipos, primero estudia la frecuencia e impacto de fallas anteriores de su propio equipo productivo, a continuación complementa dichos datos con los que surgen de comparaciones en la industria, lo que permite una estimación más exacta de la probabilidad e impacto de las fallas, y una programación más efectiva del mantenimiento preventivo. Se debe ser cauto cuando se usan eventos pasados para establecer previsiones futuras, ya que los factores que influyen en los eventos pueden cambiar con el tiempo.

II.2.6 Interpretación de Datos

La Dirección formula de manera regular juicios subjetivos sobre la incertidumbre y, al hacer esto, debe reconocer sus limitaciones inherentes. Los resultados de investigaciones psicológicas indican que las personas que toman decisiones, tienen demasiada confianza en su capacidad de estimación y no reconocen el volumen de incertidumbre real. Esta inclinación hacia el exceso de confianza al estimar la incertidumbre, puede minimizarse mediante el uso efectivo de datos empíricos generados interna o externamente.

Es frecuente que las personas tomen diferentes opciones en la búsqueda de ganancias antes que en evitar pérdidas. Al reconocer estas tendencias, los directivos pueden estructurar la información para reforzar el riesgo aceptado y el comportamiento hacia el riesgo en toda la entidad. De acuerdo a cómo la información se presente o enmarque, se puede afectar de manera significativa la interpretación de la información y su visión, así como la asociación a riesgos u oportunidades, tal como se expone en el siguiente cuadro.

Los individuos tienen reacciones diferentes ante pérdidas potenciales que frente a ganancias potenciales. La manera de enmarcar un riesgo -enfocando hacia lo positivo (una ganancia potencial) o a lo negativo (una pérdida potencial)- influirá a menudo en la respuesta. La teoría de la prospección, que explora la toma de decisiones del ser humano, dice que los individuos no son neutrales ante el riesgo y de hecho, una respuesta a pérdidas tiende a ser más extrema que otra frente a ganancias. Y con esto surge una inclinación hacia la mala interpretación de las probabilidades y las reacciones hacia la mejor solución. A modo ilustrativo, un individuo se enfrenta a dos conjuntos de opciones:

- 1. Aceptar una ganancia segura de \$240 o bien una posibilidad del 25% de ganar \$1.000 más la restante probabilidad del 75% de no ganar nada.*
- 2. Aceptar una pérdida segura de \$750 o bien una posibilidad del 75% de perder \$1.000 más la restante probabilidad del 25% de no perder nada.*

En el primer conjunto de opciones, la mayoría de las personas selecciona una "ganancia segura de \$240", debido a la inclinación a evitar riesgos en las ganancias y a las preguntas planteadas de forma positiva. En contraste, la mayoría de las personas selecciona una "posibilidad del 75% de perder \$1.000", debido a la inclinación a asumir riesgos en las pérdidas y a las preguntas planteadas de modo negativo. La teoría de la prospectiva

mantiene que las personas no quieren arriesgar lo que ya tienen o piensan que pueden tener, pero tendrán mayores tolerancias al riesgo cuando creen que pueden minimizar pérdidas.

II.2.7 Técnicas de Evaluación

La Dirección aplica técnicas cualitativas cuando los riesgos no se prestan a la cuantificación o cuando no hay datos suficientes y creíbles para una evaluación cuantitativa, o la obtención y análisis de ellos no resulte eficaz por su costo. Las técnicas cuantitativas aportan más precisión y se usan en actividades más complejas y sofisticadas, para complementar las técnicas cualitativas.

Por lo general, las técnicas cuantitativas de evaluación exigen un mayor grado de esfuerzo y rigor y a veces emplean modelos matemáticos. Estas técnicas dependen mucho de la calidad de los datos e hipótesis de soporte y resultan más relevantes para riesgos con un historial y una frecuencia de variabilidad conocidos, pues permiten una proyección fiable.

Para conseguir un consenso sobre probabilidad e impacto usando técnicas cualitativas de evaluación, las entidades pueden aplicar el mismo enfoque que usan en la identificación de eventos, tales como las entrevistas y grupos de trabajo. Un proceso de autoevaluación del riesgo capta los puntos de vista de los participantes sobre la probabilidad y el impacto potencial de eventos futuros, usando escalas descriptivas o numéricas.

Una entidad no necesita aplicar las mismas técnicas de evaluación en todas sus unidades de negocio, la selección debería reflejar la necesidad de precisión y la cultura de cada unidad. Por ejemplo, al identificar y evaluar los riesgos a nivel de proceso, una unidad usa cuestionarios de autoevaluación, mientras que otra utiliza grupos de trabajo. Los riesgos se evalúan y luego se organizan y agrupan según las categorías de riesgo y de objetivos de ambas unidades. Aunque se apliquen métodos distintos, ambos proporcionan suficiente concordancia para facilitar la evaluación de riesgos en toda la entidad.

La Dirección puede generar una medida del impacto cuantitativo de un evento en toda la entidad, cuando todas las evaluaciones individuales de riesgo referentes al mismo, se expresen en términos cuantitativos. Por ejemplo, el impacto de un cambio en el precio de la energía sobre el margen bruto se calcula en todas las unidades de negocio y se determina así el impacto global. Cuando exista una mezcla de medidas cualitativas y cuantitativas, la Dirección desarrolla una evaluación compuesta por ambos tipos de medición expresada en términos cualitativos. Establecer probabilidades comunes, términos de impacto en toda la entidad y categorías de riesgos comunes para las mediciones cualitativas, facilita estas evaluaciones compuestas de riesgo.

II.2.7.1 Escalas de Medición

Al estimar la probabilidad e impacto de posibles eventos, ya sea sobre la base del efecto inherente o residual, se debe aplicar alguna forma de medición. A

modo de ejemplo, se pueden establecer cuatro tipos generales de medida: Nominal, ordinal, de intervalo y por ratios.

Medición nominal

Es la forma más sencilla de medición e implica el agrupamiento de eventos por categorías, tales como la económica, tecnológica o medioambiental, sin situar un acontecimiento por encima de otro. Los números asignados en la medición nominal sólo tienen una función de identificación y los elementos no pueden ser ordenados, clasificados ni agregados.

Medición ordinal

En este tipo de medición, los eventos se describen en orden de importancia, con etiquetas del tipo alta, media o baja o bien clasificados a lo largo de una escala. La Dirección determina si el elemento "X" es más importante que el elemento "Y". Por ejemplo, puede estimar que la probabilidad de que un nuevo virus informático afecte a sus sistemas es superior a la probabilidad de transmisiones de información confidencial por parte del personal.

Medición de intervalo

Utiliza una escala de distancias numéricamente iguales. Si, por ejemplo, el impacto de la pérdida de producción de una máquina clave se mide como "tres", el impacto de una caída de tensión de una hora como "seis" y el efecto de 100 puestos vacantes como "nueve", la Dirección puede determinar que la diferencia en impacto entre la pérdida de producción de una máquina y una caída de tensión de una hora, es la misma que la diferencia entre una caída de tensión de una hora y la existencia de 100 puestos vacantes. Esto no significa, sin embargo, que el impacto del evento medido con un "seis" sea el doble de importante que el impacto del evento medido con un "tres".

Medición por ratios

Una escala de este tipo permite concluir que, si al impacto posible de un evento se le asigna un "tres" y al de otro se le asigna un "seis", el segundo acontecimiento presenta un posible impacto el doble de importante que el primero. Esto es así porque la medición por ratios incluye el concepto del cero verdadero, mientras que la medición de intervalo no lo hace.

En el presente trabajo, las mediciones nominal y ordinal se consideran técnicas cualitativas, mientras que las mediciones de intervalo y por ratios son cuantitativas.

II.2.7.2 Técnicas Cualitativas

Si bien algunas evaluaciones cualitativas de riesgos se establecen en términos subjetivos y otras en términos objetivos, la calidad de estas evaluaciones depende principalmente del conocimiento y del juicio de las personas implicadas, de su comprensión de los acontecimientos posibles y del contexto y dinámica que los rodea.

Las siguientes figuras presentan evaluaciones cualitativas que emplean escalas de medición ordinal. La primera ilustra una escala de la probabilidad de

acontecimientos que afectan a operaciones informáticas. En la siguiente se clasifica una gama de posibles impactos referentes al riesgo de vertido de materiales peligrosos.

Nivel	Descripción	Probabilidad de suceso	Riesgo
1	Muy improbable	Muy baja	Sistemas informáticos no operativos durante periodos prolongados debido a acciones terroristas o intencionadas.
2	Improbable	Baja	Un evento tal como una catástrofe natural o relacionado con un tercero (por ejemplo, un servicio público) requiere la puesta en marcha del plan de continuidad del negocio.
3	Posible	Moderada	Piratas informáticos se introducen en nuestro sistema de seguridad informática.
4	Probable	Alta	La plantilla utiliza recursos de la empresa para acceder a información inadecuada en Internet.
5	Prácticamente seguro	Muy alta	La plantilla utiliza recursos de la empresa para mensajería personal.

Objetivo Manejar los materiales peligrosos de acuerdo con las normativas regionales y estatales.		
Riesgo		Unidades de medición
Vertido no planificado de material peligroso		Horas productivas perdidas. Costes de contención. Lesiones con incapacidad temporal. Compensaciones y costes relacionados.
Nivel	Impacto relativo	Mediciones
1	Insignificante	<ul style="list-style-type: none"> • Ningún incidente reseñable. • Pérdida mínima de horas productivas. • Ninguna lesión.
2	Leve	<ul style="list-style-type: none"> • 1-2 incidentes reseñables. • Contención de los materiales realizada in situ por la plantilla. • Efecto inferior al 5% de las horas productivas diarias. • Ninguna lesión o lesiones leves.
3	Moderado	<ul style="list-style-type: none"> • Varios incidentes reseñables. • Contención del material in situ con apoyo externo. • Efecto entre el 5% y el 20% de las horas productivas diarias. • Tratamiento médico ambulatorio requerido
4	Grave	<ul style="list-style-type: none"> • Acontecimiento reseñable grave. • Material vertido al medio ambiente, aunque sin efectos perjudiciales reales o perceptibles. • Pérdida de producción significativa, entre el 20% y el 100% de las horas productivas diarias. • Tratamiento médico limitado con hospitalización
5	Catastrófico	<ul style="list-style-type: none"> • Múltiples acontecimientos reseñables graves o un único acontecimiento catastrófico. • Vertido al medio ambiente con efectos perjudiciales significativos, requiriendo recursos significativos de terceros. • Pérdida sustancial de capacidad productiva: más de dos días de horas productivas. • Lesiones significativas.

II.2.7.3 Técnicas Cuantitativas

Las técnicas cuantitativas pueden utilizarse cuando existe la suficiente información para estimar la probabilidad y el impacto del riesgo empleando mediciones de intervalo o por ratios. Los métodos cuantitativos incluyen técnicas probabilísticas, no probabilísticas y de benchmarking. Una consideración importante en la evaluación cuantitativa es la disponibilidad de información precisa, ya sea de fuentes internas o externas, y uno de los retos

que plantea el uso de estas técnicas es el de obtener suficientes datos válidos.

II.2.7.3.1 Técnicas probabilísticas

Las técnicas de este tipo miden la probabilidad y el impacto de un determinado número de resultados, basándose en premisas del comportamiento de los eventos en forma de distribución estadística. Las técnicas probabilísticas incluyen modelos en riesgo (incluyendo los de valor en riesgo, flujo de caja en riesgo y beneficios en riesgo), la evaluación de eventos con pérdidas asociadas y el análisis retrospectivo.

Valor en riesgo

El Valor en Riesgo (VeR) es una técnica utilizada para medir la exposición al riesgo de mercado de una cartera. Podemos definir el VeR de una cartera de inversión como la mínima pérdida esperada para un horizonte temporal y un nivel de confianza determinados, medido en una moneda de referencia específica. Por ejemplo, si el VeR a un día de una cartera es de 10 millones de pesos con un nivel de confianza del 95%, entonces existe una probabilidad del 5% que las pérdidas de la cartera en las próximas 24 horas sean superiores a los 10 millones. Es importante puntualizar que el Valor en Riesgo no representa el “peor escenario” que puede producirse, sino un nivel de pérdidas que se produce con relativa frecuencia, la cual será función del nivel de confianza elegido a la hora de calcularlo.

El nivel de confianza suele establecerse entre el 95% y el 99% de los posibles escenarios, lo que implica que a partir de ese límite, el cinco o el uno peor percentil de posibles escenarios de comportamiento esperado de un portafolio, ya no son considerados como aceptables para el inversionista o administrador de riesgos a cargo del portafolio.

La Dirección selecciona tanto la confianza deseada como el horizonte temporal a lo largo del cual se evalúa el riesgo, basándose en parte en la tolerancia al riesgo establecida.

Las mediciones del valor en riesgo se utilizan en ocasiones para racionalizar el capital requerido por las unidades de negocio mediante la estimación, con un alto grado de confianza y a lo largo de un horizonte temporal especificado, del capital necesario para cubrir posibles pérdidas. Es común que se haga coincidir el período de medición del capital con el período de evaluación del rendimiento.

Una aplicación del valor en riesgo es el valor de mercado en riesgo, utilizado por las instituciones financieras para medir el índice de riesgo de variaciones de precio que afecten a instrumentos financieros. Dicha aplicación es utilizada a su vez por instituciones no financieras.

El valor de mercado en riesgo se define como la pérdida máxima estimada para un instrumento o cartera que puede esperarse a lo largo de un horizonte temporal dado y con un nivel de confianza determinado.

El principal problema con la metodología tradicional de cálculo del VeR es que se trata de un análisis unidireccional. En el proceso de agregación y simplificación de los riesgos de la cartera se pierde gran cantidad de información que puede ser muy útil para el gestor de riesgos al determinar cuáles son las principales fuentes de riesgo, y cuáles son aquellos componentes que realmente están sirviendo como cobertura de dichos riesgos.

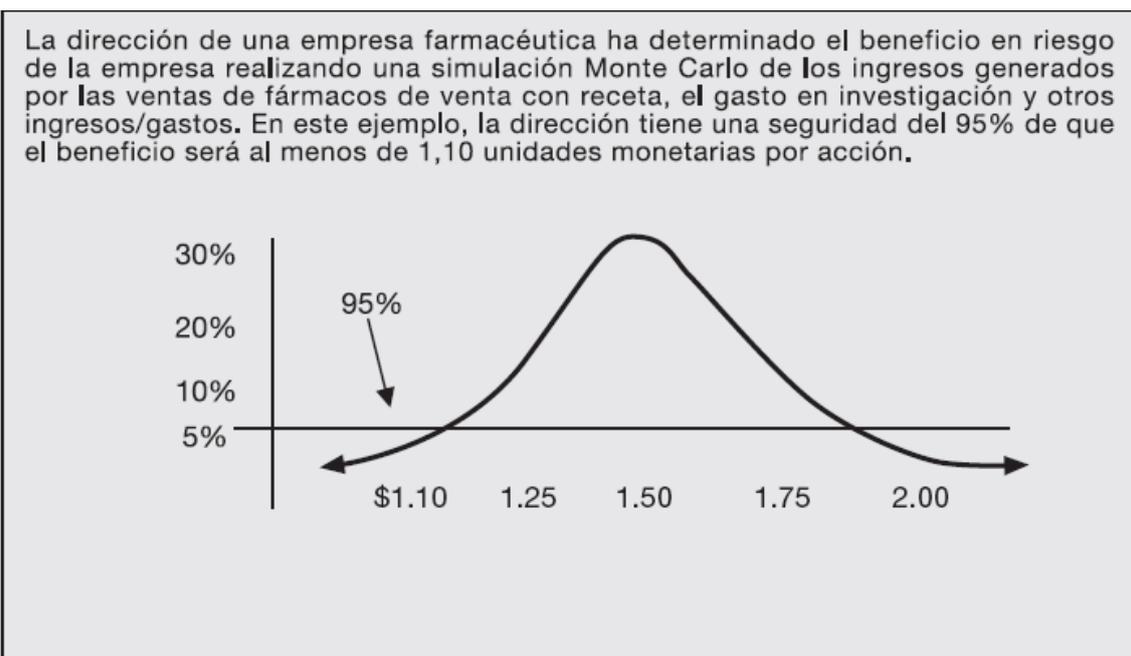
Flujo de caja en riesgo

Esta medición es similar a la de valor en riesgo, salvo en que estima una variación en los flujos de caja de una organización o unidad de negocio con relación a un objetivo esperado de flujo de caja, con un grado de confianza dado y a lo largo de un horizonte temporal definido. Está basada en hipótesis del comportamiento de cambios de los flujos de caja en forma de distribución estadística. Se emplea en negocios cuyos resultados son sensibles a las variaciones en dichos flujos relacionadas con factores ajenos al precio de mercado. Por ejemplo, un fabricante de computadoras que desee medir el riesgo presente en su flujo de caja neto, puede emplear dicha técnica incluyendo una variable como el tipo de cambio de divisas, o bien múltiples variables, como las variaciones en el producto interno bruto, la oferta y la demanda de componentes informáticos y el presupuesto corporativo en investigación y desarrollo.

Beneficio en riesgo

De manera similar al flujo de caja en riesgo, el parámetro del beneficio en riesgo estima un cambio en el beneficio contable de una organización o unidad de negocio, que no debería excederse, con un nivel de confianza dado y a lo largo de un horizonte temporal definido, basándose en premisas sobre el comportamiento de dicho beneficio en forma de distribución estadística.

La siguiente figura proporciona un ejemplo del análisis de Beneficio en Riesgo.



Distribuciones de pérdidas

Algunas estimaciones probabilísticas de pérdidas operativas o crediticias utilizan técnicas estadísticas, basadas por lo general en distribuciones no normales, con el fin de calcular las pérdidas máximas resultantes de riesgos operativos con un nivel de confianza dado. Estos análisis parten de la recolección de datos de pérdidas operativas clasificadas en categorías por su posible origen, como, por ejemplo, actividad delictiva, recursos humanos, prácticas de ventas, actividades no autorizadas, procesos de gestión y tecnología. A partir de estos datos de pérdidas y de su reflejo en los costos e ingresos de seguros relacionados, puede desarrollarse una distribución de pérdidas preliminar, que luego será perfeccionada para considerar las respuestas al riesgo.

Análisis retrospectivo (Backtesting)

En este contexto, el análisis retrospectivo consiste habitualmente en la comparación periódica de las medidas relacionadas con el riesgo de una entidad y la ganancia o pérdida que pueden generar. El análisis retrospectivo es empleado de manera habitual por instituciones financieras, comparando las ganancias y pérdidas diarias con los resultados de sus modelos de riesgo, con el fin de calibrar la calidad y precisión de sus sistemas de evaluación de riesgos.

II.2.7.3.2 Técnicas no probabilísticas

Las técnicas no probabilísticas se emplean para cuantificar el impacto de un posible evento sobre hipótesis de distribuciones estadísticas, pero sin asignar una probabilidad de ocurrencia al acontecimiento. De este modo, estas técnicas requieren, por parte de la Dirección, la determinación por separado de esta probabilidad. Algunas técnicas no probabilísticas muy utilizadas son el análisis de sensibilidad, el análisis de escenarios y las pruebas de tolerancia a situaciones límite.

Análisis de sensibilidad

El análisis de sensibilidad se utiliza para evaluar el impacto de cambios normales o rutinarios en los eventos posibles. Debido a la simplicidad relativa de cálculo, las mediciones de sensibilidad se utilizan en ocasiones como complemento a un enfoque probabilístico. El análisis de sensibilidad se utiliza con:

-  Mediciones de operaciones, como el efecto que las variaciones en el volumen de ventas tienen en el tiempo de respuesta del centro de atención telefónica o en el número de defectos de fabricación
-  Renta variable, utilizando beta. Para las acciones ordinarias, beta representa la razón entre los movimientos de una acción determinada y los movimientos de una cartera de mercado o de una variable proxy, como el índice S&P 500

Análisis de escenarios

El análisis de escenarios evalúa el efecto que uno o más eventos tienen sobre un objetivo. Puede ser utilizado en conexión con la planificación de

continuidad del negocio o con la estimación del impacto de un fallo del sistema o de la red, reflejando así el efecto en todo el negocio. También puede ser realizado a nivel de planificación estratégica, donde la Dirección aspira a vincular el crecimiento, el riesgo y el rendimiento.

Pruebas de tolerancia a situaciones límite

Las pruebas de tolerancia a situaciones límite evalúan el impacto de eventos extremos. Difieren del análisis de escenarios en el hecho de que se centran en el impacto directo de un cambio provocado por un acontecimiento o actividad en circunstancias extremas, frente al enfoque del análisis de escenarios, que se centra en cambios a escala más normal. Las pruebas de tolerancia a situaciones límite se utilizan asimismo como complemento a las mediciones probabilísticas, para examinar los resultados de eventos de baja probabilidad y alto impacto, que podrían no ser captados de forma adecuada a través de los supuestos de distribución estadística asumidos en las técnicas probabilísticas. De manera similar al análisis de sensibilidad, estas pruebas de tolerancia se utilizan para evaluar el impacto de cambios en acontecimientos operativos o movimientos en el mercado financiero, con el fin de evitar grandes sorpresas y pérdidas. Las pruebas de tolerancia a situaciones límite incluyen, por ejemplo, la estimación del efecto de los siguientes acontecimientos

-  Aumento de los defectos de fabricación de un producto
-  Movimientos en el tipo de cambio de divisas
-  Movimiento en el precio de un factor subyacente en el que se basa un producto derivado
-  Aumento de los tipos de interés en el caso de una cartera de inversión en renta fija
-  Aumento en los precios de la energía que afecten al costo de explotación de una planta de fabricación

II.2.7.3.3 Benchmarking

Spendolini, en su libro "The Benchmarking Book" define el benchmarking como el "proceso continuo y sistemático de evaluar los productos, servicios o procesos de las organizaciones que son reconocidas por ser representativas de las mejores prácticas para efectos de mejora organizacional".

Algunas empresas utilizan técnicas de benchmarking para evaluar un riesgo específico en términos de probabilidad e impacto, en el caso de que la Dirección aspire a mejorar sus decisiones de respuesta al riesgo. La información así obtenida puede proporcionar un conocimiento profundo de la probabilidad e impacto de riesgos, basándose en las experiencias de otras organizaciones. También se emplea el benchmarking con respecto a actividades de un proceso de negocio, para intentar identificar oportunidades de mejora del mismo.

Los tipos de benchmarking incluyen:

-  Interno; comparación de mediciones en un departamento o división con otros de la misma entidad, en busca de mejorar la eficiencia.
-

- Competitivo/Sectorial; comparación de mediciones entre competidores directos o grupos amplios de empresas con características similares.
- Líderes de sector; búsqueda de mediciones similares entre empresas líderes, independientemente del sector al que pertenezcan.

El proceso de benchmarking supone que las empresas están preparadas y dispuestas para hacer públicas sus mediciones. Esto suele hacerse a través de un tercero, que recoge los números de diversas organizaciones, y los publica sin identificar a la empresa específica.

II.2.7.4 Riesgo y Asignación de Capital

Algunas organizaciones utilizan este término para referirse a la cantidad de capital requerida para protegerse contra riesgos financieros. Otras la utilizan de manera diferente, como una medida del capital necesario para hacer funcionar el negocio de la manera planificada. La Dirección lo puede utilizar para establecer estrategias, asignar recursos y medir el rendimiento.

El concepto de capital económico representa el nivel de capital propio necesario en un determinado período de tiempo y con un nivel de confianza dado. Por ejemplo, el banco asume un nivel de confianza del 95% y un período de dos años para determinar sus requisitos de capital económico. Tras modelar su distribución de beneficios esperados, teniendo en cuenta los riesgos de mercado, crediticio, de operaciones y de activo inmovilizado, la Dirección identifica sus requisitos de capital económico.

Conociendo la falta de precisión de la metodología de medición del riesgo de operaciones, así como el riesgo existente más allá del nivel de confianza del 95%, el banco establece una política para crear un "colchón" adicional de capital económico sobre su nivel requerido, para así proporcionar una mayor confianza de que el valor calculado de dicho capital es suficiente.

El banco también utiliza la relación entre capital económico y capital contable como indicador. Cuando la diferencia entre el capital contable y el "colchón" de capital es menor que el capital económico requerido, la Dirección determina si debe:

- Recortar determinadas actividades del negocio
- Obtener fondos propios adicionales
- Tomar posiciones de menor riesgo en sus actividades de crédito, de inversión o de operaciones

Cuando la diferencia entre el capital contable y el "colchón" de capital es superior al capital económico requerido, la Dirección considera oportunidades de:

- Expandir su negocio a nuevos productos o mercados
 - Devolver capital a los accionistas
 - Tomar posiciones de mayor riesgo en sus actividades de crédito, de inversión o de operaciones
-

II.2.8 Presentación de Evaluaciones de Riesgos

Las organizaciones utilizan diversos métodos para presentar las evaluaciones de riesgos.

La presentación de una manera clara y concisa resulta especialmente importante en el caso de la evaluación cualitativa, dado que en este caso los riesgos no se resumen en una cifra o intervalo numérico, como sucede en las técnicas cuantitativas.

Entre las diferentes técnicas podemos encontrar **mapas de riesgo**. Un mapa de riesgo es una representación gráfica de la probabilidad e impacto de uno o más riesgos. Puede adoptar la forma de mapas de calor o diagramas de proceso que trazan estimaciones cuantitativas y cualitativas. Los riesgos se representan de manera que los más significativos (mayor probabilidad y/o impacto) resalten, diferenciándolos de los menos significativos. Dependiendo del nivel de detalle y de la profundidad del análisis, los mapas de riesgo pueden presentar la probabilidad y/o el impacto general esperado o bien incorporar un elemento de su variabilidad.

Para añadir transparencia al riesgo, y trazar un mapa que refleje la situación con exactitud, las empresas necesitan un sistema eficaz de reporte del riesgo, lo que a su vez requiere que se desarrolle una organización eficaz de gestión del riesgo. El mapa de riesgo es una herramienta que se emplea para promover el diálogo entre los miembros del Directorio, la alta Dirección, y los responsables de cada unidad de negocio. La alta Dirección debería revisarlo con frecuencia, quizás mensualmente, y el Directorio por ejemplo trimestralmente, con el fin de ayudar a los responsables a decidir si los grados de riesgo asumidos en cada momento son o no tolerables, y si la empresa tiene oportunidades atractivas que aconsejen a asumir riesgos considerablemente más elevados. Deberían plantearse preguntas como: ¿las concentraciones de riesgo están generando rendimientos elevados, o simplemente están reduciendo el valor para los accionistas? ¿Puede la empresa gestionar adecuadamente las altas concentraciones de riesgo que ha asumido?

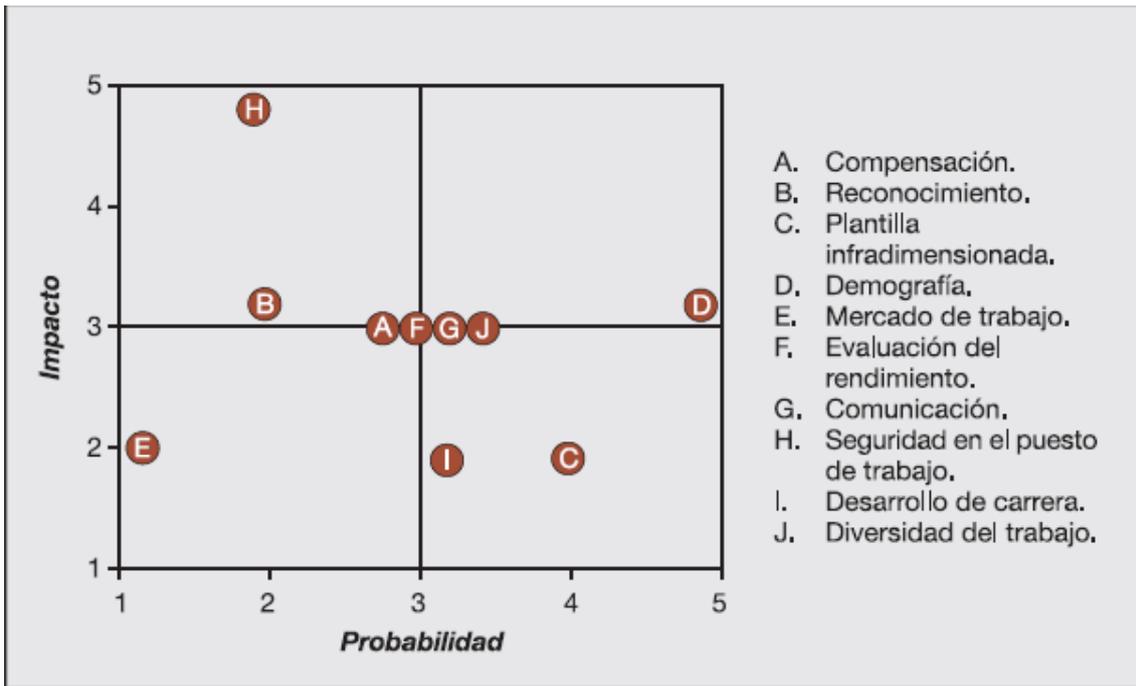
Los siguientes ejemplos de mapas de riesgo representan la evaluación de riesgos relativos al objetivo de conservar a empleados de alto rendimiento.

El siguiente cuadro ilustra un *mapa de calor* que presenta niveles de riesgo (probabilidad e impacto) con un código de color, donde el rojo representa un riesgo elevado, el amarillo un riesgo moderado y el verde un riesgo reducido.

Una empresa evalúa los riesgos que afectan a su objetivo de mantener una plantilla de calidad. La probabilidad se considera en términos de porcentaje de rotación a lo largo de un determinado periodo y el impacto en términos del coste de ineficacia operativa y de sustitución, formación y desarrollo de los empleados. El código de color resalta los riesgos con una mayor probabilidad de materialización, así como aquellos con una mayor probabilidad de tener un efecto significativo en los objetivos.

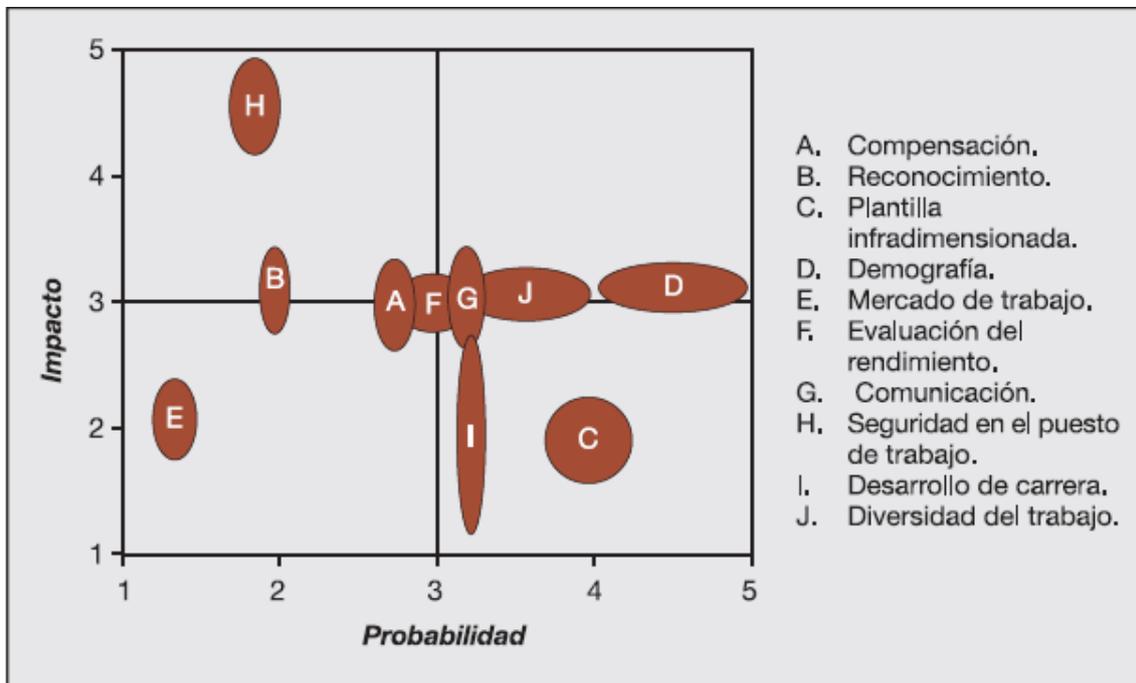
	Tema	Descripción del riesgo	Probabilidad	Impacto
A	Compensación	La insatisfacción de los empleados con la compensación recibida conduce a un mayor índice de rotación de la plantilla.	Posible	Moderado
B	Reconocimiento	Los empleados no se sienten reconocidos, lo que supone una menor concentración en las tareas y tasas superiores de error	Improbable	Leve
C	Plantilla infra-dimensionada	Los empleados están utilizados en exceso y hacen un número considerable de horas extra. Los empleados se marchan a trabajar a otras organizaciones con un mejor equilibrio entre la vida profesional y la personal.	Probable	Moderado
D	Demografía	El cambio en la composición demográfica del grupo de empleados provoca una mayor rotación.	Prácticamente seguro	Moderado
E	Mercado de trabajo	Aumento de la demanda de empleados de la empresa por parte de empresas de contratación.	Improbable	Moderado
F	Evaluación del rendimiento	La insatisfacción de los empleados con las medidas y procesos de evaluación del rendimiento provoca un descenso de la motivación, el enfoque hacia objetivos no críticos y la pérdida de personas que se van a empresas percibidas como preferidas.	Posible	Moderado
G	Comunicación	Una comunicación ineficiente entre los empleados y la dirección provoca la aparición de mensajes contradictorios y la búsqueda de un empleo alternativo.	Posible	Moderado
H	Seguridad en el puesto de trabajo	Un puesto de trabajo inseguro provoca lesiones en los empleados y renuncias por parte de los afectados, así como por parte de otros empleados preocupados por los problemas de seguridad.	Improbable	Grave
I	Desarrollo de carrera	Los empleados perciben un control limitado sobre el desarrollo de su carrera, lo que provoca una mayor rotación.	Posible	Moderado
J	Diversidad del trabajo	La insatisfacción de los empleados con el grado de variación del trabajo provoca un comportamiento rutinario, mayor número de errores en procesos clave y la búsqueda de oportunidades de trabajo más interesantes fuera de la empresa.	Posible	Moderado

Estos mismos riesgos pueden representarse en un *mapa de riesgo matricial*, donde la probabilidad se sitúa en el eje horizontal y el impacto en el vertical. Como este modelo proporciona más información, facilita a la Dirección a dar prioridad a los puntos donde es necesario prestar una mayor atención.



El siguiente cuadro, *mapa de riesgo con la variabilidad de probabilidad e impacto*, proporciona la misma información básica, pero con mayor profundidad.

Presenta la información de variabilidad en torno a la probabilidad e impacto del riesgo, proporcionando a la Dirección una perspectiva adicional sobre los riesgos.



II.2.9 Relaciones entre Eventos

Cuando los eventos potenciales no están relacionados entre sí, la Dirección los evalúa individualmente. Por ejemplo, una empresa con unidades de negocio expuestas a diferentes fluctuaciones de precios, tales como el de la pulpa de papel y el de moneda extranjera, evaluaría los riesgos sin considerar los movimientos del mercado. Pero cuando exista correlación entre los eventos o éstos se combinen e interaccionen para crear probabilidades o impactos significativamente diferentes, la Dirección los evaluará en conjunto. Aunque el impacto de un solo evento pueda ser ligero, el impacto de una secuencia o combinación de eventos puede ser más significativo. Por ejemplo, una válvula defectuosa de un depósito de propano en un almacén de distribución origina un escape de gas, mientras se mantienen cerradas las puertas de la instalación para retener el calor de las oficinas adyacentes. Cuando el conductor de un camión que se acerca al almacén activa un dispositivo a control remoto para abrir las puertas, la presencia conjunta del gas y la chispa del motor de la puerta causan una explosión. Eventos distintos interaccionan y dan como resultado un riesgo significativo. En otro ejemplo, una empresa se introduce en un mercado extranjero, donde cuenta con nuevos directivos contratados localmente, sistemas de información no probados y poca base para que la Dirección central pueda juzgar su correspondiente funcionamiento, lo que da como resultado un riesgo significativo de información errónea o fraudulenta.

Cuando sea probable que los riesgos afecten a múltiples unidades de negocio, la Dirección puede agruparlos en categorías comunes de eventos y después, considerarlos primero según unidad y luego en conjunto para toda la entidad. Por ejemplo, las unidades de una empresa de servicios están sujetas al riesgo de modificación del tipo de interés oficial y su Dirección evalúa este riesgo no sólo en cada unidad, sino también de una forma combinada global.

La naturaleza de los eventos y el hecho de que estén relacionados o no, puede afectar a las técnicas de evaluación utilizadas. Por ejemplo, al evaluar el impacto de eventos que podrían tener un efecto extremo, la Dirección puede usar pruebas de "esfuerzo" (Stress Testing), mientras que para evaluar el efecto de eventos múltiples, la Dirección puede encontrar más útil el uso de simulaciones o análisis de escenarios.

La observación de interrelaciones entre probabilidad e impacto constituye una importante responsabilidad de la Dirección. Una administración efectiva de riesgos corporativos, requiere que la evaluación de éstos no sólo sea efectuada en relación al riesgo inherente sino también respecto a la respuesta al riesgo, como se expone en el siguiente capítulo.

II.2.10 Puntos a evaluar

Para la autoevaluación por parte de la administración o la evaluación independiente de la calidad de los elementos de este componente, se deben considerar como mínimo los siguientes puntos:

- El uso de la información provista por el Establecimiento de Objetivos e Identificación de Eventos para evaluar los riesgos
- La idoneidad de la metodología y los recursos utilizados para establecer y para evaluar los riesgos
- El involucramiento de la Dirección en la evaluación de los riesgos
- La calidad de la documentación recopilada de los estudios efectuados
- La transparencia de la información sobre los resultados de la evaluación del riesgo

II.2.11 Caso de estudio

Continuando con nuestro caso práctico presentado en el capítulo anterior, en cuanto a la Evaluación de Riesgos, el proceso se inicia cuando la empresa comienza a desarrollar Matrices de Riesgo específicos por proceso, actividad o Unidad. Estas matrices reflejan el nivel de riesgo de los escenarios determinados, tanto desde el punto de vista del riesgo inherente como del riesgo residual.

Tales Matrices de Riesgo constituyen una poderosa herramienta para evaluar los riesgos a que se enfrentan las actividades o procesos desde diferentes perfiles de vulnerabilidad: perfil operacional, financiero, humano, ambiental, de imagen, entre otros aspectos.

Las etapas desarrolladas en el proceso aludido son las que se identifican a continuación:

- Las diferentes Unidades participan al crear Tablas de Valoración de las consecuencias
- Los responsables del proceso califican los escenarios en cuanto a su probabilidad e impacto (riesgo inherente y residual) tomando en cuenta el factor de vulnerabilidad
- Se investiga si dichos escenarios están dentro de la tolerancia al riesgo establecida
- Para los procesos evaluados, una vez calificados todos los escenarios, se obtienen Matrices de riesgo inherente y de riesgo residual. Son matrices globales y desglosadas para todos los factores de vulnerabilidad seleccionados

EJEMPLO TABLA DE IMPACTO

Valor	Nivel	Criterio general
7	Insignificante	No afecta / Mínima
14	Marginal	No significativa / Pequeña
35	Grave	Parcial temporal / Moderada
70	Crítico	Total temporal / Significativa
140	Desastroso	Parcial permanente / Considerable
350	Catastrófico	Total permanente / Gran magnitud

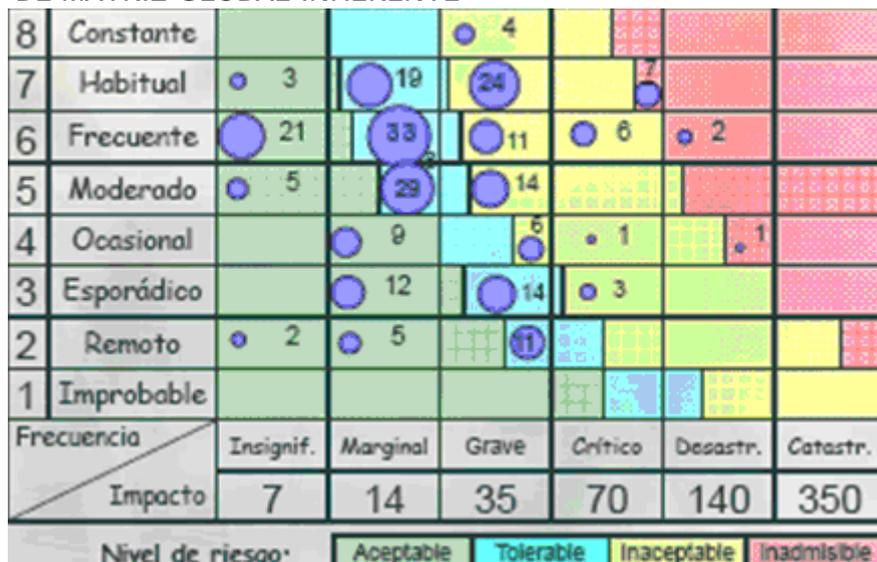
EJEMPLO TABLA DE PROBABILIDAD

Valor	Nivel	Criterio general
1	Improbable	Difícil / menos de una vez c/200 años
2	Remoto	Muy baja / 1 vez entre 100 y 200 años
3	Esporádico	Baja / 1 vez entre 50 y 100 años
4	Ocasional	Limitada / 1 vez entre 20 y 50 años
5	Moderado	Mediana / 1 vez entre 5 y 20 años
6	Frecuente	Significativa / 1 vez entre 1 y 5 años
7	Habitual	Alta / entre 1 y 12 veces al año
8	Constante	Muy alta / más de 12 veces al año

Se trabaja con procesos técnicos y administrativos de la cadena de valor de la empresa tales como:

-  producción
-  comunicaciones
-  facturación comercial y cobro
-  gestión de pasivos

EJEMPLO DE MATRIZ GLOBAL INHERENTE



II.3 Respuesta al Riesgo

Las respuestas a los riesgos se incluyen en las siguientes categorías:

-  **Evitar** - supone salir de las actividades que generen riesgos. Evitar el riesgo puede implicar el cese de una línea de producto, el corte en la expansión hacia un nuevo mercado geográfico o la venta de una división.

-  **Reducir** - implica llevar a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos a la vez, involucrando a algunas de las decisiones empresariales cotidianas.

-  **Compartir** - la probabilidad o el impacto del riesgo se reducen trasladando o compartiendo una parte del mismo. Las técnicas comunes incluyen la contratación de seguros, la realización de operaciones de cobertura o la tercerización de una actividad.

-  **Aceptar** - no se emprende ninguna acción que afecte a la probabilidad o el impacto del riesgo.

La siguiente figura muestra ejemplos de posibles respuestas a los riesgos

Evitar	Compartir
<ul style="list-style-type: none"> • Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/actividades que podrían dar lugar a riesgos. 	<ul style="list-style-type: none"> • Adoptar seguros contra pérdidas inesperadas significativas. • Entrar en una sociedad de capital riesgo/sociedad compartida. • Establecer acuerdos con otras empresas. • Protegerse contra los riesgos utilizando instrumentos del mercado de capital a largo plazo. • Externalizar procesos de negocio. • Distribuir el riesgo mediante acuerdos contractuales con clientes, proveedores u otros socios del negocio.
Reducir	Aceptar
<ul style="list-style-type: none"> • Diversificar las ofertas de productos. • Establecer límites operativos. • Establecer procesos de negocio eficaces. • Aumentar la implicación de la dirección en la toma de decisiones y el seguimiento. • Reequilibrar la cartera de activos para reducir el índice de riesgo con respecto a determinados tipos de pérdidas. • Reasignar el capital entre las unidades operativas. 	<ul style="list-style-type: none"> • Provisionar las posibles pérdidas. • Confiar en las compensaciones naturales existentes dentro de una cartera. • Aceptar el riesgo si se adapta a las tolerancias al riesgo existentes.

La respuesta de evitar el riesgo sugiere que no se identificó ninguna opción de respuesta que redujera el impacto y la probabilidad hasta un nivel aceptable. Las respuestas de reducir o compartir reducen el riesgo residual a un nivel en línea con las tolerancias de riesgo deseadas, mientras que una respuesta de aceptar sugiere que el riesgo inherente ya está dentro de las tolerancias de riesgo.

Para muchos riesgos, las opciones de respuesta adecuadas son evidentes y bien aceptadas. Por ejemplo, para el riesgo de perder la disponibilidad de los sistemas informáticos, una opción típica de respuesta es la implantación de un plan de continuidad del negocio. Para otros riesgos, las opciones disponibles pueden no ser tan evidentes, lo que exigirá investigación y análisis. Por ejemplo, las opciones de respuesta relevantes para mitigar el efecto de las actividades de un competidor sobre el valor de la marca pueden requerir un estudio y análisis del mercado.

Al determinar la respuesta a los riesgos, la Dirección debería tener en cuenta lo siguiente:

-  Los efectos de las respuestas potenciales sobre la probabilidad y el impacto del riesgo y qué opciones de respuesta están en línea con las tolerancias al riesgo de la entidad
-  Los costos versus los beneficios de las respuestas potenciales
-  Las posibles oportunidades para alcanzar los objetivos de la entidad, lo que va más allá del tratamiento de un riesgo concreto

Para los riesgos significativos, una entidad considera las respuestas posibles dentro de una gama de opciones de respuesta, lo que proporciona profundidad a la selección de respuestas y se enfrenta al "status quo".

II.3.1 Evaluación de Posibles Respuestas

Al analizar los riesgos inherentes, las respuestas a ellos se evalúan con el propósito de conseguir un nivel de riesgo residual en línea con las tolerancias al riesgo de la entidad. Es probable que cualquiera de las diversas respuestas posibles sitúe dicho riesgo residual dentro del marco de esas tolerancias y, a veces, una combinación de ellas proporcionará el resultado óptimo. Por otro lado, una respuesta puede afectar a múltiples riesgos, en cuyo caso la Dirección puede decidir que no se precisan acciones adicionales para tratar un riesgo determinado.

Al igual que en la evaluación del riesgo inherente, el riesgo residual puede ser valorado de manera cualitativa o cuantitativa. En términos generales, se utilizan las mismas mediciones en las evaluaciones de ambos tipos de riesgos.

El siguiente cuadro muestra el efecto de la respuesta al riesgo en el riesgo residual.

Objetivo estratégico	Expandir las ofertas de productos relativas a la comida saludable para gatos.				
Objetivo de operaciones	Generar 30 millones de ingresos en el año 1 a través de la introducción de un nuevo producto para “gatos sanos”.				
Unidad de medición	Ingresos por los nuevos productos				
Tolerancia de riesgo	25-35 millones en nuevos ingresos				
Riesgos	Riesgo inherente		Alternativas de respuesta al riesgo	Riesgo residual	
	Probabilidad	Impacto en los ingresos por el nuevo producto		Probabilidad	Impacto
Un competidor sale al mercado en primer lugar	40%	(10.000.000)	A – Proporcionar fondos adicionales a las divisiones de I&D y producción para salir al mercado en los próximos 90 días	20%	Un 15% menos de ingresos por los nuevos productos (4.500.000)
			B – No adoptar ninguna acción específica para ser el primero en salir al mercado	40%	(10.000.000)
La aceptación de este nuevo producto por parte del mercado es más lenta de lo que sugería la investigación de mercado	25%	(15.000.000)	C – Compartir la marca del producto con un tercero	20%	Un 10% menos de ingresos por los nuevos productos (3.000.000)
			D – Realizar un estudio piloto en un mercado de prueba y modificar el enfoque de marketing de acuerdo a los resultados	15%	Un 15% menos de ingresos por los nuevos productos (4.500.000)
			E – No adoptar ninguna acción para asegurar la aceptación en el mercado	25%	(15.000.000)

II.3.2 Evaluación del Efecto sobre la Probabilidad y el Impacto del Riesgo.

Al evaluar las opciones de respuesta, la Dirección considera el efecto sobre la probabilidad del riesgo y su impacto, reconociendo que una respuesta puede afectar a la organización de modo diferente. Por ejemplo, una empresa con

un centro informático ubicado en una región con fuerte actividad tormentosa, establece un plan de continuidad de negocio que, aunque no tiene efecto alguno sobre la probabilidad de que se produzca una tormenta, mitiga el impacto de los daños en el edificio o de la dificultad para que el personal acceda a su trabajo. Por otro lado, la opción de trasladar el centro informático a otra región no reducirá el impacto de posibles tormentas que puedan producirse, pero sí reduce la probabilidad de que tengan lugar en este nuevo centro.

Al analizar las respuestas, la Dirección puede tener en cuenta los eventos y tendencias pasadas y los posibles escenarios futuros. Al evaluar las respuestas alternativas, la Dirección determina su efecto potencial usando las mismas unidades de medición, u otras congruentes, que las usadas para el objetivo correspondiente.

II.3.3 Evaluación de Costos y Beneficios

Los recursos siempre presentan restricciones y las entidades pueden considerar los costos y beneficios derivados de opciones alternativas de respuesta a los riesgos. Las medidas de costo/beneficio para la puesta en práctica de respuestas se analizan con varios niveles de precisión.

En general, es más fácil tratar con el lado de los costos de la ecuación, el cual, en muchos casos, puede ser cuantificado casi exactamente, ya que se tienen en cuenta todos los costos directos relacionados con la implantación de una respuesta y los costos indirectos que se puedan medir de un modo práctico. Algunas entidades también incluyen los costos de oportunidad relativos al uso de recursos. En algunos casos, sin embargo, surgen retos respecto a la cuantificación al estimar el tiempo y el esfuerzo asociados a una determinada respuesta, como puede ser el caso de recabar información de mercado sobre las preferencias en evolución de los clientes, las actividades de los competidores u otra información generada externamente.

El lado de los beneficios implica valoraciones mucho más subjetivas. Por ejemplo, las ventajas de los programas de formación son evidentes, pero son difíciles de cuantificar. En muchos casos, sin embargo, el beneficio de una respuesta al riesgo puede evaluarse dentro del contexto de beneficios ligados a la consecución del objetivo correspondiente.

Al considerar las relaciones costo/beneficio, la atención a los riesgos como si estuvieran interrelacionados, permite a la Dirección agrupar las respuestas para reducir y compartir el riesgo de la entidad. Por ejemplo, cuando se comparte un riesgo mediante un seguro, puede ser beneficioso combinar los riesgos en una sola póliza, ya que el precio se reduce cuando se aseguran conjuntamente diversas exposiciones a riesgos bajo un mismo acuerdo de cobertura.

II.3.4 Oportunidades en las Opciones de Respuesta

El capítulo sobre Identificación de Eventos describe cómo la Dirección identifica aquellos eventos potenciales que afectan a la consecución de los objetivos de la empresa, bien sea positiva o negativamente. Los eventos con impacto positivo representan oportunidades y se revierten hacia los procesos de fijación de objetivos o estrategias.

De forma similar, las oportunidades pueden identificarse al contemplar las respuestas a los riesgos. Las consideraciones sobre estas respuestas no deberían limitarse sólo a la reducción de los riesgos identificados, sino que también deberían incluir la consideración de nuevas oportunidades para la entidad. La Dirección puede identificar las respuestas innovadoras que, aunque pertenezcan a las categorías de respuestas descritas con anterioridad, pueden ser desconocidas para la entidad, o incluso, para la industria. Dichas oportunidades pueden surgir cuando existen opciones de respuesta a los riesgos que están alcanzando los límites de efectividad y cuando ulteriores actualizaciones tan sólo faciliten cambios marginales en el impacto y probabilidad del riesgo. Un ejemplo es la respuesta creativa de una empresa de seguros de automóviles que, ante el alto número de siniestros en ciertos cruces de carreteras, decidió financiar mejoras en la señalización con semáforos, reduciendo así las reclamaciones por accidentes y mejorando los márgenes.

II.3.5 Respuestas Seleccionadas

Una vez evaluados los efectos de las respuestas alternativas a los riesgos, la Dirección selecciona una respuesta o una combinación de ellas, diseñada para situar la probabilidad y el impacto del riesgo dentro de las tolerancias establecidas. Cuando la respuesta seleccionada pudiera desembocar en que el riesgo residual superara la tolerancia establecida, la Dirección tiene que volver sobre sus pasos y revisar su respuesta o reconsiderar la tolerancia establecida. Por tanto, el equilibrio entre riesgo y tolerancia al mismo puede implicar un proceso iterativo.

Evaluar las respuestas alternativas a los riesgos inherentes requiere tener en cuenta los riesgos adicionales que pueden derivarse de cada respuesta, lo que puede iniciar un proceso iterativo en que la Dirección, antes de tomar su decisión, considere dichos riesgos adicionales, incluyendo aquellos que pudieran no ser evidentes de modo inmediato.

Una vez que la Dirección selecciona una respuesta, es posible que necesite desarrollar un plan de implementación para ejecutarla. Una parte crítica de dicho plan es el establecimiento de Actividades de Control, para asegurar que se lleve a cabo dicha respuesta.

La Dirección reconoce que siempre existirá algún nivel de riesgo residual, no sólo por las limitaciones de los recursos, sino también por la incertidumbre del futuro y demás limitaciones inherentes a todas las actividades.

II.3.6 Perspectiva de Portafolio de Riesgos

La administración de riesgos corporativos requiere que el riesgo se considere desde una perspectiva de toda la entidad o de portafolio. En consecuencia, la Dirección elige un enfoque en que primero se contemplan los riesgos de cada unidad de negocio, departamento o función y luego el responsable de riesgos desarrolla una evaluación conjunta, que refleja el perfil de riesgo residual respecto a sus objetivos y tolerancias al mismo.

Los riesgos de las diferentes unidades pueden estar dentro de sus respectivas tolerancias individuales, pero en conjunto pueden superar al riesgo global aceptado por la entidad, en cuyo caso hacen falta respuestas adicionales o diferentes para ubicar el riesgo dentro del nivel aceptado. A la inversa, los riesgos pueden compensarse, por ejemplo, cuando los mismos sean ocasionados tanto por eventos negativos como positivos, de tal modo que el riesgo global esté dentro del riesgo aceptado por la entidad, evitando la necesidad de una respuesta diferente a ellos.

Una perspectiva de portafolio de riesgos puede ser representada de muchas maneras. Puede alcanzarse centrándose en los principales riesgos o categorías de riesgo de las unidades de negocio o de la empresa en su totalidad, usando métricas como el capital ajustado al riesgo o el capital en riesgo. Dichas medidas compuestas son útiles para medir el riesgo frente a objetivos establecidos en términos de resultados, crecimiento u otras medidas de desempeño, a veces relacionadas con el capital asignado o disponible. Estas medidas de la perspectiva de portafolio pueden facilitar información útil para la reasignación del capital entre unidades y la modificación de la orientación estratégica.

Un ejemplo es una empresa industrial que aplica una perspectiva de portafolio de riesgos en el contexto de su objetivo de ingresos operativos. La Dirección aplica las categorías comunes de eventos para captar riesgos en todas las unidades de negocio. A continuación, elabora un gráfico que muestra, por categoría y unidad de negocio, la probabilidad de riesgo en un horizonte de tiempo y los impactos relativos sobre los ingresos. El resultado es una perspectiva compuesta, o de portafolio de riesgos, al que se enfrenta la empresa considerando la naturaleza, probabilidad y dimensión relativa de los riesgos y cómo pueden afectar a los ingresos de la entidad.

Otro ejemplo es una entidad financiera que requiera que sus unidades de negocio establezcan objetivos, tolerancias al riesgo y medidas de rendimiento, todo en términos de rendimiento del capital ajustado al riesgo. Esta métrica ayuda a la Dirección a englobar las evaluaciones combinadas de riesgo de las unidades, en una perspectiva de portafolio de riesgos para la entidad en su conjunto y le permite considerar los riesgos de las unidades por objetivo y determinar si la entidad está dentro de su riesgo aceptado.

Cuando se mira el riesgo desde una perspectiva de portafolio, la Dirección está en posición de considerar si permanece dentro del riesgo aceptado establecido. A la vez, puede volver a evaluar la naturaleza y el tipo de riesgo que desea asumir. En casos donde la perspectiva de portafolio contemple

menores riesgos que el riesgo aceptado por la entidad, la Dirección puede decidir motivar a los Directores de unidades individuales de negocio para que acepten un mayor riesgo en áreas seleccionadas, esforzándose en mejorar el crecimiento y el rendimiento global de la entidad.

II.3.7 Puntos a evaluar

Para la autoevaluación por parte de la Administración o la evaluación independiente de la calidad de los elementos de este componente, se deben considerar como mínimo los siguientes puntos:

-  La existencia de mecanismos para analizar las alternativas para apoyar la adopción de decisiones
-  La confiabilidad de la metodología utilizada para respaldar el análisis
-  La calidad de la evidencia que respalda el análisis de alternativas
-  El grado de participación de las áreas de la organización que tienen conocimientos especializados en las diferentes unidades de negocio
-  El apoyo de la Dirección a las acciones orientadas al estudio de alternativas
-  La forma en que se comunican los resultados obtenidos, a los diferentes miembros de la organización

II.3.8 Caso de estudio

Como última etapa estudiada en nuestro caso práctico, una vez calificados todos los escenarios de riesgo inherente y residual que conforman las diferentes matrices, los responsables conocen las diferentes medidas de intervención que aplican las gerencias operativas para controlar los impactos negativos de los riesgos y mantenerlos en niveles tolerables.

La eficacia del control se obtiene de la comparación entre el riesgo inherente y el riesgo residual del evento, y la eficiencia será el cociente entre la eficacia y el costo de tomar la medida.

Estas medidas que cubren diferentes perfiles de riesgos operativos, financieros, de seguridad, ambientales, entre otros, se pueden ordenar en función del daño potencial que están evitando.

Haciendo un análisis de Pareto, es decir realizando una comparación ordenada de factores relativos a un problema, identificando los "pocos" factores vitales y diferenciándolos de los "muchos" factores útiles, se determina el grupo de medidas que están mitigando la mayor parte del riesgo de la actividad o proceso analizado. Es allí donde el responsable deberá direccionar sus esfuerzos para poder evaluar dos hechos en forma simultánea:

-  Si el nivel de riesgo residual está razonablemente evaluado y por lo tanto están validando la Matriz de Riesgo elaborada
-

- Si las medidas de intervención más críticas o relevantes están implementadas correctamente y funcionan de acuerdo a lo previsto

Acciones de Cobertura de Riesgos:

Utilizando el principio de Pareto, también conocido como la regla 80-20, que establece que el 20% de una acción producirá el 80% de los efectos, mientras que el 80% restante sólo origina el 20% de los efectos, se ordenan las medidas de cobertura por orden decreciente de acuerdo al daño potencial que están evitando.

Ejemplos de Medidas de Cobertura:

- Rutinas de mantenimiento de instalaciones
- Planes de contingencia
- Sistemas de respaldo de información
- Medidas de seguridad y salud ocupacional
- Diseño de instalaciones
- Sistema de protección contra rayos
- Vigilancia y control de acceso a instalaciones
- Medidas anti-incendio
- Mantenimiento preventivo de vehículos y edificios
- Políticas de relacionamiento con la comunidad
- Otras

APLICANDO PARETO A LAS MEDIDAS

Medidas de administración de riesgo	Daño Potencial	Acumulado
Rutinas de mantenimiento	27%	27%
Plan de contingencia	20%	47%
Seguridad y Salud Ocupacional	13%	60%
Vigilancia y control de acceso	11%	71%
Sistemas de respaldo	10%	81%
Otras	19%	100%

El resultado del proceso podrá asegurar a la Dirección que los riesgos se están controlando a niveles razonables desde el punto de vista costo/beneficio y también permitirá que las gerencias operativas y la Alta Dirección prioricen el uso de los recursos para lograr los objetivos individuales y corporativos.

EJEMPLO MATRIZ GLOBAL RESIDUAL

8	Constante							
7	Habitual	1	7					
6	Frecuente	13	15	12				
5	Moderado	5	16	5				
4	Ocasional	6	13	9	2			
3	Esporádico	10	44	10				
2	Remoto	12	24	21				
1	Improbable	2	18	2				
Frecuencia / Impacto		Insignif.	Marginal	Grave	Crítico	Desastr.	Catastr.	
		7	14	35	70	140	350	
Nivel de riesgo*		Aceptable		Tolerable		Inaceptable		Inadmisible

- Se compilan todas las medidas adoptadas por las gerencias para mitigar los riesgos
- Se analiza la eficacia de la medida (riesgo inherente - riesgo residual)
- Se identifican los escenarios que presentan importante exposición al riesgo

CAPÍTULO

III



**TENDENCIAS EN LA
GESTIÓN DE RIESGOS**

III TENDENCIAS EN LA GESTIÓN DE RIESGOS

Los modelos emergentes para la Administración de Riesgos están transformando el pensamiento de los líderes acerca del riesgo, así como la forma en que ellos administran sus negocios y cómo monitorean la gestión de riesgos para que el mismo genere valor. Los líderes pueden participar en esta evolución de ERM aumentando y expandiendo las herramientas y conceptos utilizados actualmente, como se muestra en el siguiente cuadro.

La Administración de riesgos está evolucionando...

DE	PARA
Riesgo como peligro individual	Riesgo en el contexto de estrategia de negocio
Identificación y evaluación de riesgo	Desarrollo de la "cartera" de riesgo
Foco en todos los riesgos	Centralización en riesgos críticos
Mitigación de riesgo	Optimización de riesgo
Límites de riesgo	Estrategia de riesgo
Riesgos sin dueños	Responsabilidades de riesgos definidas
Cuantificación de riesgos ocasionales	Monitoreo y medición
El riesgo no es mi responsabilidad	El riesgo es responsabilidad de todos

Las economías emergentes han superado a los mercados desarrollados cuando se trata de capitalizar los beneficios de la gestión del riesgo, según revela un estudio elaborado por BT Global Services, que ha entrevistado a 2.000 ejecutivos de perfil senior en Estados Unidos, Reino Unido, Francia, Alemania, España, Suecia, Brasil, China, India y Sudáfrica.

Las empresas en Brasil, China, India y Sudáfrica tienden más que las economías desarrolladas a ver la gestión del riesgo como un medio para incrementar su ventaja competitiva (81% frente a un 44%) y para promover la innovación y la creatividad (73% comparado con un 43%). Además, son más propensas a invertir de forma significativa en estrategias de gestión del riesgo y sistemas que sus homólogas en Estados Unidos y Europa (54% frente a 36%). Esto ha sido posible gracias a que son más proclives a tener un responsable de seguridad corporativo (corporate security officer, CSO) o un responsable de riesgo corporativo (corporate risk officer, CRO) en sus Consejos de Dirección, y a considerarlo como una inversión de valor; y a que son dos veces más propensas a disponer de una estrategia de gestión del riesgo para amenazas globales. Los resultados sugieren que los países en desarrollo, de forma contraria a lo que se piensa, parecen ser los primeros en establecer iniciativas de colaboración internacional.

Respecto a las estrategias de gestión, el 72% de las empresas de China, India y Sudáfrica tienen en cuenta el impacto de los principales problemas y acontecimientos mundiales, frente a sólo el 48% de las empresas en Estados

Unidos y Europa. El problema de la energía y del agua es valorado como el mayor riesgo en todo el mundo para los próximos 12 meses, seguido por el comienzo de una desaceleración económica desencadenada por una recesión en Estados Unidos. Los negocios en los mercados maduros están menos nerviosos por los riesgos futuros, aunque un 36% todavía cree que sus empresas sufrirán el impacto de la desaceleración en mayor o menor medida.

El estudio a su vez señala que:

- El 81% de las empresas en los mercados en desarrollo tiene en sus Consejos de Dirección un CSO o CRO, frente a sólo el 59% de las compañías en los mercados desarrollados
- El 61% de las empresas en economías en desarrollo creen que las amenazas internas son similares a las que vienen de fuera de la organización

Aquí en el Uruguay, encuestas realizadas por PricewaterhouseCoopers a Auditores Internos, Directores y CEOs de diferentes empresas revelan que:

- Más de un tercio de los encuestados consideran que se encuentran posicionados de manera regular o deficiente en relación a las habilidades de evaluación y administración de riesgos
- Un 75% de los encuestados considera importante que los Auditores Internos adquieran habilidades sobre evaluación y administración de riesgos en los próximos 4 años
- Un mayor énfasis en el gerenciamiento de riesgos es considerado una de las principales tendencias macro identificadas (65%)
- Un 88% de los encuestados considera que la utilización de un software para la evaluación de riesgos será más importante en los próximos 4 años.

Con el afán de comprender aún más la realidad de las empresas radicadas en Uruguay, y buscando no sólo contemplar a las estudiadas en nuestro trabajo de campo, hemos realizado un relevamiento que, si bien no cumple las formalidades exigidas para situación actual. Del universo encuestado, el 59% de las empresas cuentan con más de 15 años de antigüedad y un 65% poseen más de 100 empleados, en tanto que asignarle valor estadístico, nos brinda un panorama de la ninguna tiene menos de 20.

A continuación presentamos las principales conclusiones a las que arribamos:

- Aún cuando el 100% tiene identificados los principales riesgos y los responsables de los mismos y el 94% conoce las interrelaciones entre ellos, tan sólo el 47% ha fijado su apetito de riesgo y sólo el 18% cuenta con herramientas para administrar el riesgo.
 - El 53% de las encuestadas considera que el riesgo puede afectar positivamente a la entidad, por ejemplo al explotar nuevos nichos de mercado. El riesgo evaluado correctamente puede generar oportunidades en relación a los demás riesgos. Es muy común, por ejemplo, que los bancos no asignen crédito a clientes que potencialmente podrían ser importantes, pero como
-

tienen ciertas reglas, dejan escapar la oportunidad que otros aprovechan, evaluando la posibilidad de asignar crédito y ganar el plus de la venta financiada, además del agradecimiento del cliente.

- Un 82% considera que las políticas de retribución al personal basadas en rendimiento y resultados inciden en la administración de riesgos. A modo de ejemplo, las políticas de incentivos, como ser un incentivo basado en metas de ventas puede generar ventas ficticias, afectando retribuciones excesivas y mostrando resultados no reales.
- Dentro de las empresas que no aplican el ERM, los argumentos más frecuentes para su no utilización fueron el desconocimiento (38%) y la no obligatoriedad de su aplicación (36%); en tanto que el 16% se basa en la falta de recursos y un 10% en otras razones. Dentro de la falta de recursos, podemos encontrar principalmente la escasez de tiempo y de capital.
- Si bien para el 59% de las encuestadas el riesgo es prioritario al diseñar los procesos operativos, solamente el 18% utiliza alguna técnica para administrarlo. La mayoría opina que no tuvo la necesidad de utilizar ninguna herramienta en particular dado que cada gerente hace su propia evaluación.

CAPÍTULO IV



TRABAJO DE
CAMPO

IV TRABAJO DE CAMPO

Nuestro trabajo práctico se enfocó en tres empresas que se encuentran en distintas fases de su proceso de implementación del ERM. Dos de ellas consideran que el proceso ya está operando razonablemente, mientras que la restante se encuentra en las etapas iniciales del proceso.

Dado que el enfoque de nuestro trabajo es teórico - práctico nos resultó interesante incluir organizaciones que se encontraran en distintas etapas frente a la aplicación de esta herramienta, con el objetivo de conocer los puntos fuertes y débiles que cada etapa conlleva.

Nuestra investigación comenzó con la búsqueda de aquellas empresas que cumplieran con el requisito de estar aplicando el ERM o en el proceso de implementación del mismo. Una vez culminado el desarrollo teórico, formulamos, en base al mismo, un cuestionario que nos permitiera conocer en detalle las técnicas por ellos aplicadas.

Previo a las entrevistas personales, enviamos el cuestionario junto a un resumen de nuestra monografía, a fin de que se fueran interiorizando en el objetivo de nuestro trabajo. En dichas entrevistas participaron las personas más vinculadas al proceso de ERM, a saber; Contadores, Auditores Internos y Gerentes.

Expondremos en primer lugar, la empresa que está comenzando a utilizar la herramienta y culminaremos con aquellas que ya la están aplicando.

IV.1 Empresa A

Es una empresa nacional conformada por capitales extranjeros, la cual se ubica en el rubro de entretenimientos y tiene 7 años en el mercado. De acuerdo a la cantidad de empleados se la puede catalogar como una empresa grande.

Respecto al *Ambiente Interno*, aún no existe una política clara de difusión de la filosofía del riesgo hacia todos los sectores de la organización. Se realiza un plan de negocios anual por parte del staff de gerentes, el cual tiene un horizonte temporal de dos años, pero al no ser difundido a mandos medios e inferiores, dificulta que el riesgo asumido implícito en dicho plan, sea conocido por toda la organización. En cuanto a la documentación de la cultura del riesgo, la empresa considera que es insuficiente. Existen casos concretos documentados, por ejemplo, respecto a las políticas de endeudamiento que definen responsables en base a distintos montos de dinero.

Como consecuencia de lo mencionado anteriormente, no todos los individuos en la organización tienen claro su rol y responsabilidad en la administración

del riesgo, aunque existen tolerancias asumidas intuitivamente por cada jefe de sector, las cuales parecen mantener cierta concordancia entre sí.

En cuanto al *Establecimiento de Objetivos*, desde fines del 2006 se han ido dando pasos con el fin de establecer estrategias de mediano y corto plazo. Para ello, se realizan reuniones periódicas del staff de gerentes, de gerentes con directores, y de directores con accionistas, a fin de corroborar que el plan estratégico elaborado sea coherente con los objetivos globales; estos objetivos son transmitidos, desde la Dirección, anualmente a los rangos de mayor jerarquía. Sin embargo, los mismos no son comunicados de forma masiva a la organización.

Mediante la observación directa, el conocimiento del negocio, el benchmarking y el análisis de situaciones similares, la gerencia ejecutiva elabora un plan de acción con el fin de alcanzar los objetivos globales.

En relación a la *Identificación de Eventos*, dado que es una empresa que se encuentra en las primeras etapas de la implementación del ERM, manejan aún la matriz FODA como herramienta principal en esta fase del proceso, puesto que ya la utilizaban con anterioridad y se sienten familiarizados con su utilización. La identificación de eventos recae sobre los gerentes y se revisa como mínimo anualmente. La intuición, la experiencia y el conocimiento del negocio, son inherentes al proceso de identificar posibles eventos que puedan afectar a la organización. Entre las técnicas utilizadas para la identificación, es frecuente el uso de "talleres de trabajo" dirigidos por el Gerente General, el cual oficia de facilitador. Cabe destacar que a la hora de identificar los eventos, se considera la interrelación que existe entre ellos.

Como principales fuentes internas de generación de eventos que han afectado o pudieran afectar a la organización mencionaron, respecto a Recursos Humanos, los paros y la ocupación del local por parte de los funcionarios, así como accidentes laborales graves y la alta rotación de personal; respecto a eventos vinculados a la Infraestructura, destacaron las malas asignaciones de capital debido a errores en el presupuesto y, respecto a la Tecnología, fallos en los sistemas. Dentro de las fuentes externas, mencionaron la cancelación de contratos con los proveedores de productos o servicios que consideran vitales para el funcionamiento de la organización, la alta dependencia de financiamiento de terceros y la aparición de nuevos competidores en el mercado.

A su vez identifican como riesgos políticos, el hecho de que el gobierno no pueda cumplir con metas inflacionarias y de contención del gasto público, lo cual originaría ajustes en aquellos contratos que tienen relación con el IPC. Otros riesgos identificados se relacionan con el incremento de la conflictividad laboral, disminución en las inversiones en bienes de capital, dificultades en la aplicación de la reforma fiscal y problemas con la matriz energética. Respecto a esto último puntualizaron su preocupación por el problema de la sequía, la cual probablemente originaría cortes programados de energía eléctrica, debiendo suplir los mismos mediante generadores, así como el posible aumento de dicha tarifa.

Ante la consulta sobre ciertos riesgos relacionados con los recursos humanos, tales como la continuidad de los directivos claves o los cambios de responsabilidades que pudieran influir en la eficacia del trabajo, si bien la organización cuenta con procesos que aseguran dicha continuidad, los mismos no están formalizados, lo cual genera a la empresa cierta vulnerabilidad ante la rotación negativa de personal. Al respecto se está trabajando en la formalización de los procesos, partiendo de la base de los ya existentes, los cuales cuentan con certificación ISO.

Continuando con la identificación de eventos relacionados con los Recursos Humanos, expresaron que la reactivación del mercado laboral, originada en gran medida por la contratación masiva por parte de los entes públicos y otros sectores, ocasiona que dicho mercado se torne más volátil. Esto dificulta el reclutamiento y la selección de personal con la celeridad requerida, así como la puja al alza de las remuneraciones.

Respecto al seguimiento del comportamiento de la competencia, nos comentaron que se realizan trabajos internos y externos para monitorear de forma constante la evolución de la competencia, analizando los cambios técnicos y las campañas de marketing. Por otra parte, anualmente se realizan visitas a las mayores exposiciones nacionales e internacionales sobre adelantos del sector.

Al referirse a los riesgos relacionados con el cumplimiento de regulaciones o acuerdos contractuales, manifestaron que existen vacíos legales en algunos contratos, de los cuales han analizado las posibles consecuencias pero no han tomado acciones correctivas debido a su escasa probabilidad de ocurrencia y bajo impacto. Por otra parte, una situación a la cual se enfrentaron y que habían desestimado, fue la ocupación de locales de trabajo, corriendo el riesgo de que se cancelara el contrato principal por su incumplimiento, o de que se generaran multas.

Al identificar eventos detectándose una oportunidad, la misma se canaliza a la estrategia mediante reuniones de directores y staff de gerentes de área.

En la *Evaluación de Riesgos*, el proceso es consistente con la etapa anterior, en la que mencionábamos la utilización de la matriz FODA. Una vez identificados los eventos, se evalúan los riesgos en base a su probabilidad e impacto desde la perspectiva de las debilidades que posee la empresa y las amenazas a las que se enfrenta. Dicha evaluación recae sobre los gerentes y se revisa anualmente. Cabe destacar que las sociedades extranjeras accionistas no exigen la utilización de dicha matriz, las mismas utilizan el Cuadro de Mando Integral.

A la hora de seleccionar técnicas que soporten la aplicación de esta herramienta, optan frecuentemente por las cualitativas, debido a que no cuentan, en todos los casos, con la información necesaria para utilizar las técnicas cuantitativas. Respecto a estas últimas, podemos encontrar la aplicación de Backtesting, ya que realizan en forma diaria la comparación del

Cashflow proyectado con el real, analizando las variaciones. A su vez, como mencionábamos en párrafos anteriores para la Identificación de Eventos, se realizan estudios de mercado, de los cuales surge la comparación de la empresa con el resto del sector, por lo que en este caso se estaría realizando Benchmarking competitivo o sectorial. En consonancia con lo anterior, cuando se ha aplicado Benchmarking interno, han notado que las distintas unidades de negocio no cuentan con criterios predefinidos al evaluar la probabilidad y el impacto de los eventos, sino que se basan en criterios subjetivos, primando la intuición, por lo que la comparación entre las distintas unidades de negocio se encuentra distorsionada. Al respecto se ha comenzado un proceso para la fijación de un estándar con el objetivo de asegurar la concordancia de las evaluaciones realizadas.

Son conscientes de que han cometido errores al subvaluar la probabilidad e impacto de algunos eventos; por ejemplo, en años anteriores se consideraba que el efecto que podría tener la presencia de un sindicato en la organización era insignificante, sin embargo, con el tiempo el mismo se convirtió en uno de los principales factores de riesgo. Otro caso que no anticiparon en forma debida fue la existencia de un tipo de cambio a la baja, originándose mayores costos por haber optado por el financiamiento en otra moneda.

Consultados por la posible incidencia de la crisis mundial en la organización, nos comentaron que han asistido a diversas charlas informativas, pero aún no se ha cuantificado la probabilidad de ocurrencia ni su posible impacto. Cabe destacar que, en este rubro en particular, en épocas de crisis han tendido a aumentar las ventas.

Al analizar las *Respuestas al Riesgo*, se tienen en cuenta, primordialmente, aquellos eventos que afectan la continuidad del plan de negocios. Hasta la fecha, las respuestas se han tomado en base a decisiones de cada gerente de área o a reuniones del staff de gerentes, pero no hay un lineamiento predefinido por parte del Directorio ni documentación que las respalde. La revisión de las respuestas adoptadas no se realiza con una asiduidad específica, dado que este componente aún no ha sido profundizado, siendo ésta una de las metas para el primer trimestre del 2009.

Entre los distintos tipos de respuestas que han adoptado, podemos encontrar los siguientes ejemplos;

-  **Aceptar** la rotación de personal, ya que hasta el momento la ecuación costo/beneficio que han evaluado no amerita que se tomen acciones correctivas.
-  **Reducir** el impacto que podría tener en las ventas la acción de los competidores, invirtiendo activamente en publicidad y promociones.
-  **Evitar** el riesgo asociado a las fluctuaciones originadas por el tipo de cambio, manteniendo una posición monetaria neta tendiente a cero.
-  **Compartir** los riesgos con compañías aseguradoras.

Como mencionábamos en párrafos anteriores, son conscientes que uno de los problemas a los que se enfrenta la organización es la rotación de personal, pero cabe destacar que a la hora de seleccionarlo, toman en cuenta si el

mismo será temporario o permanente, contratando en casos específicos personal zafra, con el que nutren, a posteriori, una bolsa interna de trabajo seleccionando a los más capacitados y con un rendimiento acorde al exigido.

Como *Actividades de Control* se realizan periódicamente auditorías operativas y de cumplimiento externas, con el objetivo de verificar que se cumplan las exigencias legales y contractuales. A su vez, se realizan controles periódicos que buscan cotejar la información suministrada por los distintos presupuestos con la realidad. También se hace énfasis en el control de los valores, realizándose arqueos sorpresivos con regularidad. Sin embargo, las actividades de control existentes no se revisan con la periodicidad adecuada a fin de comprobar que continúen siendo apropiadas, teniendo en cuenta su relevancia y adecuación a la respuesta al riesgo y su correspondiente objetivo.

En cuanto a la *Información y Comunicación*, sólo se maneja la información contable, siendo ésta la base de la identificación, evaluación y respuesta a los riesgos. La información obtenida desde el sector contable, fluye hacia los mandos superiores verticalmente.

El componente *Monitoreo* aún no ha sido abordado con profundidad por la empresa.

El gerenciamiento de riesgos es considerado fundamental, siendo uno de los objetivos para este 2009 tener implementado el ERM, apostando a liderar desde esta perspectiva, el sector en el que se encuentran.

La necesidad de implementar el ERM surge de la búsqueda de optimizar los costos a fin de maximizar los beneficios, aunque su implementación se ha visto limitada por motivos presupuestales y por la cultura existente en la organización. Un claro ejemplo es el hecho de que la capacitación a los gerentes respecto al tratamiento del riesgo se ha postergado en reiteradas oportunidades por problemas presupuestales.

En relación a la posibilidad de la utilización de un software específico de gestión de riesgos, consideran que sería de gran ayuda a la hora de ordenar y realizar un seguimiento del proceso, por lo cual ya han comenzado la búsqueda de distintos proveedores.

IV.2 Empresa B

Es una empresa nacional conformada por capitales extranjeros, la cual se ubica en el rubro financiero y tiene 13 años en el mercado. De acuerdo a la cantidad de empleados se la puede catalogar como una empresa mediana.

Respecto al *Ambiente Interno*, el Consejo de Administración está interesado en la difusión de la filosofía del riesgo en la organización. Un claro ejemplo de esto, es el hecho de que el área de Administración de Riesgo Operativo junto con el área de Compliance, han lanzado en meses anteriores un programa al que denominaron "Semana de Concientización". Con este programa lo que se

busca es la toma de conciencia del riesgo existente en las operaciones diarias del negocio para proteger la información de los *stake-holders* (clientes, proveedores, etc.) y la reputación de la compañía. El objetivo del programa es apoyar el compromiso de la organización respecto a la integridad de la información y a los altos estándares éticos, en todas las transacciones del negocio.

La gerencia procura que todas las políticas de la organización sean conocidas por todos sus miembros para que, de esta manera, se comience a afianzar la cultura del riesgo, que va de la mano de la cultura de alto desempeño. Con ello se logra que los riesgos sean comprendidos y que todos los individuos entiendan que absolutamente todas las acciones que se realizan poseen cierto grado de riesgo.

Respecto al apetito de riesgo, el mismo está definido en todos los procesos operativos de la organización, buscando asegurar un nivel de riesgo aceptable en las operaciones críticas. El apetito de riesgo operativo se monitorea de la siguiente manera:

- Con las tolerancias al riesgo definidas en los “Indicadores de Riesgo Clave”
- Mediante la aceptación de riesgo, según lo establecido en la “Autoevaluación de Riesgos y Controles”
- Con los objetivos de riesgo operativo
- Con las tolerancias mínimas para la presentación de reportes de incidentes

Para todos aquellos riesgos que se deciden “aceptar”, es decir, convivir con ellos sin necesidad de ningún plan de acción, la Gerencia debe argumentar su decisión y presentarla ante el Comité de Riesgo Operacional, junto con los planes de acción para aquellos riesgos que se decidió mitigar. Los riesgos aceptados deberán ser revisados anualmente con el fin de monitorearlos.

La empresa ha establecido tolerancias al riesgo; para ello ha definido “Indicadores de Riesgo Clave” para cada área dentro de la organización, con el fin de monitorearlas.

Respecto al *Establecimiento de Objetivos*, éstos se encuentran alineados con las tolerancias al riesgo establecidas. Los objetivos se dividen por unidad de negocio y la gerencia corrobora que sean coherentes con los objetivos globales.

El procedimiento que se utiliza para la *Identificación de Eventos*, se desprende de una política corporativa llamada “Autoevaluación de Riesgos y Controles”. Dicho proceso consiste en 5 fases: Preparación y Alcance, Identificación, Medición, Mitigación y Plan de acción.

Existe también otra política corporativa llamada “Reporte de Incidentes”, la cual establece un procedimiento que alcanza a todas las compañías donde la firma tenga participación accionaria y *management control*. Por consiguiente, este procedimiento alcanza a todos los procesos operativos, desde el reporte de los incidentes hasta el seguimiento de los planes de acción.

Cuando se detecta un evento, se deberá determinar si realmente se está ante un incidente que deba ser reportado, verificando si se cumple alguna de las siguientes condiciones:

- Se genere una pérdida financiera efectiva y significativa
- La situación detectada pueda generar una pérdida potencial significativa
- Esté en riesgo la imagen o reputación de la Compañía
- No se esté respetando el código de Compliance
- Se detecte alguna actividad de robo, hurto o fraude en la unidad de negocio
- Se detecte alguna situación que pueda ir en contra de la Ley o las normas del país

Cabe destacar que según la política de "Reporte de Incidentes", cualquier miembro de la firma puede detectar un evento de riesgo, el que debe reportar inmediatamente, de manera de minimizar lo más rápido posible el riesgo asociado. La centralización y administración de la Base de Datos de incidentes se encuentra a cargo del área de ORM (Operative Risk Management). El motivo de tener dicha base es el de poder recolectar información que permita identificar, clasificar, cuantificar, mitigar y realizar seguimiento de los incidentes reportados, con el objetivo de tomar medidas que garanticen su corrección, estableciendo lecciones aprendidas.

Si nos referimos a la política de "Autoevaluación de Riesgos y Controles", la identificación de eventos representa un esfuerzo conjunto de la primera y la segunda línea de defensa. Dentro de la primera línea de defensa se encuentran todas las unidades de negocio, mientras que en la segunda línea de defensa se encuentran áreas como las de ORM, IRM (Information Risk Management), Compliance, entre otras.

La política corporativa referente a los incidentes, establece que una vez al mes se deben revisar los incidentes reportados por todos los miembros de la organización y presentarse ante el Comité de Riesgo Operacional. Pueden existir incidentes que requieran de un reporte inmediato; es decir, que quien lo identifique deba denunciarlo al departamento de ORM local. Algunos ejemplos de incidentes inmediatos son: incidentes de crisis, incidentes reputacionales, ataques informáticos, demandas legales, fallas de seguridad en IT.

En lo que respecta a la identificación de eventos mediante la política de Autoevaluación de Riesgos y Controles, ésta se realiza una vez al año.

En relación a las herramientas utilizadas, las mismas se pueden dividir en función de las políticas de Identificación de Eventos. Respecto al Reporte de Incidentes, utilizan un *esquema de decisión*, el cual ayuda a identificar si el evento detectado es un incidente que pueda llegar a afectar a la organización. Respecto a la Autoevaluación de Riesgos y Controles, utilizan dos técnicas: *open-end* y *closed-end*. La técnica de open-end comienza con una "lluvia de ideas" para identificar las actividades que generan los riesgos

más importantes, mientras la técnica de closed-end utiliza cuestionarios, riesgos predefinidos, amenazas y vulnerabilidades, para identificar los riesgos.

Las principales fuentes de eventos que han afectado o pudieran afectar a la organización deben ser clasificadas de acuerdo a la siguiente categorización:

- ❑ Unauthorized Activity (Actividad no Autorizada): pérdida producida por un empleado no autorizado, una aprobación no autorizada o por sobrepasar una autoridad (overstepping of authority)
- ❑ Internal Crime & Fraud (Crimen interno o fraude): Pérdida por actividad fraudulenta, que involucre al menos una persona de la firma
- ❑ Information Security failure (Fallo en la seguridad de la información): Pérdida producida por la disponibilidad, integridad o confidencialidad de los datos
- ❑ External Crime & Fraud (Crimen o fraude externo): Pérdida por actividad fraudulenta, que no involucra funcionarios pertenecientes a la organización
- ❑ Employment malpractice and workplace safety failure (negligencia en el empleo y falta de seguridad en el lugar de trabajo): Pérdidas por actos inconsistentes en el empleo de normas legales de seguridad laboral, que pudieran originar pagos por reclamos de personas afectadas por el trabajo o por discriminación
- ❑ Client, products and business malpractice (Negligencia en el negocio, con productos o clientes): Pérdidas por negligencia producida al no poder cumplir las obligaciones profesionales con algún cliente específico, o debido a la naturaleza o diseño del producto
- ❑ Business Disruption (Interrupción del negocio): Pérdidas por eventos externos naturales (terremotos, huracanes, etc.) o producidos por el hombre (bomba, vandalismo, etc.)
- ❑ Systems Failure (Falla en los sistemas): Pérdidas producidas por un diseño inadecuado de los sistemas, por discontinuidad de los sistemas de IT, por fallas en software o hardware
- ❑ Processing Failure (Fallas en el procesamiento): Pérdidas por errores humanos sin intención durante un procesamiento
- ❑ Control Failure (Fallas en los controles): Pérdidas producidas por no cumplir con los lineamientos o estándares establecidos por el negocio (internos o externos)

Consultados por la particularidad de ciertos riesgos relacionados con los recursos humanos, tales como la continuidad de los directivos clave, los cambios de responsabilidades que pudieran influir en la eficacia del trabajo, los efectos potenciales sobre las reducciones de plantilla o las reasignaciones de capital, nos comentaron que debido a que el área de RRHH es clave dentro de la organización, hay una política corporativa específica. Dicha política se aplica a todos los individuos contratados y a aquellos que se pretendan contratar. Dado que esta política se basa en el riesgo, la gerencia local deberá decidir si debe emitir procedimientos más rigurosos para las posiciones que requieran estándares más elevados de integridad.

En cuanto a los riesgos relacionados con las desvinculaciones de personal de la empresa, se basan en el cuadro que se detalla a continuación:

Tipo de cese	Tipo de puesto	Riesgo
Despido	Puesto de Confianza	Alto
	Empleados en general	Alto
Renuncia	Puesto de Confianza	Medio
	Empleados en general	Bajo

Respecto a los riesgos provenientes de los sistemas de información, el Departamento de IT es quien realiza la primera evaluación del Incidente que puede acarrear algún riesgo a la organización. Analiza el Reporte y se determina si el incidente es un ataque real o una falsa alarma. De ser un ataque real, se identifica el tipo específico de ataque. Algunos tipos comunes de incidentes incluyen:

- 📁 Ataques a Website
- 📁 Ataques de denegación de servicio
- 📁 Barrido de puertos
- 📁 Ingeniería social
- 📁 Acceso no autorizado
- 📁 Infección de virus

Categorizar el incidente por tipo, contribuye a hacerle un seguimiento y a entender el riesgo al que se encuentra sometida la organización. El Departamento de IT es quien se encargará de evaluar la categoría del incidente, el impacto del problema (Bajo, Medio, Alto o Urgente), clasificarlo según su daño potencial, así como planificar las acciones correctivas de manera de devolver a los equipos informáticos comprometidos un estado seguro. Realizará el análisis de riesgo en torno al incidente para determinar los controles finales y evaluará si se requiere apoyo externo especializado y/o apoyo por parte de algún distribuidor.

En la *Evaluación de Riesgos*, la metodología seguida en este proceso se encuentra comprendida dentro de la política de "Autoevaluación de Riesgos y Controles".

Los riesgos deben ser evaluados en 3 niveles, a saber:

- 📁 **Riesgo inherente:** Evaluación de los riesgos asumiendo que no hay controles o mitigaciones.
- 📁 **Riesgo de gestión:** Evaluación de los riesgos en su actual entorno de control. La evaluación de la gestión de riesgo requiere la identificación de todos los controles existentes y la evaluación de la eficacia de los mismos.
- 📁 **Riesgo residual:** Evaluación de los riesgos residuales después de las acciones de mitigación previstas y relacionadas con el apetito de riesgo (primera línea de defensa). Los riesgos residuales críticos y altos son los que superan el nivel de tolerancia, por lo que deben asignarse determinados recursos para poder mitigarlos. Los riesgos medios no superan el nivel de tolerancia; no obstante, si están más allá del apetito de riesgo establecido, se deberán desarrollar acciones de mitigación. Los riesgos bajos no son materiales, pero la Gerencia

deberá hacerles un seguimiento y tomar las medidas apropiadas, a fin de prevenir su conversión en materiales.

La Evaluación de Riesgos es realizada en un taller conjunto, para garantizar la participación de los expertos del negocio (primera línea de defensa) y la segunda línea de defensa.

El proceso de "Autoevaluación de Riesgos y Controles" se realiza una vez al año.

Para la Evaluación de Riesgos, se utiliza la Matriz de Riesgos en términos de probabilidad e impacto. Ambos determinan el nivel de gestión actual de cada riesgo.

PROBABILIDAD	Casi Seguro					
	Probable					
	Posible					
	Poco probable					
	Raro					
		Insignificante	Menor	Moderado	Mayor	Catastrófico
	IMPACTO					

El objetivo de ORM es trasladar el riesgo con la más alta probabilidad/impacto a la esquina inferior izquierda tanto como sea posible, reduciendo las causas o impactos de los riesgos mediante la implementación de controles adecuados. Dicha Matriz se utiliza debido a una política corporativa.

El siguiente cuadro es un ejemplo de cómo el impacto podría ser traducido en cifras absolutas, dependiendo del alcance y del objeto del negocio o proceso:

Medidas cualitativas	Medidas cuantitativas (\$)
Insignificante	< 10.000
Menor	10.000 - 100.000
Moderado	100.000 - 1:
Mayor	1: - 10:
Catastrófico	> 10:

El siguiente cuadro es un ejemplo de cómo la probabilidad de ocurrencia de un riesgo operacional puede ser medida:

Medidas cualitativas	Medidas cuantitativas
Casi seguro	Todos los días
Probable	Una vez por mes
Posible	Una vez al año
Poco probable	Una vez cada 2 años
Raro	Una vez cada 10 años

A la hora de seleccionar técnicas cualitativas o cuantitativas, esta empresa no tiene preferencia por ninguna de las dos. Los riesgos deben ser evaluados a partir del impacto financiero (cuantitativo) o a través de su impacto no financiero (cualitativo). Los valores financieros son asignados a un riesgo sólo cuando los valores monetarios pueden ser razonablemente medidos, de lo contrario se utilizan las herramientas no financieras. Este es el criterio adoptado para todas las unidades de negocio.

Para la medición del impacto financiero sobre los riesgos se utiliza una escala de 11 niveles, que se detalla a continuación:

Financial impact											
€	< 10K	< 30K	< 100K	< 300K	< 1 mln	< 3 mln	< 10 mln	< 30 mln	< 100 mln	< 300 mln	> 300 mln
	Insignificant		Minor		Moderate		Major		Catastrophic		
	1	2	3	4	5	6	7	8	9	10	11

Los criterios utilizados para medir la probabilidad y el impacto, se detallan a continuación:

Casi Seguro	A	A	E	E	E
Probable	M	A	A	E	E
Posible	B	M	M	A	E
Poco probable	B	B	M	A	E
Raro	B	B	M	A	E
	Insignificante	Menor	Moderado	Mayor	Catastrófico

Escala de niveles de riesgo:

-  **E:** Extremo: Riesgo con pérdidas que ponen en peligro la existencia del negocio. Riesgo que requiere prioridad inmediata de la Dirección
-  **A:** Alto: Riesgo que requiere atención inmediata de la Dirección
-  **M:** Medio: Riesgo que no necesita atención inmediata, pero debe programarse su mitigación. Generalmente se asocia a riesgos que no presentan pérdidas materializadas hasta el momento, pero es probable que en algún momento se incremente su frecuencia y/o impacto

-  **B: Bajo:** Existen debilidades en los procesos pero las mismas se ven compensadas por los controles. No es generador de eventos de pérdida

Las evaluaciones de riesgo, junto con otras políticas corporativas se exponen a través del "NFR Dashboard" (Non Financial Risk Dashboard). Dicho Dashboard consta de:

-  Resumen Ejecutivo
-  "Heat map"
-  "Risk Footprint" para cada zona de riesgo
-  Principales incidentes
-  Tendencias del sector
-  Dos apéndices: Cumplimiento y Documentos de información

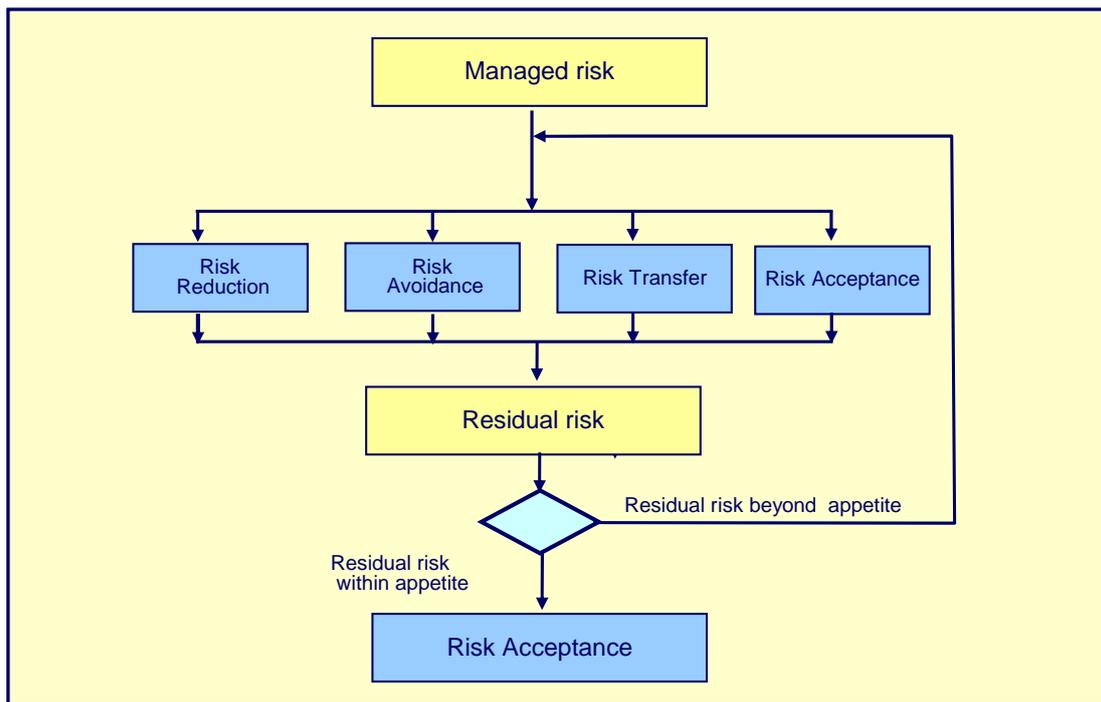
Consultados ante la posible incidencia de la crisis mundial en la firma, nos informaron que el departamento de ORM no ha evaluado aún dicho impacto.

Las estrategias de *Respuesta al Riesgo* para aquellos que exceden los niveles de tolerancia, se definen preferiblemente en un taller conjunto para garantizar la participación de los expertos (1^a y 2^a línea de defensa).

La respuesta al riesgo se puede lograr a través de varias combinaciones de las estrategias de mitigación que se detallan a continuación:

-  **Reducir el riesgo:** reducir la probabilidad de ocurrencia y/o el impacto.
-  **Evitar el riesgo:** dejar de desarrollar la actividad que genera el riesgo.
-  **Transferir el riesgo:** transferir o compartir el riesgo con otras partes. Algunos riesgos no financieros pueden ser transferidos al mercado de seguros, si los mismos son significativos pero no rentables para mitigarlos.
-  **Aceptar el riesgo:** los riesgos son aceptados bajo la justificación de que se encuentran dentro del nivel de riesgo establecido. Dicha decisión es tomada por el Comité de Riesgo Operacional.

El proceso de Respuesta al riesgo que se lleva a cabo es el siguiente:



Como *Actividades de Control* se define un *plan de acción* para la aplicación de controles adicionales o para mejorar los existentes, a fin de asegurar que las respuestas a los riesgos se llevan a cabo eficazmente. Se determinan las personas y/o funciones o departamentos que serán asignadas como responsables para su ejecución, así como también las fechas de vencimiento para la presentación práctica del plan. La empresa considera que uno de los principales beneficios de la autoevaluación es que los resultados provengan de las "partes interesadas", pues esto aumenta la aceptación de las decisiones adoptadas. Tanto la Gerencia General como el Comité son quienes decidirán cuáles son las medidas de mitigación a implementar que serán incluidas en el plan de acción. Esto se considera la última acción realizada dentro de la evaluación y del proceso de mitigación.

Luego de obtenida la aprobación por parte del Comité de Riesgo Operacional, se comienza con las acciones correctivas o medidas de mitigación, las cuales se llevan a cabo hasta que culmina su implementación y se obtienen los resultados esperados.

En cuanto a la *Información y Comunicación*, la información se suministra oportunamente de modo que permita actuar y vincularla a la necesidad de identificar, evaluar y responder a los riesgos. La información relevante se comunica al área de ORM, quien la envía al exterior en fechas límites prefijadas, para su control y aprobación.

En relación al componente *Monitoreo*, el mismo está integrado al componente Actividades de Control, y definido dentro de la política Autoevaluación de Riesgos y Controles.

La firma considera que el gerenciamiento de riesgos es sumamente importante. Trata de aplicar el enfoque de control definido por la "Política de Riesgo Operacional" de su accionista, el cual está basado en el desarrollo de un ambiente de control preventivo sobre los riesgos asociados a los procesos, actividades y sistemas que la soportan.

El posicionamiento de la empresa en cuanto a las habilidades de evaluación y administración de riesgos con respecto al mercado, es muy bueno, ya que cuenta con políticas corporativas que son el sustento de su control interno.

Cabe destacar que existen sistemas de capacitación continua dirigidos a los responsables del gerenciamiento del riesgo. Por otro lado, hasta el momento no han experimentado la necesidad de utilizar un software específico de gestión de riesgos.

Por el momento la única limitación en la implementación del ERM que esta empresa detecta, es la falta de compromiso que se requiere de todas las áreas de la firma, para dar razonable seguridad al proceso de gestión de riesgos.

IV.3 Empresa C

Es una sucursal de una empresa extranjera, la cual pertenece al rubro financiero y tiene cerca de 100 años en nuestro país. De acuerdo a la cantidad de empleados se la puede catalogar como una empresa grande.

Respecto al *Ambiente Interno*, existe por requerimientos tanto corporativos como por regulaciones locales, la obligación de difundir la filosofía del riesgo asumida por la organización, lo cual es realizado por la Gerencia General. Existen manuales en los cuales están definidas las distintas familias de riesgos, procedimientos y políticas que son utilizadas por las diferentes áreas según su responsabilidad, para llevar adelante las actividades asignadas. Dichas políticas establecen, por ejemplo, la responsabilidad y el rol de los funcionarios en la administración del riesgo, independientemente del nivel jerárquico ocupado en la organización.

Respecto al apetito de riesgo, ante la premisa de que cualquier actividad implica en sí misma un riesgo, como regla general se establece una tolerancia cero, lo cual luego se analiza por tipo de riesgo estableciéndose parámetros basados en el criterio de costo/beneficio. De todos modos hay riesgos, por ejemplo de franquicia, fraudes, legales, etc. que mantienen tolerancia cero, aún cuando el costo de mitigarlo sea mayor al beneficio.

En cuanto al *Establecimiento de Objetivos*, existen planes de negocios y presupuestos, alineados con las tolerancias al riesgo establecidas. Todas las áreas de la empresa funcionan en forma coordinada, teniendo objetivos específicos que permiten controlar el cumplimiento de las normas y los parámetros de tolerancia. Los objetivos se fijan anualmente y son revisados al menos trimestralmente o cuando puntualmente es requerido.

A fin de identificar las acciones para que se consigan los objetivos globales de la entidad, se definen y documentan los procesos y controles, y se realiza una verificación del cumplimiento de los mismos de manera periódica.

En cuanto a la *Identificación de Eventos*, además de los eventos que puedan ser identificados por el proceso normal del negocio, y utilizando la idoneidad de las personas en los controles, cuentan con un proceso de autoevaluación basado en listados de eventos. Dichos listados o inventarios de eventos son elaborados por la casa matriz y son adaptados a fin de incluir los riesgos propios de nuestra realidad nacional. La cultura y política corporativa de la empresa conlleva a que todas las personas, independientemente de su posición jerárquica, sean responsables por la identificación de eventos. El proceso formal recae en cada gerente de área, además de los aportes que específicamente realiza la Auditoría Interna.

Cuando se produce un evento, se considera el proceso y sus controles en un esquema end to end, o sea, no sólo se evalúa el evento en sí, sino todo el circuito con el que tuvo relación. Dependiendo del tipo de operativa/proceso/negocio, hay parámetros y métricas para detectar comportamientos irregulares y/o cambios en las tendencias, lo cual dispara alertas que les permiten estar preparados ante eventos anormales.

Dentro de las fuentes internas de generación de eventos, manifestaron que las mismas pueden surgir de errores en el diseño de los controles y de los sistemas, incumplimientos no detectados oportunamente, abuso de confianza y acuerdos entre dos o más personas para incumplir o violar los procedimientos y controles. Dentro de las fuentes externas, además de los riesgos propios de un negocio financiero (riesgos de mercado, crédito, etc.), se está expuesto a intentos de fraudes, siendo los más comunes los relacionados con tarjetas de crédito, redes de cajeros automáticos y cartas de crédito falsas.

Consultados por la particularidad de ciertos riesgos relacionados con los recursos humanos, nos manifestaron que la organización posee un sistema de identificación de puestos claves y de evaluación del personal para tener back up que permita la continuidad del negocio. Asimismo, por ser ésta una organización multinacional, en casos extremos pueden utilizarse recursos regionales para dar soporte. A fin de mantener el nivel de competitividad de la entidad dentro de su sector, la institución realiza encuestas sobre salarios y beneficios. Además de los laudos por convenios, se define una estrategia respecto al nivel salarial que la institución quiere mantener en relación al promedio de salarios del mercado.

Los riesgos que pudieran afectar la financiación, son analizados por comités integrados por el tesorero, la gerencia de créditos y el departamento de análisis de riesgos, que conjuntamente analizan la viabilidad de los negocios, financiación, riesgos, costo del dinero, tasas a cobrar, etc.

Para la *Evaluación de Riesgos*, se siguen los lineamientos establecidos por la casa matriz, basados en matrices de riesgos y sus controles asociados. La evaluación se realiza de forma trimestral y recae sobre cada gerente de área.

No utilizan un único método, para cada familia de riesgo se realizan distintos tipos de análisis para tomar medidas ante diferentes clases de eventos. Por ejemplo, ante el riesgo de liquidez, además de las previsiones de disponibilidades, se realizan simulaciones periódicas (Stress Testing) mediante la aplicación de diferentes modelos. En el caso del riesgo de liquidez y el riesgo de crédito, por ser una entidad financiera regulada por el BCU, existen modelos y requerimientos legales a cumplir para el normal funcionamiento.

El sistema corporativo utilizado en este componente, se basa en el registro de los riesgos, sus controles y la definición de resultados y planes de acción para regularizar las fallas. Con dichos resultados, se obtiene un rating sobre la calidad de los controles, y en los casos de incumplimientos o detección de brechas de control, se definen planes de acción para regularizarlos, asignándose responsables y plazos.

A modo de ejemplo, desarrollaremos el proceso de control que se realiza respecto a la prevención de actividades delictivas, conocidas como "lavado de dinero". En este proceso podemos identificar varias etapas:

-  Conocer al cliente - Aquí se deben cumplir todos los requisitos, tanto internos como regulatorios, para establecer una relación con un cliente y permitir la apertura de una cuenta en el banco. Aquí se incluyen, además de la información demográfica, controles de antecedentes (ej. Clearing de Informes), referencias bancarias, etc.
-  Controlar el origen de los fondos: Se obtiene la documentación que justifique el patrimonio que el cliente declara poseer y los fondos que regularmente tendrá depositados en el banco.
-  Monitorear: Más allá de lo que el cliente declara, mensualmente hay sistemas que analizan las transacciones realizadas, emitiéndose alarmas cuando dichas transacciones difieren del perfil esperado para ese cliente. Es común que personas sin antecedentes delictivos y que presentan información real para la apertura de una cuenta, luego manejen fondos que no se correspondan con su capacidad económica, lo cual se convierte en una actividad sospechosa.

A la hora de exponer las distintas evaluaciones, se utiliza un sistema corporativo que agrupa las mismas según familias de riesgos.

Las *Respuestas al Riesgo* están definidas en las políticas; aquellos riesgos no contemplados por las mismas o que superen las tolerancias establecidas localmente, son escalados dentro de la organización. Dichas respuestas son abordadas por las distintas gerencias, de acuerdo a sus potestades.

La elección de la respuesta se realiza sobre casos puntuales, no como parte de un proceso iterativo. Se evalúa en cada caso si los riesgos residuales están de acuerdo a las tolerancias establecidas por las políticas corporativas. La evaluación costo/beneficio, considerada a la hora de seleccionar las

respuestas, se basa en la probabilidad de ocurrencia y posible impacto del evento.

A fin de garantizar la seguridad y el respaldo de los sistemas de información, se siguen los lineamientos establecidos en los planes de contingencia, existiendo respaldos de información, equipamiento (Data Center duplicado) y alojamiento como para asegurar la continuidad del negocio.

Como *Actividades de Control* se utilizan métricas, resultados de revisiones y autoevaluaciones. Se hacen revisiones regulares, tanto por parte de Auditoría Interna como de Auditoría Corporativa, verificándose el cumplimiento y a su vez, que los controles sean adecuados. Dichas revisiones se llevan a cabo anualmente.

En cuanto al componente *Información y Comunicación*, la información relevante se comunica oportunamente a las gerencias locales y regionales.

Existen evaluaciones internas y externas con relación al proceso de gestión de riesgos llevadas a cabo por personal idóneo. Dicho *Monitoreo* se realiza sobre las áreas donde previamente se habían definido respuestas; si un área no tiene por su actividad importantes riesgos asociados, no se incluye en la rutina de control regular, pero sí es monitoreada a efectos de verificar que no ha sufrido cambios que impliquen riesgos no identificados.

Debido al sector al que pertenece, consideran que la gestión de riesgos es un pilar para su organización, ya que el negocio bancario tiene implícitos una pluralidad de riesgos que hay que afrontar diariamente. La necesidad de implementar el ERM surgió por iniciativa corporativa, siendo fundamental su contribución a la consecución de los objetivos globales de la entidad. Hoy en día, la metodología aplicada por esta empresa, es apreciada en el mercado financiero.

Cabe destacar que existen sistemas de formación continua dirigidos a los responsables del gerenciamiento de riesgos, entre los cuales se encuentra la capacitación respecto al software específico utilizado. Dicho software permite sistematizar y estandarizar el proceso, dando también accesibilidad a toda la organización.

La principal limitación que han encontrado respecto a la implementación del ERM, ha sido la dificultad de llevar a cabo un cambio en la cultura de los integrantes de la empresa.

CAPÍTULO V



**ANÁLISIS
COMPARATIVO**

V ANÁLISIS COMPARATIVO

Previo a comenzar con el análisis, creemos necesario destacar nuevamente que de las tres empresas que formaron parte del trabajo de campo, dos de ellas (empresas B y C) se encuentran avanzadas en el proceso de gestión de riesgos, mientras que la empresa A se encuentra en las primeras fases de implementación del mismo.

Nuestro análisis consistirá en comparar las tres empresas respecto a cada uno de los componentes del ERM, tratando de encontrar similitudes y señalar las diferencias que se nos presentaron al arribar a las conclusiones del trabajo.

Ambiente Interno

La empresa A aún no ha podido sortear el desafío que significa establecer la cultura del riesgo en toda organización, sin lograr que todos los individuos conozcan su rol en la Administración del riesgo. En la empresa B en cambio, la cultura del riesgo está internalizada, contando con programas específicos que impulsan la toma de conciencia del riesgo existente en las operaciones diarias del negocio. Respecto al apetito de riesgo, éste alcanza a todos los procesos operativos de la organización y se busca asegurar que el riesgo se encuentre en niveles aceptables. La empresa ha establecido tolerancias al riesgo, definiendo “Indicadores de Riesgo Clave” para cada área. En la empresa C, al igual que en la anterior, la cultura del riesgo está internalizada, existiendo políticas claras que definen la responsabilidad y el rol de cada integrante de la organización en la Administración del riesgo. Respecto al apetito de riesgo, como regla general se establece una tolerancia cero.

Establecimiento de Objetivos

En las tres empresas existen, aunque con sus particularidades, planes de negocios y presupuestos alineados con las tolerancias al riesgo establecidas. La principal diferencia que encontramos es respecto al grado de comunicación de los objetivos, siendo ésta una falencia en la empresa A, ya que tan sólo son comunicados a los mandos superiores.

Identificación de Eventos

La empresa A maneja la matriz FODA como base principal en este componente, y utiliza talleres de trabajo como técnica preferencial. La metodología utilizada por la empresa B, se desprende de dos políticas corporativas, “Autoevaluación de Riesgos y Controles” y “Reporte de Incidentes”. En cuanto a la empresa C, cuenta con un proceso de autoevaluación basado en listados de eventos.

En las tres empresas la Identificación de Eventos es liderada por gerentes de área y jefes, aunque es clara la diferenciación que surge respecto a la empresa A, donde debido a que la cultura del riesgo no se ha instaurado aún, el grado de involucramiento del resto del personal, es sensiblemente menor comparado con las otras dos empresas, donde todos los integrantes se sienten involucrados en la identificación de eventos. La empresa C utiliza además de

los mencionados listados de eventos, dispositivos de escala o umbral que funcionan como disparadores para aplicar respuestas preseleccionadas. Las empresas B y C se basan en políticas corporativas, mientras que el proceso de identificación de la empresa A, no viene predefinido por sus accionistas, y se otorga libertad a la Dirección para establecer sus propios lineamientos.

En relación a las principales fuentes de generación de eventos que han afectado o pudieran afectar a las organizaciones, la empresa A hace énfasis en aquellas originadas en los Recursos Humanos, como por ejemplo los paros, la ocupación del local y la alta rotación de personal, asociada a la dificultad de selección de personal. Las empresas B y C, por su parte, sin desestimar los riesgos relacionados con los RRHH, destacan fallas en los sistemas de información, como ser posibles fraudes, y fallas en los sistemas de IT, como por ejemplo ataques informáticos que generen problemas respecto a disponibilidad, integridad y confiabilidad de los datos. Esta priorización respecto a las fuentes de eventos, se basa en el grado de exposición al que se enfrentan o que se han enfrentado dichas organizaciones.

Evaluación de Riesgos

La empresa A, siendo consistente con la etapa anterior, utiliza la matriz FODA. Una vez identificados los eventos, los gerentes evalúan los riesgos en base a su probabilidad e impacto, desde la perspectiva de las debilidades que posee y las amenazas a las que se enfrenta. En la empresa B, los lineamientos establecidos en la política Autoevaluación de Riesgos y Controles, indican que dicha evaluación debe ser realizada por un taller conjunto, para garantizar la participación de los expertos de negocio. La empresa C sigue los principios establecidos por su casa matriz, basándose en matrices de riesgos y sus controles asociados y las principales responsabilidades recaen sobre cada gerente de área.

A la hora de seleccionar técnicas que soporten la aplicación de la herramienta, la empresa A opta por las cualitativas, debido a que no cuenta, en todos los casos, con la información necesaria para utilizar una técnica cuantitativa. En las restantes empresas, no existe preferencia por ningún tipo de técnica, dependiendo de las circunstancias, el uso de unas u otras.

En cuanto a las herramientas de Evaluación de Riesgos, la empresa A utiliza principalmente Backtesting, Benchmarking competitivo o sectorial e interno; la empresa B maneja la Matriz de Riesgos en términos de impacto y frecuencia; en tanto que la empresa C no utiliza un único método, sino que para cada familia de riesgos, se realizan distintos tipos de análisis. Por ejemplo, ante el riesgo de liquidez se aplica Stress Testing; y por ser una entidad financiera regulada por el BCU, existen modelos y requerimientos legales a aplicarse para otras familias de riesgos.

Tanto la empresa B como la C cuentan con criterios predefinidos a la hora de evaluar la probabilidad e impacto de los eventos, mientras que en la empresa A, las distintas unidades de negocio se basan en criterios subjetivos, primando la intuición. Esto último ha ocasionado que en el pasado, ante ciertos eventos, se haya subvaluado la probabilidad o impacto de los mismos.

Respuesta al Riesgo

En relación a las Respuestas al Riesgo, en la empresa A, las mismas se han tomado en base a decisiones de cada gerente de área o reuniones del staff de gerentes, pero no hay un lineamiento predefinido por el Directorio ni documentación que respalde las mismas. En la empresa B las estrategias de Respuesta al Riesgo, para aquellos riesgos que exceden los niveles de tolerancia, deben ser definidas preferiblemente en un taller conjunto que garantice la participación de los expertos. En relación a la empresa C, éstas se encuentran definidas en las políticas; aquellos riesgos no cubiertos por las mismas o que superen las tolerancias establecidas localmente, son escalados dentro de la organización. Dichas respuestas son abordadas por las distintas gerencias y la elección de las mismas se realiza sobre casos puntuales, no como parte de un proceso iterativo.

Actividades de Control

En la empresa A se realizan auditorías de cumplimiento externas con el fin de verificar que se respeten las exigencias establecidas. A su vez, se realizan controles periódicos que buscan cotejar la información suministrada por los distintos presupuestos con la realidad de las distintas unidades de negocio. Sin embargo, las actividades de control no se revisan con la periodicidad adecuada, a fin de comprobar que continúen siendo apropiadas. En la empresa B se define un plan de acción para la aplicación de controles adicionales o para mejorar los existentes, con el objetivo de asegurar que las respuestas a los riesgos se lleven a cabo eficazmente. Consideran que uno de los principales beneficios de la autoevaluación es que los resultados provengan de las "partes interesadas" pues esto aumenta la aceptación de las decisiones adoptadas. La empresa C, por su parte, utiliza métricas, resultados de revisiones y autoevaluaciones, las que, a su vez, son evaluadas en forma regular, tanto por parte de la Auditoría Interna como de la Auditoría Corporativa.

Información y Comunicación

La empresa A tan sólo maneja oportunamente la información contable, la cual fluye hacia los mandos superiores verticalmente. En la empresa B toda la información se suministra oportunamente, de modo que permita actuar y vincularla a la necesidad de identificar, evaluar y responder a los riesgos, comunicándose aquella que sea relevante al área de ORM. Por su parte, en la empresa C la información se comunica oportunamente a las gerencias locales y regionales.

Monitoreo

El componente Monitoreo, aún no ha sido abordado sistemáticamente por la empresa A; en la empresa B, es abordado conjuntamente con las Actividades de Control; mientras que en la empresa C existen evaluaciones internas y externas con relación al proceso de gestión de riesgos, llevadas a cabo por personal idóneo sobre las áreas donde previamente se habían definido respuestas; si un área no tiene importantes riesgos asociados, no se incluye en la rutina de control regular, pero sí es monitoreada a efectos de verificar que no sufrió cambios que involucren riesgos no identificados con anterioridad.

CAPÍTULO VI



CONCLUSIONES

VI CONCLUSIONES

Encontrar la metodología para la aplicación del ERM que más se adapte a las empresas uruguayas es un proceso difícil, ya que las mismas tienen realidades muy diferentes no sólo entre ellas sino también con relación a sus homónimas del exterior. A pesar de ello, se puede observar en las organizaciones una tendencia creciente a migrar hacia una cultura y estructura que promueve la Gestión de Riesgos, generada por las necesidades impuestas por cambios dinámicos en los contextos económicos globalizados.

Creemos que el ERM debería ser de aplicación obligatoria en Uruguay para ciertos tipos de entidades, tanto públicas como privadas, como por ejemplo empresas que coticen en Bolsa, que emitan obligaciones negociables o instituciones financieras, ya que el mismo proporciona principios integrados, terminología común y una orientación práctica que da soporte a la implantación de la Gestión de Riesgos en la empresa.

Consideramos vital para la aplicación del ERM, comenzar por definir la cultura del riesgo y luego difundirla a todos los niveles de la organización, ya que esto redundará en una actitud proactiva de todos los integrantes frente a la Administración del Riesgo. Entendemos la dificultad que esto conlleva, basándonos, entre otras cosas, en que dos de las empresas analizadas, identificaron este aspecto como el principal obstáculo al que se enfrentaron. Debería generarse una estructura apropiada que cuente con la definición de un Gerente de Riesgos y la conformación de un Comité de Riesgos, que lideren todo el proceso. Una buena medida que soporte el mismo, es la creación de programas impulsados por el Consejo de Administración, que busquen concientizar a todos los integrantes de la organización. Un ejemplo de ello es la "Semana de la Concientización" observada en una de las empresas.

El Ambiente Interno es considerado la base para los demás componentes de la gestión de riesgos, ya que provee de la filosofía respecto a los mismos, que la Dirección impulsa, proporcionando a las organizaciones capacidades para identificar, evaluar y responder a los riesgos. Un elemento relevante a considerar en dicho componente lo constituye el Riesgo Aceptado.

Luego de que se logre contar con un Ambiente Interno propicio, la empresa debe asegurarse que los objetivos sean coherentes con el Riesgo Aceptado. Dichos objetivos deben fijarse antes que la institución pueda identificar potenciales eventos (riesgos u oportunidades) que afecten su concretización. Los mismos deben ser revisados periódicamente con el propósito de verificar que continúen siendo válidos.

Una vez establecidos los objetivos, se procede a identificar los eventos. Al identificarlos, la Dirección reconoce que existen incertidumbres, dado que no sabe si el evento ocurrirá, cuándo acontecerá o cuál será su impacto preciso. Sin embargo, en esta etapa sólo se procederá a identificar eventos, sin tomar en consideración su probabilidad de ocurrencia ni su posible impacto.

Si tomamos al riesgo como la diferencia entre lo ocurrido y lo esperado, podemos admitir que lo ocurrido puede resultar mejor o peor que lo esperado. Esto implica por un lado, la existencia de un evento que ocurrirá en el futuro y a su vez, la presencia de variables aleatorias, pues si las variables no contaran tal característica, no habría riesgo.

En relación a los factores que generan los eventos, la Dirección deberá entender la importancia de aquellos que afecten en mayor medida a la empresa y el tipo de evento que pueden provocar. Por ejemplo, una empresa que se enfrente a una rotación negativa de personal, como es el caso de una de las empresas analizadas, deberá considerar como factores más influyentes aquellos relacionados con los recursos humanos, sin embargo una empresa que se enfrente al riesgo de fraude, deberá considerar que también pueden influir en dicho evento los factores tecnológicos. El priorizar determinados factores, no significa que se deba desestimar el resto de los mismos.

De acuerdo al documento Marco Integrado ERM, se pueden utilizar distintas técnicas a la hora de identificar eventos. Una empresa podría comenzar el proceso de identificación realizando un análisis del flujo de procesos, a los efectos de considerar las entradas, tareas, responsabilidades, y salidas que están presentes en el mismo. Esta técnica debería ser acompañada por talleres de trabajo, para así aprovechar el conocimiento y la experiencia acumulada de la Dirección, el personal y los grupos de interés en dicho proceso, a través de discusiones estructuradas. De la combinación de ambas técnicas, surgirá un listado detallado de acontecimientos potenciales que podrían originarse en la empresa. Creemos oportuno contar con dispositivos de escala o umbral para que éstos alerten a la dirección respecto a áreas con potenciales problemas, comparando transacciones o eventos actuales con criterios predefinidos. En nuestro trabajo de campo observamos la aplicación de diferentes técnicas con distintos grados de avance; sin embargo las técnicas previamente mencionadas, no pretenden ser una lista taxativa, sino simplemente una guía para la implementación de la Gestión de Riesgos. Por otro lado, las técnicas que se mencionan en el Marco Integrado ERM, pueden ser adaptadas o suplantadas por otras que se adecuen mejor a la realidad de cada empresa. Por ejemplo la técnica de "reporte de incidentes" utilizada por una de las empresas, es una adaptación de la técnica propuesta por el ERM denominada "indicadores de eventos importantes".

Si bien es importante que la Dirección encamine las acciones necesarias a la hora de identificar eventos, esta etapa se ve reforzada si se cuenta con un alto nivel de participación de todos los miembros de la organización. Por otro lado es necesario contar con mecanismos de difusión de los eventos identificados, así como con mecanismos de actualización e investigación de nuevos acontecimientos.

Como último punto de este componente, cabe recordar que los eventos no ocurren de forma aislada, por lo que un acontecimiento puede ser desencadenante de otro, y al identificarlo la Dirección deberá entender cómo estos eventos se relacionan entre sí. A modo de ejemplo, en una de las empresas analizadas, cuando se produce un evento, se considera el proceso y

sus controles en un esquema end to end, no sólo evaluando el hecho en sí, sino también su interrelación con otros.

Una vez identificados los eventos potencialmente negativos, es necesaria su evaluación. Para llevarla a cabo, el primer paso es medir la probabilidad y el impacto de los eventos identificados. Existen diferentes formas de realizar tal evaluación, algunas basadas en técnicas cualitativas y otras en técnicas cuantitativas. Una manera práctica de comenzar el proceso, es evaluar los eventos basándose en las experiencias pasadas de la propia empresa, lo que le otorgará un mayor grado de objetividad que apoyándose solamente en la intuición de quien evalúe los eventos. Por otro lado, la comparación con otras empresas del sector (Benchmarking), puede otorgar un conocimiento más profundo, ya que toma en cuenta las experiencias de otras organizaciones. En nuestro trabajo de campo, pudimos observar que dicha técnica es aplicada por algunas empresas en nuestro medio. A su vez existen otras técnicas más sofisticadas, algunas de las cuales son aplicadas por las empresas estudiadas; por ejemplo una de ellas aplica Backtesting, comparando el cashflow real con el proyectado; otra empresa, por su parte, aplica Stress Testing, simulando situaciones extremas para poder observar el impacto que podría tener un evento si ocurriera en el futuro. Al igual que en la etapa de Identificación, el ERM proporciona ejemplos de técnicas a utilizar al evaluar los riesgos, las cuales tampoco son taxativas, siendo factible su adaptación al contexto de la empresa. Por ejemplo, una de las empresas utiliza para esta etapa, la herramienta de Autoevaluación de Riesgos y Controles, mediante la cual maneja técnicas cuantitativas para los riesgos con impacto financiero y cualitativas para los no financieros. Poseen escalas de medición predeterminadas, tanto de la probabilidad como del impacto, que relacionan medidas cuantitativas con cualitativas.

Las distintas evaluaciones deben presentarse de una manera clara y concisa, más aún al tratarse de evaluaciones cualitativas, ya que los riesgos no se traducen en una cifra o intervalo numérico, como sucede en las técnicas cuantitativas. Entre las diferentes formas de exposición podemos encontrar Mapas de Riesgos, los cuales pueden ser presentados como mapas de calor o flujos de procesos y mapas de riesgo matricial y mapas de riesgo con la variabilidad de probabilidad e impacto. A nuestro entender la forma más clara de presentación es mediante los mapas de calor, utilizados por una de las empresas de nuestro trabajo de campo.

Una vez evaluados los riesgos, se deberá optar por aquella respuesta más eficiente, no significando esto, que los mismos deban ser necesariamente eliminados. Algunos no podrán eliminarse debido, no sólo a la existencia de riesgos no diversificables, sino por el hecho de que al evaluarlos, pueda incluso optarse por convivir con ellos, dado que el costo de deshacerse de los mismos, pueda llegar a ser más elevado que el que podría llegar a ocasionar la ocurrencia del evento.

La elección de la respuesta deberá tener en cuenta las tolerancias establecidas al fijarse los objetivos, ya que si al aplicar determinada respuesta, la misma no minimiza el impacto y/o la probabilidad hasta fijar al

riesgo en un nivel tolerable, se deberán seguir aplicando recursos hasta alcanzar dicha meta o se deberán reevaluar las tolerancias. A su vez, la Dirección no sólo deberá considerar los riesgos desde una perspectiva individual, sino que debería hacerlo en conjunto, obteniendo así una visión de portafolio de riesgos. Dicha visión permite determinar si el perfil de riesgo residual de la entidad está en consonancia con riesgo aceptado global.

En este momento, se consideran con mayor énfasis aquellos eventos que pudieran resultar en un efecto positivo para la organización, por lo que la gerencia deberá encauzar las acciones necesarias a fin de canalizarlos hacia la estrategia.

Es recomendable que la decisión sobre una determinada respuesta sea tomada en acuerdo entre la Dirección y las distintas gerencias, a fin de que la misma sea consistente con las estrategias previamente establecidas.

Para asegurar que las respuestas se lleven a cabo eficazmente, se establecen políticas y procedimientos que constituyen las actividades de control. Sobre las mismas se recomienda la realización de auditorías, tanto internas como externas, a fin de verificar su eficaz cumplimiento y, a su vez, que dichos controles sean los adecuados. Esto fue observado en detalle en una de las empresas.

Respecto a la Comunicación e Información, creemos oportuno destacar que debe estar presente en cada uno de los componentes del ERM. La organización deberá contar con los canales necesarios, a fin de que cada miembro de la misma pueda transmitir la información relevante oportunamente, sin encontrar obstáculos ni interferencias.

En el proceso de administración del riesgo es importante que se ejecute el Monitoreo, supervisando tal proceso permanentemente y realizando las modificaciones que se consideren oportunas. Como se pudo observar en una de las empresas, el monitoreo se realiza sobre las áreas donde previamente se habían definido respuestas: si un área no tiene riesgos asociados no se incluye en la rutina de control, pero sí se monitorea para verificar que no sufrió cambios que impliquen riesgos asociados.

La gestión de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en el que cada componente influye en el otro.

Consideramos que la utilización de un software de gestión de riesgos puede ser una herramienta útil a la hora de implementar el proceso, así como para facilitar la participación de todos los miembros de la organización y la comunicación de los resultados obtenidos.

Del relevamiento realizado, podemos concluir, que si bien el riesgo es considerado prioritario a la hora de diseñar los procesos operativos, muy pocas organizaciones cuentan con técnicas sofisticadas para administrarlo. Uno de los factores determinantes, es el alto costo asociado a su

implementación, ya que, según lo investigado, aún hoy es difícil de visualizar, por parte de los empresarios, el beneficio que el ERM otorga. Otro factor podría encontrarse en el hecho de que en Uruguay no es obligatoria la aplicación de técnicas de gerenciamiento de riesgos tal como se exponen en el ERM, aunque podemos encontrar, por ejemplo, el caso de las empresas financieras, las cuales están obligadas a la utilización de Basilea II. En nuestro trabajo de campo, la utilización del ERM por parte de algunas de las empresas, surgió por iniciativa corporativa, lo cual nos hace suponer que hasta que no exista una reglamentación que lo exija, el mismo no será de aplicación masiva en nuestro país. Esta realidad hace que las empresas, en el Uruguay, queden rezagadas respecto a sus pares del exterior, al no aprovechar las herramientas disponibles, ya que la Administración de Riesgos está tomando cada vez mayor relevancia a nivel mundial.

Una vez que las organizaciones comienzan a aplicar el ERM, su utilización sistematiza los procesos de administración de riesgos, logrando que todos los individuos participen de manera proactiva en la identificación, evaluación y respuesta a los riesgos, tornando más eficiente a la organización.

CAPÍTULO VII



CUESTIONARIO

VII ANEXO - CUESTIONARIO TRABAJO DE CAMPO

Datos generales de la empresa

- 1) ¿En qué rubro se desempeña?
- 2) ¿Qué antigüedad tiene en el Uruguay?
- 3) ¿Qué cantidad de empleados posee?
- 4) ¿Es una empresa nacional o subsidiaria de una extranjera?

Ambiente interno

- 5) ¿Considera que el Consejo de Administración está interesado en la difusión de la "cultura del riesgo" en la organización?
- 6) ¿Cómo procura la gerencia que la cultura del riesgo esté lo suficientemente reconocida y valorada en la organización? ¿Existe alguna documentación al respecto?
- 7) ¿Considera usted que cada individuo entiende su rol y responsabilidad en la administración del riesgo?
- 8) ¿Cuánto riesgo está dispuesta a asumir la organización? ¿Se ha fijado un apetito de riesgo global o sectorizado? ¿Qué elementos fueron considerados a la hora de fijarlo?
- 9) ¿Se han definido tolerancias al riesgo?

Establecimiento de objetivos

- 10) ¿Mediante qué acciones se corrobora que el plan estratégico elaborado tiene en cuenta y es coherente con los objetivos globales? Estos objetivos, ¿se alinean con la tolerancia al riesgo establecida?
- 11) ¿Con qué periodicidad se comunican los objetivos globales a la gerencia y demás empleados de la organización?
- 12) ¿De qué manera la Gerencia Ejecutiva identifica las acciones que deben llevarse a cabo con éxito, o las fallas que han de evitarse, para que se consigan los objetivos globales de la entidad?

Identificación de eventos

- 13) ¿Podría Ud. describir el proceso utilizado por la empresa para la identificación de eventos?
-

- 14) ¿Sobre quiénes recae la identificación de eventos?
 - 15) ¿Con qué periodicidad se revisa el proceso de identificación de eventos?
 - 16) ¿Qué herramienta/s se utilizan para identificar posibles eventos que la puedan afectar?
 - 17) ¿Considera la interrelación de eventos al momento de identificarlos?
¿Cómo?
 - 18) ¿Qué mecanismo utiliza la organización para la detección e identificación oportuna de eventos no esperados?
 - 19) Los eventos son generados por fuentes internas y externas, ¿podría identificar las principales fuentes que han afectado o pudieran afectar a su organización?
 - 20) ¿Cómo considera usted que podrían afectar a la organización los riesgos relacionados con los recursos humanos, tales como la continuidad de los directivos clave o los cambios de responsabilidades que pudieran influir en la eficacia del trabajo?
 - 21) ¿Se busca detectar los riesgos resultantes de las relaciones laborales, por ejemplo, los vinculados a los programas de remuneraciones y otros beneficios que buscan mantener el nivel de competitividad de la entidad dentro de su sector?
 - 22) ¿Se analizan los efectos potenciales sobre las reducciones de plantilla o las reasignaciones de personal?
 - 23) ¿Qué medidas se toman al analizar los riesgos que puedan afectar la financiación, es decir, la disponibilidad de fondos para las iniciativas nuevas o la continuación de programas claves?
 - 24) ¿Cómo detectan los riesgos provenientes de los sistemas de información?
 - 25) ¿Se realizan investigaciones de mercado para identificar las principales variaciones en la naturaleza, preferencias y tendencias de los clientes?
 - 26) ¿Se efectúa un seguimiento a las nuevas tecnologías o aplicaciones desarrolladas por la competencia?
 - 27) ¿Se han identificado riesgos relacionados con el cumplimiento de regulaciones o acuerdos contractuales?
 - 28) Al identificar eventos detectándose una oportunidad, ¿cuál es el procedimiento a seguir para canalizarla a la estrategia?
-

Evaluación de riesgos

- 29) ¿Podría Ud. describir el proceso utilizado por la empresa para la evaluación de riesgos como continuación del proceso anterior?
- 30) ¿Sobre quiénes recae la evaluación de riesgos?
- 31) ¿Con qué periodicidad se revisa el proceso?
- 32) ¿Qué herramienta/s utiliza para evaluarlos?
- 33) ¿Por qué optó por ellas? ¿Cuáles fueron las herramientas específicamente descartadas?
- 34) A la hora de seleccionar técnicas ¿tiene preferencia por las cuantitativas o las cualitativas?
- 35) Teniendo en cuenta que algunas unidades de negocio pueden utilizar técnicas cualitativas y otras cuantitativas; ¿cómo asegura la concordancia entre las evaluaciones realizadas?
- 36) ¿Qué criterios se utilizan para medir la probabilidad e impacto de los eventos?
- 37) ¿Han sucedido eventos con alto impacto que hubieran sido previamente descartados por su escasa probabilidad de ocurrencia? En caso afirmativo ejemplifique
- 38) Al evaluar el impacto y la probabilidad, ¿la Gerencia utiliza la misma unidad de medida que la empleada para la medición del objetivo?
- 39) ¿Qué herramientas utilizan para exponer las evaluaciones de riesgo?
- 40) ¿Evalúa la probabilidad y el impacto en la productividad ante la eventualidad de inasistencias en el personal?
- 41) ¿Ha evaluado la probabilidad y el impacto de la actual crisis mundial en la organización?

Respuesta al riesgo

- 42) ¿Podría Ud. describir el proceso para la selección de respuestas al riesgo utilizado por la empresa como continuación del proceso anterior?
 - 43) ¿Sobre quiénes recae la decisión de adoptar determinada respuesta al riesgo?
 - 44) ¿La elección de la respuesta forma parte de un proceso iterativo? ¿Con qué periodicidad se replantea la misma?
-

- 45) ¿Qué opciones de respuestas -evitar, reducir, aceptar y compartir- ha aplicado? ¿Podría darnos un ejemplo de cada una de las opciones?
- 46) ¿Qué criterios considera al evaluar si los riesgos residuales están dentro de la tolerancia al riesgo establecida?
- 47) ¿De qué manera tiene en cuenta la Gerencia los costos en relación a los beneficios al optar por determinada respuesta?
- 48) ¿Qué acciones se toman ante los eventos que pudieran provocar cambios significativos en el personal, ya sean externos o internos, y que pudieran afectar al nivel profesional del personal disponible?
- 49) ¿Se incrementa en lo necesario el número de empleados de operaciones, contabilidad y procesamiento de datos para hacer frente al aumento en el volumen de actividad? ¿Se tiene en cuenta si son aumentos permanentes o temporarios?
- 50) ¿Qué medidas se llevan a cabo para garantizar la seguridad y el respaldo de los sistemas de información?
- 51) Al identificar respuestas; ¿han descubierto oportunidades que no habían sido consideradas?

Actividades de control

- 52) ¿Qué mecanismos de seguimiento se establecen a fin de asegurar que las respuestas a los riesgos se llevan a cabo eficazmente?
- 53) ¿Con qué periodicidad se analiza si las actividades de control existentes continúan siendo apropiadas teniendo en cuenta su relevancia y adecuación a la respuesta al riesgo y su correspondiente objetivo?

Información y comunicación

- 54) ¿La información se suministra oportunamente de modo que permita actuar y vincularla a la necesidad de identificar, evaluar y responder a los riesgos?
- 55) ¿A quién se comunica la información relevante obtenida en dicho proceso?

Monitoreo

- 56) ¿Existen evaluaciones internas o externas con relación al proceso de gestión de riesgos?
-

- 57) ¿El evaluador comprende cada una de las actividades del ente y cada componente de la gestión del riesgo empresarial abordados?
- 58) ¿Se realiza monitoreo en aquellas áreas donde no se han definido respuestas a los riesgos?

Genéricas

- 59) ¿Qué tan relevante considera usted que es el gerenciamiento de riesgos para su organización?
 - 60) ¿Cuál es su perspectiva sobre el posicionamiento de la empresa en cuanto a las habilidades de evaluación y administración de riesgos con respecto al mercado?
 - 61) ¿Cómo surgió la necesidad de implementar el ERM? ¿Comenzaron por algún área en particular? ¿Cuál?
 - 62) ¿Cómo valora la contribución de la aplicación del ERM a la consecución de los objetivos globales de la entidad?
 - 63) ¿Existen sistemas de capacitación continua dirigidos a los responsables del gerenciamiento de riesgos?
 - 64) ¿Qué ventajas encuentra o encontraría en la utilización de un software específico de gestión de riesgos?
 - 65) ¿Se realizan auditorías al proceso de ERM? ¿Con qué periodicidad?
 - 66) ¿Ha encontrado limitaciones en la implementación del ERM? ¿Cuáles fueron las principales?
-

CAPÍTULO VIII



GLOSARIO

VIII GLOSARIO

Categoría de Objetivos

Cada una de las cuatro categorías de objetivos de la entidad; estratégica, efectividad y eficiencia en las operaciones, confiabilidad de la información y cumplimiento de leyes y regulaciones aplicables. Las categorías se trasladan, de modo que un objetivo determinado puede incidir en más de una categoría.

Componente

Hay ocho componentes en la administración de riesgos corporativos; ambiente interno de la entidad, establecimiento de objetivos, identificación de eventos, evaluación de riesgos, respuesta a los riesgos, actividades de control, información y comunicación, y monitoreo.

Consejo de Administración

Grupo directivo de una sociedad empresarial integrado por personas elegidas por la asamblea general de accionistas. Su función es de dirección y vigilancia. Jerárquicamente se localiza entre la asamblea general de accionistas y la dirección o gerencia general.

Control

- Sustantivo que indica un concepto, por ejemplo, existencia de un control, una política o procedimiento que forma parte del control interno. Un control puede existir en cualquiera de los ocho componentes.
- Sustantivo que indica un estado o condición, por ejemplo, efectuar control, el resultado de políticas y procedimientos diseñados para controlar.
- Verbo como palabra derivada, por ejemplo, controlar, regular. Establecer o implantar una política que efectúe el control.

Controles de aplicación

Procedimientos programados en el software de aplicación y procedimientos manuales relacionados con ellos, diseñados para ayudar a asegurar la completitud y exactitud del procesamiento de la información. Los ejemplos incluyen comprobaciones automáticas de edición, verificaciones de secuencia numérica y procedimientos manuales para seguir temas identificados en los informes de incidencias.

Controles generales

Políticas y procedimientos que ayudan a asegurar el funcionamiento adecuado y permanente de los sistemas de información. Se incluyen los controles de gestión de la tecnología de información, de la infraestructura de la tecnología informática, de la gestión de la seguridad y de la adquisición, desarrollo y mantenimiento del software. Los controles generales apoyan el funcionamiento de los controles de aplicación programados.

Control interno

Proceso efectuado por el Consejo de Administración, la Dirección y demás personal de la entidad, diseñado para proporcionar una seguridad razonable respecto a la consecución de los objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de los reportes financieros
- Cumplimiento de leyes y regulaciones aplicables

Crterios

Conjunto de normas que utiliza la administración de riesgos corporativos al determinar su efectividad. Los ocho componentes de la administración de riesgos corporativos, tomados en el contexto de las limitaciones inherentes a dicha gestión, representan criterios de efectividad de la administración de riesgos corporativos para cada una de sus cuatro categorías de objetivos.

Cumplimiento

Término usado en relación con el concepto "objetivos" y que tiene que ver con el cumplimiento de leyes y regulaciones aplicables a la entidad.

Debilidad Material

Una condición en la cual uno o más de los componentes del control interno, no reducen a un nivel relativamente bajo el riesgo que errores o irregularidades por montos, que podrían ser de importancia en relación a los estados contables, puedan ocurrir y no sean detectados oportunamente por los empleados en el curso normal del desarrollo de sus funciones.

Deficiencia

Una condición dentro de la administración de riesgos corporativos merecedora de atención, que puede representar una debilidad percibida, potencial o real, o una oportunidad para fortalecer dicha gestión y propiciar una mayor probabilidad de que se alcancen los objetivos de la entidad.

Diseño

- Intención. Según aparece en su propia definición, la administración de riesgos corporativos intenta identificar los eventos potenciales que puedan afectar a la entidad y gestionar los riesgos dentro del riesgo aceptado, proporcionando una seguridad razonable del logro de los objetivos.
- Plan. La manera como se espera que funcione un proceso, que puede contrastar con la realidad de cómo funciona.

Entidad

Una organización de cualquier dimensión establecida para servir un propósito determinado. Una entidad, por ejemplo, puede ser una empresa, una organización sin ánimo de lucro, un organismo gubernamental o una institución universitaria. Otros términos sinónimos son organización y empresa.

Estratégico

Término usado en relación con el concepto "objetivos". Tiene que ver con los objetivos de alto nivel que están alineados con la misión (o visión) de la entidad y que la apoyan.

Evento

Un incidente o acontecimiento, derivado de fuentes internas o externas a la entidad, que afectan a la consecución de objetivos.

Grupos de interés

Son todos aquellos individuos, grupos u organizaciones que recibirán el impacto o estarán interesados en el plan estratégico de la organización. Deben ser identificados y sus intereses deben ser determinados (es decir, cómo sus recursos, situación, libertad de acción, relacionamiento y actividades pueden, desde su punto de vista, ser afectados por los cambios en la orientación de la organización). Éstos incluyen empleados (considerando gerentes), clientes y consumidores, proveedores, gobiernos, sindicatos, acreedores, propietarios, accionistas y miembros de la comunidad que creen tener un interés (stake) en la organización, más allá de que esa creencia sea exacta o razonable.

Impacto

Resultado o efecto de un evento. Puede existir una gama de posibles impactos asociados a un evento. Puede ser positivo o negativo sobre los objetivos relacionados de la entidad.

Incertidumbre

Las empresas actúan en ámbitos donde factores tales como la globalización, la tecnología, las normas, las reestructuras, los mercados cambiantes y la competencia crean incertidumbre. La incertidumbre proviene de la dificultad de determinar anticipadamente con precisión la probabilidad de ocurrencia de acontecimientos eventuales y sus consecuencias asociadas.

Integridad

La calidad o condición de tener principios morales sólidos, de poseer virtud, honradez y sinceridad, de desear hacer lo correcto y de profesar y vivir una serie de valores y expectativas.

Limitaciones inherentes

Son las limitaciones de la administración de riesgos corporativos, que se relacionan con los límites del juicio humano, las restricciones de los recursos, la necesidad de tener en cuenta el costo de los controles respecto a los beneficios esperados, la realidad de que los fallos puedan ocurrir y la posibilidad de que la Dirección prescinda de los controles o esté en confabulación para incumplirlos.

Operativos

Término usado en relación con el concepto "objetivos". Tiene que ver con la efectividad y eficiencia de las actividades de una entidad, incluyendo metas de desempeño y rentabilidad, y con la salvaguarda de recursos frente a pérdidas.

Oportunidad

La posibilidad de que un evento ocurra y afecte positivamente a la consecución de objetivos.

Política

Las directrices de la Dirección de lo que debería hacerse para efectuar el control. Una política sirve como base para la implantación de procedimientos.

Probabilidad

La posibilidad de que un evento dado ocurra. Los términos a veces adquieren connotaciones más específicas y, así, "probabilidad" tanto puede indicar dicha posibilidad en términos cualitativos como alto, medio y bajo o derivados de otras escalas de juicio o bien indicarla mediante una medida cuantitativa, como porcentaje, frecuencia de ocurrencia u otra métrica numérica.

Procedimiento

Una acción para poner en práctica una política.

Proceso de gestión

La serie de acciones tomadas por la Dirección para conducir una entidad. La administración de riesgos corporativos es una parte del proceso de gestión y está integrada a él.

Riesgo

Proviene del italiano *risicare*, que significa desafiar, retar, enfrentar, atreverse. La posibilidad de que un evento ocurra y afecte adversamente a la consecución de objetivos.

Riesgo aceptado (risk appetite)

La cuantía, más amplia del riesgo que una entidad está dispuesta a asumir para realizar su misión (o visión).

Seguridad razonable

Grado de certeza que proporciona el proceso de gestión de riesgos Corporativos a la Dirección. Dicho proceso, por muy bien diseñado y operativo que esté, no puede proporcionar una garantía absoluta de la consecución de objetivos de la entidad, debido a las limitaciones inherentes a dicha gestión.

Valor

El valor es creado, preservado o deteriorado por las decisiones de la gerencia, que van desde la adopción de la estrategia hasta la operación de la empresa día a día. El reconocimiento del riesgo y de la oportunidad es inherente a las decisiones y requiere que la gerencia considere información relacionada con el entorno interno y el externo, despliegue recursos de alto valor y adapte las actividades de la empresa a las circunstancias cambiantes.

CAPÍTULO IX



BIBLIOGRAFÍA

IX BIBLIOGRAFÍA

-  Administración de Riesgos Corporativos - Marco Integrado
 -  Administración de Riesgos Corporativos - Técnicas de Aplicación
 -  Material preparado por la Cátedra de Control Interno y Organización de Sistemas Contables de la Facultad de Ciencias Económicas y de Administración de la UDELAR
 -  "Administración de Riesgo Empresarial - Marco de referencia ERM"
Trabajo monográfico A. Caillava, D González - 2007
 -  Web "The Institute of Internal Auditors" - www.theiia.org
 -  Web "Committee Of Sponsoring Organizations" - www.coso.org
 -  The McKinsey Quarterly 2003 Número 4
 -  Manuales y documentos proporcionados por KPMG - 2003
 -  Importancia del Valor en Riesgo (Var) como instrumento de Administración Integral de Riesgos para las Instituciones de Seguros y Fianzas-2002- Francisco Javier Olivares Ramírez
 -  Web www.degerencia.com - Benchmarking
 -  "Threatening Skies - Risk in the Global Economy" www.bt.com
 -  PricewaterhouseCoopers - Estado de la Profesión de Auditoría Interna y Tendencias-2008
 -  Política de Administración de Riesgos en el Instituto Mexicano de la Propiedad Industrial. Lic. Jorge Amigo Castañeda. Setiembre 2007
 -  Estándar Australiano de Administración del Riesgo AS/NZS 4360:1999
 -  Conceptos Básicos sobre Gestión de Riesgos - Superintendencia de Pensiones - www.educacionfinanciera.gob.sv
 -  "La Gestión Estratégica del Riesgo Corporativo" Lorenzo A. Preve - www.iaecuador.com
-