UNIVERSIDAD NACIONAL DE TUCUMÁN

FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL TUCUMAN

GESTION DE RIESGO CORPORATIVO EN UNA ENTIDAD BANCARIA

Autores: Chediac, Carla Sofía
Marrades, Michelle Alejandra
Schujman, Enrique Martin

Director: Peña Critto, Gerardo

2016

Trabajo de Seminario: Contador Público Nacional

RESUMEN

El presente trabajo tiene como objetivo analizar la evolución a través de los años del proceso de auditoría, el impacto de la misma en las Comunicaciones dictadas por el Banco Central de la República Argentina y estudiar si estos avances generan o no una mejora en el desempeño de los procesos de las entidades bancarias, utilizando al Banco XX como unidad de análisis.

El desarrollo de los procesos de auditoría comenzó a llevarse a cabo mediante la implementación de las directivas impuestas por el Informe N°5, profundizado en el Informe COSO. Estos determinaban que la misma debía llevarse a cabo mediante la implementación del control interno.

Con la globalización y la creciente complejidad de los procesos involucrados en las diferentes actividades, muchas organizaciones y entidades comenzaron a enfocarse en la gestión de riesgos corporativo. El Marco Integrado de Gestión de Riesgos Corporativos surgió al reconocer la necesidad de una guía definitiva para la gestión de riesgos, este sugiere un lenguaje común y provee los lineamientos para eficientizar las tareas.

El avance producido en el marco teórico y la probada eficiencia de los nuevos métodos produjo que el BCRA emitiera la comunicación A4793 que llevo a las entidades a generar cambios en su estructura incorporando nuevos departamentos enfocados completamente en la detección de riesgos en el análisis de los mismos y en la generación de planes de contingencias

para reaccionar ante posibles problemas, teniendo una idea o lineamiento de cómo desenvolverse en el caso de que dichos imprevistos sucedieran.

PROLOGO

Esta monografía se realizo como trabajo final para la materia de Seminario de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán.

Como veremos en los capítulos siguientes el crecimiento del mercado, la complejidad de las actividades desarrolladas por las entidades y la globalización llevaron a que las empresas reconozcan nuevas formas de implementar los procesos de auditoría, centrándose en la gestión de riesgos corporativos.

Este avance llevo a que el Banco Central de la República Argentina como entidad de contralor dictara nuevas normativas centradas en esta forma de llevar a cabo los procesos, reconociendo la supuesta eficiencia que este método generaría.

Luego del análisis de las exigencias del BCRA y lo que dicta la normativa pudimos observar que debido al contexto tanto nacional como internacional al que pertenecía el Banco XX la aplicación de la Comunicación en su actividad implicaba un mero cumplimiento normativo debido a que por tratarse de una entidad que por su gran envergadura había desarrollado anteriormente dicha área por una política interna para mejorar sus procesos y minimizar sus pérdidas hoy, le representa más un costo que un beneficio tangible o intangible.

Este trabajo no hubiera sido posible sin la ayuda de nuestro director de tesis, el profesor, Gerardo Peña Critto, quien nos brindó desinteresadamente su apoyo, tiempo y conocimientos para el desarrollo de este trabajo, así como también al Cr. Reinaldo Paez Murga quien por ser un catedrático en el tema pudo encaminarnos en cuanto al desarrollo y además presentarnos al Subgerente del Banco XX y a los departamentos de Gestión de Riesgo Operacional y Gestión de Riesgo de Tecnología Informática a quienes nos encontramos enteramente agradecidos por su completa predisposición e interés a la hora de introducirnos en el mundo de las entidades bancarias.

CAPITULO I

El CONTROL INTERNO SEGÚN EL INFORME N° 5 Y EL INFORME COSO.

Sumario: 1. El control organizacional; 2. El control interno.

1 El Control organizacional.

Control ha sido definido como el proceso de ejercitar una influencia directiva o restrictiva sobre las actividades de un objeto organismo o sistema.

Influencia directiva implica que el control intenta que las actividades del sistema se realicen de modo tal que produzca determinados resultados o alcance de objetivos específicos predefinidos.

Influencia restrictiva significa que el control se ejerce de modo que se evite que las actividades de un sistema produzcan resultados no deseados

Existen controles correctivos y no correctivos. Los primeros implican la determinación de los desvíos y su informe a quien deba actuar sobre estos, en tanto los segundos son los que no suponen información y medición de los mismos.

Existen cuatro elementos de control de un sistema:

- Una característica que deberá ser medida. Este elemento puede ser la producción de un sistema durante cualquier etapa de los

procesos o puede ser una condición que ha resultado de la producción del sistema.

- Un artefacto o método sensor para medir las características o condiciones controladas o sea la medida del rendimiento
- Un grupo o equipo de control que compara los datos medidos con el rendimiento planeado, determina la necesidad de corrección y pone en acción la información que permitirá corregir la producción de un sistema
- Un grupo o mecanismo activador que es capaz de producir un cambio en el sistema operante o realizar la acción correctiva.

Ejemplo:

- Característica o condición controlada: cantidad almacenada y movimientos de un periodo.
- Sensor: registros de inventario que miden la cantidad almacenada, y los movimientos del periodo.
- Grupo de control: quien compara los objetivos con la medición.
- Grupo activante: será quien toma las medidas correctivas sobre los desvíos determinados.

La descripción de los elementos de control lleva a la conclusión que cada control es un sistema en sí mismo o bien un conjunto de elementos interrelacionados que cumplen las condiciones establecidas para la existencia de un sistema.

1.1. Economicidad de control

La necesidad de que el costo que implica la existencia de un control sea menor que el beneficio que produce con su acción de regulación en un sistema es la consecuencia lógica de la finalidad del control. El control puede

no abarcar todos los resultados de la actividad, si no los necesarios para conocer los desvíos que se producen y tomar las medidas correctivas.

2. El control interno

Comprende el plan de organización y el conjunto coordinado de métodos y medidas adoptadas dentro de una empresa para salvaguardar sus activos, verificar la exactitud y confiabilidad de su información contable, promover la eficiencia de las operaciones y alentar la adhesión a las políticas establecidas por la gerencia.[1]

De esta definición de control interno, surgen los siguientes **elementos que lo integran:**

- Plan de organización (estructura)
- Normas de autorización y procedimientos de registro de operaciones
- Personal

También de ella se desprenden los **objetivos que procura el control interno** a saber:

- Salvaguardar los activos
- Verificar la exactitud y confiabilidad de los datos contables
- Promover la eficiencia operativa
- Estimular la adhesión a las prescripciones gerenciales

- [1] CONSEJO EMISOR DE NORMAS DE CONTABILIDAD Y AUDITORIA, INFORME Nº 5 (Buenos Aires), passim.

2.1. Controles típicos de la organización

El siguiente es un listado enunciativo en el que se incluyen algunos **estándares básicos importantes desde la perspectiva de auditoría** de estados contables

- Definición de autoridad responsabilidad y funciones entre los miembros de la organización
- Separación en las operaciones de la entidad de las funciones incompatibles como:
  - Autorización
  - Ejecución
  - Custodia de los activos
  - Registros contables

Métodos de control a implementar en una organización para minimizar fallas de control interno:[2]

– Restricción en el acceso a los activos de la empresa y establecimiento de medidas adecuadas de seguridad provistas interna o externamente.

– Descripción de los procedimientos operativos de cada subsistema de la organización.

– Implementación de los controles dirigidos al cumplimiento de los procedimientos establecidos.

– Empleo de formularios adecuados en su caso, pre numerados que expliciten los datos relevantes de cada fase de operaciones.

[2] Ibidem, pág. 9.

- Existencia de archivos ordenados y completos.
- Uso de medios de procesamiento de datos adecuados y disposición eficiente de registros.
- Empleo de planes y manuales de cuentas aptos para clasificar y evaluar la información que fluye de los subsistemas funcionales de acuerdo con las normas contables vigentes
- Conciliación periódica de las cuentas de control con los mayores auxiliares y con la documentación respaldatoria.
- Registro y emisión oportuna de la información contable.
- Disposición de una política adecuada de personal en orden a sus selección evaluación promoción retribución capacitación y rotación.

Un objetivo clave del estudio del control interno consiste en ayudar a la Dirección de las empresas y de otras entidades a mejorar el desempeño de las actividades de sus organizaciones. Sin embargo, el término “control interno” no tiene el mismo significado para todo el mundo y la amplia variedad de términos y significados con que se utiliza dificulta que se logre una comprensión común del control interno.

El Informe COSO[3], *Committee of Sponsoring Organizations of the Treadway Commission*, fue una iniciativa de 5 organismos para la mejora de control interno dentro de las organizaciones.

El control interno según el Informe COSO, es un proceso efectuado por el Consejo de Administración, la Dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto al logro de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.

[3]COMMITTE OF SPONSORING OF THE TREADWAY COMMISION, Marco integrado de gestión de riesgo corporativo (Estados Unidos, 2004), passim.

- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

La anterior definición refleja ciertos **conceptos fundamentales**:

- El control interno es un proceso. Es un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El control interno lo llevan a cabo las personas. No se trata solamente de manuales de políticas y formularios, sino de personas en cada nivel de la organización.
- El control interno sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la Dirección y al Consejo de Administración de la entidad.
- El control interno está pensado para facilitar el logro de objetivos en una o más de las diferentes categorías que, al mismo tiempo, se solapan.

Un proceso

En los negocios se llevan a cabo procesos que se coordinan en función de los procesos de gestión básicos de planificación, ejecución y supervisión. El control interno es parte de dichos procesos y está integrado en ellos, permitiendo su funcionamiento adecuado y supervisando su comportamiento y aplicabilidad en cada momento. Constituye una herramienta útil para la gestión, pero no un sustituto de ésta.

La incorporación de controles puede influir directamente en la capacidad de la entidad de conseguir sus objetivos, además de apoyar sus iniciativas de calidad. La búsqueda de la calidad está directamente vinculada con la forma en que se gestionen y controlen los negocios. Las iniciativas de control se convierten en parte de la estructura operativa de la empresa.

La incorporación de controles repercute de forma importante en la reducción de costos y en los tiempos de respuesta:

- La mayoría de las empresas deben hacer frente a mercados muy competitivos y a la necesidad de controlar sus costos.
- La práctica de incorporar controles en la estructura operativa fomenta el desarrollo de nuevos controles necesarios para llevar a cabo las nuevas actividades empresariales. Las reacciones automáticas de este tipo hacen que las entidades sean más ágiles y competitivas.

Las personas

El control interno es llevado a cabo por el Consejo de Administración, la Dirección y los demás miembros de la entidad, mediante sus acciones y palabras. De la misma forma, el control interno afecta a la actuación de las personas. Los empleados deben conocer sus responsabilidades y los límites de su autoridad.

Por consiguiente, ha de existir un vínculo estrecho entre las funciones de cada individuo y la forma de ejecución de dichas funciones, así como con los objetivos de la entidad.

Seguridad razonable

El control interno, por muy bien diseñado e implantado que esté, solamente puede aportar un grado de seguridad razonable a la Dirección y al Consejo de Administración acerca del logro de los objetivos de la entidad. Las posibilidades de conseguir tales objetivos se ven afectadas por las limitaciones que son inherentes a todos los sistemas de control interno.

Estas incluyen ciertos hechos innegables: las opiniones en que se basan las decisiones pueden ser erróneas, los empleados encargados del establecimiento de controles tienen que analizar los costos y beneficios relativos de los mismos y pueden producirse problemas en el funcionamiento del sistema como consecuencia de fallas humanas, aunque se trate de un simple error o equivocación.

Objetivos

Cada entidad tiene una misión, la cual determina sus objetivos y las estrategias necesarias para alcanzarlos. Los objetivos pueden establecerse para la organización como conjunto o dirigirse a determinadas actividades dentro de la misma. Aunque muchos objetivos son específicos de una sola entidad, otros son ampliamente compartidos.

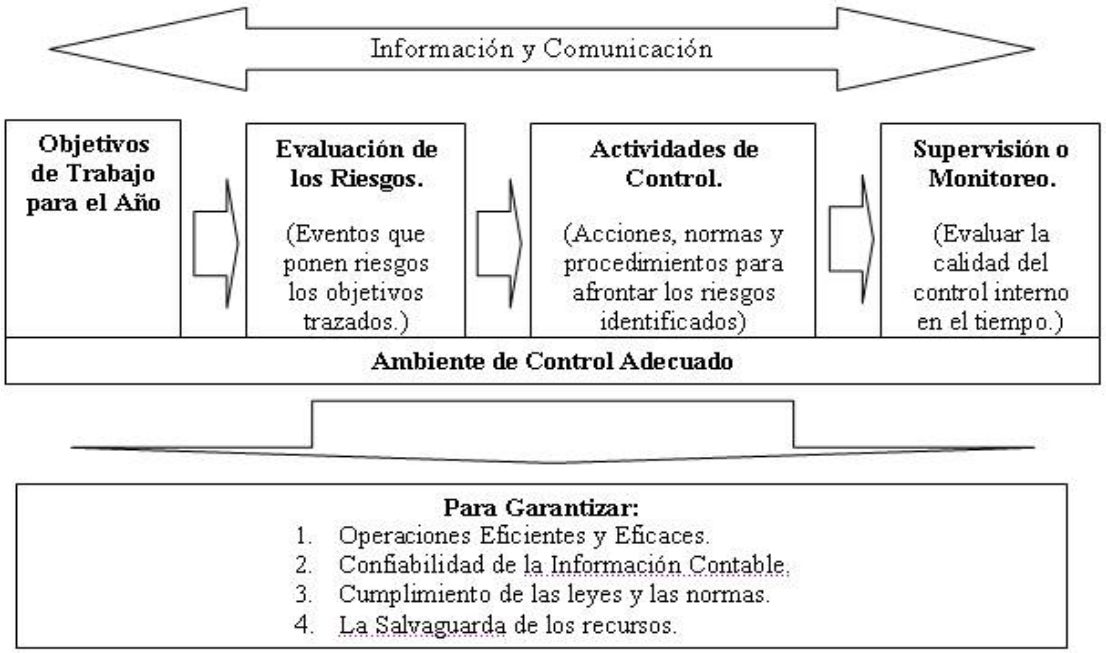
Podemos clasificarlos en **tres categorías**:

- Operacionales. – Referente a la utilización eficaz y eficiente de los recursos de la entidad.
- Información financiera. – Referente a la preparación y publicación de estados financieros confiables.
- Cumplimiento. – Referente al cumplimiento por parte de la entidad de las leyes y normas que le sean aplicables.

El control interno no es capaz de prevenir las opiniones o decisiones equivocadas, o los acontecimientos externos que pueden evitar que se alcancen las metas operativas. Respecto a tales objetivos, el sistema de control interno solamente puede aportar un nivel razonable de seguridad de que la Dirección y, en su papel de supervisor, el Consejo, estén informados puntualmente del grado de avance en la consecución de dichos objetivos.

El informe COSO plantea la siguiente estructura del control:[4]

[4] Ibidem, pág. 12.



Fuente: www.campusvirtual.edu.ar

O sea, las empresas delimitaran objetivos encaminados a la eficiencia y eficacia de las operaciones, la confiabilidad de la información financiera, el cumplimiento de las leyes y el resguardo de los recursos que mantiene. Identificarán y evaluarán los riesgos que pongan en peligro la consecución de estos objetivos; trazarán actividades de control para minimizar el impacto de estos riesgos; y activarán sistemas de supervisión para evaluar la calidad de este proceso. Todo lo anterior, con el sostén de un ambiente de control eficaz, y retroalimentado con un sistema de información y comunicación efectivo.

0

Eficacia

Los sistemas de control interno de las diferentes entidades funcionan a distintos niveles de eficacia. De la misma forma, un sistema determinado puede funcionar de manera diferente en momentos distintos. Cuando un sistema de control interno alcanza el estándar descripto a continuación, puede considerarse un sistema “eficaz”.

El control interno puede considerarse eficaz en cada una de las tres categorías, si el Consejo de Administración y la Dirección tienen una seguridad razonable que:

- Disponen de información adecuada sobre la medida en que se están logrando los objetivos operacionales de la entidad.
- Se preparan de forma confiable los estados financieros públicos.
- Se cumplen las leyes y normas aplicables.

Mientras que el control interno es un proceso, su eficacia es un estado o condición del proceso en un momento dado.

La determinación de si un sistema de control interno es “eficaz” o no, constituye una toma de postura subjetiva que resulta del análisis de si están presentes y funcionando eficazmente los cinco componentes. Su funcionamiento eficaz proporciona un grado de seguridad razonable de que una o más de las categorías de objetivos establecidas van a cumplirse. Por consiguiente, estos componentes también son criterios para determinar si el control interno es eficaz.

Aunque los cinco criterios deben cumplirse, esto no significa que cada componente haya de funcionar de forma idéntica, ni siquiera al mismo nivel, en distintas entidades. Puede existir una cierta compensación entre los distintos componentes. Debido a que los controles pueden tener múltiples propósitos, los controles de un componente pueden cumplir el objetivo de

controles que normalmente están presentes en otro componente. Por otra parte, es posible que existan diferencias en cuanto al grado en que los distintos controles abarquen un riesgo específico, de modo que los controles complementarios, cada uno con un efecto limitado, pueden ser satisfactorios en su conjunto.

Los mencionados componentes y criterios se aplican a un sistema de control interno en su conjunto, o a una o más categorías de objetivos. Al considerar una categoría determinada (controles sobre la información financiera, por ejemplo) se deben cumplir los cinco criterios para poder concluir que el control interno de la información financiera es eficaz.

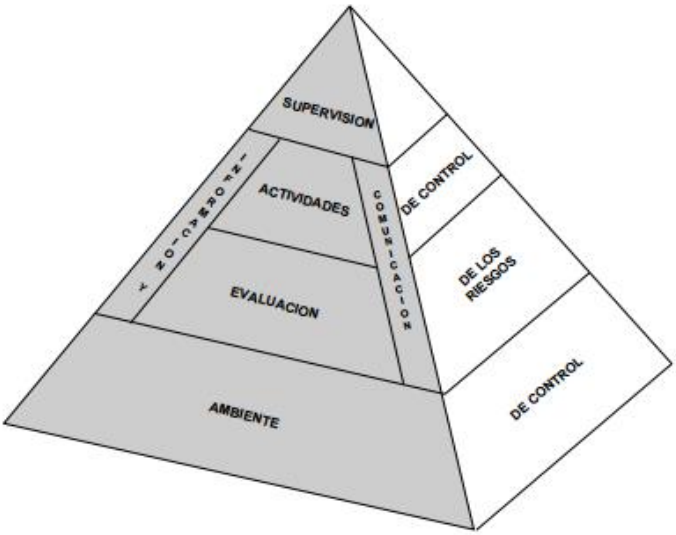
2.2. Componentes del control interno.

El control interno consta de **cinco componentes relacionados entre sí**. Estos se derivan del estilo de dirección del negocio y están integrados en el proceso de gestión. Los componentes son los siguientes:

- Ambiente de control. – El núcleo de un negocio es su personal (sus atributos individuales, incluyendo la integridad, los valores éticos y la profesionalidad) y el entorno en el que trabaja. Los empleados son el motor que impulsa la entidad y los cimientos sobre los que descansa todo.
- Evaluación de los riesgos. – La entidad debe conocer y abordar los riesgos con los que se enfrenta. Ha de fijar objetivos, integrados en las actividades de ventas, producción, comercialización, finanzas, etc., para que la organización funcione de forma coordinada. Igualmente debe establecer mecanismos para identificar, analizar y tratar los riesgos correspondientes.
- Actividades de control. – Deben establecerse y ejecutarse políticas y procedimientos que ayuden a conseguir una seguridad razonable de que se llevan a cabo de forma eficaz las acciones consideradas necesarias para afrontar los riesgos que existen respecto al logro de los objetivos de la entidad.

- Información y comunicación. – Las mencionadas actividades están rodeadas de sistemas de información y comunicación. Estos permiten que el personal de la entidad capte e intercambie la información requerida para desarrollar, gestionar y controlar sus operaciones.

- Supervisión. – Todo el proceso ha de ser supervisado, introduciéndose las modificaciones pertinentes cuando se estime oportuno. De esta forma, el sistema puede reaccionar ágilmente y cambiar de acuerdo a las circunstancias.



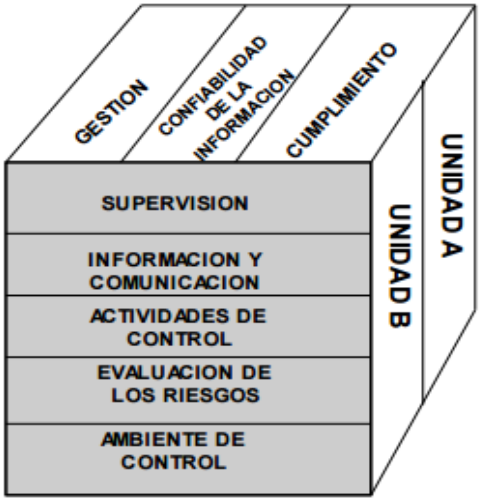
Fuente: www.campusvirtual.edu.ar

El ambiente de control aporta el clima en el que las personas desarrollan sus actividades y cumplen con sus responsabilidades de control. Sirve como base de los otros componentes. Dentro de este entorno, los directivos evalúan los riesgos relacionados con el cumplimiento de determinados objetivos. Las actividades de control se establecen para ayudar a asegurar que se pongan en práctica las directrices de la Dirección para hacer frente a dichos riesgos. Mientras tanto, la información relevante se capta y se comunica por toda la organización. Todo este proceso es

supervisado y modificado según las circunstancias. Estos componentes de control interno y los vínculos existentes entre ellos se reflejan de forma gráfica en un modelo que se presenta en la ilustración anterior. El modelo refleja el dinamismo de los sistemas de control interno. Por ejemplo, la evaluación de riesgos no sólo influye en las actividades de control, sino que también puede poner de relieve que las necesidades de información y de comunicación o las actividades de supervisión deberían reconsiderarse. Por lo tanto, el control interno no es un proceso en serie, en el que un componente influye exclusivamente en el siguiente, sino un proceso interactivo multidireccional, en el que prácticamente cualquier componente puede influir, y de hecho influye, en otro. Los sistemas de control interno no son, ni deben ser, iguales en todos los casos. Las entidades y sus necesidades de control interno varían mucho dependiendo del sector en el que operen, su tamaño, su cultura o su filosofía de gestión. Así pues, aunque todas las entidades necesitan cada uno de los componentes para lograr mantener el control sobre sus actividades, el sistema de control interno de una entidad suele asemejarse muy poco a la otra.

Existe una relación directa entre los objetivos, que es lo que la entidad se esfuerza por conseguir, y los componentes, que representan lo que se necesita para cumplir dichos objetivos. Esta relación puede ilustrarse mediante una matriz tridimensional, tal y como se presenta en la Ilustración:

Relación entre objetivos y componentes



Fuente: www.campusvirtual.edu.ar

- Las tres categorías de objetivos: operacionales, de información financiera y de cumplimiento están representadas por las columnas verticales.
- Los cinco componentes están representados por filas.
- Las unidades o actividades de la entidad que están relacionadas con el control interno, se representan en la tercera dimensión de la matriz.

Cada fila de componentes “cruza” las tres categorías de objetivos y es aplicable a las tres. Asimismo, los cinco componentes tienen relevancia para cada categoría de objetivos. Por ejemplo, en la categoría de eficacia y eficiencia de las operaciones los cinco componentes son aplicables e importantes para su consecución.

El control interno es importante para la empresa en su totalidad o para cada una de sus partes. Esta relación se refleja con la tercera dimensión, que representa las filiales, las divisiones y otras unidades de

negocio y las actividades funcionales o de otro tipo, como compras, producción y marketing. Por lo tanto, uno puede centrar su atención en cualquier célula de la matriz. Por ejemplo, se podría considerar aisladamente la célula situada en la parte inferior izquierda delantera, que representa el ambiente de control y su relación con los objetivos de operaciones de una división determinada de la empresa.

2.2.1. Ambiente de control

El ambiente de control marca las pautas de comportamiento en una organización, y tiene una influencia directa en el nivel de concientización del personal respecto del control. Constituye la base de todos los demás elementos del control interno, aportando disciplina y estructura. Entre los factores que constituyen el ambiente de control se encuentran la integridad, los valores éticos y la capacidad del personal; la filosofía de la Dirección y su forma de actuar; la manera en que la Dirección distribuye la autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados, así como la atención y orientación que proporciona el Consejo de Administración.

2.2.1.1. Factores del ambiente de control

El ambiente de control engloba una serie de factores que se comentan a continuación. Aunque todos son importantes, la medida en que cada uno será considerado variará en función de la organización. Por ejemplo, es posible que el Director General de una entidad con una plantilla pequeña y operaciones centralizadas no establezca responsabilidades formales ni políticas de explotación detalladas y, sin embargo, la entidad tenga un ambiente de control apropiado.

2.2.1.2. Integridad y valores éticos

La integridad y los valores éticos son elementos esenciales del ambiente de control y afectan el diseño, la administración y la supervisión de los demás elementos del control interno.

La integridad es un requisito previo al comportamiento ético en todos los aspectos de las actividades de una empresa. Tal como estableció la *Treadway Commission*, “un clima ético vigoroso dentro de la empresa, y a todos los niveles de la misma, es esencial para el bienestar de la organización, de todos sus componentes y del público en general. Un clima así contribuye de forma significativa a la eficacia de las políticas y de los sistemas de control de la empresa y permite influir sobre los comportamientos que no están sujetos ni a los sistemas de control más elaborados.”[5]

El comportamiento ético así como la integridad de la Dirección son productos de una “cultura corporativa”. La cultura corporativa se materializa en las normas éticas y de comportamiento y en la forma en que éstas se comunican y refuerzan en la práctica. Las políticas oficiales especifican lo que la Dirección desea que ocurra. La cultura corporativa determina lo que en realidad ocurre y las reglas que se obedecen, modifican o ignoran. La alta Dirección, empezando por la Dirección General, desempeña un papel clave a la hora de determinar la cultura corporativa. Normalmente, la Dirección General es la figura dominante de la organización y a menudo da la pauta ética de la misma.

2.2.1.3. Compromiso de competencia profesional

El nivel de competencia debe reflejar el conocimiento y las habilidades necesarias para llevar a cabo las tareas de cada puesto de trabajo. Suele ser función de la Dirección determinar el grado de perfección

[5] Report of National Commission of Fraudulent Financial Reporting (National Commission on Fraudulent Financial Reporting, 1987)

con el que debe llevarse a cabo cada tarea, función que debe desarrollarse teniendo en cuenta los objetivos de la entidad, así como las estrategias y los planes de la Dirección para su consecución. Suele buscarse un equilibrio entre el nivel de competencia deseado y el costo involucrado.

La Dirección debe especificar el nivel de competencia para cada trabajo y traducir estos niveles en conocimientos y habilidades. A su vez, estos conocimientos y habilidades pueden estar en función de la inteligencia, formación y experiencia de cada persona. Entre los muchos factores a tener en cuenta a la hora de desarrollar conocimientos y niveles de habilidad están la naturaleza y el grado de juicio profesional aplicables a un trabajo específico. Debe buscarse el equilibrio entre el nivel de supervisión y la capacidad exigida del individuo.

2.2.1.4. Consejo de Administración y Comité de Auditoría

El ambiente de control y la cultura de la organización están influenciados de forma significativa por el Consejo de Administración y el Comité de Auditoría. Los factores a tener en cuenta incluyen el grado de independencia del Consejo o del Comité de Auditoría respecto de la Dirección, la experiencia y calidad de sus miembros, el grado de involucramiento y vigilancia y el acierto de sus acciones, la interacción del Consejo o el Comité de Auditoría con los auditores internos o externos constituye otro factor que incide en el ambiente de control.

Debido a su importancia, la actividad del Consejo de Administración u otro órgano similar es esencial para garantizar la eficacia del control interno. Debido a que el Consejo debe estar preparado para cuestionar y supervisar las actividades de la Dirección, presentar opiniones alternativas y tener disposición para actuar cuando surgen incidentes o problemas, debe incluir entre sus miembros a consejeros externos ajenos a la entidad.

2.2.1.5. Filosofía de dirección y estilo de gestión

La filosofía de dirección y el estilo de gestión afectan la manera en que la empresa es conducida e, incluso, el tipo de riesgo empresarial que se acepta. Una entidad que ha tenido éxito a la hora de correr riesgos significativos puede tener una perspectiva distinta del control interno que una empresa que se haya tenido que enfrentar a consecuencias adversas desde el punto de vista económico o administrativo por haberse adentrado en territorios peligrosos. Una empresa gestionada de manera informal puede controlar las operaciones llevadas a cabo básicamente a través del contacto cara a cara con los directores clave. Una empresa gestionada de forma más formal puede depender en mayor medida de políticas escritas, indicadores de rendimiento e informes de excepciones.

Otros componentes de la filosofía de la dirección y su forma de actuar son la actitud adoptada en la presentación de la información financiera, la selección de las alternativas disponibles respecto a los principios de contabilidad aplicables, la escrupulosidad y prudencia con que se obtienen las estimaciones contables y las actitudes hacia las funciones informáticas y contables, así como hacia el personal.

2.2.1.6. Estructura organizativa

La estructura organizativa proporciona el marco en el que se planifican, ejecutan, controlan y supervisan las actividades para el logro de objetivos en el ámbito de la empresa. Las actividades pueden referirse a lo que a veces se denomina la cadena de valor, es decir, la recepción, la producción de bienes o servicios, y las actividades de envío, comercialización y venta. Puede haber funciones de apoyo a las anteriores relacionadas con la administración, recursos humanos o desarrollo tecnológico.

Entre los aspectos más significativos a tener en cuenta a la hora de establecer la estructura organizativa correspondiente, están la definición de las áreas clave de autoridad y responsabilidad y el establecimiento de vías

adecuadas de comunicación. Por ejemplo, el Departamento de Auditoría Interna debe tener libre acceso a un directivo que sea el responsable directo de preparar los estados financieros de la empresa pero que tenga el rango suficiente para garantizar que no se impone ninguna limitación al trabajo de Auditoría Interna y que se hace un seguimiento de sus resultados y recomendaciones.

Una entidad desarrolla la estructura organizativa que mejor se adapta a sus necesidades. Algunas entidades desarrollan estructuras centralizadas, otras descentralizadas. Algunas desarrollan estructuras piramidales, mientras que la estructura de otras se asemeja más a una matriz. Algunas entidades están organizadas por sector o línea de producto, por zona o por red de distribución o comercialización. Otras entidades, incluyendo muchas unidades estatales o municipales e instituciones sin fines de lucro, están organizadas de manera funcional.

La adecuación de la estructura organizativa de una entidad depende, en parte, de su tamaño y de la naturaleza de las actividades que desarrolla. Una organización altamente estructurada, con líneas de comunicación y responsabilidades formales, puede resultar apropiada para una entidad grande con varias divisiones operativas, incluyendo divisiones en el extranjero. Sin embargo, puede obstaculizar el flujo de información en una entidad pequeña. Sea cual fuere la estructura, las actividades de una entidad deben estar organizadas con el fin de llevar a cabo las estrategias diseñadas para conseguir los objetivos específicos de la misma.

2.2.1.7. Asignación de autoridad y responsabilidad

Este aspecto del control interno incluye tanto la asignación de autoridad y responsabilidad para las actividades de gestión como para el establecimiento de las relaciones de jerarquía y de las políticas de autorización. Se refiere a la medida en que se autoriza e impulsa al personal, tanto a nivel individual como de equipo, a utilizar su iniciativa a la hora de

abordar temas y solucionar problemas y establecer límites a su autoridad. Asimismo, trata de las políticas que describen las prácticas empresariales adecuadas, conocimientos y experiencia del personal clave, y los recursos puestos a su disposición para llevar a cabo sus funciones.

Hay una tendencia creciente a delegar la autoridad hacia niveles inferiores, para situar el proceso de toma de decisiones más cerca del personal de “primera línea”. Una entidad puede adoptar este enfoque con el fin de dirigirse más al mercado o concentrarse en la calidad, quizá para eliminar defectos, reducir la duración de los ciclos o aumentar el grado de satisfacción del cliente. Para ello, la empresa necesita reconocer y responder a la evolución del mercado de las relaciones empresariales y de las expectativas del público.[6]

A menudo, la delegación de autoridad y responsabilidad está diseñada para fomentar la iniciativa individual dentro de unos límites. La delegación de autoridad significa, por lo general, entregar el control central sobre determinadas decisiones empresariales a los niveles inferiores de la organización, a las personas que están más cerca de las operaciones diarias.

Un desafío crítico es delegar únicamente en la medida necesaria para conseguir los objetivos. Por tanto, es necesario garantizar que los riesgos se asumen en función de la capacidad de los responsables de identificar y minimizar los mismos en base a prácticas prudentes y de sopesar las pérdidas contra los beneficios potenciales de una buena decisión empresaria.

Una mayor delegación puede exigir implícitamente un mayor nivel de competencia al personal así como mayor responsabilidad. También hace necesario la existencia de procedimientos eficaces que permitan a la dirección supervisar los resultados. De hecho, si bien fomenta unas

[6] PAEZ MURGA, Reinaldo, Curso: Auditoría interna, Gerente auditoría AUREN (San Miguel de Tucumán, 2016).

decisiones mejor orientadas hacia el mercado, la delegación puede aumentar el número de decisiones no deseadas o inesperadas. El hecho de que el personal sepa que se le puede declarar responsable tiene un impacto significativo sobre el ambiente de control.

2.2.1.8. Políticas y prácticas en materia de recursos humanos

Las prácticas aplicadas en el campo de los recursos humanos indican a los empleados los niveles de integridad, comportamiento ético y competencia que se espera de ellos. Estas prácticas se refieren a las acciones de contratación, orientación, formación, evaluación, asesoramiento, promoción, remuneración y corrección.

Por ejemplo, las normas para contratar personal calificado, en las que se destaca el antecedente académico, la experiencia profesional, los logros y las pruebas de integridad y comportamiento ético, sirven para probar el compromiso de una entidad hacia la contratación de personal competente y confiable. Las prácticas de reclutamiento que incluyen entrevistas formales y detalladas y presentaciones informativas e indagaciones sobre los antecedentes, cultura y estilo operativo de la entidad transmiten el mensaje de que la misma está comprometida con sus empleados.

Las políticas de formación que indican las funciones y responsabilidades futuras e incluyen prácticas tales como escuelas de formación y seminarios, estudios monográficos simulados y cursos de habilidades gerenciales basados en juegos, sirven para demostrar los niveles esperados de rendimiento y comportamiento. La rotación de personal y los ascensos fomentados por evaluaciones periódicas demuestran el compromiso de la entidad con el progreso del personal calificado. Los programas de remuneración competitiva que incluyen incentivos sirven para motivar y reforzar actuaciones sobresalientes. Las acciones disciplinarias transmiten el mensaje de que no se tolerarán comportamientos que no estén en línea con lo esperado.

Es indispensable que el personal esté preparado para hacer frente a nuevos retos a medida que las empresas se enfrentan a cambios y se hacen más complejas, debido en parte a los rápidos cambios que se están produciendo en el mundo de la tecnología y al aumento de la competencia. La instrucción y la formación ya sea mediante cursos, autoformación o formación en el puesto de trabajo, deben preparar al personal para que pueda mantener el ritmo y hacer frente de forma eficaz al entorno cambiante. Asimismo, aumentará la capacidad de la entidad para poner en marcha iniciativas de calidad. La contratación de personal competente y la formación esporádica no son suficientes. El proceso de formación debe ser continuo.

2.2.2. Evaluación de los riesgos

Toda entidad debe hacer frente a una serie de riesgos tanto de origen interno como externo que deben evaluarse. Una condición previa a la evaluación de los riesgos es el establecimiento de objetivos en cada nivel de la organización que sean coherentes entre sí. La evaluación del riesgo consiste en la identificación y el análisis de los factores que podrían afectar el logro de los objetivos y, sobre la base de dicho análisis, determinar la forma en que los riesgos deben ser administrados. Debido a que las condiciones económicas, industriales, normativas y operacionales se modifican en forma continua, se necesitan mecanismos para identificar y hacer frente a los riesgos especiales asociados con el cambio.

Todas las empresas, independientemente de su tamaño, estructura, naturaleza o sector al que pertenecen, enfrentan riesgos en todos los niveles de su organización. Los riesgos afectan la habilidad de cada entidad para sobrevivir, competir con éxito dentro de su sector, mantener una posición financiera fuerte y una imagen pública positiva así como la calidad global de sus productos, servicios y empleados. No existe ninguna forma

práctica de reducir el riesgo a cero. De hecho, el riesgo es inherente a los negocios. La Dirección debe determinar cuál es el nivel de riesgo que se considera aceptable y esforzarse para mantenerlo dentro de los límites marcados.

El establecimiento de objetivos es una condición previa a la evaluación de los riesgos. La Dirección debe fijar primero los objetivos antes de identificar los riesgos que pueden tener un impacto sobre su consecución y tomar las medidas oportunas. Por tanto, el establecimiento de objetivos es una fase clave de los procesos de gestión. Si bien no constituye un componente del control interno, es un requisito previo que permite garantizar el funcionamiento del mismo.

2.2.2.1. Objetivos

El establecimiento de objetivos puede ser un proceso muy estructurado o, por el contrario, informal. Los objetivos pueden estar claramente identificados o estar implícitos. Los objetivos generales de una entidad están representados normalmente por la misión y los valores que la entidad considera prioritarios. Estos objetivos, junto con la evaluación de los puntos fuertes y débiles de la entidad y de las oportunidades y amenazas del ambiente, llevan a definir una estrategia global. Generalmente, el plan estratégico se establece en términos amplios, y trata la asignación de recursos entre las distintas unidades del negocio y las prioridades a nivel global.

Los objetivos específicos se derivan de la estrategia global de la entidad. Los objetivos globales de la empresa están relacionados e integrados en objetivos más específicos establecidos para las diversas actividades (tales como ventas, producción e ingeniería), asegurándose de que sean coherentes entre sí. Estossubobjetivos u objetivos a nivel de actividad incluyen el establecimiento de metas concretas y pueden consistir

en objetivos de una línea de productos, de mercado de financiación o de resultados.

Al establecer objetivos globales y por actividad, una entidad puede identificar los factores críticos del éxito. Estos son los hechos que deben producirse o las condiciones que deben existir para que los objetivos puedan ser alcanzados. Los factores críticos del éxito existen para la entidad, para una unidad empresarial, una función, un departamento o un individuo. El establecimiento de objetivos permite a la dirección identificar los criterios para medir el rendimiento, poniendo especial énfasis en los factores críticos del éxito.

A pesar de su diversidad, **los objetivos pueden agruparse en tres grandes categorías:**

- Objetivos relacionados con las operaciones – se refieren a la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y la salvaguarda de los recursos contra posibles pérdidas. Estos objetivos varían en función de la elección de la Dirección respecto a estructuras y rendimiento.
- Objetivos relacionados con la información financiera – se refieren a la preparación de estados financieros confiables y a la prevención de la falsificación de la información financiera publicada. A menudo, estos objetivos están condicionados por requerimientos externos.
- Objetivos de cumplimiento – estos objetivos se refieren al cumplimento de las leyes y normas a las que está sujeta la entidad. Dependen de factores externos (tales como la reglamentación en materia de medio ambiente), y tienden a ser parecidos en todas las entidades, en algunos casos, o en todo un sector, en otros.

Un objetivo dentro de una categoría puede solaparse con un objetivo de otra, deben ser complementarios y estar relacionados entre sí. Los objetivos globales de la entidad no sólo deben ser coherentes con las

capacidades y expectativas de la misma, sino que también deben serlo con los objetivos de sus unidades empresariales y funciones. Los objetivos relativos a las actividades deben ser claros, es decir, deben resultar fácilmente comprensibles para los individuos responsables de su realización. También deben ser medibles. Los empleados y la Dirección deben haber llegado a un consenso sobre lo que ha de conseguirse y sobre la forma de determinar en qué medida se han alcanzado los objetivos.

Existe una diferencia en cuanto a los objetivos relacionados con las operaciones. Primero, no están basados en pautas externas. Segundo, una entidad puede desarrollar actividades según tenía planeado pero puede verse superadas por un competidor. Asimismo, puede verse sometida a acontecimientos externos –un cambio de gobierno, condiciones climatológicas adversas, etc.- que no puede controlar. Incluso puede que haya tenido en cuenta algunos de estos acontecimientos en el proceso de establecer objetivos y los haya considerado como de baja probabilidad habiendo desarrollado también un plan de contingencias por si se producían. Sin embargo, un plan de este tipo únicamente amortigua el impacto de los acontecimientos externos. No garantiza la consecución de los objetivos. Unas operaciones adecuadas y coherentes con la meta de los objetivos no garantizan el éxito.

La meta del control interno en esta área fundamentalmente se centra en el desarrollo de objetivos y metas coherentes en toda la organización, la identificación de factores clave de éxito y la presentación oportuna a la Dirección de información sobre el rendimiento y expectativas del negocio. Aunque no se puede garantizar el éxito, la Dirección debe tener la seguridad razonable de que se advertirá la situación en el caso que exista peligro de que no vayan a conseguirse los objetivos.

2.2.2.2. Riesgos

La identificación y el análisis de los riesgos es un proceso interactivo continuo y constituye un componente fundamental de un sistema de control interno eficaz. La Dirección debe examinar detalladamente los riesgos existentes a todos los niveles de la empresa y tomar las medidas oportunas para administrarlos.

Identificación de los riesgos

El rendimiento de una entidad puede verse amenazado tanto por factores internos como externos. Dichos factores, a su vez, pueden repercutir tanto en los objetivos explícitos como en los implícitos. El nivel de riesgo aumenta en la medida en que los objetivos se distancien de las pautas de comportamiento de la entidad en el pasado. A menudo, la entidad no fija objetivos explícitos globales en algunas áreas del negocio, puesto que considera que su rendimiento es aceptable. Aunque posiblemente no exista un objetivo explícito o escrito, en estos casos sí existe el objetivo implícito de “no cambiar”, o de “dejar las cosas como están”. Esto no significa que un objetivo implícito no conlleve un riesgo interno o externo. Por ejemplo, una entidad puede considerar que la calidad de los servicios que presta es satisfactoria pero, debido al cambio de política de un competidor, sus clientes no tengan una percepción tan favorable de los mismos.

Independientemente de que el objetivo sea explícito o implícito, el proceso de evaluación de riesgos de una entidad debería tener en cuenta los riesgos que puedan surgir. Es esencial que todos los riesgos sean identificados. Deben considerarse todas las interacciones significativasque se producen entre una entidad y los terceros. Dichos terceros comprenden los proveedores, inversores, acreedores, accionistas, empleados, clientes, compradores, intermediarios y competidores, tanto los actuales como los

potenciales, así como las instituciones públicas y los medios de comunicación.

La identificación de los riesgos es un proceso interactivo y suele estar integrado con el proceso de planificación. También es útil considerar los riesgos “desde cero”, en lugar simplemente de analizar su evolución a partir de un análisis anterior.

En el ámbito de la empresa, los riesgos pueden ser la consecuencia tanto de factores externos como internos. A continuación se exponen algunos ejemplos:

2.2.2.3. Factores externos

- Los avances tecnológicos pueden influir en la naturaleza y la evolución de los trabajos de investigación y desarrollo, o provocar cambios respecto a los suministros.
- Las necesidades o expectativas cambiantes de los clientes pueden influir en el desarrollo de productos, el proceso de producción, el servicio al cliente, la fijación de precios y las garantías.
- La competencia puede provocar cambios de actividades de marketing o de servicios.
- Las nuevas normas y reglamentos a veces obligan a que se modifiquen las políticas y las estrategias.
- Los desastres naturales pueden causar alteraciones en los sistemas de operaciones o de información, además de subrayar la necesidad de desarrollar planes de emergencia.
- Los cambios económicos pueden repercutir en las decisiones sobre financiación, inversiones y desarrollo.

2.2.2.4. Factores internos

- Las averías en los sistemas informáticos pueden perjudicar las operaciones de la entidad.
- La calidad de los empleados y los métodos de formación y motivación pueden influir en el nivel de concientización sobre el control dentro de la entidad.
- Los cambios de responsabilidades de los directivos pueden afectar la forma de realizar determinados controles.
- La naturaleza de las actividades de la entidad, así como el nivel de acceso del personal a los activos, pueden ser causas de apropiación indebida de los recursos.
- Un Consejo de Administración o un Comité de Auditoría débil o ineficaz pueden dar lugar a que se produzcan indiscreciones.

La identificación de los factores externos e internos que contribuyen a que aumente el riesgo a nivel de entidad resulta esencial para una evaluación eficaz de los riesgos. Una vez identificados los factores más importantes, los directivos pueden analizar su relevancia y, en la medida de lo posible, establecer vínculos entre los factores de riesgo y las actividades del negocio.

Además de identificar los riesgos a nivel de empresa, éstos deben ser identificados para cada actividad de la empresa. El tratar los riesgos a nivel de actividad ayuda a enfocar la evaluación de los mismos en las unidades o funciones más importantes del negocio, como ventas, producción, marketing, desarrollo tecnológico, e investigación y desarrollo. La correcta evaluación de los riesgos a nivel de actividad contribuye también a que se mantenga un nivel aceptable del mismo para el conjunto de la entidad.

2.2.2.5. Análisis de los riesgos

Después que se hayan identificado los riesgos a nivel de la entidad y de las actividades, debe llevarse a cabo un análisis de los mismos. La metodología de análisis de riesgos puede variar, principalmente porque muchos de ellos son difíciles de cuantificar. Sin embargo, el proceso, que puede ser más o menos formal, normalmente incluirá:

- Una estimación de la importancia del riesgo.
- Una evaluación de la probabilidad (o la frecuencia) de que el riesgo se materialice.
- Un análisis de cómo ha de administrarse el riesgo; es decir, debe realizarse una evaluación de las medidas que conviene adoptar.

Un riesgo que no tiene un efecto significativo en la entidad y cuya probabilidad de materialización es baja generalmente no será motivo de preocupación. En cambio, un riesgo importante y que es muy probable que se materialice, normalmente requerirá un análisis profundo. Entre estos dos extremos, el análisis de los riesgos es difícil y ha de efectuarse de forma racional y minuciosa.

Existen numerosos métodos para estimar el costo de la pérdida provocada por un riesgo identificado. La Dirección debe tener conocimiento de tales métodos y aplicarlos cuando sea preciso. Sin embargo, la envergadura de muchos riesgos no es fácil de precisar: en el mejor de los casos, pueden clasificarse como “altos”, “moderados” o “bajos”.

Una vez analizadas la importancia y la probabilidad de un riesgo, la Dirección debe estudiar la mejor forma de administrarlo. Para ello, ha de aplicar su juicio en base a ciertas hipótesis acerca del riesgo, además de efectuar un análisis de los costos en los que puede incurrir para reducir el riesgo.

Paralelamente a las medidas adoptadas para administrar el riesgo, existen los procedimientos que permiten que la Dirección efectúe el seguimiento de la implementación y la eficacia de las acciones. Por ejemplo, una de las acciones que una organización podría realizar para administrar el riesgo de la pérdida de servicios informáticos esenciales sería la formulación de un plan de contingencia. Los procedimientos necesarios se establecerían posteriormente para asegurar que el plan estuviera correctamente diseñado e implementado. Dichos procedimientos representarían “actividades de control”.

Antes de establecer unos procedimientos complementarios, la Dirección debe decidir si los existentes son adecuados a la vista de los riesgos identificados. En la medida en que unos procedimientos pueden satisfacer diversos objetivos, la Dirección de la empresa puede darse cuenta de que la adopción de medidas complementarias no está justificada, siendo los procedimientos existentes suficientes o debiendo, simplemente, ser aplicados de forma más rigurosa.

Por otra parte, la Dirección de la empresa debe tener en cuenta que siempre habrá cierto nivel de riesgo residual, no sólo porque los recursos no son ilimitados, sino por otras limitaciones inherentes a todo sistema de control interno.

2.2.3. Actividades de control

Las actividades de control consisten en las políticas y los procedimientos que tienden a asegurar que se cumplen las directrices de la dirección. También tienden a asegurar que se toman las medidas necesarias para afrontar los riesgos que pone en peligro el logro de los objetivos de la entidad. Las actividades de control se llevan a cabo en cualquier parte de la organización, en todos sus niveles y en todas sus funciones y comprenden una serie de actividades tan diferentes como pueden ser aprobaciones y

autorizaciones, verificaciones, conciliaciones, el análisis de los resultados de las operaciones, la salvaguarda de activos y la segregación de funciones.

Las actividades de control son las normas y procedimientos (que constituyen las acciones necesarias para implementar las políticas) que pretenden asegurar que se cumplan las directrices que la Dirección ha establecido con el fin de controlar los riesgos. Las actividades de control pueden dividirse en tres categorías, según el tipo de objetivo de la entidad con el que están relacionadas: las operaciones, la confiabilidad de la información financiera o el cumplimiento de la legislación aplicable.

Aunque algunos tipos de control están relacionados solamente con un área específica, con frecuencia afectan a más de una. Dependiendo de las circunstancias, una determinada actividad de control puede ayudar a alcanzar objetivos de la entidad que corresponden a diversas categorías. De este modo, los controles operacionales también pueden contribuir a la confiabilidad de la información financiera, los controles sobre la confiabilidad de la información financiera pueden contribuir al cumplimento de la legislación aplicable, y así, sucesivamente.

Existen muchas descripciones de tipos de actividades de control, que incluyen desde controles preventivos a controles detectivos, controles manuales, controles informáticos y controles de dirección. La categoría de una actividad de control puede venir determinada por los objetivos de control a los que corresponde como, por ejemplo, el asegurar la integridad y exactitud del procesamiento de datos. Las actividades de control que a continuación se exponen generalmente son llevadas a cabo por el personal a todos los niveles de una organización.

- Análisis efectuados por la Dirección - Los resultados obtenidos se analizan comparándolos con los presupuestos, las previsiones, los resultados de ejercicios anteriores y los de los competidores. Con el fin de evaluar en qué medida se están alcanzando los objetivos, la Dirección realiza

un seguimiento de las iniciativas principales como campañas comerciales, programas de mejora de los procesos de producción, programas de contención o reducción de costos. Las acciones de la Dirección relacionadas con el análisis y el seguimiento de dicha información representan actividades de control.

- Gestión directa de funciones por actividades – Los responsables de las diversas funciones o actividades revisan los informes sobre los resultados alcanzados. En el seno de un banco, por ejemplo, el responsable de los préstamos para consumo analiza los informes obtenidos por sucursal, región y tipo de préstamo, verifica los resúmenes, identifica las tendencias y relaciona los resultados con las estadísticas económicas y los objetivos. Los directores de las sucursales, a su vez, reciben información sobre los nuevos préstamos, distribuidos por responsable encargado y por segmento del mercado. Los directores de sucursal también se preocupan del cumplimiento de la legislación, mediante el análisis, por ejemplo, de los informes requeridos por los organismos de control para los nuevos depósitos que superen un importe determinado. Los flujos de caja diarios se concilian con las posiciones netas comunicadas a la oficina central con el objetivo de que éstas puedan efectuar las transferencias e inversiones oportunas.

- Proceso de información – Se realiza una serie de controles para comprobar la exactitud, integridad y autorización de las transacciones. Los datos introducidos en el sistema se comprueban a través del punteo manual de las ediciones o por comparación automática con los ficheros de control aprobados. Por ejemplo, el pedido de un cliente no se acepta hasta después de su comprobación a través del archivo de clientes y de la aprobación del límite de crédito. Se controla la secuencia numérica de las transacciones, los importes totales de los ficheros se comparan y se concilian con los saldos anteriores y con las cuentas de control. Las anomalías que requieren un seguimiento son analizadas por personal administrativo y son transmitidas a

los responsables cuando resulta necesario. Se controla el desarrollo de nuevos sistemas y la modificación de los existentes, al igual que el acceso a los datos, archivos y programas informáticos.

- Controles físicos – Los equipos de fabricación, las inversiones financieras, la tesorería y otros activos son objeto de protección y periódicamente se someten a recuentos físicos cuyos resultados se comparan con las cifras que figuran en los registros de control.

- Indicadores de rendimiento – El análisis combinado de diferentes conjuntos de datos (operativos o financieros) junto con la puesta en marcha de acciones correctivas, constituyen actividades de control. Los indicadores de rendimiento incluyen, por ejemplo, las fluctuaciones de los precios de compra, el porcentaje de pedidos urgentes y la proporción de devoluciones sobre el total de pedidos: mediante la investigación de los resultados inesperados o las tendencias anormales, la Dirección identifica las circunstancias en las que existe el peligro de que no se consigan objetivos relativos al suministro de materiales. Si esta información se utiliza sólo como soporte de la toma de decisiones operacionales, el análisis de los indicadores de rendimiento actúa, exclusivamente, como un control relativo a las operaciones. Si, por el contrario, dicha información también se utiliza para el seguimiento de resultados inesperados procedentes del sistema de información financiera, el análisis de indicadores de rendimiento también contribuye al control relativo a la confiabilidad de la información financiera.

- Segregación de funciones – Con el fin de reducir el riesgo que se cometan errores o irregularidades, las tareas se reparten entre los empleados. Así por ejemplo, se separan las responsabilidades de autorizar transacciones, de registrarlas y de gestionar los activos correspondientes. La persona que autoriza ventas a crédito no será responsable de los registros contables de la cuenta de clientes o de gestionar los ingresos en efectivo. De

la misma manera, los vendedores no pueden modificar el fichero de precios de venta ni el de porcentajes de las comisiones.

Estos son solamente algunos ejemplos de los múltiples procedimientos que, aplicados de forma cotidiana en las empresas, permiten que se refuerce el cumplimiento de los planes de acción establecidos y que sus organizaciones se mantengan en el camino adecuado para la consecución de sus objetivos.

Las actividades de control generalmente se apoyan en dos elementos: las políticas que determinan lo que debería hacerse (constituyen la base del segundo elemento) y los procedimientos necesarios para llevar a cabo las políticas.

De forma paralela a la evaluación de los riesgos, la Dirección debería establecer y aplicar el plan de acción necesario para afrontarlos. Una vez identificadas, estas acciones también serán útiles para definir las operaciones de control que se aplicarán para garantizar su ejecución de forma correcta, y en el tiempo deseado.

Las actividades de control forman una parte esencial del proceso mediante el cual una empresa intenta lograr sus objetivos de explotación. Las actividades de control no son un fin en sí mismas, ni tampoco deben existir simplemente porque parece que “es lo que hay que hacer”. Las actividades de control sirven como mecanismos para asegurar el cumplimiento del objetivo. El control es un elemento integrado en el proceso de gestión.

Los sistemas de información, que desempeñan un papel fundamental en la gestión de las empresas, deben necesariamente ser controlados, con independencia de su tamaño o que las informaciones obtenidas sean de naturaleza financiera, relativas a las actividades o se relacionen con la reglamentación vigente.

Las actividades de control en los sistemas de información pueden agruparse en dos categorías. La primera abarca los controles generales, que son aplicables a muchas o todas las operaciones y que ayudan a asegurar su correcto funcionamiento. La segunda categoría comprende controles de aplicación que incluyen los procedimientos programados en el seno de las aplicaciones y los procedimientos manuales asociados para asegurar el control de proceso de los diversos tipos de transacciones. Juntos, estos controles sirven para asegurar la totalidad, exactitud, y autorización de la información financiera y de otro tipo, almacenada en el sistema.

Estas dos categorías de control de los sistemas informáticos están relacionadas entre sí: los controles generales son necesarios para asegurar el funcionamiento adecuado de los controles de aplicación que dependen de los procesos informáticos.

Por ejemplo, mediante los controles de aplicación se pueden examinar, cotejar y editar los datos en el momento de ser introducidos. Estos controles proporcionan información al instante cuando algo no cuadra o tiene un formato equivocado, para que puedan efectuarse de inmediato las correcciones correspondientes. Asimismo, generan mensajes en la pantalla que indican dónde se halla el error en los datos y hacen informes de excepciones para su seguimiento.

Si los controles generales son inadecuados, no es posible apoyarse en los controles de aplicación que suponen que el sistema propiamente dicho funciona correctamente: comprobación con el fichero adecuado, mensajes de error identificando adecuadamente los problemas o informes de excepciones sin omisiones.

Otro ejemplo del equilibrio que se necesita entre los controles generales y los de aplicación es el control de integridad, que se utiliza con frecuencia para ciertos tipos de transacciones en las que se utilizan

documentos pre numerados (suele tratarse de documentos internos, como los pedidos de compra). Sobre la base de dicho control, las transacciones duplicadas son identificadas como tal o rechazadas por el sistema. Para llevar a cabo este control, según el diseño elegido, el sistema rechazará las partidas anómalas o las mantendrá en suspenso al mismo tiempo que les facilita a los usuarios informes sobre los números que falten, las partidas duplicadas así como las partidas cuyas características excedan los límites de los parámetros preestablecidos.

La relación entre los controles de aplicación y los controles generales consiste en que éstos son indispensables para el funcionamiento de los controles de aplicación, y que ambos son necesarios para garantizar el proceso completo y correcto de la información.

2.2.4. Información y Comunicación

Es necesario identificar, recoger y comunicar la información relevante de un modo y en un plazo tal que permita a cada uno asumir sus responsabilidades. Los sistemas de información generan informes, que recogen información operacional, financiera y la correspondiente al cumplimiento, que posibilitan la dirección y el control del negocio. Dichos informes contemplan, no sólo, los datos generados internamente, sino también información sobre incidencias, actividades y condiciones externas, necesarias para la toma de decisiones y para formular informes financieros. Por otra parte, se debe establecer una comunicación eficaz en el sentido más amplio, lo cual implica una circulación multidireccional de la información, es decir ascendente, descendente y transversal. La Dirección debe transmitir un mensaje claro a todo el personal sobre la importancia de las responsabilidades de cada uno en materia de control. Los empleados deben comprender el papel que deben desempeñar dentro del sistema de control

interno, así como la relación existente entre las actividades propias y las de los demás empleados. El personal deberá disponer de un sistema para comunicar información importante a los niveles superiores de la empresa. Asimismo, es necesaria una comunicación eficaz con terceros, tales como los clientes, los proveedores, los organismos de control y los accionistas.

Todas las empresas han de obtener información relevante, tanto financiera como de otro tipo, relacionada con las actividades y acontecimientos internos y externos. La información a recoger debe ser de la naturaleza que la Dirección haya estimado relevante para la gestión del negocio y debe llegar a las personas que la necesiten en la forma y el plazo que permita la realización de sus responsabilidades de control y de sus otras funciones.

2.2.4.1. Información

La gestión de la empresa y el progreso hacia los objetivos que se han fijado (sean relativos a las operaciones, a la información financiera o al cumplimiento de las leyes y normas) implican que la información es necesaria en todos los niveles de la empresa. En este sentido, la información financiera no se utiliza únicamente para formular los estados financieros para su difusión general, sino también para la toma de decisiones relativas a la explotación, incluyendo, a modo de ejemplo, las correspondientes al control del rendimiento y la asignación de recursos.

Los sistemas de información permiten identificar, recoger, procesar y divulgar estos datos. El término “sistemas de información” se utiliza generalmente para denominar el procesamiento de datos generado internamente, relativo a las transacciones (tales como compras y ventas), y a las actividades operativas internas (tal como el proceso de producción).

Efectivamente, los sistemas de información (que pueden ser informatizados, manuales o bien una mezcla de los dos) cubren dichas

áreas. Sin embargo, aquí se utiliza el término en un sentido mucho más amplio, incorporando también la información sobre hechos, actividades y factores externos: los datos económicos correspondientes a un determinado mercado o industria que señalan cambios en la demanda de los productos o servicios de la empresa, la información sobre bienes y servicios necesarios en el proceso de producción, las investigaciones de mercado sobre la evolución en las preferencias y exigencias de los clientes, la información sobre las actividades de desarrollo de productos por la competencia y respecto a iniciativas en materia de leyes y normativa.

Existen sistemas de información formales e informales, pues las conversaciones con clientes, proveedores, organismos de control y empleados a menudo proporcionan parte de la información más vital para poder identificar riesgos y oportunidades. Asimismo, se puede obtener una información muy valiosa asistiendo a seminarios profesionales o sectoriales, o formando parte de asociaciones mercantiles y de otros tipos.

Resulta especialmente importante mantener la información acorde con las necesidades de la empresa, al actuar ésta en un entorno de cambios constantes, con competidores muy innovadores y ágiles, y donde la demanda evoluciona rápidamente.

La calidad de la información

La calidad de la información generada por el sistema afecta la capacidad de la Dirección de tomar decisiones adecuadas al gestionar y controlar las actividades de la entidad. Generalmente, los sistemas modernos incorporan una opción de consulta en línea, para que se pueda obtener información actualizada en todo momento.

Resulta imprescindible que los informes ofrezcan suficientes datos relevantes para posibilitar un control eficaz. La calidad de la información se refiere a los siguientes aspectos:

- Contenido. ¿Contiene todos los datos necesarios?

- Oportunidad. ¿Se provee en el tiempo adecuado?
- Actualidad. ¿Es la más reciente disponible?
- Exactitud. ¿Los datos son concretos?
- Accesibilidad. ¿Puede ser obtenida fácilmente por las personas adecuadas?

El diseño del sistema debe responder a todas estas preguntas. En caso contrario, el sistema seguramente no facilitará la información necesaria a la Dirección y otros empleados.

2.2.4.2. Comunicación

La comunicación es inherente a los sistemas de información. Según se ha comentado anteriormente, los sistemas de información deben proporcionar información a las personas adecuadas, de forma que éstas puedan cumplir con sus responsabilidades operacionales, de información financiera o de cumplimiento. Sin embargo, también debe existir una comunicación más amplia, que aborde las expectativas y responsabilidades de las personas y los grupos, así como otras cuestiones importantes.

Tanto la claridad del mensaje como la eficacia de su comunicación son importantes. Además, cada función concreta ha de especificarse con claridad. Cada persona tiene que entender los aspectos relevantes del sistema de control interno, cómo funciona el mismo y saber cuál es su papel y responsabilidad en el sistema. De lo contrario, es probable que surjan problemas.

A la hora de llevar a cabo sus funciones, el personal de la empresa debe saber que cuando se produzca una incidencia conviene prestar atención no sólo al propio acontecimiento, sino también a su causa. De esta forma, se podrán identificar la deficiencia potencial en el sistema, tomando las medidas necesarias para evitar que se repita. Por ejemplo, la detección de existencias no comercializables no debería conducir solamente al registro

de una previsión en los estados financieros, sino también a la determinación de las razones que originaron la imposibilidad de comercializar las existencias afectadas.

Asimismo, el personal tiene que saber cómo sus actividades están relacionadas con el trabajo de los demás. Este conocimiento es necesario para reconocer los problemas y determinar sus causas y la medida correctiva adecuada. El personal tiene que saber los comportamientos esperados, aceptados e inaceptables.

Los empleados también necesitan disponer de un mecanismo para comunicar información relevante a los niveles superiores de la organización. Los empleados de primera línea, que manejan aspectos clave de la explotación todos los días, generalmente son los más capacitados para reconocer los problemas en el momento en que se producen. Para que la información llegue a los niveles superiores deben existir líneas abiertas de comunicación y la clara voluntad de escuchar por parte de los directivos. Las personas tienen que creer que sus superiores realmente quieren enterarse de las incidencias producidas y que las resolverán de manera adecuada.

La comunicación entre la Dirección, el Consejo de Administración y los Comités constituidos por éste, es de una importancia básica. La Dirección debe mantener al Consejo informado respecto de la rentabilidad, los desarrollos, los riesgos, las iniciativas significativas y demás acontecimientos e incidencias relevantes. Al ser más fluidas las comunicaciones al Consejo, éste podrá actuar de modo más eficaz al cumplir con sus responsabilidades de supervisión, sirviendo de foro para el debate de cuestiones importantes y ofreciendo su asesoría. De igual manera, el Consejo debería informar a la Dirección de sus necesidades de información, orientándola y comentando su actuación.

Además de una buena comunicación interna, ha de existir una eficaz comunicación externa. Al disponer de líneas abiertas de comunicación,

los clientes y proveedores podrán aportar información de gran valor sobre el diseño y la calidad de los productos y servicios de la empresa, permitiendo que la entidad responda a los cambios en las exigencias y preferencias de los clientes. Por otra parte, toda persona que entre en contacto con la entidad debe entender que no se tolerarán actos indebidos, como sobornos y otros pagos ilegítimos.

Las comunicaciones recibidas de terceros a veces proporcionan información importante sobre el funcionamiento del sistema de control interno. El conocimiento que tienen los auditores externos de las operaciones de la entidad y otros aspectos relacionados, es una importante fuente de información para la Dirección y el Consejo sobre el sistema de control.

La comunicación establecida entre la Dirección y los interlocutores externos, sea o no dinámica, realizada de forma abierta y sincera, permite transmitir en uno u otro caso un mensaje a todos los ámbitos de la entidad.

La comunicación se materializa en manuales de políticas, memorias, avisos en el tablón de anuncios o mensajes. Cuando los mensajes se transmiten verbalmente (a grupos grandes, reuniones o a una sola persona) la entonación y el lenguaje corporal sirven para dar énfasis al mensaje verbal.

Otro potente medio de comunicación lo constituye la actuación de la Dirección al tratar con sus subordinados. Los directivos deberían recordar siempre que “una acción vale más que mil palabras”. La actuación de la Dirección, a su vez, está influenciada por la historia y la cultura de la entidad, basándose en el tratamiento seguido en situaciones similares por parte de sus propios predecesores.

La entidad que tiene una larga historia de actuar con integridad y cuya cultura es bien comprendida por las personas que componen la organización no tendrá dificultades para comunicar su mensaje. Las

entidades que no cuentan con una tradición similar probablemente tendrán que dedicar más esfuerzos a la comunicación adecuada de mensajes.

2.2.5. Supervisión

Resulta necesario realizar una supervisión de los sistemas de control interno, evaluando la calidad de su rendimiento. Dicho seguimiento tomará la forma de actividades de supervisión continuada, de evaluaciones periódicas o una combinación de los dos anteriores. La supervisión continuada se inscribe en el marco de las actividades corrientes y comprende unos controles regulares efectuados por la Dirección, así como determinadas tareas que realiza el personal en el cumplimiento de sus funciones. El alcance y la frecuencia de las evaluaciones puntuales se determinarán principalmente en función de una evaluación de riesgos y de la eficacia de los procedimientos de supervisión continuada. Las deficiencias en el sistema de control interno, en su caso, deberán ser puestas en conocimiento de la gerencia y los asuntos de importancia serán comunicados al primer nivel directivo y al Consejo de Administración.

Los sistemas de control interno y, en ocasiones, la forma en que los controles se aplican, evolucionan con el tiempo, por lo que procedimientos que eran eficaces en un momento dado, pueden perder su eficacia o dejar de aplicarse. Las causas pueden ser la incorporación de nuevos empleados, defectos en la formación y supervisión, restricciones de tiempo y recursos, y presiones adicionales. Asimismo, las circunstancias en base a las cuales se configuró el sistema de control interno en un principio también pueden cambiar, reduciendo su capacidad de advertir los riesgos originados por las nuevas circunstancias. En consecuencia, la Dirección tendrá que determinar si el sistema de control interno es, en todo momento, adecuado y evaluar su capacidad de asimilar los nuevos riesgos.

El proceso de supervisión asegura que el control interno continúa funcionando adecuadamente. Este proceso comprende la evaluación, por parte de empleados de nivel adecuado, de la manera en que se han diseñado los controles, de su funcionamiento, y de la forma en que se adoptan las medidas necesarias. Se aplicará a todas las actividades dentro de la entidad y a veces también a externos contratados.

Las operaciones de supervisión se materializan en dos formas: actividades continuadas o evaluaciones puntuales. Normalmente los sistemas de control interno aseguran, en mayor o menor medida, su propia supervisión. En este sentido, cuanto mayor sea el nivel y la eficacia de la supervisión continuada, menor será la necesidad de evaluaciones puntuales. La frecuencia necesaria de las evaluaciones puntuales para que la Dirección tenga una seguridad razonable de la eficacia del sistema de control interno se deja a juicio de la Dirección.

A la hora de determinar dicha frecuencia, habrá que tener en cuenta lo siguiente: la naturaleza e importancia de los cambios y los riesgos que éstos conllevan, la competencia y experiencia de las personas que aplican los controles, así como los resultados conseguidos por la supervisión continuada. Una combinación de supervisión continuada y evaluaciones puntuales normalmente asegura el mantenimiento de la eficacia del sistema de control interno.

Conviene reconocer que las actividades normales y recurrentes de la entidad incorporan procedimientos de supervisión continuada que, ejecutándose en tiempo real y arraigados en la entidad, responden de manera dinámica a las circunstancias de cada momento. En consecuencia, resultan más eficaces que los procedimientos aplicados en la evaluación independiente. Esta se realiza a posteriori, por lo que el seguimiento continuado permite identificar los posibles problemas con mayor rapidez. No obstante, algunas entidades con actividades estables de supervisión

continuada realizan evaluaciones independientes de su sistema de control interno o partes del mismo, de forma regular (por ejemplo, de forma rotativa en varios años). Si la entidad advierte la necesidad de frecuentes evaluaciones puntuales, deberá centrar sus esfuerzos en mejorar las actividades de supervisión continuada, poniendo más énfasis en los “controles integrados” que en los “controles complementarios”.

2.2.5.1. Actividades de supervisión continuada

Existe una gran variedad de actividades que permiten efectuar un seguimiento de la eficacia del control interno en el desarrollo normal del negocio. Comprenden actividades corrientes de gestión y supervisión, comparaciones, conciliaciones y otras tareas rutinarias.

Se exponen a continuación algunos ejemplos de actividades de supervisión continuada:

- Los diferentes Directores de explotación comprueban que el sistema de control interno continúa funcionando a través del cumplimiento de sus funciones de gestión. Al incluir o conciliar los distintos informes de explotación con los informes financieros, empleando los mismos continuamente en la gestión de la explotación, es probable que se identifiquen de manera rápida los errores importantes o las excepciones en los resultados previstos.
- Las comunicaciones recibidas de terceros confirman la información generada internamente o señalan la existencia de problemas. En este sentido, los clientes corroboran los datos de facturación implícitamente al pagar sus facturas. Por el contrario, los reclamos respecto de la facturación podrían indicar la existencia de deficiencias en los controles sobre el proceso de las transacciones comerciales.
- Una estructura adecuada y unas actividades de supervisión apropiadas permiten comprobar las funciones de control e identificar las

deficiencias existentes. En este sentido, como rutina normal se supervisará las tareas administrativas que actúan de control sobre la exactitud y totalidad del proceso de las transacciones. Asimismo, se establecerá una segregación de funciones de manera que se ejerza una verificación recíproca, lo que servirá además de disuasión al fraude, ya que dificulta el disimular las actividades sospechosas.

- Los datos registrados por los sistemas de información se comparan con los activos físicos. Los resultados de estos recuentos se comparan con los registros contables y se comunican las diferencias detectadas.

- Los seminarios de formación, las sesiones de planificación y otras reuniones, le permiten a la Dirección obtener información importante respecto de la eficacia de los controles. Además de los problemas concretos que indiquen temas de control, la cultura de control de los participantes quedará manifiesta en dichas reuniones.

- Con una determinada frecuencia, se puede solicitar una manifestación explícita por parte del personal, en el sentido de si comprenden y cumplen con el código de conducta de la entidad. De igual forma, se solicitan manifestaciones del personal implicado en la explotación y en temas financieros, respecto a la realización periódica de determinados procedimientos de control, como sería la conciliación de determinados saldos. La Dirección o Auditoría Interna procederá a continuación a verificar la veracidad de dichas manifestaciones.

Es evidente que las anteriores actividades de supervisión continuada hacen frente a aspectos importantes de cada uno de los componentes del control interno.

2.2.5.2. Evaluaciones puntuales

Aunque los procedimientos de supervisión continuada suelen proporcionar información importante sobre la eficacia de otros componentes

de control, de vez en cuando un replanteo del sistema resultará útil. Con ocasión del mismo, se puede examinar la continuidad de la eficacia de los procedimientos de supervisión continuada.

El alcance y la frecuencia de la evaluación del control interno varían según la magnitud de los riesgos objeto de control y la importancia de los controles para la reducción de aquellos. Así los controles que actúan sobre los riesgos de mayor prioridad y los más críticos para la reducción de un determinado riesgo, serán objeto de evaluación con más frecuencia. La evaluación de todo el sistema de control interno (que normalmente no resultará necesaria con la frecuencia de las evaluaciones de controles específicos) puede estar motivada por diferentes razones: cambios importantes en la estrategia o en la Dirección, importantes adquisiciones o enajenaciones, o modificaciones de envergadura efectuadas en la explotación o en los métodos utilizados en el proceso de la información financiera.

A menudo las supervisiones se efectúan en forma de autoevaluación, llevada a cabo por las personas responsables de una unidad o función específica que determinarán la eficacia de los controles aplicados a sus actividades. El Director de una división, por ejemplo, gestionará la evaluación de su sistema de control interno, evaluando personalmente los factores relativos al ambiente de control y asignando a los encargados de las distintas actividades operativas de la división la evaluación de la eficacia de los demás componentes del control. Los jefes de línea centrarán su atención principalmente en los objetivos operacionales y de cumplimiento, mientras que el responsable financiero de la división se centrará en el objetivo de confiabilidad de la información financiera. A continuación, todos los resultados serán presentados a la Dirección responsable para su revisión. Posteriormente, las evaluaciones de la división serán analizadas por la

Dirección General, junto a las evaluaciones de control interno de las otras divisiones.

La evaluación del control interno forma parte de las funciones normales de Auditoría Interna y también resulta de peticiones especiales por parte del Consejo de Administración, la Dirección General y los Directores de filial o de división. Por otra parte, el trabajo realizado por los auditores externos constituye un elemento de análisis a la hora de determinar la eficacia del control interno. Una combinación del trabajo de las dos auditorías, la interna y la externa, posibilita la realización de los procedimientos de evaluación que la Dirección considere necesarios.

2.2.5.3. Comunicación de deficiencias

Las deficiencias en el sistema de control interno pueden ser detectadas tanto a través de los procedimientos de supervisión continuada realizados en la entidad como de las evaluaciones puntuales del sistema de control interno, así como a través de terceros.

El término “deficiencia” se usa aquí en un sentido amplio como referencia a un elemento del sistema de control interno que merece atención, por lo que una deficiencia puede representar un defecto percibido, potencial o real, o bien una oportunidad para reforzar el sistema de control interno con la finalidad de favorecer la consecución de los objetivos de la entidad.

¿De qué deficiencias se debe informar? No es posible que una sola respuesta sea aplicable a todas las entidades, siendo un tema muy susceptible de interpretación subjetiva. No obstante, se pueden delimitar algunos parámetros. Naturalmente, todas las deficiencias que puedan afectar a la consecución de los objetivos de la entidad deben ponerse en conocimiento de las personas que pueden tomar las medidas necesarias. La naturaleza de los temas a comunicar dependerá del nivel de autoridad

asignada al que detecta las incidencias para resolverlas a medida que vayan surgiendo, así como de las actividades de supervisión de los superiores.

Para determinar qué deficiencias se deben comunicar, conviene examinar el impacto de las mismas. Por ejemplo, un comercial señala un error de cálculo en las comisiones de ventas. El departamento de nómina investiga el tema, descubriendo que se utilizó el precio antiguo de un determinado producto, por lo que las comisiones estaban subvaluadas, así como la facturación a los clientes. Las medidas a tomar incluyen la rectificación de todas las comisiones y todas las facturas emitidas desde que entró en vigor el cambio de precios.

No obstante, es posible que esta medida no cubra una serie de cuestiones importantes relacionadas: ¿Por qué no se utilizó el precio nuevo en un principio? ¿Qué controles existen para asegurar que los incrementos de precio se introduzcan correctamente en el sistema informático y en el momento debido? ¿Existe algún problema en los programas informáticos que calculan las comisiones y la facturación? En caso afirmativo, ¿requieren atención los controles sobre el desarrollo de software y sobre su mantenimiento? En caso que el representante no hubiese comunicado el error, ¿otro componente del control interno habría identificado la deficiencia de forma oportuna?

De esta manera, un problema aparentemente sencillo con una solución evidente puede tener implicancias de mayor trascendencia para el control interno. Esto viene a subrayar la necesidad de comunicar los errores u otras incidencias a niveles de mayor autoridad en la entidad, siendo vital que, además de comunicar la transacción o incidencia concreta, se vuelvan a evaluar los controles potencialmente defectuosos.

La información generada por los empleados en el curso normal de sus tareas se comunica a través de los canales habituales a su superior inmediato, quien, a su vez, puede llevar la información a niveles superiores u

horizontalmente en la organización, de forma que llegue a las personas que pueden y deben tomar medidas. Deberían existir líneas alternativas para comunicar información sensible, tal como la relativa a posibles actuaciones ilegales o incorrectas.

Al detectar una deficiencia del control interno, se debe comunicar el hecho a la persona responsable de la función o actividad implicada, que podrá tomar medidas correctivas, así como al nivel superior en la entidad. Este proceso permite que el responsable dé el apoyo y la supervisión necesaria para las acciones correctivas a tomar e informe a las otras personas en la organización cuyas actividades pueden verse afectadas. En el caso que la deficiencia tenga un efecto horizontal, la comunicación del hecho también debe ser horizontal y alcanzar el nivel suficiente para asegurar que se tomen las medidas correspondientes.

Además el control interno debe ir acompañado de los siguientes elementos para que en coordinación puedan lograr un efectivo desarrollo de la actividad detectando oportunamente fallas y desvíos.

Un organigrama es la representación gráfica de la estructura de una empresa o cualquier otra organización. Incluyen las estructuras departamentales, indicando las líneas de mando, para reconocer e identificar bien quien es el superior de quien y asegurarnos que haya una unidad de jerarquía, ya que una persona no puede responder a dos superiores.

El organigrama es un modelo abstracto y sistemático que permite obtener una idea uniforme y sintética de la estructura formal de una organización:

- Desempeña un papel informativo.
- Presenta todos los elementos de autoridad, los niveles de jerarquía y la relación entre ellos.

Todo organigrama tiene el compromiso de cumplir los siguientes requisitos:

- Tiene que ser fácil de entender y sencillo de utilizar.
- Debe contener únicamente los elementos indispensables.

Un manual de funciones comprende las funciones o responsabilidades de cada área de la empresa, por ejemplo gerencia, producción, ventas, almacenes, etc. describiendo como intervienen en el funcionamiento general de la empresa, contiene la visión, misión, los objetivos, metas y la descripción de cada área así como sus responsabilidades.

Por otra parte existe el manual de procedimientos, es la descripción de todos y cada uno de los procesos que integran la secuencia de producción, o servicio que otorga la empresa, con las actividades que le corresponden a cada puesto, en algunas empresas contiene hasta la descripción del manejo de la maquinaria. Generalmente están separados por áreas.

Los cursogramas son una herramienta que permite visualizar de forma gráfica los procedimientos de la empresa y detectar con facilidad cualquier error, repetición o demora innecesaria (por ejemplo, materiales que se compran sin controlar el stock existente, falta de alertas de cobro o pago, documentos inútiles).

CAPITULO II

EVOLUCION DE LA AUDITORIA CON LA APARICION DEL INFORME COSO II: MARCO INTEGRADO DE GESTION DE RIESGO CORPORATIVO

Sumario: 1. Gestión del riesgo corporativo

A través de los años los conceptos enunciados anteriormente sirvieron como pilar tanto de la auditoría, como del control dentro de las entidades del mundo. El Informe N° 5 y el Informe COSO eran quienes delimitaban las acciones a seguir en cuanto al desarrollo de estas áreas en las diferentes empresas. Debido a la globalización, el crecimiento y la complejidad que adquirían las distintas actividades llevada a cabo por los entes fue que tiempo después, se emitió otro documento, denominado "*Enterprise Risk Management (ERM) - Integrated Framework*"[7], que en la actualidad se conoce como COSO II o COSO ERM.

Si bien hasta ese momento muchas organizaciones y entidades habían desarrollado enfoques para encarar la auditoria y el control mediante la gestión de riesgos, y a decir verdad existía una gran cantidad de literatura

[7]Gestión del riesgo empresarial (ERM) en el negocio incluye los métodos y procesos utilizados por las organizaciones para gestionar los riesgos y aprovechar las oportunidades relacionadas con la consecución de sus objetivos. Proporciona un marco para la gestión de riesgos, que generalmente implica la identificación de los eventos o circunstancias particulares relevantes para los objetivos de la organización y la evaluación de ellos en términos de probabilidad y la magnitud.

al respecto, no había una terminología común para el tema ni se habían elaborado principios ampliamente aceptados que pudieran ser utilizados por las empresas como una guía en el desarrollo de una estrategia efectiva para la administración de riesgos. El COSO II vino a llenar ese vacío: al reconocer la necesidad de una guía definitiva para la gestión de riesgos, el Comité inició un proyecto, el cual fue liderado por *Price wáter house Coopery* contó con la asistencia de un consejo compuesto por miembros de las cinco entidades patrocinantes del Comité. El *framework* define los componentes esenciales de la administración de riesgos, analiza los principios y conceptos del ERM, sugiere un lenguaje común y provee guías para eficientizar las tareas. Volviéndose en la actualidad el método más efectivo a emplear por las empresas, las cuales con el tiempo irán adoptándolo a medida que se observen sus resultados y su eficacia.

1. Gestión de riesgo corporativo.

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 ausencia de certeza y el reto para su dirección es determinar cuánta incertidumbre se puede aceptar mientras se esfuerzan en incrementar el valor para sus grupos de interés.

La incertidumbre implica riesgos y oportunidades y posee el potencial de erosionar 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 una estrategia y objetivos para encontrar un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad y los riesgos asociados, además de desplegar 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 correspondientes y desarrollando mecanismos para gestionar los riesgos asociados.

- 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 pérdidas operativas

Las entidades consiguen mejorar su capacidad para identificar los eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costes 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 y 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 eficazmente las necesidades globales de capital y mejorar su asignación.

Estas capacidades, inherentes en la gestión de riesgos corporativos, ayudan a la dirección a alcanzar los objetivos de rendimiento y rentabilidad de la entidad y prevenir la pérdida de recursos. La gestión de riesgos corporativos permite asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a 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 baches y sorpresas por el camino.

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 reviertan en la estrategia y el proceso de definición de objetivos, y formula planes que permitan aprovecharlas.

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.

Conceptos básicos de la gestión de riesgos corporativos:

- Es un proceso continuo que fluye por toda la entidad.
- Es realizado por su 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 adoptar una perspectiva del riesgo a nivel conjunto 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 orientada al logro de objetivos dentro de unas 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 organizaciones, industrias y sectores. Se centra directamente 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.

1.3. Consecución de Objetivos

Dentro del contexto de misión o 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. El presente Marco de gestión de riesgos corporativos está orientado a alcanzar los objetivos de la entidad, que se pueden clasificar en cuatro categorías:

- Estrategia: Objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo
- Operaciones: 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. Otra categoría utilizada por algunas entidades es la salvaguarda de activos.

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.

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 talante 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 revierten hacia la estrategia de la dirección o 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.

- Supervisión

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.

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 estrategia, operaciones, 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.

Eficacia

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, respectivamente, 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 la 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.

Limitaciones

Aunque la gestión de riesgos corporativos proporciona ventajas importantes, también presenta limitaciones. Además de los factores comentados anteriormente, 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 costes y beneficios relativos, que pueden darse fallos por error humano, que pueden eludirse los controles mediante connivencia 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.

Inclusión del Control Interno

El control interno constituye una parte integral de la gestión de riesgos corporativos. Este Marco lo incluye, constituyendo una conceptualización y una herramienta más sólidas para la dirección. El control interno se define y describe en el documento Control Interno Marco integrado. Dado que éste ha perdurado a lo largo del tiempo y es la base para las reglas, normas y leyes existentes, se mantiene vigente para definir y enmarcar el control interno.

Aunque el presente documento sólo recoge partes de Control Interno Marco integrado, su estructura entera se incorpora en él a través de referencias.

Roles y Responsabilidades

Todas las personas que integran una entidad tienen alguna responsabilidad en la gestión de riesgos corporativos. El consejero delegado es su responsable último y debería asumir su titularidad. Otros directivos

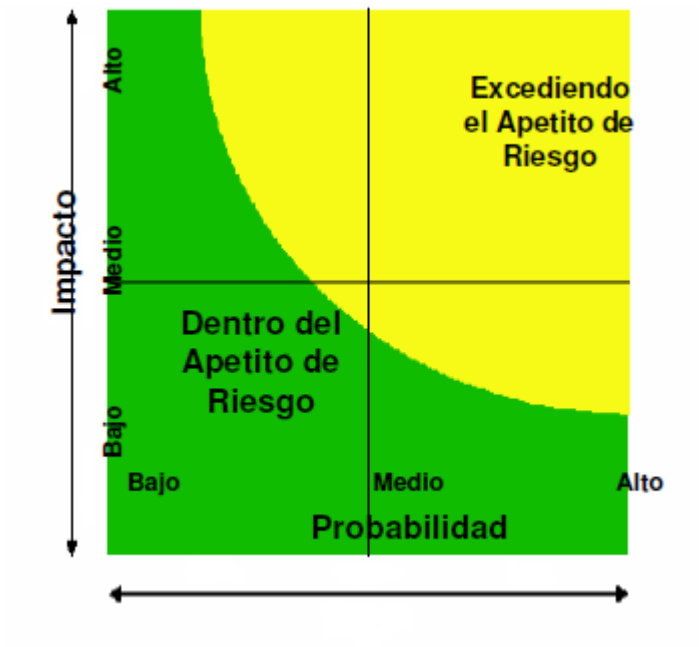
apoyan la filosofía de gestión de riesgos de la entidad, promueven el cumplimiento del riesgo aceptado y gestionan los riesgos dentro de sus áreas de responsabilidad en conformidad con la tolerancia al riesgo. El director de riesgos, director financiero, auditor interno u otros, desempeñan normalmente 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 consciente del riesgo aceptado por la entidad y está de acuerdo con él.

Algunos terceros, como los clientes, proveedores, colaboradores, auditores externos, reguladores y analistas financieros, proporcionan a menudo información útil para el desarrollo de la gestión de riesgos corporativos, aunque no son responsables de su eficacia en la entidad ni forman parte de ella.

1.6. Apetito del riesgo

El apetito del riesgo es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar; es una guía en el establecimiento de la estrategia. La gerencia lo expresa como un balance entre: crecimiento, riesgo y retorno. Dirige la asignación de recursos y alinea la organización, personal, procesos e infraestructura.

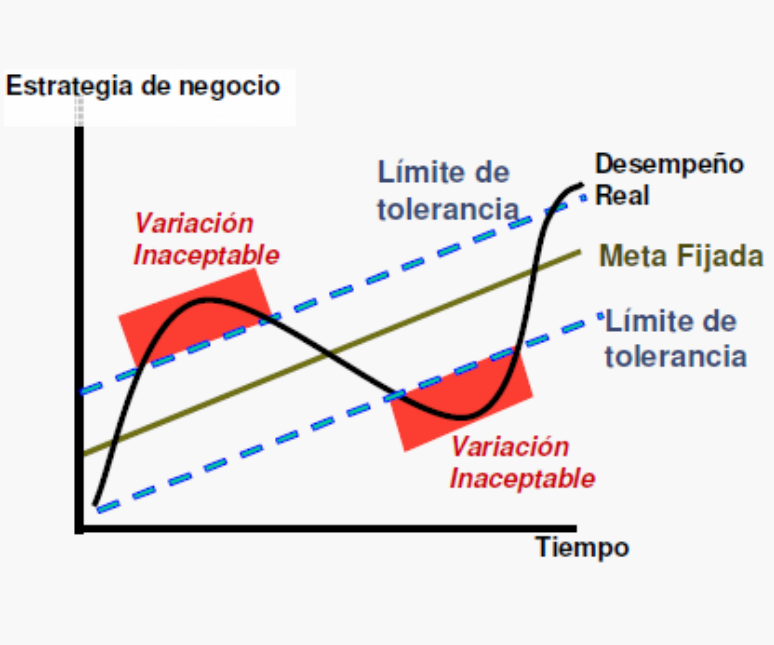


Fuente: Marco integrado de gestión de riesgo corporativo - Técnicas de aplicación.

1.7. Tolerancia del riesgo

Son los niveles aceptables de variación de las metas fijadas.

La tolerancia al riesgo se puede medir preferiblemente en las mismas unidades que los objetivos relacionados.



Fuente: Marco integrado de gestión de riesgo corporativo - Técnicas de aplicación.

1.8. Riesgo y Oportunidades

Los riesgos tienen un impacto negativo que puede 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.

1.9. Tipos de riesgos

Riesgo Inherente: Son aquellos que se presentan inherentes a las características del Sistema de Control Interno de la empresa.

Riesgo de Control: Son aquellos que existen y se propician por falta de control de las actividades de la empresa, y puede generar deficiencias del Sistema de Control Interno.

Riesgo de Detección: Es aquél que se asume por parte de los auditores que en su revisión no detecten deficiencias en el Sistema de Control Interno.

CAPITULO III

GESTIÓN DEL RIESGO CORPORATIVO – MARCO INTEGRADO – TÉCNICAS DE APLICACION

Sumario: 1. Elementos claves de la Gestión de Riesgo Corporativo

Esta parte del documento Gestión de riesgos corporativos - Marco integrado proporciona ejemplos prácticos de técnicas empleadas en diversos niveles de una entidad para aplicarlos principios de gestión de riesgos corporativos. La organización aludida aquí es análoga a la del Marco. Para poder obtener los beneficios deseados de este material, sus lectores deberán estar familiarizados con el Marco.

1. Elementos claves de la Gestión de Riesgo Corporativo

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.1. Ambiente interno

El ambiente interno abarca el talante de una organización, que influye en la conciencia de sus empleados sobre el riesgo y forma la base de los otros componentes de la gestión de riesgos corporativos, proporcionando disciplina y estructura. Los factores del ambiente interno incluyen la filosofía de gestión de riesgos de una entidad, su riesgo aceptado, la supervisión ejercida por el consejo de administración, la integridad, valores éticos y competencia de su personal y la forma en que la dirección asigna la autoridad y responsabilidad y organiza y desarrolla a sus empleados.

Impacto

El ambiente interno de una organización tiene un impacto significativo en el modo como se implanta la gestión de riesgos corporativos y en su funcionamiento continuado, constituyendo el contexto en que se aplican otros componentes de la gestión de riesgos corporativos, con un importante efecto positivo o negativo sobre ellos.

1.2. Establecimiento de objetivos

Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten a su consecución. Se fijan a escala estratégica, estableciendo con ellos una base para los objetivos operativos, de información y de cumplimiento. Cada entidad se enfrenta a una gama de riesgos procedentes de fuentes externas e internas y una condición previa para la identificación eficaz de eventos, la evaluación de sus riesgos y la respuesta a ellos es fijar los objetivos, que tienen que estar

alineados con el riesgo aceptado por la entidad, que orienta a su vez los niveles de tolerancia al riesgo de la misma.

Al considerar las posibles formas alternativas de alcanzar los objetivos estratégicos, la dirección identifica los riesgos asociados a una gama amplia de elecciones estratégicas y considera sus implicaciones. Se pueden aplicar diferentes técnicas de identificación y evaluación de los riesgos, que se expondrán posteriormente durante el proceso de establecimiento de la estrategia.

Objetivos relacionados

Los objetivos al nivel de empresa están vinculados y se integran con otros objetivos más específicos, que repercuten en cascada en la organización hasta llegar a subobjetivos establecidos, por ejemplo, en las diversas actividades de ventas ,producción, ingeniería e infraestructura.

1.3. 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 revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.

La dirección identifica los eventos potenciales que, de ocurrir, afectarán a la entidad y determina si representan oportunidades o si pueden afectar negativamente a la capacidad de la empresa para implantar la estrategia y lograr los objetivos con éxito. Los eventos con impacto negativo representan riesgos, que exigen la evaluación y respuesta de la dirección. Los eventos con impacto positivo representan oportunidades, que la dirección reconduce hacia la estrategia y el proceso de fijación de objetivos. Cuando identifica los eventos, la dirección contempla una serie de factores

internos y externos que pueden dar lugar a riesgos y oportunidades, en el contexto del ámbito global de la organización.

1.3.1. Técnicas de identificación de eventos

La metodología de identificación de eventos en una entidad puede comprender una combinación de técnicas y herramientas de apoyo. Las técnicas de identificación de eventos se basan tanto en el pasado como en el futuro.

La dirección utiliza diversas técnicas para identificar posibles acontecimientos que afecten al logro de los objetivos. Estas técnicas se emplean en la identificación de riesgos y oportunidades.

A continuación, se presenta una serie de técnicas comunes de identificación de eventos y su aplicación.

1.3.2. Inventarios de eventos

Las direcciones utilizan listados de eventos posibles comunes a un sector o área funcional específica. Estos listados se elaboran por el personal de la entidad o bien son listas externas genéricas y se utilizan, por ejemplo, con relación a n proyecto, proceso o actividad determinada, pudiendo resultar útiles a la hora de asegurar una visión coherente con otras actividades similares de la organización. Cuando se trata de listados generados externamente, el inventario se revisa y somete a mejoras, adaptando su contenido a las circunstancias de la entidad, para presentar una mejor relación con los riesgos de la organización y ser consecuentes con el lenguaje común de gestión de riesgos corporativos de la entidad.

1.3.3. Talleres de trabajo

Los talleres o grupos de trabajo dirigidos para identificar eventos reúnen habitualmente a personal de muy diversas funciones o niveles, con el

propósito de aprovechar el conocimiento colectivo del grupo y desarrollar una lista de acontecimientos relacionados, por ejemplo, con los objetivos estratégicos de una unidad de negocio o de procesos de la empresa. Los resultados de estos talleres dependen habitualmente de la profundidad y amplitud de la información que aportan los participantes.

Algunas organizaciones, en conexión con el establecimiento de objetivos, ponen en marcha un taller en que participa la alta dirección, a fin de identificar eventos que podrían afectar al logro de objetivos corporativos estratégicos.

1.3.4. Entrevistas

Las entrevistas se desarrollan habitualmente entre entrevistador y entrevistado o, en ocasiones, con dos entrevistadores para cada persona entrevistada, en cuyo caso el entrevistador está acompañado por un compañero que toma notas. Su propósito es averiguar los puntos de vista y conocimientos sinceros del entrevistado en relación con los acontecimientos pasados y los posibles acontecimientos futuros.

1.3.5. Cuestionarios y encuestas

Los cuestionarios abordan una amplia gama de cuestiones que los participantes deben considerar, centrando su reflexión en los factores internos y externos que han dado, o pueden dar lugar, a eventos. Las preguntas pueden ser abiertas o cerradas, según sea el objetivo de la encuesta. Pueden dirigirse a un individuo o a varios o bien pueden emplearse en conexión con una encuesta de base más amplia, ya sea dentro de una organización o esté dirigida a clientes, proveedores u otros terceros.

Análisis del flujo de procesos

El análisis del flujo de procesos implica normalmente la representación esquemática de un proceso, con el objetivo de comprender

las interrelaciones entre las entradas, tareas, salidas y responsabilidades de sus componentes. Una vez realizado este esquema, los acontecimientos pueden ser identificados y considerados frente a los objetivos del proceso. Al igual que con otras técnicas de identificación de eventos, el análisis del flujo de procesos puede utilizarse en una visión de la organización a nivel global o a un nivel de detalle.

1.3.6. Principales indicadores de eventos e indicadores de alarma

Los principales indicadores de eventos, a menudo denominados principales indicadores de riesgo, son mediciones cualitativas o cuantitativas que proporcionan un mayor conocimiento de los riesgos potenciales, tales como el precio del combustible, la rotación de las cuentas de valores de los inversores y el tráfico de un sitio de Internet. Para resultar útiles, los principales indicadores de riesgo deben estar disponibles para la dirección de manera oportuna, lo que, dependiendo de la información, puede implicar una frecuencia diaria, semanal, mensual o en tiempo real.

Los indicadores de alarma se centran habitualmente en operaciones diarias y se emiten ,sobre la base de excepciones, cuando se sobrepasa un umbral preestablecido.

Las empresas poseen a menudo indicadores de alarma establecidos en unidades de negocio o departamentos. Estos indicadores, para ser eficaces, deben establecer el momento en que deberá informarse a los directivos partiendo del tiempo necesario para poner en marcha una acción.

1.3.7. Seguimiento de datos de eventos con pérdidas

El seguimiento de la información relevante puede ayudar a una organización a identificar acontecimientos pasados con un impacto negativo y a cuantificar las pérdidas asociadas, a fin de predecir futuros sucesos. La

información de eventos se emplea habitualmente en la evaluación de riesgos –basándose en la propia experiencia acerca de su probabilidad e impacto– pero también puede ser útil para identificar eventos mediante la creación de una base de discusión basada en hechos, la institucionalización del conocimiento (que resulta particularmente útil en situaciones de alta rotación del personal) y servir como fuente para comprender las interdependencias entre eventos con pérdidas asociadas y desarrollar modelos predictivos y causales.

Existen bases de datos externas, desarrolladas y mantenidas por proveedores deservicios y disponibles mediante suscripción, que hacen referencia a eventos con pérdidas asociadas. En algunos sectores, como el de banca, se han formado consorcios para compartir información interna.

Las bases de datos de eventos con pérdidas asociadas contienen información sobre aquellos acontecimientos reales que cumplen criterios específicos. La información de bases de datos externas puede resultar útil para complementar la información generada internamente para estimar la probabilidad e impacto de eventos futuros, en particular para acontecimientos posibles con una baja probabilidad (que es altamente improbable que la empresa haya experimentado en el pasado), pero con un alto impacto. Por ejemplo, una de estas bases de datos contiene información de eventos con pérdidas asociadas para varios sectores, donde se declararon pérdidas operativas superiores a un millón de dólares.

Algunas empresas realizan el seguimiento de una gama de datos externos. Por ejemplo, las grandes empresas realizan el seguimiento de varios de los principales indicadores económicos, con el fin de identificar movimientos que apunten a un cambio en la demanda de sus productos y servicios. De manera similar, las instituciones financieras realizan el seguimiento de cambios en las políticas mundiales para identificar principales indicadores que apunten a una modificación en las estrategias futuras de

inversión, así como acontecimientos que exijan una modificación inmediata de las carteras de inversión

Identificación continúa de eventos

Las técnicas anteriormente presentadas se aplican, normalmente, en circunstancias particulares que se presentan con una frecuencia variable a lo largo del tiempo.

También se identifican eventos posibles de manera continua en conexión con las actividades diarias propias del negocio. La Figura 4.10 ilustra algunas de estas técnicas, que resultan útiles para aportar luz sobre los riesgos y oportunidades que pueden resultar importantes para el logro de objetivos de una organización. Este ejemplo muestra el modo que utiliza la empresa para comparar sus 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.

1.3.8. Interrelación de eventos que pueden afectar a los objetivos

Bajo determinadas circunstancias, son muchos los eventos que pueden tener impacto sobre el logro de un objetivo. Para conseguir una mejor visión y comprensión acerca de sus interrelaciones, algunas empresas utilizan diagramas de eventos en árbol, también conocidos como diagramas de espina de pescado. Un diagrama de este tipo proporciona un medio para identificar y representar de manera gráfica la incertidumbre, centrándose por lo general en un objetivo y en el modo en que múltiples eventos afectan a su logro.

1.3.9. Clasificación de eventos por categorías

Mediante la agrupación de posibles eventos de características similares, la dirección puede determinar con más precisión las oportunidades y los riesgos.

Algunas entidades clasifican los eventos posibles, para ayudar a asegurar que los esfuerzos para su identificación sean completos. Esto también puede ayudar a desarrollar posteriormente una perspectiva de cartera.

1.4. Evaluación de riesgos

La evaluación de riesgos permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos. La dirección evalúa estos acontecimientos desde una doble perspectiva –probabilidad e impacto– y normalmente usa una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente y riesgo residual.

1.4.1. Riesgo inherente y residual

El **riesgo inherente** 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 aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos.

El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente. Estas acciones pueden incluir las estrategias de diversificación relativas a las concentraciones de clientes, productos u otras, las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y la aprobación de

transacciones. Además, pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

1.4.2. Metodología y técnicas cualitativas y cuantitativas

La metodología de evaluación de riesgos de una entidad consiste en una combinación de técnicas cualitativas y cuantitativas. La dirección aplica a menudo técnicas cualitativas cuando los riesgos no se prestan a la cuantificación o cuando no están disponibles datos suficientes y creíbles para una evaluación cuantitativa o la obtención y análisis de ellos no resulte eficaz por su coste. Las técnicas cuantitativas típicamente aportan más precisión y se usan en actividades más complejas y sofisticadas, para complementar las técnicas cualitativas.

1.4.3. 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.

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 juicio de las personas implicadas, su comprensión de los acontecimientos posibles y del contexto y dinámica que los rodea.

Técnicas cuantitativas

Las técnicas cuantitativas pueden utilizarse cuando existe la suficiente información para estimar la probabilidad o el impacto del riesgo empleando mediciones de intervalo de razón. 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.

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.

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 ampliamente utilizadas son el análisis de sensibilidad, el análisis de escenarios y las pruebas de tolerancia a situaciones límite.

1.4.4. Riesgo y asignación de capital

Algunas organizaciones, en particular las instituciones financieras, estiman el capital económico. Algunas empresas 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.

1.4.5. 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.

1.4.6. Perspectiva al nivel de organización

Como parte de las evaluaciones de riesgos, la dirección puede apoyarse en las realizadas en una unidad de negocio o bien llevar a cabo una evaluación independiente utilizando las técnicas ilustradas anteriormente, para formar un perfil de riesgo al nivel de toda la organización. Las evaluaciones generales de riesgos pueden tomar la forma de una medición agregada de ellos cuando las mediciones subyacentes del riesgo son de tipos similares y cuando se consideran las correlaciones entre los riesgos. Otro enfoque de agregación consiste en traducir mediciones de riesgo relacionadas entre sí, pero diferentes, para formar una unidad de medida común.

Cuando no es posible realizar una agregación directa de mediciones de riesgo, la dirección encuentra útil, en ocasiones, compilar mediciones en un informe resumen, con el fin de facilitar la presentación de conclusiones y la toma de decisiones. En estos casos, incluso si no se agregan directamente las mediciones, la dirección sitúa subjetivamente los riesgos en la misma escala cualitativa o cuantitativa, con el fin de evaluarla

probabilidad e impacto de múltiples riesgos que afecten a un único objetivo o bien el efecto de un riesgo sobre múltiples objetivos.

1.5. Respuesta al riesgo

Una vez evaluados los riesgos relevantes, la dirección determina cómo responder a ellos. Las respuestas pueden ser las de evitar, reducir, compartir y aceptar el riesgo. Al considerar su respuesta, la dirección evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costes y beneficios, y selecciona aquella que sitúe el riesgo residual dentro de las tolerancias al riesgo establecidas. La dirección identifica cualquier oportunidad que pueda existir y asume una perspectiva del riesgo globalmente para la entidad o bien una perspectiva de la cartera de riesgos, determinando si el riesgo residual global concuerda con el riesgo aceptado por la entidad.

Evitar, Reducir, Compartir y Aceptar

Para los riesgos significativos, una entidad considera típicamente las respuestas posibles dentro de una gama de opciones de respuesta.

Evitar	Compartir
• Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/actividades que podrían dar lugar a riesgos.	• 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**
• 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.	• 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.

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.5.1. Consideración de respuestas al riesgo

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 del riesgo inherente y el riesgo residual.

Para determinados riesgos, la dirección puede confiar en múltiples técnicas para reducir e lriesgo residual general hasta situarlo dentro de las tolerancias al riesgo.

1.5.2. Costes y Beneficios

Prácticamente todas las respuestas al riesgo implican algún tipo de coste directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el coste inicial del diseño e implantación de

una respuesta (procesos, personal y tecnología),así como el coste de mantener la respuesta de manera continua. Los costes y beneficios asociados pueden medirse cuantitativa o cualitativamente, empleando normalmente una unidad de medida coherente con la empleada para establecer el objetivo y las tolerancias al riesgo relacionadas.

1.5.3. Perspectiva de cartera del riesgo residual

A partir del enfoque de gestión del riesgo para unidades individuales, la alta dirección de una empresa está en buena posición para crear una perspectiva de cartera, a fin de determinar si el perfil de riesgo de la organización es acorde con su riesgo aceptado en relación con sus objetivos.

1.6. Actividades de control

Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las respuestas de la dirección a los riesgos. Las actividades de control tienen lugar a través de la organización, a todos los niveles y en todas las funciones. Incluyen una gama de actividades –tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones.

Integración con la respuesta al riesgo Después de haber seleccionado las respuestas al riesgo, la dirección identifica las actividades de control necesarias para ayudar a asegurar que las respuestas a los riesgos se lleven a cabo adecuada y oportunamente.

Uso de las actividades de control como respuesta a los riesgos Si bien las actividades de control se establecen, por norma general, para asegurar que se llevan a cabo de manera adecuada la respuesta a los riesgos,

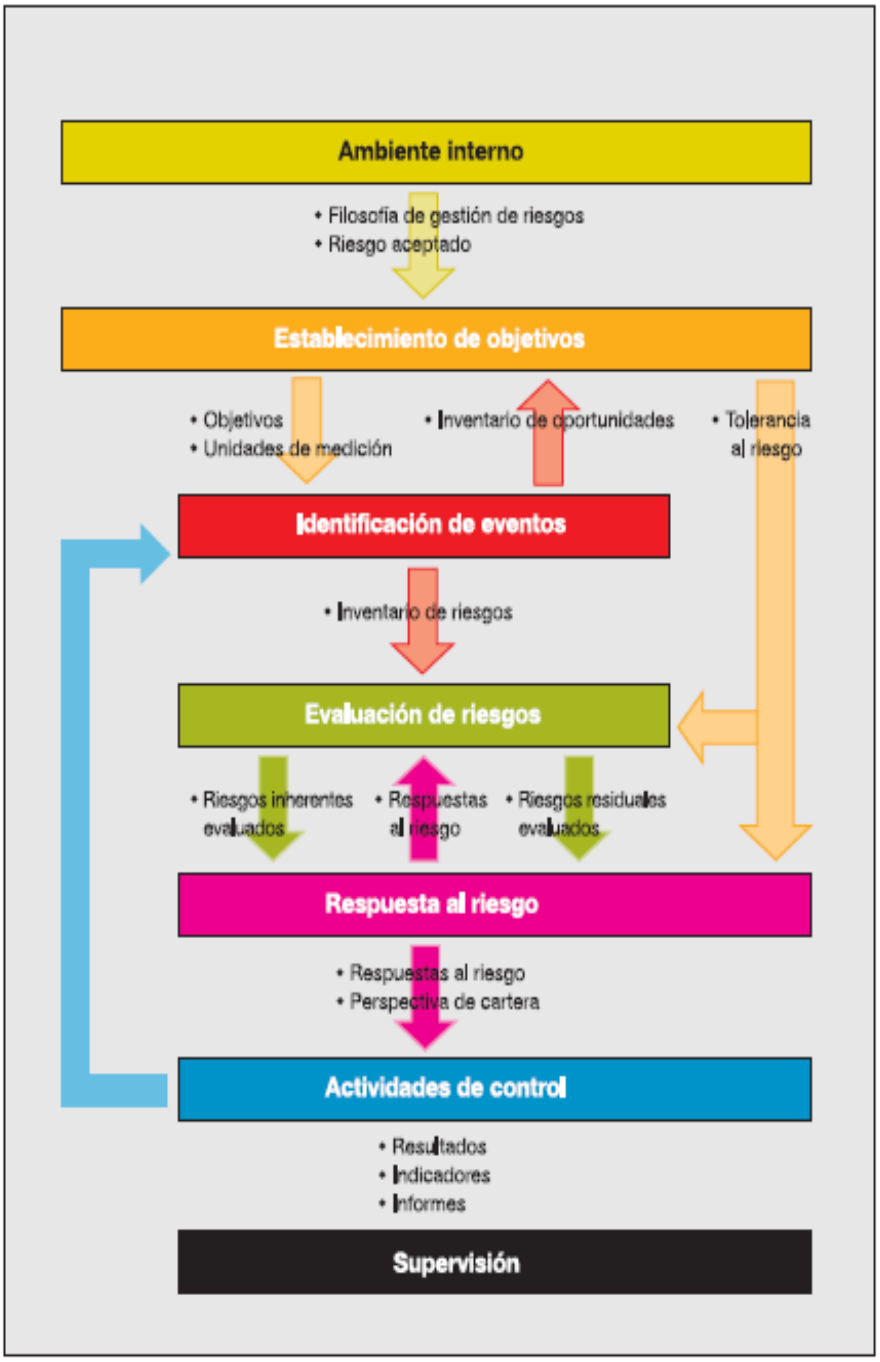
en el caso de ciertos objetivos las propias actividades de control constituyen la respuesta al riesgo.

1.7. Información y comunicación

La información pertinente se identifica, capta y comunica de una forma y en un marco de tiempo que permiten a las personas llevar a cabo sus responsabilidades Los sistemas de información usan datos generados internamente y otras entradas de fuentes externas y sus salidas informativas facilitan la gestión de riesgos y la toma de decisiones informadas relativas a los objetivos. También existe una comunicación eficaz fluyendo en todas direcciones dentro de la organización. Todo el personal recibe un mensaje claro desde la alta dirección de que deben considerar seriamente las responsabilidades de gestión de los riesgos corporativos. Las personas entienden su papel en dicha gestión y cómo las actividades individuales se relacionan con el trabajo de los demás. Asimismo, deben tener unos medios para comunicar hacia arriba la información significativa. También debe haber una comunicación eficaz con terceros, tales como los clientes, proveedores, reguladores y accionistas.

1.7.1. Información

La información se necesita a todos los niveles de la organización para identificar, evaluar y responder a los riesgos y por otra parte dirigir la entidad y conseguir sus objetivos. La información, tanto si procede de fuentes externas como internas, se recopila y analiza para establecer la estrategia y los objetivos, identificar eventos, analizar riesgos, determinar respuestas a ellos y, en general, llevar a cabo la gestión de riesgos corporativos y otras actividades de gestión.



Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.7.1.1. Sistemas estratégicos e integrados

El diseño de una arquitectura de sistemas de información y la adquisición de la tecnología son aspectos importantes de la estrategia de una entidad y las decisiones respecto a la tecnología pueden resultar críticas para lograr los objetivos. La tecnología juega un papel crítico al permitir el flujo de información en una organización, incluyendo la información directamente relevante para la gestión de riesgos corporativos. La selección de tecnologías específicas para apoyar esta gestión es habitualmente reflejo de:

• La manera de abordar la gestión de riesgos corporativos por parte de la empresa y su grado de sofisticación.

• Los tipos de acontecimientos que afectan a la organización.

• La arquitectura informática general de la entidad.

• El grado de centralización de la tecnología de apoyo. En determinadas organizaciones, la información es gestionada de manera independiente por cada unidad o función, mientras que otras poseen sistemas integrados

Con la atención centrada en la información necesaria para desarrollar la gestión de riesgos, algunas organizaciones han mejorado sus arquitecturas tecnológicas para conseguir una mejor conectividad y manejo de datos, utilizando algunas de ellas Internet y las capacidades de intercambio de información. Las estrategias de información basadas en servicios Web permiten captar datos, mantenerlos y distribuirlos en tiempo real por unidades y funciones, perfeccionando a menudo su captación, controlando mejor las múltiples fuentes de datos, minimizando su procesamiento manual y permitiendo el análisis, extracción y generación de informes automáticos. Bajo una arquitectura abierta, se utilizan tecnologías como XBRL, XML y servicios Web para facilitar la agregación de datos, su transferencia y la conectividad entre sistemas dispares o autónomos. XBRL,

acrónimo de *eXtensible Business ReportingLanguage*, es una evolución de XML (*eXtensibleMarkupLanguage*) y es un estándar abierto basado en Internet y libre de derechos de autor para la generación de informes corporativos de todo tipo. XBRL etiqueta los datos, con lo que se proporcionan en un contexto que permanece con ellos y da conformidad a los nombres por los cuales serán posteriormente reconocidos por aplicaciones dispares de *sotfware.*

Los servicios *Web* son un protocolo de Internet para el transporte de datos entre aplicaciones distintas, ya sea dentro de una misma empresa o entre varias empresas. El uso conjunto de XBRL y los servicios Web facilita el intercambio automatizado de información a través de plataformas y aplicaciones diversas y automatiza los procesos de generación de informes corporativos.

1.7.1.2. Integración con las operaciones

Muchas organizaciones poseen infraestructuras informáticas de elevada complejidad, desarrolladas a lo largo del tiempo para apoyar a los objetivos operativos, de control de gestión y cumplimiento. En muchos casos, la información generada por estos sistemas en el curso normal del negocio está integrada en el proceso de gestión de riesgos corporativos.

1.7.1.3. Profundidad y oportunidad de la información

Los avances en la recogida, procesamiento y almacenamiento de datos han dado como resultado un crecimiento exponencial del volumen de datos. Con más datos disponibles –a menudo en tiempo real– para más gente en una organización, el reto es evitar la “sobrecarga de información”, asegurando el flujo de la información adecuada, en la forma adecuada, al nivel de detalle adecuado, a las personas adecuadas y en el momento adecuado.

Muchas organizaciones han establecido un enfoque estructurado de la gestión de la información, lo que permite a la dirección identificar el valor de ésta, clasificarla en categorías por su importancia y desarrollar procesos eficaces y adecuadas herramientas y métodos para la recogida, almacenamiento y distribución de los datos.

El departamento de riesgos de mercado de un importante banco comercial hace el seguimiento de los índices reales de riesgo reales y los posibles de la organización ante movimientos diarios en los tipos de interés. A fin de identificar la información necesaria para realizar las evaluaciones de riesgos y asegurar que el banco permanece dentro de sus tolerancias al riesgo, la dirección tiene en cuenta los siguientes elementos de la información:

Principales

- **Proporcionar y capturar**

  Tiene que ver con la forma en que se genera y capta la información, ya sea desde fuentes internas o externas. Se abordan en este nivel las reglas para modificar o transformar los datos, los métodos de extracción y los criterios de selección. Para la función de riesgos de mercado, los datos se obtienen de múltiples sistemas internos, incluyendo los sistemas de procesamiento de transacciones internas y de limitación del riesgo de mercado, así como de fuentes externas, incluyendo el suministro de índices por parte de un proveedor de datos de mercado. Los datos se captan por interfaces automáticas para cada una de las fuentes.

- **Procesar y analizar**

  Define el modo en que se mantiene la información una vez se encuentra en producción. Los ejercicios de integridad, calidad y depuración de datos se realizan en este nivel. Los datos de la función de riesgos de mercado se procesan, utilizando modelos de dicho riesgo, para calcular su índice correspondiente. La dirección analiza la información resultante, para evaluar el índice de riesgo de la organización frente a las tolerancias preestablecidas y los límites del riesgo de mercado.

- **Informar**

  Se relaciona con la forma de distribuir la información a los usuarios finales. En este nivel, se abordan los criterios de agregación de datos, las consideraciones de autorización y las decisiones de distribución de la información, bien de manera no elaborada o bien a través de informes normalizados o personalizados. En este caso, los sistemas informan a los responsables de línea de las excepciones en tiempo real y resumen la posición general diaria para enviarla a la alta dirección.

Secundarios

- **Gobierno corporativo** – Define la política, la estructura de la organización y los mandatos que apoyan a las características principales.
- **Políticas** – Alude a los principios generales, normas y estructura de integración
- **Procesos** – Define los procedimientos y normas empleados para apoyar a las características principales.
- **Tecnología** – Relativo a la arquitectura, aplicaciones, bases de datos, seguridad y controles que apoyan a las características principales.

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.7.2. Comunicación

La dirección proporciona comunicaciones específicas y orientadas que se dirigen a las expectativas de comportamiento y las responsabilidades del personal. Esto incluye una exposición clara de la filosofía y enfoque de la gestión de riesgos corporativos de la entidad y una delegación clara de autoridad. La comunicación sobre procesos y procedimientos debería alinearse con la cultura deseada y reforzarla. La comunicación resulta clave para crear el entorno “adecuado” y para apoyar al resto de componentes de la gestión de riesgos corporativos. Por ejemplo, las comunicaciones descendentes sobre la filosofía de la empresa y lo que se espera del personal de la organización, junto con el necesario flujo de información ascendente, ayudan a introducir la filosofía de gestión de riesgos en la cultura de una entidad. De manera similar, la dirección refuerza o modifica la cultura de una organización con sus palabras y sus acciones diarias. Una empresa adoptó un programa de comunicación interna como el presentado en la Figura 8.13, específicamente destinada a apoyar la integración de su filosofía de gestión de riesgos y a ayudar a reforzar un ambiente interno de ética.

Un objetivo deseable es el de conseguir introducir a lo largo del tiempo la comunicación sobre gestión de riesgos corporativos en los programas de comunicación de la empresa, al nivel más amplio, en coherencia con la idea de incorporar la gestión de riesgos corporativos al tejido de la organización. Muchas empresas utilizan la tecnología para facilitar la comunicación continua sobre la gestión de riesgos corporativos. Las soluciones tecnológicas, como puede ser una intranet, pueden poner la información sobre dicha gestión al alcance de todos los empleados de una manera sencilla y constante.

1.8. Supervisión

La gestión de riesgos corporativos se supervisa - revisando la presencia y funcionamiento de sus componentes a lo largo del tiempo, lo que se lleva a cabo mediante actividades permanentes de supervisión, evaluaciones independientes o una combinación de ambas técnicas.

Durante el transcurso normal de las actividades de gestión, tiene lugar una supervisión permanente. El alcance y frecuencia de las evaluaciones independientes dependerá fundamentalmente de la evaluación de riesgos y la eficacia de los procedimientos de supervisión permanente. Las deficiencias en la gestión de riesgos corporativos se comunican de forma ascendente, trasladando los temas más importantes a la alta dirección y al consejo de administración.

1.8.1. Actividades de supervisión permanente

Diferentes actividades llevadas a cabo en el curso normal de la gestión de un negocio pueden servir para realizar la supervisión de la eficacia de los componentes de la gestión de riesgos corporativos. Estas actividades incluyen la revisión diaria de información de las gestiones normales del negocio.

Ejemplos de actividades de supervisión permanente

• La dirección revisa informes de indicadores claves de actividad del negocio, tales como datos resumidos de nuevas ventas o sobre la posición de liquidez e información sobre la cartera de pedidos atrasados, márgenes brutos y otras estadísticas claves financieras y operativas.

• La dirección operativa compara la producción, inventario, medidas de calidad, ventas y otra información obtenida en el curso de las actividades diarias con información generada en el sistema, así como con el presupuesto y la planificación.

• La dirección revisa el rendimiento, comparándolo con los límites establecidos para los índices de riesgo, como es el caso de tasas de error aceptables, artículos en tránsito, partidas de conciliación, balances de riesgo en divisa extranjera o índice de riesgo equivalente.

• La dirección revisa transacciones comunicadas a través de indicadores de alerta.

• La dirección revisa indicadores clave de rendimiento, tales como tendencias en la dirección y magnitud de los riesgos, estado de las iniciativas estratégicas y tácticas, tendencias delas variaciones en los resultados reales con respecto al presupuesto o a periodos anterior ese indicadores de acontecimientos, como se describe en el capítulo de Identificación de eventos.

1.8.2. Evaluaciones independientes

Aunque los procedimientos de seguimiento permanente normalmente proporcionan una retroalimentación importante sobre la eficacia de otros componentes de la gestión de riesgos corporativos, puede resultar provechoso echar un nuevo vistazo de vezen cuando, centrándose directamente sobre la eficacia de dicha gestión.

Habitualmente, las evaluaciones independientes de la gestión de riesgos corporativos se llevan a cabo periódicamente. En algunos casos, son originadas por un cambio en la estrategia, procesos clave o estructura de la entidad. Las evaluaciones independientes son llevadas a cabo por la dirección, el departamento de auditoría interna, especialistas externos o por una alguna combinación de estas funciones.

Las evaluaciones independientes tienen a veces un alcance amplio, incluyendo toda la entidad y todos los componentes de gestión de riesgos corporativos. En otros casos, la evaluación se limita a una unidad de

negocio, proceso o departamento específico, abordando otras áreas del negocio más adelante.

1.8.2.1. Revisiones de auditoría interna

El departamento de auditoría interna proporciona una evaluación de los riesgos y actividades de control de una unidad de negocio, proceso o departamento. Estas evaluaciones proveen de una perspectiva objetiva sobre cualquiera de los componentes de la gestión de riesgos corporativos o sobre todos ellos, desde el ámbito interno de la empresa hasta la supervisión. En algunos casos, se presta especial atención a la identificación de riesgos, el análisis de probabilidad e impacto, la respuesta al riesgo, las actividades de control y la información y comunicación. La auditoría interna, basada en el conocimiento del negocio, puede estar en posición de considerar el modo en que las nuevas iniciativas y circunstancias de la empresa podrían afectar a la aplicación de la gestión de riesgos corporativos, lo que podría tener en cuenta en su revisión y comprobación de la información relevante. Hay más información disponible en los consejos para la práctica profesional de la auditoría interna publicados por el *Institute of Internal Auditors*, que establecen pautas para la evaluación y generación de informes sobre la eficacia de la gestión de riesgos.

1.8.2.2. El proceso de evaluación

La evaluación de la gestión de riesgos corporativos constituye un proceso en sí misma. Aunque los enfoques o técnicas varían, hay que aportar al proceso una disciplina, con ciertos fundamentos inherentes a ella.

Un proceso metódico proporciona una base sólida para una evaluación. Se utilizan los más diversos enfoques y técnicas, en general dependiendo de las circunstancias de la empresa y la naturaleza y alcance de la evaluación a realizar.

Planificación

- Definir los objetivos y alcance de la evaluación.
- Identificar un directivo con la autoridad necesaria para gestionar la evaluación.
- Identificar el equipo de evaluación, el personal de apoyo y las personas de contacto clave de la unidad de negocio.
- Definir la metodología y calendario de la evaluación, así como los pasos a seguir.
- Acordar un plan de evaluación.

Ejecución

- Obtener un conocimiento de las actividades de la unidad de negocio/proceso.
- Comprender el modo en que está diseñado el proceso de gestión de riesgos de la unidad/proceso.
- Aplicar los métodos acordados a la evaluación del proceso de gestión de riesgos.
- Analizar los resultados en comparación con los estándares de auditoría interna y seguimiento de la empresa según sea necesario.
- Documentar deficiencias y soluciones propuestas, si fuera aplicable.
- Revisar y validar los resultados con el personal adecuado.

Generación de informes y acciones correctivas

- Revisar los resultados con la dirección de la unidad de negocio/proceso y con otros directivos, según corresponda.
- Obtener comentarios y planes de corrección por parte de la dirección de la unidad/proceso de negocio.
- Incorporar la retroalimentación de la dirección al informe final de la evaluación.

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.8.3. Metodología

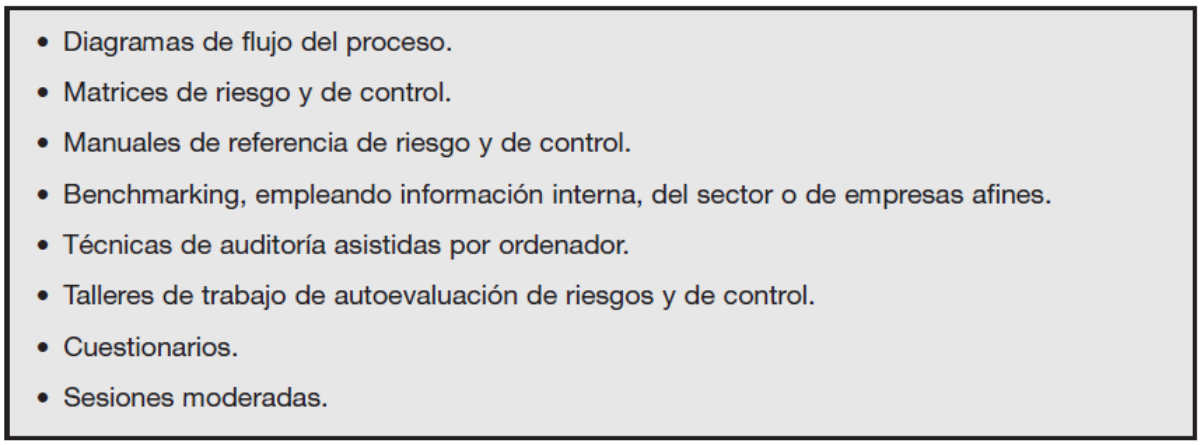
Se dispone de una variedad de metodologías y herramientas de evaluación, incluyendo listas de comprobación, cuestionarios, cuadros de mando y técnicas de diagramas de flujo.

Los evaluadores identifican las metodologías y herramientas necesarias para apoyar al proceso de evaluación. Existen diversas de ellas

bien estructuradas, que se emplean para documentar y evaluar aspectos específicos de la gestión de riesgos corporativos.

Los factores de selección de dichas metodologías y herramientas de evaluación son los de su facilidad de uso por parte del personal asignado, su relevancia para el alcance dado y su adecuación a la naturaleza y frecuencia esperada de la evaluación.

Por ejemplo, cuando el alcance incluye la comprensión y documentación de diferencias entre el diseño del proceso de negocio y su comportamiento real, el equipo de evaluación podría revisar o desarrollar diagramas de flujo del proceso y matrices de control, mientras que un alcance limitado a evaluar la presencia de determinadas actividades de control obligatorias podría sugerir el uso de un cuestionario preestablecido.



Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.8.4. Documentación

El nivel de documentación de la gestión de riesgos corporativos de una entidad varía según su dimensión, complejidad y factores similares.

El nivel deseado de documentación de la gestión de riesgos corporativos varía por empresa, a menudo en función del tamaño, complejidad y estilo de gestión. Además de la amplitud y profundidad de la documentación, las consideraciones al respecto incluyen si estará en soporte papel o electrónico, si estará centralizada o distribuida y cuáles son los medios de acceso para actualización y revisión.

Al evaluar la gestión de riesgos corporativos, se revisa la documentación existente de los procesos y otras actividades e, incluso, puede crearse dicha documentación, para permitir al equipo de evaluación comprender fácilmente los riesgos de la unidad, proceso o departamento y las respuestas a ellos. La documentación considerada en una evaluación puede incluir:

- Organigramas.
- Descripción de papeles, autoridad y responsabilidades claves.
- Manuales de políticas.
- Procedimientos operativos.
- Diagramas de flujo del proceso.
- Controles relevantes y sus responsabilidades asociadas.
- Indicadores claves de rendimiento.
- Riesgos claves identificados.
- Mediciones claves del riesgo.

Dicha documentación puede constituir la base para el desarrollo de procesos de revisión que incluyan pruebas para determinar si los procesos, junto con las políticas y procedimientos relacionados que se hayan establecido, son adecuados para enfrentarse a los riesgos de la entidad y si son respetados.

En referencia a qué documentación del propio proceso de evaluación debe desarrollarse, el equipo de evaluación tiene que considerar hasta qué punto se espera que dicha documentación alcance los objetivos de:

• Proporcionar una "pista de auditoría" de las evaluaciones y pruebas del equipo de evaluación.

• Comunicar los resultados de la evaluación – observaciones, conclusiones y recomendaciones.

• Facilitar la revisión por parte del personal de supervisión.

• Facilitar las evaluaciones en periodos posteriores.

• Identificar y comunicar problemas más amplios.

• Identificar papeles y responsabilidades individuales en el proceso de evaluación.

• Completar la documentación existente sobre gestión de riesgos corporativos, cuando se considere insuficiente.

1.8.5. Informes de deficiencias

Todas las deficiencias identificadas de gestión de riesgos corporativos que afectan ala capacidad de la entidad para desarrollar e implantar su estrategia y establecer y alcanzar sus objetivos deberían comunicarse a quienes se encuentran en posición de tomar las medidas necesarias.

1.8.5.1. Pautas de comunicación de deficiencias

• Las deficiencias se comunican a las personas directamente responsables de alcanzar los objetivos de negocio afectados por dicha deficiencia.

• Las deficiencias se comunican a la persona directamente responsable de la actividad y a una persona que se encuentre en un nivel al menos inmediatamente superior.

• Existen canales alternativos de comunicación para la comunicación de información sensible, como puede ser el caso de actuaciones ilegales o inadecuadas.

• Determinados tipos específicos de deficiencias se comunican directamente a niveles directivos más altos.

• Se han establecido protocolos para determinar lo que debe comunicarse al consejo de administración o a un comité específico del consejo.

• La información relativa a las acciones correctoras emprendidas o que deban iniciarse se traslada de vuelta al personal relevante implicado en el proceso de comunicación.

1.8.5.2. Criterios para las comunicaciones a la alta dirección

Las deficiencias se comunicarán en el caso de que la probabilidad de que se produzca un evento no sea insignificante y su impacto sea tal que podría darse como resultado:

• Un impacto adverso en la seguridad de la plantilla o de terceros.
• Un acto ilegal o inadecuado.
• Una pérdida significativa de activos.
• Un fracaso en la consecución de objetivos clave.
• Un efecto negativo en la reputación de la entidad.
• Una generación de informes externos inadecuados.

1.8.6. Roles y Responsabilidades

Todo el personal de una entidad tiene alguna responsabilidad en la gestión de riesgos corporativos. El consejero delegado es responsable en último lugar y debería asumir su “titularidad”.

Otros directivos apoyan la filosofía de gestión de riesgos, promocionan el cumplimiento del riesgo aceptado y gestionan los riesgos dentro de sus áreas de responsabilidad, en coherencia con las tolerancias al riesgo. Otras personas son responsables de desarrollar la gestión de riesgos corporativos según las directivas y protocolos establecidos. El consejo de administración proporciona una importante supervisión de dicha gestión. Algunos terceros facilitan a menudo información útil para llevarla a cabo, aunque no sean responsables de su eficacia.

Una característica que define el modo en que se implanta la gestión de riesgos corporativos es el nivel de detalle para definir claramente papeles y responsabilidades, así como el hecho de que se asignen de forma centralizada o descentralizada. Si bien el modo de hacer esto varía de una entidad a otra, pueden observarse elementos comunes.

Tres enfoques organizativos:

El enfoque 1 representa un modelo en que la identificación de eventos y la evaluación de riesgos se realizan en la dirección de los departamentos o unidades de negocio, pero la autoridad para determinar la respuesta al riesgo y las actividades de control relacionadas permanecen en los servicios centrales, desde donde se comunican los riesgos hacia la alta dirección y el consejo. Este enfoque puede funcionar en entidades de tamaño pequeño en las que la dirección central posee líneas claras de visión de las actividades de negocio, pero las autoridades claves de decisión permanecen en el centro de gestión.

El enfoque 2 representa un modelo en que la identificación de eventos, la evaluación de riesgos, la respuesta a ellos, las actividades de control y la generación de informes son responsabilidad principal de las líneas de negocio. Los servicios centrales están implicados en la supervisión

del proceso y también podrían poseer un papel amplio en la generación de informes.

El enfoque 3 es una variante del enfoque 2 e ilustra que determinados riesgos pueden ser abordados en los servicios centrales, tales como los riesgos al nivel de entidad relativos a movimientos en el precio de productos básicos o divisas extranjeras, que se supervisan y gestionan globalmente.

Enfoque		
1	*2*	*3*
Ventajas		
• Eficaz identificación de eventos y evaluación de riesgos por las personas más cercanas a los problemas que emergen. • Las respuestas a los riesgos se determinan por parte de altos directivos.	• La titularidad de la respuesta al riesgo y de las actividades de control recae en los directivos más cercanos a los problemas. • Capacidad de generar una información de gestión más completa. • Mejor capacidad para gestionar actividades basadas en el riesgo.	• Los riesgos más importantes son abordados por los altos directivos. • Facilita la gestión de riesgos al nivel de entidad.
Retos		
• Puede darse una desconexión entre la evaluación de riesgos y la respuesta a los mismos. • Falta de titularidad de los receptores del riesgo en la respuesta al riesgo.	• Posibilidad de una gestión de riesgos menos consistente (pero esta queda reducida mediante una función central eficaz de apoyo/supervisión).	• Requiere una comunicación y coordinación eficaces con las unidades de negocio.

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.8.7. Consejo de Administración

El consejo facilita su supervisión con respecto a la gestión de riesgos corporativos.

El consejo de administración juega un papel fundamental en la supervisión de la gestión de riesgos corporativos. El consejo deberá estar informado oportunamente de los riesgos más significativos, la evaluación de la dirección y su respuesta planificada y, lo que es más importante, tener la seguridad de que están en marcha los procesos adecuados y que la dirección está dispuesta a identificar, evaluar y responder al riesgo, así como para trasladar información relevante al consejo.

Preguntas planteadas por los consejeros sobre la gestión de riesgos corporativos:

• ¿Qué información recibimos acerca de los riesgos a que se enfrenta nuestra organización para cumplir con nuestras responsabilidades de gestión corporativa fiduciaria y de asesoramiento?

• ¿Cuándo y cómo nos proporciona información sobre riesgos la alta dirección?

• ¿Cómo podemos saber que la información que recibimos sobre riesgos y gestión de riesgos es exacta y completa para nuestras necesidades?

• ¿Hemos comunicado de manera eficaz nuestras expectativas a la alta dirección en relación con el proceso de gestión de riesgos de la empresa? ¿Existe una buena comprensión de estas expectativas, incluyendo la información que esperamos recibir?

• ¿Cómo aseguramos que la organización se está comportando de acuerdo con los límites establecidos de tolerancias de riesgo y de riesgo aceptado global?

• ¿Cómo podemos ayudar, como consejo de administración, a establecer el talante adecuado al más alto nivel para reforzar los valores de la organización y promover una cultura de conciencia del riesgo?

• ¿Estamos cumpliendo de manera eficaz la responsabilidad propia del consejo de administración de supervisar la gestión de riesgos?

1.8.8. Comité de Auditoría

No resulta infrecuente que la responsabilidad de supervisión de la gestión de riesgos corporativos sea asignada a un comité de auditoría. En muchos casos, se cree que, estando su atención centrada en el control interno de la gestión financiera y, posiblemente de manera más amplia, en el control interno, el comité de auditoría se encuentra ya en buena posición para expandir su responsabilidad a la supervisión dela gestión de riesgos corporativos. Algunos observadores apuntan a determinadas normas que promueven la asignación de dicha responsabilidad a este comité.

1.8.9. Comité de Riesgos

Algunos consejos de administración han establecido un comité de riesgos centrado directamente en la gestión de riesgos corporativos.

En este caso, los altos directivos asisten a sus reuniones, mientras que sus responsabilidades reflejan un trabajo conjunto con la dirección, abordando cuestiones tales como el desarrollo y perfeccionamiento del riesgo aceptado y las tolerancias al riesgo al nivel de empresa.

1.8.9.1. Objetivos

El consejo de administración (actuando a través de su comité de riesgos) reconoce su responsabilidad de garantizar la existencia de un sistema para gestionar dichos riesgos, que incluya políticas, programas, mediciones y competencias para identificarlos, evaluarlos y gestionarlos, con

el fin de apoyar a la alta dirección en la gestión del crecimiento en un entorno de constante cambio.

A este respecto, los objetivos específicos del comité de riesgos incluyen asegurar que:

• La dirección comprende y acepta su responsabilidad en la identificación, evaluación y gestión de riesgos.

• La alta dirección y la dirección de las unidades de negocio se hallan centradas en la estrategia de riesgo al nivel de la empresa.

• Se proporcionan herramientas y procesos a las unidades de negocio para facilitar el logro de sus responsabilidades de gestión de riesgos.

• Las evaluaciones de riesgos de las unidades de negocio se llevan a cabo periódicamente y de manera completa.

• Las actividades de mitigación de riesgos de la unidad de negocio consiguen: Salvaguardarlos activos, mantener estándares apropiados con relación al medio ambiente y las cuestiones de seguridad e higiene, cumplir las obligaciones legales y normativas y reforzarlos valores de la organización centrándose en las necesidades de los grupos de interés.

• Se mantienen registros contables adecuados, se adoptan políticas contables correctas y la información financiera es exhaustiva y exacta.

• Hay programas eficaces de mitigación de riesgos/pruebas de control, y se evalúa y actúa sobre los resultados obtenidos.

1.8.9.2. Responsabilidades

Las responsabilidades del comité de riesgos incluyen:

• Supervisar el desarrollo y la participación en un análisis anual de estrategias de riesgos al nivel de empresa.

• Desarrollar y perfeccionar el riesgo aceptado y la tolerancia al riesgo al nivel de empresa.

• Proporcionar guías y supervisión al director del área de riesgos y a los líderes globales de riesgo.

• Evaluar índices de riesgo materiales e informar al Consejo.

• Evaluar el informe de índices de riesgo al nivel de empresa.

• Evaluar el informe de tendencias de riesgo de la empresa y garantizar que la estrategia corporativa responde a las cuestiones planteadas.

• Supervisar los papeles y responsabilidades de la auditoría interna.

• Revisar las cuentas consolidadas semestrales y anuales.

1.8.9.3. Materialidad y enfoque

El comité se encarga de garantizar que la capacidad de identificar, evaluar y gestionar los riesgos sigue evolucionando con relación al riesgo aceptado por la organización. Para ello, se centrará principalmente en la eficacia de la gestión de riesgos corporativos.

El comité deberá revisar aquellos riesgos que puedan considerarse materiales, mediante un acuerdo entre el comité y el director del área de riesgos. Las consideraciones de materialidad se basarán tanto en la exposición al riesgo financiero inmediato para los accionistas como en la exposición al riesgo financiero a largo plazo.

La meta del comité consiste en fomentar una reflexión más amplia por parte de la dirección con relación a los riesgos, de tal manera que se aplique un enfoque más amplio para seguir transformando las competencias de la organización y su visión de la gestión de riesgos.

1.8.9.4. Estructura y pertenencia

• Los miembros del comité serán designados mediante resolución del consejo.

• El comité comprenderá cuatro vocales no ejecutivos del consejo, siendo designado presidente uno de ellos.

1.8.9.5. Reuniones

• Las reuniones se mantendrán trimestralmente antes de las reuniones del consejo.

• El secretario general estará presente en las reuniones y levantará acta de ellas como secretario del comité.

• También asistirán a ellas el consejero delegado y el director financiero.

• Se presentará un informe de cada reunión en la siguiente reunión del consejo de administración.

1.8.9.6. Dirección

La dirección es responsable de todas las actividades de una entidad, incluyendo la gestión de riesgos corporativos.

1.8.9.7. Consejero delegado

Las responsabilidades del Consejero Delegado incluyen asegurar que todos los componentes de la gestión de riesgos corporativos se encuentran en funcionamiento.

El Consejero Delegado posee la responsabilidad última de titularidad de la gestión de riesgos corporativos. Cumple normalmente con esta responsabilidad proporcionando liderazgo y orientación a la alta dirección y estableciendo políticas amplias que reflejen la filosofía de gestión de riesgos de la entidad, así como su riesgo aceptado.

Varios consejeros delegados han decidido identificar a un alto directivo que proporcione pautas a la organización, bajo los auspicios del consejero delegado, en lo referente a la implantación de la gestión de riesgos corporativos. Algunos consejeros delegados han preferido establecer un comité para que proporcione estas pautas. Otro enfoque, utilizado por un

número creciente de empresas, consiste en establecer un director de riesgos que proporcione liderazgo, pautas, apoyo y seguimiento a los directores de línea en la gestión de riesgos corporativos.

1.8.10. Comité Ejecutivo de Gestión de Riesgos Corporativos

En algunas organizaciones grandes, el consejero delegado ha establecido un comité de altos directivos para la gestión de riesgos corporativos, consistente en un grupo perteneciente a la alta dirección, incluyendo directores funcionales tales como el director financiero, el director de auditoría, el director de comunicaciones y otros.

Las funciones y responsabilidades de este Comité incluyen aspectos tales como:

• Responsabilidad global del proceso de gestión de riesgos corporativos, incluyendo los procesos utilizados para identificar, evaluar, responder e informar sobre el riesgo.

• Definición de papeles, responsabilidades y obligaciones de rendir cuenta ante la alta dirección.

• Dotación de políticas, marcos, metodologías y herramientas a las unidades de negocio, para la identificación, evaluación y gestión de riesgos.

• Revisión del perfil de riesgo de la empresa.

• Revisión de las mediciones de rendimiento frente a las tolerancias y la recomendación de acciones correctoras cuando sea necesario.

• Comunicación del proceso de gestión de riesgos al consejero delegado y al consejo.

1.8.10.1. Responsable de riesgos

Algunas empresas han establecido un punto centralizado de coordinación para facilitar la gestión de riesgos corporativos. Un responsable de riesgo – denominado en algunas organizaciones como director o gerente

de riesgos- trabaja junto a otros directivos para establecer una gestión eficaz de riesgos corporativos en sus respectivas áreas de responsabilidad.

Las empresas que poseen un puesto de director de riesgos tienden a ser empresas grandes y complejas. Una alternativa a la creación de este puesto es asignar este papel a un alto directivo, por ejemplo, el director financiero, el asesor jurídico o el director de cumplimiento. Algunas empresas que seleccionaron inicialmente este enfoque se encontraron, con el tiempo, conque la amplitud y el alcance que implica la gestión efectiva del riesgo requieren más tiempo y esfuerzo del que tienen disponible los altos directivos, con lo que han ido evolucionando hacia el establecimiento de un director de riesgos independiente.

Un modelo para el director de riesgos que varias empresas han utilizado con éxito, comienza estableciendo con claridad las responsabilidades y obligaciones de rendición de cuentas del mismo. Si bien algunas empresas asignan la responsabilidad directa de la gestión eficaz de riesgos al director de riesgos, muchas otras han obtenido un resultado muy bueno manteniendo la responsabilidad de dicha gestión en los responsables de las unidades funcionales y de las diferentes líneas, asignando al director de riesgos responsabilidades de soporte, guía y supervisión.

La experiencia muestra que el éxito también depende de que el director de riesgos posea el suficiente nivel dentro de la organización, así como los recursos necesarios para realizar su labor. Algunas empresas proporcionan personal al director de riesgos procedente de departamentos, unidades de negocio y filiales, para asegurar que la plantilla de apoyo al director de riesgos se encuentra cercana a las actividades operativas de la entidad.

El responsable de riesgos depende de:

Presidente - comité de riesgos del consejo y consejero delegado.

Dependencias directas:

• Líderes globales de riesgo y especialistas de riesgo del grupo (pertenecientes a cuestiones de riesgos).

• Coordinadores de riesgo de las unidades de negocio y Auditoría interna.

1.8.10.2. Responsabilidades:

• Facilitar el cumplimiento de las responsabilidades del comité de riesgo del consejo, como figura en sus estatutos.

• Comunicar y gestionar el establecimiento y mantenimiento continuo de la gestión de riesgos corporativos en aplicación de la visión de gestión de riesgos de la empresa.

• Asegurar la adecuada titularidad de la gestión de riesgos por parte de los consejeros delegados de las unidades de negocio, así como una supervisión efectiva por parte de los consejos regionales/de empresa.

• Validar que la gestión de riesgos corporativos funciona en cada unidad de negocio y que se reconocen y gestionan de manera eficaz todos los riesgos.

• Mantener comunicaciones con el comité de riesgo en relación con el estado de la gestión de riesgos corporativos.

• Promover el modelo de gestión de riesgos corporativos entre el consejero delegado y los responsables de las unidades de negocio, contribuir a su integración en los planes de negocio y un permanente control de gestión.

• Garantizar que se desarrolla y mantiene una capacidad de gestión de riesgos en todas las unidades de negocio y empresas, incluyendo nuevas adquisiciones e inversiones en sociedades de capital riesgo.

1.8.10.3. Actividades específicas:

• Desarrollar procedimientos integrados para informar acerca de riesgos importantes.

• Visitar con regularidad las unidades de negocio y acordar encuentros con sus altos directivos, para promover la inclusión de la gestión de riesgos en la cultura y actividades diarias.

• Desarrollar un modelo estandarizado y un proceso automatizado de información sobre riesgos y garantizar que puede utilizarse en toda la organización.

• Mantener un enfoque coste-beneficio de la gestión de riesgos corporativos.

• Asegurar que los empleados son instruidos en la gestión de riesgos. Transferir conocimiento e información y, de forma general, contribuir a la gestión eficaz del riesgo, ayudando a mantener una cultura de riesgo adecuada.

• Trabajar con los líderes de las unidades de negocio para garantizar que los planes de negocio y presupuestos incluyen la identificación y gestión de riesgos.

• Trabajar con las unidades de negocio para garantizar el seguimiento y control de gestión necesarios que permitan asegurar el cumplimiento de los estándares de la organización y la comunicación de los riesgos más significativos.

• Informar al comité de riesgo en relación con:

- El avance de la gestión de riesgos corporativos y su implantación.

- Los índices de riesgo significativos y trascendentes y recomendaciones a lo largo de la organización.

- El plan consolidado de gestión de riesgos corporativos, comprendiendo el análisis y las recomendaciones.

1.8.10.4. Atributos profesionales:

• Fundamentos sobre la gestión de riesgos corporativos.

• Capacidad de demostrar claramente un conocimiento amplio de los principios de la infraestructura de gestión de riesgos corporativos de la organización.

• Creatividad, con independencia de criterio.

• Experiencia global en culturas diferentes.

• Buena presencia ejecutiva.

• Excepcionales habilidades comunicativas interpersonales.

• Capacidad para obtener el respeto del consejo y las unidades de negocio

• Experiencia en la alta dirección, es decir, como miembro de un equipo ejecutivo responsable de un grupo amplio de personas o bien experiencia como director financiero o director general.

• Excelentes habilidades de presentación y elocuencia.

• Sobresalientes cualidades de moderador.

• Extensa experiencia en la gestión de proyectos.

• Fuerte capacidad analítica.

• Habilidades excepcionales de resolución de problemas.

Depende de:

Presidente - comité de riesgos del consejo y consejero delegado.

Dependencias directas:

- Líderes globales de riesgo y especialistas de riesgo del grupo (pertenecientes a cuestiones de riesgos).
- Coordinadores de riesgo de las unidades de negocio y Auditoría interna.

Responsabilidades:

- Facilitar el cumplimiento de las responsabilidades del comité de riesgo del consejo, como figura en sus estatutos.
- Comunicar y gestionar el establecimiento y mantenimiento continuo de la gestión de riesgos corporativos en aplicación de la visión de gestión de riesgos de la empresa.
- Asegurar la adecuada titularidad de la gestión de riesgos por parte de los consejeros delegados de las unidades de negocio, así como una supervisión efectiva por parte de los consejos regionales/de empresa.
- Validar que la gestión de riesgos corporativos funciona en cada unidad de negocio y que se reconocen y gestionan de manera eficaz todos los riesgos.
- Mantener comunicaciones con el comité de riesgo en relación con el estado de la gestión de riesgos corporativos.
- Promover el modelo de gestión de riesgos corporativos entre el consejero delegado y los responsables de las unidades de negocio, contribuir a su integración en los planes de negocio y un permanente control de gestión.
- Garantizar que se desarrolla y mantiene una capacidad de gestión de riesgos en todas las unidades de negocio y empresas, incluyendo nuevas adquisiciones e inversiones en sociedades de capital riesgo.

Actividades específicas:

- Desarrollar procedimientos integrados para informar acerca de riesgos importantes.
- Visitar con regularidad las unidades de negocio y acordar encuentros con sus altos directivos, para promover la inclusión de la gestión de riesgos en la cultura y actividades diarias.
- Desarrollar un modelo estandarizado y un proceso automatizado de información sobre riesgos y garantizar que puede utilizarse en toda la organización.
- Mantener un enfoque coste-beneficio de la gestión de riesgos corporativos.
- Asegurar que los empleados son instruidos en la gestión de riesgos. Transferir conocimiento e información y, de forma general, contribuir a la gestión eficaz del riesgo, ayudando a mantener una cultura de riesgo adecuada.
- Trabajar con los líderes de las unidades de negocio para garantizar que los planes de negocio y presupuestos incluyen la identificación y gestión de riesgos.
- Trabajar con las unidades de negocio para garantizar el seguimiento y control de gestión necesarios que permitan asegurar el cumplimiento de los estándares de la organización y la comunicación de los riesgos más significativos.
- Informar al comité de riesgo en relación con:
  - El avance de la gestión de riesgos corporativos y su implantación.
  - Los índices de riesgo significativos y trascendentes y recomendaciones a lo largo de la organización.
  - El plan consolidado de gestión de riesgos corporativos, comprendiendo el análisis y las recomendaciones.

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

Atributos profesionales:

- Fundamentos sobre la gestión de riesgos corporativos.
- Capacidad de demostrar claramente un conocimiento amplio de los principios de la infraestructura de gestión de riesgos corporativos de la organización.
- Creatividad, con independencia de criterio.
- Experiencia global en culturas diferentes.
- Buena presencia ejecutiva.
- Excepcionales habilidades comunicativas interpersonales.
- Capacidad para obtener el respeto del consejo y las unidades de negocio
- Experiencia en la alta dirección, es decir, como miembro de un equipo ejecutivo responsable de un grupo amplio de personas o bien experiencia como director financiero o director general.
- Excelentes habilidades de presentación y elocuencia.
- Sobresalientes cualidades de moderador.
- Extensa experiencia en la gestión de proyectos.
- Fuerte capacidad analítica.
- Habilidades excepcionales de resolución de problemas.

Fuente: Marco integrado de la gestión de riesgo corporativo- Técnicas de aplicación.

1.8.10.5. Dirección

Los altos directivos a cargo de las unidades organizativas tienen la responsabilidad de gestionar los riesgos relacionados con a los objetivos de sus unidades .Los responsables de las unidades de negocio, procesos de negocio y departamentos funcionales de las distintas líneas son quienes deben identificar, evaluar y responder al riesgo en relación con el logro de sus objetivos. Ellos deben asegurar que los procesos empleados cumplen las políticas de gestión de riesgos corporativos de la entidad y que sus actividades se encuentran dentro de los niveles establecidos de tolerancia al riesgo. En algunas empresas, las descripciones de los puestos correspondientes a estos directivos reflejan de manera explícita sus responsabilidades de gestión de riesgos corporativos, así como las mediciones de rendimiento asociadas. Los responsables de las unidades elaboran habitualmente informes de progreso directamente para el director

de riesgos y/o para algún otro directivo. Estos responsables delegan de manera natural la responsabilidad de actividades específicas de gestión de riesgos corporativos a los gerentes de sus unidades, que tendrán responsabilidad para tratar asuntos tales como:

2. El cumplimiento de las políticas de gestión de riesgos corporativos y el desarrollo de técnicas adaptadas a las actividades de la unidad.

3. La aplicación de técnicas y metodologías de gestión de riesgos corporativos para garantizar la adecuada identificación, evaluación, respuesta, comunicación y seguimiento de los riesgos.

4. La obligación de gestionar los riesgos diariamente.

5. La aportación al responsable de una unidad de informes completos y exactos sobre la naturaleza y alcance de los riesgos en las actividades del negocio.

Al igual que en el caso de los responsables de unidad, las descripciones de los puestos de trabajo de algunas empresas reflejan sus responsabilidades en la gestión de riesgos corporativos, así como sus mediciones de rendimiento asociadas.

Auditores internos

En muchas empresas, los auditores internos juegan un papel fundamental en el funcionamiento de la gestión de riesgos corporativos, proporcionando un seguimiento objetivo de su aplicación y eficacia. Los auditores internos pueden llevar a cabo revisiones para proporcionar una evaluación objetiva del proceso completo de gestión de riesgos corporativos o de partes de él. Dentro de este papel, los auditores internos pueden apoyar a la dirección proporcionando garantías sobre:

• Los procesos de gestión de riesgos corporativos – tanto su diseño como sus funciones.

• La eficacia y eficiencia de las respuestas al riesgo y actividades de control relacionadas.

• La integridad y exactitud de la información generada sobre la gestión de riesgos corporativos.

Los auditores internos adoptan en ocasiones un papel de consultoría en el que sugieren mejoras en el proceso de gestión de riesgos corporativos de la organización. En esta situación, los auditores internos pueden, entre otras actividades, promover el desarrollo de un conocimiento común de la gestión de riesgos corporativos, formar ala dirección en los conceptos de gestión de riesgos, moderar grupos de trabajo sobre riesgos y proporcionar herramientas y técnicas para ayudar a los directivos a analizarlos riesgos y diseñar actividades de control.

Estructura de este Documento

El presente documento se divide en dos partes. La primera contiene los conceptos más importantes tanto del informe 5 como del informe COSO[8].La segunda, el Marco y un Resumen Ejecutivo que define la gestión de riesgos corporativos y describe principios y conceptos, proporcionando orientación a todos los niveles de dirección en empresas y otras organizaciones para ser usada en la evaluación y mejora de la eficacia de dicha gestión y las Técnicas de aplicación y proporciona ejemplos de técnicas útiles para aplicar los componentes del Marco.

Las acciones sugeridas que podrían adoptarse como resultado de este documento dependen de la posición y papel de las partes implicadas:

Consejo de Administración

El consejo debería comentar con la alta dirección el estado de la gestión de riesgos corporativos de la entidad y aportar su supervisión según

[8]COMMITTE OF SPONSORING OF THE TREADWAY COMMISION Op.Cit., pág. 12.

se necesite. Asimismo, debería asegurarse de que es informado de los riesgos más significativos, de las acciones que la dirección está realizando y cómo ésta asegura una gestión eficaz de riesgos.

Alta dirección

Este documento sugiere que el consejero delegado evalúe las capacidades de gestión de riesgos corporativos de la organización. Por ejemplo, un consejero delegado reúne a los responsables de unidad de negocio y al personal clave del *staff* para comentar una evaluación inicial de las capacidades y eficacia de la gestión de riesgos corporativos. Sea cual sea su forma, esta evaluación inicial debería determinar si existe la necesidad de otra evaluación más profunda y amplia y, en caso afirmativo, cómo proceder a realizarla.

Otro personal de la entidad

Los directivos y demás personal deberían considerar cómo están desempeñando sus responsabilidades a la luz del presente Marco y comentar sus ideas con responsables superiores para reforzar la gestión de riesgos corporativos. Los auditores internos deberían considerar el alcance de su enfoque sobre dicha gestión.

Reguladores

Este Marco puede fomentar una visión compartida de la gestión de riesgos corporativos, incluyendo lo que se puede hacer y sus limitaciones. Los reguladores pueden referirse a este Marco al establecer sus expectativas, bien mediante normas o guías o en la realización de inspecciones en las entidades bajo su supervisión.

Organizaciones profesionales

Las entidades encargadas de establecer normas y otras organizaciones que proporcionan orientación sobre gestión financiera, auditoría y temas afines, deberían considerar sus normas y guías a la luz de este Marco. A medida que se eliminen divergencias de conceptos y terminología, todas las partes se beneficiarán de ello.

CAPITULO IV

LA INCIDENCIA DE LA COMUNICACIÓN A4793 DEL BANCO CENTRAL DE LA REPÚBLICA ARGENTINA EN EL BANCO XX

Sumario: 1. Antecedentes; 2. La Comunicación A4793; 3. El Banco Central como órgano de contralor.

1. Antecedentes

"El Banco Macro es un banco argentino de capitales privados nacionales, integrante del *holding* Grupo Macro. Comenzó a operar como banco en el año 1988. Por su gran envergadura en Marzo de 2006 anexo tomó la decisión de cotizar en *Wall Street* adquiriendo prestigio y convirtiéndose en la primera empresa Argentina en llegar al mercado internacional de acciones luego del *default"*. [9]

Wall Street (en inglés: 'Calle del Muro') es una calle neoyorquina situada en el bajo Manhattan, entre Broadway y el río Este. Considerado el corazón histórico del distrito financiero, es el principal y permanente hogar de la Bolsa de Valores de Nueva York. El término se usa para referirse tanto al mercado financiero estadounidense como a las instituciones financieras.

[9] BENITEZ, Rodrigo, Subgerente Banco Macro, Ex BCRA, (San Miguel de Tucumán, 20 de Octubre de 2016).

No cualquier empresa cotiza en bolsa, la misma impone requisitos muy importantes para el ingreso, entre los cuales podemos mencionar cumplir con la ley SOx[10] y montos mínimos de capitales.

Ley Sarbanes Oxley (SOx) nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

Al centrarnos en el Banco XX, que hoy integra el Grupo Macro y el cual será el centro de nuestro estudio observamos que al representar este el 10% del paquete accionario debía adaptarse a las normativas que se le exigían al grupo, así como además las opiniones debían convergir en cuanto a las medidas adoptadas y respuestas otorgadas hacia las diferentes entidades entre ellas, el Banco Central de la República Argentina.[11]

El Banco Central de la República Argentina (BCRA) es el organismo rector del sistema financiero de la Argentina, encargado de la política monetaria del país.

Esto implicaba que el Banco XX, al momento del ingreso del grupo en el mercado de valores debía cumplir también con la ley SOx, la cual conlleva un análisis del recorrido de todos los procesos que realiza la entidad y la certificación de que estos se encuentran correctamente expuestos en la contabilidad. Por estas exigencias se analizaron, mejoraron y enlistaron los procesos para lograr cumplir con la normativa.

2. La Comunicación A4793 y su impacto en el Banco XX.

A partir del 2008 el Banco Central de la República Argentina publica la Comunicación “A4793" – Lineamientos para la gestión del riesgo

[11] Ibidem, pág. 117.

operacional en las entidades financieras, en la cual se exige la implementación de un sistema para gestionar el riesgo operacional, como disciplina integral y separada de los restantes riesgos. (Anexo 1).

Debido a que la entidad se había adaptado a los requerimientos del mercado internacional, la adopción de los requisitos de la nueva normativa bancaria no le implicaba un gran cambio en el análisis de los procesos y la detección de los riesgos, área en la cual la empresa venia por una decisión de la alta gerencia liderando en la materia. Para lo que había tomado medidas como la inclusión al personal de la organización de uno de los mayores referentes del sector, quien había trabajado en el Banco Central durante 25 años, el Contador Público Alberto Figueroa; transformando la adopción de la Comunicación del Banco Central en un mero cumplimiento normativo más que en un avance en el desempeño de los procesos de control del banco.

Según exige el órgano rector, el Banco XX debió integrar a la estructura organizacional un departamento exclusivo de Gestión de Riesgo Operacional, dependiente de la Gerencia General y un departamento de Gestión de Riesgo de Tecnología informática, el cual tiene una relación de *staff* con la Subgerencia General en convergencia con el departamento de Auditoría Interna, el cual desarrolla también la certificación anual de SOx. Esta generalmente es presentada en Octubre o Noviembre en donde se firman las distintas declaraciones de los recorridos de los procesos todos los años y se realiza un muestreo de la documentación de cada uno, la cual consiste en analizar 30 muestras de comprobantes de cada uno de los procedimientos y de no cumplir con algún parámetro el muestreo es elevado al doble y así sucesivamente.

El término convergencia implica que las valoraciones, resultados y conclusiones sobre los distintos procesos de la empresa, la determinación del riesgo y los informes presentados por las distintas áreas deben coincidir

entre ellos dando cohesión y coherencia tanto a la empresa como a la información producida y presentada antes los distintos órganos de contralor en el plano nacional e internacional.

2.1. Gestión de Riesgo Corporativo.

Para realizar la Gestión de Riesgo Operacional es necesario definir todos los Ciclos, Procesos y Actividades existentes en la Entidad, y sus respectivos Responsables, los cuales el banco tenia por las implicancias de la Ley SOx completamente identificados.

2.1.1. Metodología

La metodología para la Gestión del Riesgo Operacional consiste en la Identificación, Evaluación, Mitigación y Monitoreo del Riesgo Operacional, **mediante un modelo integrado para la administración del Riesgo Operacional.**

(Ver apéndice 1).

2.1.1.1. Identificación

Una vez identificados los procesos, se focaliza la observación en la detección de los riesgos existentes asociados a cada proceso y los controles que los minimicen.

Fuentes de identificación de Riesgos:

- Normas y procedimientos vigentes del proceso analizado.
- Comunicaciones de Organismos de Contralor.
- Entrevistas/Reuniones con las Áreas.
- Análisis de la Base de Eventos de Pérdidas (se definen como eventos de un proceso de negocio difiera del resultado esperado, debido a

las fallas en los procesos internos, las personas, los sistemas o por eventos externos).

2.1.1.2. Evaluación

El proceso de medición se basa en evaluar el **riesgo residual** estableciendo la probabilidad de ocurrencia del mismo y el impacto de sus consecuencias, con el fin de obtener información para establecer su nivel (aceptable, tolerable, moderado, importante, grave) y las acciones a implementarse en caso de corresponder.

En la evaluación de los riesgos residuales se deberá tener en cuenta dos aspectos: la Probabilidad de Ocurrencia y el Nivel de Impacto.

- Probabilidad de Ocurrencia: se entiende como la posibilidad de que el riesgo identificado se convierta en un hecho concreto. Puede ser medida con criterios de frecuencia (si se ha materializado) o factibilidad (teniendo en cuenta factores internos o externos que pueden propiciar el riesgo, si no se ha materializado).
- Nivel de impacto: se entiende como el impacto, las consecuencias que puede generar la materialización del evento.

El resultado de evaluación de los riesgos residuales permite obtener el nivel de riesgo residual, que según las calificaciones de la probabilidad e impacto conformarán diferentes combinaciones:

Los niveles que pueden tomar los riesgos residuales se describen en el siguiente cuadro: (ver apéndice 2)

2.1.1.3. Mitigación de riesgos

Una vez determinado el nivel de cada riesgo residual, se debe especificar cuál será el tratamiento que se le dará en función de dicha calificación establecida en el proceso de medición.

Se entiende por dar tratamiento a los riesgos a la ejecución de aquellas acciones a ser tomadas por el Banco respecto del nivel de riesgo residual existente para cada riesgo analizado. Las acciones que pueden ejecutarse son las siguientes:

- **Reducir/evitar el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad de ocurrencia como el nivel de impacto. Se consigue mediante la optimización de los procedimientos y la implementación de controles, entre otros.
- **Compartir o Transferir el riesgo:** se reduce a su efecto a través de compartir o traspasar los riesgos a otras organizaciones, como en el caso de los contratos de seguros.
- **Asumir el riesgo:** luego que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, puede aceptarse simplemente una pérdida y elaborarse planes de mitigación para el tratamiento de dicho riesgo residual.

Se deben definir **Planes de Mitigación** para aquellos riesgos residuales que sean evaluados como Moderado, Importante o Grave.

Cada uno de estos planes de mitigación deberá contener explícitamente un Responsable encargado de su cumplimiento y se deberá efectuar un seguimiento de las acciones a ejecutar, los plazos acordados y las etapas de cumplimiento.

2.1.1.4. Monitoreo

Comprende el establecimiento de un proceso de monitoreo periódico de los riesgos incluyendo los eventos de Riesgo Operacional, sus

indicadores asociados, la calidad y adecuación de los controles y sus efectos relacionados.

2.1.2. Cierre del Análisis de Riesgos de los procesos

Se deberán documentar los resultados obtenidos en:

- **La matriz de Riesgo Operativo** la cual deberá ser considerada por la totalidad de los participantes en el proceso de identificación de riesgos de acuerdo a los Sectores involucrados en el proceso bajo análisis.
- **La minuta de cierre de procesos y/o Informe de Cierre** la cual contendrá el detalle de las acciones de mejora y/o planes de mitigación consensuados con los participantes de los procesos y en la cual se establecerán los Responsables de su cumplimiento y los plazos para su ejecución. El presente documento deberá ser consensuado (mediante firma o a través de mail) por la totalidad de los participantes en el proceso de mitigación de riesgo

Estos informes son los que respaldan el cumplimiento de la Normativa del BCRA.

El Riesgo Operacional valorizado tanto cualitativa y cuantitativamente.

2.1.1. Análisis Cualitativo.

Empleando la normativa del BCRA se analiza si el mismo dictaminó nuevas formas de llevar a cabo los procesos y esto posiblemente nos lleve a la detección de nuevos riesgos en el desempeño de los mismos. Una vez reconocido el riesgo es analizado en conjunto entre el sector de Riesgo Operacional y el encargado de área, quien califica el mismo en base a su

probabilidad de ocurrencia y el impacto financiero que este provocaría. En base a este análisis se desarrolla una matriz de riesgo que será evaluada por el departamento y la subgerencia, con el fin de determinar si la misma es realmente lógica, y en ella, la valoración del riesgo, es representativa de la realidad del banco; ya que muchas veces lo que es importante para el gerente o encargado de un área, se vuelve irrelevante a nivel general del banco teniendo en cuenta la incidencia de otros procesos.

Una vez detectado, analizado y calificado cualitativamente se monitorea el proceso con la intención de determinar la incidencia o los indicadores que éste podría despertar y se determinan los controles a implementar.

2.2.2 Análisis Cuantitativo.

El proceso de cuantificación se ha desarrollado mediante la aplicación de matrices para la auto-evaluación por parte de los responsables de los procesos a efectos de obtener la primera estimación cuantitativa (basada en supuestos subjetivos y datos proporcionados o validados por dichos responsables).

El análisis y valoración de riesgos incluyo, entre otras, las siguientes etapas:

Cuantificación de riesgos: en esta fase los designados como expertos en la Entidad para cada uno de los procesos general y valoran los riesgos considerando, entre otros, su propio conocimiento del negocio, los procesos o productos afectados, la evolución del mercado, el sector y la propia Entidad, la información interna histórica existente o los eventos de pérdida.

Obtención de resultados: para cada uno de los riesgos se obtiene, como resultado una estimación de las pérdidas recurrentes o esperadas, así

como de las pérdidas máximas potenciales que podrían exceder a las anteriores (inesperadas) bajo determinado nivel de confianza.

Los aspectos a evaluar por parte del experto dentro de los cuestionarios, para cada uno de los riesgos definidos, son los siguientes:

Frecuencia

Frecuencia del riesgo: número de veces que, en media, se produce el riesgo en un período determinado. En el presente proyecto dicho período e ha establecido en un año.

En estos casos se aplica el criterio de Impacto Residual, entendiendo el mismo como el impacto resultante luego de la aplicación de los controles.

Impactos máximos

Peor escenario: en el caso de producirse pérdida, cuál sería la misma en el escenario más pesimista que pueda producirse dentro de una situación “razonable”, esto es, sin llegar a considerar sucesos catastróficos.

2.3. Plan de Continuidad del Negocio

El plan de continuidad del negocio es un plan de acción detallado de cómo reaccionar y recuperar las actividades de negocio a partir del impacto de un desastre o una crisis que puede amenazar o interrumpir las actividades normales de la Entidad.

Este plan de acción define una estructura formal para guiar y coordinar las distintas tareas previstas en caso de contingencia.

Se establecen tres niveles de estructura para la administración y ejecución del Plan:

- **Comité de Crisis:** es un grupo reducido formado por las máximas autoridades de la Entidad, que se encarga de la comunicación formal de la situación de contingencia hacia los medios de comunicación formal de la situación de contingencia hacia los medios de la comunicación u organismos reguladores; además de autorizar y disponer en forma inmediata de recursos y gastos que permitan aliviar la situación de contingencia y con la información recabada toma/aprueba la decisión de activar el Plan, de acuerdo a las necesidades de la contingencia.
- **Equipo Coordinador de Contingencia (ECC):** coordinará las actividades de todos los Equipos de Contingencia en caso de impedimento de la continuidad de los procesos de negocios de la Entidad. El ECC se encuentra integrado por las gerencias necesarias para poner operativamente al Banco frente a una Contingencia y se encargará de la organización del proceso de recuperación de las actividades desde el momento en que la situación ocurre hasta la reanudación de las operaciones del negocio.
- **Equipo de contingencias por Área (EDC):** serán los responsables de ejecutar las tareas operativas de recuperación del negocio. Estos equipos se formarán en el momento en que se genera la situación de Contingencia y estarán organizados por Área/Procesos. Cada EDC tendrá un responsable de aplicar el procedimiento de Contingencia que mantendrá comunicación directa con el ECC y será el encargado de transmitir al resto del EDC las actividades y tareas a realizar dispuestas por el equipo coordinador.

(Ver Anexo 2)

2.3.1. Análisis.

- **RIA -** Análisis de Riesgos – *Risk Impact Analysis*

Se realiza este análisis de riesgos sobre los eventos que podrían afectar el normal desempeño de las operaciones del Banco. Se focalizó en identificar las amenazas que podrían afectar la continuidad del negocio e investigar la probabilidad de ocurrencia, dándole una escala numerada de cero a cinco, representando este ultimo la probabilidad más alta.

A continuación vemos la matriz en donde se muestran las amenazas y su valoración en cuanto a la probabilidad de ocurrencia.

(ver apéndice 3)

- **BIA -** Análisis de Impacto en el negocio- *Business Impact Analysis*

Tiene el propósito de:

1. Identificar el potencial impacto de eventos descriptivos en procesos claves de negocios.
2. Proveer recomendaciones sobre la priorización en la recuperación de los procesos de negocios.
3. Proveer recomendaciones sobre la priorización en la recuperación de aplicaciones claves de negocio.
4. Proveer información sobre los requerimientos de recursos y tiempos requeridos para desarrollar estrategias para la definición del plan de continuidad del negocio.

- **PRP –** Plan de Recuperación de Procedimientos

Definido el BIA, se identificaron los procesos más críticos para el negocio detallando para cada uno, las principales tareas a desarrollar para

permitir la continuidad de la operatoria en caso de ocurrencia de un evento de desastre, interrupción mayor o contingencia parcial.

Escenarios de contingencia

Los escenarios definidos corresponden a las características del impacto que un evento o conjunto de eventos afectan la disponibilidad de los recursos de la Entidad.

1. Indisponibilidad de contingencia

Este escenario contempla las amenazas que impidan el acceso físico del personal a las instalaciones del área de trabajo (edificio u oficinas). Esta situación impide el normal desempeño de las tareas desarrolladas por cada área. Priorizando siempre la protección de los empleados.-

2. Indisponibilidad edilicia

Este escenario contempla las amenazas que impidan la utilización de la infraestructura de la Entidad y que podría suponer riesgos para la integridad y seguridad de las personas. Distinto del escenario anterior, las instalaciones no pueden utilizarse y pueden ser inseguras para poder desarrollar actividades dentro de ellas.

3. Indisponibilidad de comunicaciones

Este escenario contempla la interrupción de las comunicaciones telefónicas y de red de datos. La ocurrencia de este escenario implica que los equipos no pueden cursas mensajes o datos a través de la red del Banco y que las comunicaciones telefónicas se encuentran seriamente limitadas.

4. Indisponibilidad de sistemas

Este escenario contempla la interrupción de los sistemas que soportan los procesos de negocio. Para preservar la continuidad de los procesos de negocios, es necesario mantener operativos los sistemas que dan soporte a los procesos críticos de negocio.

4. Riesgos corporativos en el Banco XX

En total en el Banco XX existen alrededor de 4,700 riesgos detectados y setenta y dos unidades de negocios

Entre los riesgos más importantes a los que se enfrenta el banco podemos enumerar a:

El riesgo relacionado con la Tecnología Informática, posee su propia unidad de *staff* que es la encargada de analizar los aplicativos, sus errores y seguridad y determina a través de una fórmula si cierto proceso es riesgoso o no.

El Banco posee por ejemplo, una sola maquina procesadora de información conocida como centro de cómputo que se encuentra en la sucursal de San Martin 721, en la cual convergen todas las sucursales del banco y ésta procesa la información.

El Banco realiza un solo *back up* a las diez de la mañana, si el sistema se cae antes o luego de dicha hora la información en el sistema se pierde, por lo que debe ser ingresada a mano con los comprobantes, para lo que se montan cajeros paralelos ficticios que se encargan de procesar de nuevo la información como si el cliente estuviera presente, lo que posibilita cometer numerosos errores. Este mecanismo este mecanismo esta determinado en el BIA de modo de saber cómo reaccionar ante esta situación y puede implementarse cuando la proveedora del sistema I.B.M dé al banco una solución dentro de un plazo medianamente corto, si el proveedor determina que se necesitará más que unos minutos o unas pocas horas el Gerente del banco se encuentra ante la difícil decisión de dejar de atender al público o seguir haciéndolo para luego cargar todas las operaciones manualmente. De optar por la segunda opción se establecen límites para minimizar errores como podría ser por ejemplo transacciones de

hasta dos mil pesos, ya que el cajero encargado de llevar a cabo la operación no puede observar si el saldo se encuentra realmente disponible.

Para solucionar este problema se adquirió una nueva máquina de respaldo que en este momento todavía no se pudo poner en marcha, luego de solucionado esto se deberá atender el problema de la comunicación, es decir el contrato con telefónica para que todo funcione correctamente.

Existen casos muy excepcionales que a veces no implican una delimitación de un plan de contingencias por su inexistente capacidad de ocurrencia pero que sin pensarlo sucede, en ese caso la entidad no cuenta con un plan ni sabe cómo responder a este problema y es donde la experiencia y preparación de sus gerentes es un recurso vital como ocurrió en el banco hace aproximadamente dos años cuando la maquina procesadora fallo a mitad de la noche impidiendo que el dinero perteneciente a los jubilados se trasladara a sus cuentas de ahorro, una situación jamás antes vivida y según la proveedora de sistemas imposible, reiniciar el sistema hubiese implicado que el banco no pudiese abrir sus puertas, violando la ley que los obliga a atender todos los días, entonces de procedió a abrir las puertas asumiendo el riesgo de que los jubilados se presenten y no encuentren su dinero y un escándalo publico por la situación. Al abrir sus puertas el banco se dio con la realidad de que el dinero si estaba en las cuentas pero no se podía ver por los ATM, esto llevo a que se destine una oficina encargada de llamar a todos los centros de jubilados de la provincia y pedirles que por favor envíen a los jubilados a cobrar por ventanilla directamente.

Así podemos ver que a pesar de existir el plan de contingencias en el banco por su envergadura nunca es posible desarrollar un plan de contingencias para todo y muchas veces se va resolviendo sobre la marcha.

Uno de los procesos operacionales con mayor riesgo es el *clearing,* en relación a los cheques cobrados que pertenecen a otros bancos y el

dinero que debería enviarse o recibirse de la cámara compensatoria. Hasta el día de hoy el banco nunca incumplió con la presentación de la información y el depósito a la cámara, pero de producirse un atraso, si bien es posible pedir una ventana, es decir, una extensión del tiempo de presentación, el banco debería tomar la decisión de pagar los cheques ajenos asumiendo el riesgo de que realmente los mismos no tengan fondos, hasta que una vez solucionado pueda éste saber cuál era la situación de las respectivas cuentas. En el caso que esto sucediera seguramente se establecerán límites para minimizar los riesgos.

Otra medida relacionada a los problemas con los procesos que involucran cheques y la cámara compensatoria, que se encuentra expresado en los planes de contingencias del banco, se da en estos momentos en donde los bancos realizan paros sistemáticos como protesta y les impide realizar las presentaciones a la cámara, por lo que todos los cheques son rechazados por fuerza mayor durante esos días para NO asumir el riesgo de que los mismos no tengan fondos o no cumplan con las condiciones para ser pagados.

A veces impensado pero de altísima importancia en el banco son los riesgos que involucran al personal de vigilancia. Los bancos en general cuentan con un protocolo de seguridad que deben cumplir pero por las disponibilidades del personal en el momento deben decidir si asumir el riesgo o esperar a que el plan de recuperación funcione, que consistiría en esperar la llegada de más efectivos desde las dependencias policiales o desde el sistema de seguridad privado, por lo general el tiempo de respuesta de estas entidades es más lenta que el desenvolver normal de las actividades bancarias por lo que se asume el riesgo, una vez más, de incumplir con los planes para no alterar los procesos, como por ejemplo a la hora de apertura del banco, de la apertura de cajeros automáticos y de la recepción de los cajeros blindados.

Como culminación y explicación grafica de el accionar del banco en la delimitación de los riesgos, su análisis cualitativo y cuantitativo y demás pasos enumerados anteriormente incluimos esta matriz en donde se puede observar cómo se trabaja realmente en el departamento de gestión de riesgo operacional. Apéndice 4.

4. El Banco Central de la República Argentina como órgano de contralor.

El Banco Central siendo el órgano que regula el ejercicio de la actividad bancaria establece lineamientos para controlarlos y la forma en la que las entidades deberán rendir cuentas.

Por un lado los bancos deberán enviar informes, por ejemplo informes trimestrales, que consisten en una base de pérdidas mayores a mil pesos de Riesgo Operacional. El Banco XX en los últimos informes envió ciento cincuenta y nueve eventos entre los que podemos nombrar pago de jubilaciones y desconocimientos de gastos con tarjeta de crédito como los más recurrentes, el último muchas veces desembocando en un riesgo asumido del que termina por hacerse cargo la entidad. Al momento de enlistar las pérdidas en los informes para el BCRA, el banco analiza los antecedentes de cada una para determinar si se deben a faltas de parametrización, si es un problema en los procesos o si se refiere a un fraude externo, como podría ser el caso de las tarjetas de crédito adoptando a veces medidas de control.

Por otro lado, con auditorías realizadas por el BCRA las cuales se encuentran reglada con un manual que establece los procedimientos para llevarla a cabo. Pueden ser supervisiones generales referidas al todo, supervisiones del sistema o control de auditores.

Hace un año y con el cambio de Gobierno Nacional por un lado el banco instó más fuertemente a los bancos a adoptar esta postura de análisis del riesgo pero por otro lado, se volvió mucho más flexible o cómodo, por así decirlo, en el análisis de la información y al momento de dictar las Comunicaciones, redactando las mismas en base al estudio de las presentaciones llevadas a cabo por distintos bancos volviendo mucho más viables los requerimientos.

CONCLUSION

Hoy en día la detección de Riesgos es algo que los bancos lograron abordar para estar a la altura de las exigencias, los problemas más arduos se presentarán al momento de aplicar los nuevos procesos que implican el uso de tecnología de avanzada como depósitos de cheque con el empleo del celular, lo que si bien ya estaría reglado las entidades se encuentran muy lejos de poder implementar.

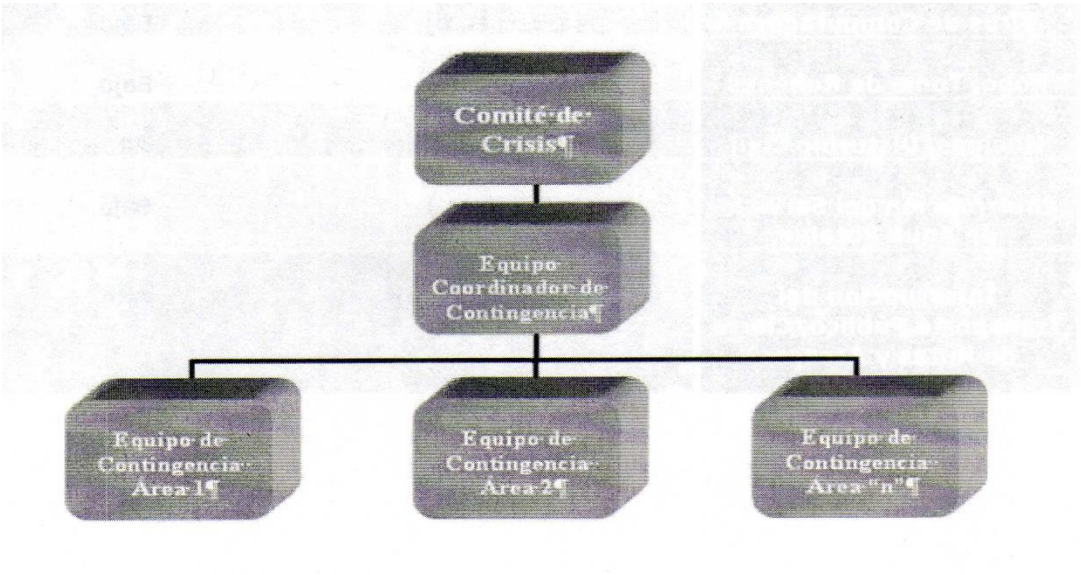
Si bien la implementación del riesgo operacional le da a la entidad la posibilidad de conocer y resaltar los riesgos y posibles contingencias que por el transitar diario de las operaciones se pasarían por alto, hoy para este banco, por la adopción de políticas propias y la adecuación de la información bajo la Ley SOx, el cumplimiento de la normativa del BCRA y la gestión del riesgo operacional es más por mero cumplimiento normativo, que por que realmente le brinde un beneficio ya sea tangible o intangible. Según palabras del Subgerente sería mejor destinar el personal avocado hoy al análisis del riesgo operacional a la reingeniería de los procesos.

La gestión de riesgo operacional constituye solamente una herramienta de control y le sirve para prepararse para hacer frente a las contingencias. Es más una consultoría que una auditoria, un pre, una suposición que reduce los desvíos.

ANEXOS

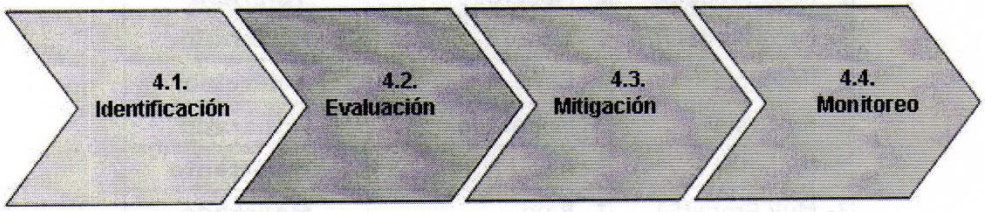
Anexo 2:

Estructura dentro de la entidad bancaria de para la administración y ejecución del Plan de continuidad de negocio:



APENDICE:

Apéndice 1:



Apendice 2:

Probabilidad	Impacto	Nivel de Riesgo Residual
1- Poco Probable	1- Bajo	**Aceptable**
1- Poco Probable	2- Moderado	**Tolerable**
1- Poco Probable	3- Alto	**Moderado**
2- Probable	1- Bajo	**Tolerable**
2- Probable	2- Moderado	**Moderado**
2- Probable	3- Alto	**Importante**
3- Muy Probable	1- Bajo	**Moderado**
3- Muy Probable	2- Moderado	**Importante**
3- Muy Probable	3- Alto	**Grave**

Apéndice 2:

Nro	Riesgos	Detalle	Formula	Nivel Riesgos verdes	Nivel Riesgos amarillos	Nivel Riesgos rojos
1	Fallas en los procesos de las operaciones	Indice de rotacion del personal	Altas + bajas / dotacion	0....0,10	>0,10 y < 0,30	=>0,30
2	Multas por incumplimientos normativos	Total de multas abonadas en $	Total de multas abonadas en pesos / mes	$ 0	< $ 100.000.-	=> $ 100.000.-
3	Perdidas de clientes	Tiempo de resolucion de reclamos	Total tiempo por reclamo	48 hs	>48 hs y < 72 hs	=> 72 hs

Apéndice 3:

Amenaza	Probabilidad	Probabilidad de ser afectado ante la amenaza
Terremoto	2 (Ocasional)	Bajo
Huracán/Tornado	0 (Nulo)	Bajo
Inundación	0 (Nulo)	Bajo
Incendio	3 (Poco Frecuente)	Bajo
Daños por Filtraciones de Agua	3 (Poco Frecuente)	Bajo
Contaminación Tóxica	2 (Ocasional)	Bajo
Amenaza de Bomba	3 (Poco Frecuente)	Bajo
Fallas de Energía	5 (Muy Frecuente)	Bajo
Falla de Comunicaciones y LAN	4 (Frecuente)	Bajo
Pandemia	4 (Frecuente)	Medio
Virus de Computadora	4 (Frecuente)	Bajo
Robo/Toma de Rehenes	2 (Ocasional)	Bajo
Huelgas/Disturbio Civil	5 (Muy Frecuente)	Alto
Interrupción del Servicio de Agua Potable	2 (Ocasional)	Bajo
Interrupción del Transporte Público/Cierre de Rutas y Accesos	5 (Muy Frecuente)	Alto

PROCESO: DEPOSITOS A PLAZO (PLAZO FIJO)

					EVALUACION CUALITATIVO			CUANTITATIVA						
Ciclo	Proceso	Actividad	Riesgo	Control	Impacto	P.Ocu	Nivel Riesgo	Frecuencia Residual	Impacto Residual	Frecuencia Máxima	Impacto Máximo	Riesgo Esperado	Riesgo Máximo	Riesgo Potencial
DISTRIBUCION Y VENTAS	Depósitos a Plazo	Concertación Renovación	La pérdida de la Documentación Original firmada por los titulares debido a un inadecuado resguardo puede producir reprocesos, insatisfacción en los clientes e inconvenientes legales con los mismos.	A efectos de respaldar la identificación del Cliente, se habilitará un legajo que se ordenará por número de documento, donde será archivada toda la documentación recibida e integrada por el Cliente.En el caso de PJ solo se mantendrá legajo de No Clientes	Bajo	Poco Probable	Bajo	0,1				$ 1,00	$ 1,00	$ 0,00
DISTRIBUCION Y VENTAS	Depósitos a Plazo	Concertación Renovación	La presencia de errores u omisiones en el control del estado de los Plazos Fijos del cliente (bloqueo por algún motivo o garantizando alguna operación) al momento de la renovación o cancelación puede generar pérdidas operativas/ financieras a la Entidad	El Ejecutivo de Clientes verifica que el certificado se encuentre vencido y que no esté bloqueado ni garantizando alguna operación.- Interviene al dorso del certificado con sello y firma, como constancia de los controles efectuados.	Bajo	Poco Probable	Bajo	35	$ 3,15	35	$ 7,86	$ 110,25	$ 275,10	$ 164,85
DISTRIBUCION Y VENTAS	Depósitos a Plazo	Concertación Renovación	Posibilidad de errores o alteraciones de los plazos de los depósitos al momento de liquidar las operaciones en el sistema.	Al momento de constituir las imposiciones, se deberán tener en cuenta los montos mínimos y plazos mínimos de constitución, según Grilla de Plazo Fijo publicada en Intranet.	Bajo	Poco Probable	Bajo	0,1	$ 10,00				$ 1,00	$ 0,00
DISTRIBUCION Y VENTAS	Depósitos a Plazo	Concertación Renovación	Se admiten depósitos que pueden provenir de operaciones ilícitas, y por lo tanto el Banco puede incurrir en el delito de lavado de dinero.	En la constitución de plazos fijo por importes mayores a $40.000, el cliente debe completar el formulario "Declaracion Jurada sobre licitud y origen de los fondos Persona fisica" (o juridica si corresponde)	Bajo	Poco Probable	Bajo	35	$ 3,15	35	$ 4,72	$ 110,25	$ 165,20	$ 54,95
DISTRIBUCION Y VENTAS	Depósitos a Plazo	Concertación Renovación	Se emiten Certificados de Plazo Fijo sin autorización.	El Ejecutivo de Clientes interviene (firma y sello aclaratorio) y solicita intervención en el original y en el duplicado del certificado, de una persona autorizada, que pueden ser el Resp. Operativo, Tesorero, el Asistente de RO o el Gte/Resp. Sucursal	Bajo	Poco Probable	Bajo	35	$ 3,15	35	$ 4,72	$ 110,25	$ 165,20	$ 54,95
DISTRIBUCION Y VENTAS	Depósitos a Plazo	Concertación Renovación	Se producen errores en los movimientos (altas y bajas) de plazos fijos en el sistema.	Al final del día, el Ejecutivo de Clientes imprime aplicativo del sistema, que contiene los movimientos de plazo fijo efectuados durante el día y los movimientos de los certificados inmovilizados y lo compara contra los certificados de plazo fijo	Bajo	Poco Probable	Bajo	35	$ 3,15	35	$ 7,86	$ 110,25	$ 275,10	$ 164,85

• Criterio de frecuencia mínima

Este criterio consiste en determinar como frecuencia mínima una periodicidad de una vez cada diez años (0,1), para cuantificar las frecuencias de riesgos cuya manifestación es muy poco probable pero posible.

• Hay riesgos que de producirse, no repercutiría en una pérdida económica

Sin embargo, se estableció un criterio de valoración por horas hombre, el cual consiste en cuantificar el costo que acarrearía reversar la situación.

INDICE BIBLIOGRAFICO.

ESPECIAL

- CONSEJO EMISOR DE NORMAS DE CONTABILIDAD Y AUDITORIA, INFORME Nº 5 (Buenos Aires)
- COMMITTE OF SPONSORING OF THE TREADWAY COMMISION, COSO, (Estados Unidos, 1985)
- COMMITTE OF SPONSORING OF THE TREADWAY COMMISION , Marco integrado de gestión de riesgo corporativo (Estados Unidos, 2004).
- COMMITTE OF SPONSORING OF THE TREADWAY COMMISION, Marco integrado de gestión de riesgo corporativo técnicas de aplicación, (Estados Unidos, 2004)

GENERAL

- ESPIÑEIRA SHELDON Y ASOCIADOS, Gestión de riesgos, Edición conjunta ESA y UCAB, 1º Edición, (Estados Unidos, 2008)

- ESPIÑEIRA SHELDON Y ASOCIADOS, Gestión Integral de riesgos, Edición conjunta ESA y UCAB, 2º Edición, (Estados Unidos, 2008)

- LUIS, Ernesto Cañas Pacheco, Desarrollo e implementación de sistemas de Gestión, (Buenos Aires, 2009)

- BANCO CENTRAL DE LA REPUBLICA ARGENTINA, Comunicación "A"4793, (Buenos Aires, 2008)

OTRAS PUBLICACIONES

- ASCARATE, Lidia Inés, Curso: Organización contable de empresas, Apuntes de clase teóricas, Facultad de Ciencias Económicas, U.N.T. (San Miguel de Tucumán, 2014).

– Consultas a bases de información en Internet:

http://www.bcra.gov.ar/default.asp (12/10/2016)

www.bcra.gov.ar/pdfs/comytexord/A4793.pdf*(12/10/2016)*

https://www.bancotucuman.com.ar (15/10/2016)

https://www.macro.com.ar(15/10/2016)

http://bibliotecadigital.uca.edu.ar (28/10/2016)

www.bcra.gov.ar/pdfs/comytexord/A4793.pdf *(19/10/2016)*

http://www.ambito.com/832252-banco-macro-dio-campanazo-de-apertura-de-wall-street *(22/10/2016)*

INDICE