UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE ECONOMÍA

"ADMINISTRACIÓN DEL RIESGO OPERACIONAL EN EL SECTOR BANCARIO MEXICANO: UNA PROPUESTA DE SU GESTIÓN EN 2020"

TESINA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN ACTUARÍA

PRESENTA:

MARTHA GUADALUPE LÓPEZ MENDIOLA

ASESOR:
M. EN E. C. ÁNGELES MORALES VERÓNICA

REVISORES:

D. EN ADM. D.E. DELIA ESPERANZA GARCÍA VENCES
ELIZABETH ALMAZÁN TORRES

TOLUCA, ESTADO DE MÉXICO **JUNIO 2021**

Introducción

Los bancos se encuentran expuestos a diversos riesgos tanto internos como externos, ante un mundo cada vez más globalizado, en donde es claro que los problemas de un sector pueden trasladarse rápidamente a otro, y contar con una adecuada gestión de riesgos puede ser la gran diferencia en una situación adversa entre mantenerse a flote, caer y en el mejor de los casos pudiera representar una oportunidad para la generación de negocio.

Tal es el caso de la crisis a inicio de los dos miles en donde el problema había sido originado en el sector inmobiliario en Estados Unidos, y se trasladó al sector bancario, automotriz, entre otros, que al final originó una crisis mundial.

Diversas autoridades reguladoras y organizaciones privadas en su preocupación han desarrollado marcos de referencia para la administración de riesgos y de control interno.

Sin embargo, toda la información publicada son una serie de regulaciones, leyes o normas, sobre lo que se espera que las instituciones realicen para la gestión de sus riesgos, lo cual al momento de su ejecución existen vacíos o subjetividades sobre el cómo realizarlas, tal es el caso del riesgo operacional para el cual su gestión y medición requiere de métodos cuantitativos y cualitativos. Para ello, en esta investigación se realiza una exploración de diversos marcos de referencia, metodologías y guías, para proponer el flujo de gestión del riesgo operacional en un banco, así como cada una de las herramientas a implementar para su administración.

La administración del riesgo operacional tiene un efecto directo en las pérdidas en que se pudieran incurrir ante su materialización y a su vez, en el capital mínimo con el que debe de contar un banco para hacer frente ante este tipo de eventos y no poner en peligro la existencia de la institución y generar inestabilidad económica, por lo anterior, se explorarán diversos métodos bajo los cuales los bancos pueden realizar el cálculo de dichos requerimientos mínimos.

Planteamiento del problema

La gestión de riesgos de las instituciones financieras es importante debido a que no se cuenta con la certeza de lo que sucederá en el futuro, por lo que es necesario tener un entorno de control que ayude a evitar sorpresas que pudieran poner en riesgo a la organización. Crisis financieras, bancarrota de empresas o pérdidas millonarias pudieron evitarse o minimizado de haber mantenido una adecuada administración de riesgos.

Un ejemplo claro de lo que pudiera ocasionar la ausencia o una inadecuada gestión de riesgos es la crisis internacional de 2008, la cual tuvo sus orígenes en un desmesurado otorgamiento de créditos *subprime* este tipo de créditos hipotecarios son considerados de alto riesgo debido a que son enfocados a personas con poca capacidad de pago o sin historial crediticio.

El problema vino cuando los créditos *subprime* al tener una tasa baja de interés se volvieron instrumentos atractivos que prometían un rendimiento considerable y en poco tiempo, como estos créditos no requerían un historial crediticio ni capacidad de pago, la personas solicitaban créditos que rebasaban su capacidad de pago y los bancos continuaban otorgándolos, estos a su vez diseñaron instrumentos complejos con la finalidad de garantizar el valor de la garantía en caso de incumplimiento del acreditado.

Uno de los primeros síntomas de la crisis financiera hipotecaria fue el incremento de la tasa de realizados por la Reserva Federal en junio de 2004 incrementándose *"desde 1%, su nivel más bajo desde la década de los cincuenta, hasta 5.25%; la tasa se incrementó en 17 ocasiones al tratar de contener la inflación, y en junio de 2006 el alza en las tasas concluyó"* (Zurita González, Martínez Pérez, & Rodríguez Montoya, 2009, pág. 22), a partir de ese momento el crecimiento que había en los bienes raíces se desplomaron, Freddie Mac y Fannie Mae las dos más importantes inmobiliarias en Estados Unidos se declararon en bancarrota.

La crisis en el sector inmobiliario también afectó a las instituciones financieras. El banco de inversión *Bear Stearns* el cual contaba con una alta concentración de obligaciones de deuda garantizada *CDO* (*Collaterized Debt Obligation*) por sus siglas en inglés, enfrentó problemas de liquidez irremediables por lo que fue comparado por *JP Morgan Chase*,

este caso generó alerta en otros bancos que contaban con los mismos instrumentos como fue el caso de *Lehman Brother* y *Merilin Lynch*, siendo así el inicio de la crisis financiera global.

Las instituciones si bien ya contaban con procesos de administración de riesgos apegados a las recomendaciones emitidas por el Comité de Basilea, existieron organizaciones que también se vieron comprometidas a raíz de la crisis, por esta razón esa organización realizó mejoras a sus publicaciones.

El proceso de administración de riesgos además de prevenir las pérdidas en las que pudiera incurrir una organización también permite alcanzar los objetivos definidos por el gobierno corporativo, mismos que se vuelven alcanzables a través del desarrollo de una estrategia.

El gobierno corporativo además de definir los objetivos y las estrategias a través de las cuales estos se volverán alcanzables también define cuál es el apetito al riesgo o el nivel de tolerancia al riesgo, es decir, cuánto riesgo la institución está dispuesta a asumir por realizar algunas de las actividades para hacer negocio.

Para realizar la gestión de riesgos de una institución es fundamental contar con conocimiento del contexto que se busca administrar, lo cual permite identificar los riesgos a los que pudiera estar expuesta la organización.

El riesgo operacional de acuerdo con el Comité de Basilea se define como “el riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, personas o sistemas internos o bien a causa de acontecimientos externos” (Comité de Supervisión Bancaria de Basilea, 2003, pág. 8) esta definición de riesgo operacional incluye al riesgo legal y excluye al riesgo reputacional.

Si bien el riesgo operacional a primera vista no da un valor directo al negocio, su importancia radica en la reducción de pérdidas y por ende del riesgo mismo. La materialización del riesgo operacional además de conllevar un impacto directo en la organización, puede ocasionar daños colaterales, en otros riesgos, tal como es el caso del riesgo de reputación pues en el contexto actual la facilidad en que una noticia puede trascender fronteras es de manera casi inmediata y la percepción que tendrían los

interesados en la institución como clientes o inversionistas se degradaría de manera importante, pudiendo perder la capacidad de retenerlos o de atraer nuevos, ocasionando que el evento también conlleve a problemas de liquidez.

La ocurrencia de un evento de riesgo operacional además de poner en peligro la existencia de una institución bancaria, puede representar un riesgo sistémico, es decir, que también origine que otras instituciones bancarias tengan repercusiones económicas lo cual pudiera originar incluso crisis nacionales e internacionales.

Ante la necesidad de evitar que los riesgos originen problemas económicos existen organizaciones con el objetivo de garantizar la solidez del sistema financiero global tal como lo es el Comité de Supervisión Bancaria de Basilea, mismo que ha realizado una serie de publicaciones con recomendaciones para llevar a cabo la gestión de riesgos, si bien estas recomendaciones no son obligatorias, diversos países las han adoptado como un marco de referencia considerándolas como mejores prácticas, estas son implementadas a través de sus diferentes bancos centrales y organizaciones competentes. En México, el Banco de México y la Comisión Nacional Bancaria y de Valores (CNBV), son las instituciones responsables de garantizar que el país cuente con los estándares mínimos de administración de riesgos.

La CNBV emite una serie de requisitos publicados en la Circular Única de Bancos (CUB) donde se establecen los requerimientos mínimos con los que una Institución de Banca Múltiple debería de contar en materia de riesgo operacional, sin embargo, esta no es limitativa a que cada institución utilice la metodología que mejor le convenga ya sea por su tamaño o por la complejidad de sus operaciones, siempre y cuando se garantice que se cumplen con los estándares ahí establecidos. Para efectos de este trabajo de investigación y la propuesta de la administración del riesgo operacional, se tomará principalmente como base el marco de referencia definido por el "*Committee of Sponsoring Organizations of the Treadway"* de ahora en adelante se hará referencia a este comité como COSO*,* así como las publicaciones realizadas por el Comité de Basilea*.*

En esta investigación se busca además de indagar en aspectos teóricos de COSO, es proponer los elementos con los que deben de contar cada una de las herramientas que permiten realizar la administración de riesgos operacionales dentro de una organización

bancaria, este documento está enfocado a especialistas en riesgos o bien, a cualquier persona que tenga el interés en conocer la gestión del riesgo operacional.

Objetivo General

Propuesta de una metodología para gestionar el riesgo operacional en el sector bancario mexicano en el año 2020.

Objetivos Específicos

- Conceptualizar a la gestión de riesgos en una Institución Bancaria
- Definir los tipos de riesgo a los que una organización podría estar expuesta
- Conceptualizar la terminología que se estará utilizando en la gestión del riesgo operacional
- Sugerir el flujo de gestión de riesgos operacionales[1]
- Detallar las herramientas a utilizar en el flujo para realizar la gestión de riesgos operacional

Justificación

La CNBV define al riesgo operacional como “la pérdida potencial por fallas o deficiencias en los controles internos, por errores en el procesamiento y almacenamiento de las Operaciones o en la transmisión de información, así como por resoluciones administrativas y judiciales adversas, fraudes o robos y comprende, entre otros, al riesgo tecnológico y al riesgo legal”.
(Comisión Nacional Bancaria y de Valores, pág. 47)

Se exponen los aspectos teóricos de la gestión de los riesgos operacionales para proponer una alternativa práctica de administrarlos, el flujo de administración, así como las herramientas que se utilizarán en él, pues actualmente si bien se cuenta con

[1] Se refiere a cada una de las etapas que componen la gestión del riesgo operacional dentro de una institución bancaria.

información que sustente los aspectos técnicos de la administración de riesgos operacionales se carece de una guía de cómo deben de gestionarse.

El presente documento está dirigido a profesionistas que estén involucrados en la gestión de riesgos operacionales en instituciones bancarias, pudiendo también ser utilizada para todos los interesados en realizar una gestión de riesgos operacionales, sin embargo, su aplicabilidad no es limitativa a que dicha propuesta sea aplicable a diversas instituciones financieras, pues el principio para realizar una gestión de riesgos podría adecuarse a otro tipo de institución.

Diseño Metodológico

El desarrollo de la propuesta para realizar la gestión de riesgos operacionales se realizó a través de un estudio cualitativo, por medio de un análisis documental por los diversos marcos de referencia nacionales e internacionales.

Se realizó la revisión de documentos que permitieron conceptualizar la gestión de riesgos, para posteriormente poder definir los tipos de riesgos a los que pudiera estar expuesta una institución.

Una vez revisados los marcos de referencia de la gestión de riesgo operacional, se sugiere un flujo para realizar la gestión del riesgo operacional, describiendo cada una de las etapas del ciclo de gestión.

Se detallaron las herramientas que se estarán utilizando en cada una de las etapas del flujo de gestión del riesgo operacional.

Por último, se exponen los diversos métodos de cálculo de requerimiento de capital por riesgo operacional como lo son: método del indicador básico, método estándar, método estándar alternativo y el método avanzado. También detallaron las metodologías de cuantificación para la estimación de este tipo de riesgo.

Descripción

El trabajo de investigación consta de cuatro capítulos que parten de manera general de las definiciones de cada uno de los riesgos, los marcos de referencia de la gestión de riesgos y controles, para llegar de manera particular a la administración del riesgo operacional y los métodos de requerimiento de capital con el que deben de contar las instituciones bancarias.

En el primer capítulo de la investigación se presentan las definiciones de la gestión de riesgos, del riesgo mismo, así como de sus categorías, siendo estos conceptos necesarios para comprender la administración de riesgos dentro de una institución financiera.

Una vez definidos los tipos de riesgo se detallan los principales marcos de referencia y guías para su gestión, presentando el marco normativo internacional que es el Comité de Basilea y la comparación entre Basilea I, II y III, el marco de referencia COSO y la comparación entre COSO I, COSO II, COSO III y COSO IV, así como la Organización Internacional para la Estandarización, La Ley Sarbanes Oxley y el Control de Objetivos para las Tecnologías de Información y Relacionadas.

De la información recolectada de los diferentes marcos de referencia y mejores prácticas se muestra cómo se encuentra estructurado el modelo de tres líneas de defensa, quiénes participan en cada una de ellas, así como sus roles y responsabilidades. Una vez definido lo anterior se mostrará el flujo a través del cual se propone se realice la gestión del riesgo operacional y las herramientas por medio de las cuales se podrá dar cumplimiento a cada una de etapas del flujo de gestión.

Por último, como resultado de la gestión de riesgos operacionales las entidades reguladoras, con el propósito de incentivar a los bancos sobre su gestión interna de riesgo operacional, proponen diversos métodos de cálculo del requerimiento de capital por riesgo operacional, razón por la cual se expondrán los diferentes métodos de cálculo, así como los requerimientos que deben de cumplir las instituciones para lograr la utilización de alguno de ellos.

Índice

Capítulo I El riesgo y sus clasificaciones

Para realizar la administración de riesgos es indispensable saber a qué se refiere, qué tipo de riesgos existen, si son cuantificables o no, esto con la intención de contar con los elementos necesarios para elegir los métodos que mejor se adecuen a cada uno de los riesgos y poder gestionarlos de manera adecuada, razón por la cual este capítulo es el punto de partida para el resto de la investigación.

1.1 Riesgo

A lo largo de la historia de las instituciones bancarias se han valido de asumir riesgos debido a los beneficios económicos que traen consigo, sin embargo, dichos beneficios también han conllevado a pérdidas financieras catastróficas que provocaron la bancarrota de bancos e incluso, han originado crisis a nivel internacional, de ahí radica la importancia de la gestión de los riesgos dentro de una institución.

Antes de dar inicio de manera formal a lo que la gestión de riesgos se refiere, resulta indispensable definir al riesgo y sus tipos.

El riesgo puede definirse, como la probabilidad de que un evento adverso suceda y que conlleve a una pérdida; en el caso de una institución financiera como lo es un banco, se puede definir como la probabilidad de que ocurra un evento que genere pérdidas para éste las cuales afecten el logro de los objetivos de la Institución.

Los riesgos a su vez pueden definirse de acuerdo con su razón de ser, o bien, en lo que corresponde a su medición. De acuerdo con la CNBV (Comisión Nacional Bancaria y de Valores[CNBV], 2019) en la CUB se definen de la siguiente manera:

- Riesgos cuantificables: corresponden a aquellos riesgos sobre los cuales se pueden realizar bases estadísticas para con esa información poder estimar pérdidas potenciales.
- Riesgos no cuantificables: corresponden a aquellos riesgos que no se pueden medir numéricamente, es por ello por lo que no es posible conformar una base estadística que permita estimar pérdidas potenciales, principalmente por la rareza de la ocurrencia de ese tipo de eventos, en esta categoría se pudieran incluir los riesgos como el tecnológico, reputacional y el estratégico.

- Riesgos discrecionales: corresponden a aquellos riesgos que la organización asume con la finalidad de obtener un beneficio. La gestión de riesgos pretende encontrar la manera en que la institución pueda no verse afectada ante dichos riesgos y lograr obtener beneficios.
- Riesgos no discrecionales: se refiere a riesgos de los que no se pretende obtener un beneficio directo de asumirlos, sino que son inherentes a las actividades que se realizan.

1.2 Riesgos discrecionales cuantificables

- Riesgo de mercado: la CNBV en la CUB define que el riesgo de mercado es la pérdida potencial en la que se pudiera incurrir ante la pérdida de valor de un activo, a dicho acontecimiento pueden estar asociados diferentes causales, a lo que se les conoce como factores de riesgo, los cuales pueden ser fluctuaciones en las tasas de interés, en los tipos de cambio, volatilidad cambiaria, por mencionar algunos.

  Para realizar la cuantificación del riesgo de mercado existen diversos métodos, como lo son, el valor en riesgo también conocido como VaR por sus siglas en inglés *Value at Risk*, la duración, el análisis del peor escenario, entre otros. Aunque existen esos métodos el más usual es el valor en riesgo o VaR, el cual “es un estimado de la máxima pérdida esperada que puede sufrir un portafolios durante un periodo de tiempo específico y con un nivel o de confianza o probabilidad definido”. (Haro, Medición y Control de Riesgos Financieros, 2005, pág. 19)

- Riesgo de liquidez: la CNBV en la CUB define al riesgo de liquidez como la pérdida potencial en la que pudiera incurrir una institución ante la imposibilidad de hacer frente a sus obligaciones inmediatas o bien, a la imposibilidad de que los activos de una empresa puedan ser convertidos en efectivo en el corto plazo, la pérdida potencial por el cambio en la estructura del balance general de la Institución debido a la diferencia de plazos entre activos y pasivos.

- Riesgo de crédito: la CNBV en la CUB define que el riesgo de crédito corresponde a la pérdida potencial en la que pudiera incurrir una institución ante la imposibilidad de poder hacer efectivas las obligaciones con sus clientes o contrapartes financieras.

Para poder realizar el cálculo de exposición a este tipo de riesgo existen diversos métodos, los cuales consisten en el conocimiento del cliente y de diversos factores que pudieran influir en que estos decidan no hacer frente a sus obligaciones contraídas, tales como son el análisis de crédito tradicional:

A lo largo de la historia los bancos han realizado sus estudios de crédito basados en lo que se conoce como las cinco “Ces” con las que debe de contar el solicitante ya sea una persona o empresa las cuales consisten en lo siguiente según (Haro, 2018):

  - Conocer: se refiere a saber cuál es la solvencia, reputación y disposición para hacer frente a las obligaciones del solicitante
  - Capacidad de Pago: se refiere al análisis que se realiza al solicitante con base en los ingresos que éste ha obtenido históricamente
  - Capital: para el otorgamiento del crédito es necesario conocer la capacidad de endeudamiento estimado en función de recursos propios y relación con los de terceros
  - Colateral: este punto se refiere a las garantías del crédito, es decir, en el caso de incumplimiento de la garantía o garantías ésta debe de cubrir la pérdida en la que el prestamista pudiera incurrir
  - Condiciones Cíclicas: este factor hace referencia a determinar la exposición, esto debido a la sensibilidad que diversas instituciones puedan tener a los ciclos económicos
- Riesgo de concentración: la CNBV en la CUB define al riesgo de concentración como la pérdida potencial atribuida a la elevada y desproporcional exposición a factores de riesgo particulares dentro de una misma categoría o entre distintas categorías de riesgo.

1.3 Riesgos no discrecionales cuantificables

- Riesgo operacional: el riesgo operacional se puede definir como la pérdida potencial en la que pudiera incurrir una institución por fallas en los procesos internos, personas, por eventos externos o bien, por eventos tecnológicos. Esta definición incluye al riesgo legal, pero excluye al riesgo reputacional y al riesgo estratégico.

  Como se puede observar el riesgo operacional se encuentra inherente a todas las actividades que se realizan en una Institución bancaria, por lo tanto, mientras una institución exista el riesgo operacional estará siempre presente.

- Riesgo legal: como se mencionó anteriormente, el riesgo legal se encuentra contemplado en la definición de riesgo operacional, la CNBV en la CUB indica que el riesgo legal se refiere a la pérdida potencial derivada de no poder ejercer un contrato con una contraparte, o bien, a las pérdidas derivadas del incumplimiento de la normativa lo cual pudiera ocasionar multas para la institución, en el riesgo legal también se incluyen aquellas pérdidas en las que pudiera incurrir una institución bancaria por procedimientos legales.

- Riesgo tecnológico: la CNBV en la CUB (2019) a este riesgo se refiere como las pérdidas potenciales derivadas de la interrupción de los sistemas de telecomunicaciones, así como fallos en *software* y/o hardware, se tiene que considerar este riesgo cuando existan servicios o sistemas que sean externos a la institución, como riesgo propio de la institución toda vez que las repercusiones económicas ante una eventualidad de esta naturaleza el banco es el responsable en primera instancia.

1.4 Categorías de Riesgo Operacional

Una institución está expuesta a diversos riesgos operacionales y cuando estos son identificados suelen ser descritos con base a la apreciación de la persona que lo descubre, esto puede originar que el manejo de esa información sea complicada y subjetiva, para evitarlo el Comité de Basilea ha definido las siguientes categorías de Riesgo Operacional (Comité de Supervisión Bancaria de Basilea, 2003):

- Fraude interno: corresponde a aquellas pérdidas derivadas de acciones de personal interno de la institución, las cuales son realizadas para tener un beneficio y en detrimento de la institución.
- Fraude externo: se refiere a aquellas pérdidas derivadas de las actividades que un externo realice con la intención de defraudar a la Institución.
- Relaciones laborales y seguridad en el puesto de trabajo: esta categoría corresponde a las pérdidas derivadas de no cumplir con la legislación en lo que se refiere a las relaciones laborales. En esta categoría también se incluyen aquellas reclamaciones o demandas que personal de la institución realice por daños personales, o bien, por haber sido víctimas de discriminación.
- Actividades Empresariales: se refiere a todas aquellas pérdidas derivadas de realizar actividades impropias con clientes o contrapartes, en esta categoría también se incluyen a aquellas pérdidas que hayan sido derivadas de diseños deficientes de los productos.
- Eventos externos: corresponden a aquellas pérdidas en los activos por eventos de origen natural como lo son huracanes, terremotos, inundaciones etcétera. También en esta categoría se contemplan los eventos que son provocados por el hombre como lo son el vandalismo, mítines, huelgas, solo por mencionar algunos.
- Tecnológicos: representa a las pérdidas derivadas de eventos asociados a interrupción en las telecomunicaciones, errores en el *software* utilizado o bien, el *hardware* con el que cuente la institución.
- Procesos: corresponde a todas las pérdidas derivadas por fallas en los procesos internos de la institución, así como incumplimientos a la normativa, también incluyéndose la incorrecta gestión de clientes o contrapartes, y también proveedores.

1.5 Riesgos no cuantificables

- Riesgo reputacional: la CNBV en la CUB define al riesgo reputacional como *"la pérdida potencial en el desarrollo de la actividad de la Institución provocado por*

el deterioro en la percepción que tienen las distintas partes interesadas, tanto internas como externas, sobre su solvencia y viabilidad".

El riesgo reputacional, puede tener su origen en la materialización de un riesgo operacional, como lo son las fallas en los servicios tecnológicos que la Institución ofrezca a sus clientes. Como la definición lo sugiere pueden ser opiniones negativas, aunque estas pueden no ser verídicas, las cuales no estarían asociadas al riesgo operacional directamente, sin embargo, ante la percepción negativa de las partes interesadas, es decir, los clientes e inversionistas, pudieran poner en peligro la estabilidad económica de la institución.

Este tipo de riesgo no se cuenta tan explorado en cuanto a su medición se refiere, sin embargo, resulta de suma importancia su gestión, pues ante un sector financiero cada vez más globalizado y donde las redes sociales juegan un papel crucial en la distribución de la información de manera casi inmediata, la reputación de una institución pudiera ser quebrantada tan abruptamente que pudiera ser irrecuperable.

- Riesgo estratégico: la CNBV en la CUB define al riesgo estratégico como:

  "la pérdida potencial por fallas o deficiencias en la toma de decisiones, en la implementación de los procedimientos y acciones para llevar a cabo el modelo de negocio y las estrategias de la Institución, así como por desconocimiento sobre los riesgos a los que esta se expone por el desarrollo de su actividad de negocio y que inciden en los resultados esperados para alcanzar los objetivos acordados por la Institución dentro de su plan estratégico".

1.6 Administración de Riesgos

Los riesgos se encuentran en todas las actividades de una institución, ya sea por la decisión de obtener algún beneficio al asumirlos como es el caso de los riesgos discrecionales o bien, porque son inherentes a las actividades que el banco realiza.

La administración de riesgos se entiende como el conjunto de objetivos, políticas, procedimientos y acciones que se llevan a cabo para identificar, medir, vigilar, limitar,

controlar, informar y revelar los distintos riesgos a los que se encuentran expuestas las instituciones.

Ahora bien, la gestión de riesgos de una institución bancaria puede tener implicaciones directas con clientes, inversionistas, proveedores e incluso, dada la experiencia originar efectos en la economía, local, nacional e internacional. Para lograr la gestión de riesgos existen organizaciones quien en su preocupación han emitido diversas publicaciones como el Comité de Basilea, COSO, la Organización Internacional para la Estandarización, Objetivos de Control para las Tecnologías de la Información y Relacionadas, todas ellas en el ánimo de su competencia.

Capítulo II Organizaciones y normas para la gestión de riesgos

La preocupación internacional para tener una estabilidad financiera en lo que compete a la gestión de riesgos ha dado paso a la creación de diversas organizaciones, leyes y normas para asegurar que los bancos cuenten con los elementos necesarios para una correcta gestión de riesgos.

2.1 Comité de Basilea

El Comité de Basilea de Supervisión Bancaria (BCBS, por sus siglas en inglés *Basel Commite on Banking*) de ahora en adelante nos referiremos a él como el Comité o Comité de Basilea fue fundado en 1974, en sus inicios estuvo conformado por el grupo de los 10 Bélgica, Canadá, Francia, Italia, Japón, los Países Bajos, el Reino Unido, los Estados Unidos, Alemania y Suecia, y actualmente está conformado por 27 países, el Comité de Basilea tiene su secretariado en la sede del Banco Internacional de Pagos (*BIS*), el cual fue fundado en la ciudad de Basilea Suiza, del cual tomó su nombre.

El objetivo del Comité de Basilea consiste en mejorar la estabilidad internacional de los bancos a través de recomendaciones que éste emite consideradas como “mejores prácticas internacionales”. Sin embargo, han sido los países quienes han decidido adoptarlas a través de leyes impuestas por sus bancos centrales y otros órganos reguladores, en el caso de México dichas obligaciones son emitidas por el Banco de México y la CNBV.

Desde su creación el Comité de Basilea ha publicado tres acuerdos, los cuales han servido para fortalecer entre otros el capital de los bancos a través de la gestión de riesgos.

2.1.1 Basilea I.

En 1988 fue emitido el acuerdo “Convergencia internacional de medición de capital y estándares de Capital” también conocido como “Acuerdo de capital de Basilea I”, en él se estableció el método para el cálculo del requerimiento de capital por riesgo de crédito, cuya finalidad era asegurar la estabilidad del sistema bancario internacional, así como homogenizar la regulación del sector bancario disminuyendo de esa manera la desigualdad competitiva de los bancos. Si bien dentro de sus características se encuentran el establecimiento mínimo del requerimiento de capital del 8% y la búsqueda

de la estandarización de la constitución del capital básico. Este capital tendría que ser suficiente para absorber las pérdidas derivadas de los riesgos de mercado y crédito.

En esta publicación no se consideraba como parte del requerimiento de capital, la exposición al riesgo operacional y 8% tenía que cubrir la totalidad de los riesgos a los que los bancos se exponían.

2.1.2 Basilea II.

A pesar de que en Basilea I se emitió el requerimiento de capital del 8%, éste sólo consideraba como componente principal al riesgo de crédito y este capital también debería de cubrir al riesgo de mercado. Sin embargo, no se tenía en cuenta la complejidad de los instrumentos que se operaban, dejando de lado además al riesgo operacional. En respuesta a ello en 2004 el Comité publicó el documento “Convergencia internacional de medidas y normas de capital” también conocido como Acuerdo de Basilea II.

El propósito inicial de Basilea II consistía en que los bancos constituyesen un requerimiento de capital más sensible al riesgo y acorde al tipo y niveles de riesgo, esto con la finalidad de ofrecer mayor estabilidad al sector financiero internacional. Una de las características principales es que en el segundo acuerdo se introdujeron tres pilares los cuales consistían en:

Primer Pilar: Requerimientos mínimos de capital.

En este pilar fue contemplada por primera vez la calidad crediticia, además de considerar en el cálculo de requerimiento de capital al riesgo de mercado y al riesgo operacional. Adicional de la integración del requerimiento de capital de esos tres riesgos, se introdujo el cálculo bajo métodos internos, es decir, el Comité establece el capital mínimo con el que deberá de contar el banco, sin embargo este capital podría estar por encima del capital que representaría la exposición de esos tres riesgos ante un escenario adverso, por ello los bancos podrían optar por el uso de métodos internos bajo los cuales sus modelos de riesgo demuestren la conveniencia de su utilización, la implementación de dichos métodos se mantienen a discreción de los reguladores locales así como de los

bancos mismos, cuyo objetivo es incentivar a las instituciones a una gestión de riesgos más adecuada a través de una mayor concientización del riesgo fomentando así a una mayor cultura del riesgo en los bancos a través de la implementación o fortalecimiento de controles.

El índice de capitalización se calcula de la siguiente manera:

$$\text{IC} = \frac{\text{Capital Total}}{\text{Riesgo de Crédito} + \text{Riesgo de Mercado} + \text{Riesgo Operativo}} \geq 8\% \quad 2.1$$

Dónde:

En México el riesgo de Crédito de acuerdo con la CNBV en el Título Primero Bis Requerimientos de Capital de las Instituciones de Crédito de la Circular Única de Bancos CNBV (2019) puede ser calculado bajo las siguientes metodologías:

- Método estándar: basado en ponderadores de crédito, dependiendo del tipo de crédito que se trate.
- Método de Calificaciones Internas: este tipo de método corresponde al que la institución haya optado de acuerdo con sus calificaciones internas en lo que respecta a la calificación de la cartera crediticia y la estimación de reservas preventivas para utilizar este método la institución interesada deberá de realizar una solicitud ante la CNBV.
- Método de Calificaciones Avanzado: este tipo de método corresponde al que la institución haya optado de acuerdo con sus calificaciones internas en lo que respecta probabilidad de incumplimiento, la severidad de la pérdida en caso de incumplimiento, la exposición al incumplimiento y el plazo efectivo o de vencimiento de sus posiciones sujetas a riesgo de crédito, para utilizar este método la institución interesada deberá de realizar una solicitud ante esa Comisión.

En México el riesgo de mercado de acuerdo con lo establecido por la CNBV (2019) puede ser calculado bajo el siguiente método:

- Método estándar: dicho método es basado en ponderadores de riesgo de mercado, en atención a la clasificación de sus operaciones, como lo son operaciones en moneda nacional, en divisas o indizadas a tipo de cambio.

El riesgo operacional puede ser calculado bajo los siguientes cuatro métodos:

- Método del indicador básico: se calcula mediante el 15% del promedio de los últimos 36 meses de los ingresos positivos.
- Método estandarizado: en este caso el requerimiento de capital corresponde a diferentes ponderadores por las ocho líneas de negocio Que son: Finanzas corporativas, Negociación y ventas, Banca minorista, Banca comercial, Pagos y liquidación, Servicios de agencia, Administración de activos Intermediación minorista / operaciones de corretaje al menudeo.
- Método estándar alternativo: al igual que el método estandarizado tiene diferentes ponderadores por la línea de negocio, especialmente para las líneas de negocio de banca minorista y comercial.
- Modelos avanzados internos: corresponde a la medida de riesgo generada por el modelo de evaluación del riesgo operacional de la Institución.

En lo que respecta a los métodos de requerimiento de capital por riesgo operacional serán descritos a mayor detalle en el capítulo 4 de esta investigación. Los métodos mencionados han sido implementados por la CNBV, y son los que en la actualidad rigen el requerimiento de capital en las instituciones Bancarias.

Segundo Pilar.

- Proceso de examen supervisor: En el segundo pilar se enuncian los lineamientos para que los supervisores nacionales implementen las mejores prácticas de esta publicación, con la finalidad de que los bancos se aseguren de que cuenten con los mecanismos para una correcta gestión de riesgos, fortaleciendo las medidas del capital mínimo, el cual, si el Comité así lo solicita, tiene la facultad de requerir

capital adicional a aquellos bancos que no cumplan con lo establecido, es decir, se esperaba que los bancos operasen por encima de los niveles de capital mínimos exigibles. Para el caso en los que bancos optaran por la utilización de métodos internos de cálculo de capital previa autorización de los reguladores locales, en esas recomendaciones se enlistan los requisitos con los que los bancos deberán de cumplir, enfocados principalmente para asegurarse que lleva una gestión de riesgos robusta.

Tercer Pilar.

- Disciplina de mercado: su función principal es garantizar la transparencia informativa que los bancos publican, estableciendo un compendio de requisitos mínimos con los que debe de cumplir la información que es proporcionada por los bancos, cuya finalidad es que esta sea confiable y que exprese la situación que dichas instituciones guardan, esto para que todos los interesados como lo son los inversionistas o clientes tomen decisiones oportunas.

2.1.3 Basilea III.

En los años 2011 y 2013 el Banco Internacional de Pagos realizó la publicación de dos documentos cuyos nombres son Basilea III Marco Regulador Global para reforzar los bancos y sistemas bancarios así como Basilea III: Marco internacional para la medición, normalización y seguimiento del riesgo de liquidez, el objetivo de estos documentos consiste en fortalecer a los bancos para que ante problemas financieros o económicos, se pueda reducir o contener el riesgo al sector sin afectar a la economía, y fue hasta 2017 que el tercer acuerdo de Basilea se publicó el cual consiste principalmente en la corrección de las recomendaciones de las publicaciones previas en lo que respecta al fortalecimiento e incremento del capital requerido, manteniéndose también la estructura de tres pilares y la incorporación de la gestión de la liquidez:

Primer Pilar.

Requerimientos mínimos de capital.

- El capital mínimo con el que los bancos deben de contar se incrementa tanto en cantidad como en calidad, las instituciones deberán de contar con un capital neto el cual contemple los riesgos de crédito, mercado y operacional.

- Se introduce la necesidad de contar con un "colchón de conservación de capital", el cual debe de incrementarse en el momento en que se encuentren condiciones de crecimiento económico del país, permitiendo que se pueda hacer uso de éste en momentos de crisis, o bien, en aquellos casos en los que se incurra en pérdidas, para los casos en los que la situación económica entre en recesión las instituciones no aplicarán este suplemento.

- Colchón contra cíclico de capital: este amerita para los casos en los que se cuente con un crecimiento importante del crédito, se requerirá más capital esto con la finalidad de que se eviten la creación de "burbujas".

- Para aquellos bancos de importancia sistémica[2] mundial la autoridad puede solicitar requerimientos de capital adicionales pudiendo ser un 1%, esto con la finalidad de mejorar su capacidad de pérdida, así como la disuasión de incrementar su importancia sistémica en el futuro.

  Una medida adicional para fortalecer el capital es el coeficiente de apalancamiento, cuya finalidad es el de prevenir un exceso de apalancamiento en el sector bancario.

- Mejora de cobertura de riesgo: una vez revisados los métodos de cálculo para los riesgos de mercado, crédito y operacional, se vuelve más estricta la utilización de los métodos internos de cálculo haciéndolos más restrictivos con el objetivo de disminuir la variabilidad de los cálculos de los activos ponderados por riesgo[3] entre los bancos.

[2] Un banco de importancia sistémica se refiere a aquellas entidades financieras de tamaño grande y con importancia relevante en el sistema financiero que ante una quiebra o desaparición pudiera ocasionar efectos de gran magnitud en la economía de un país o, incluso a nivel internacional.
[3] Los activos ponderados se refieren al total de los activos de la institución financiera, que son ponderados por el tipo de riesgo

En lo que respecta al requerimiento de capital por riesgo operacional y ante la propuesta del Comité de Basilea de reducir el uso de métodos internos para su cálculo ha derogado los cuatro métodos: Método del Indicador Básico, Método Estandarizado, Método Estandarizado Alternativo y los Métodos Avanzados Internos por medio de las reformas modificatorias de Basilea III, esto en respuesta a evitar que bancos de importancia sistémica ante escenarios adversos pongan en peligro la economía mundial y a su vez, que los bancos con menor participación puedan tener una reducción del requerimiento de capital, todo ello a través de la implementación de un solo Método Estándar.

Este cambio tiene implicaciones principales para los datos internos de pérdida de los bancos y cómo podrían ser usados para derivar valor de negocio y perspectiva de la administración del riesgo.

Los objetivos específicos de la reforma incluyen:

- Simplificar la estructura de Basilea mediante reemplazar los cuatro enfoques actuales con un solo enfoque estandarizado.
- Hacer la estructura más sensible al riesgo mediante combinar una medida de ingresos brutos con la historia de pérdidas internas a 10 años del banco.
- Facilidad para comparar los activos ponderados por riesgo de banco a banco mediante remover la opción para usar múltiples enfoques y modelos internos.

El Método Estándar se basa en los siguientes componentes:

- El indicador del negocio o *Business Indicator* (BI), que es una aproximación al riesgo operacional basada en los estados financieros.
- El componente indicador del negocio o *Business Indicator Component* (BIC), que es calculado mediante multiplicar el BI por un conjunto de coeficientes marginales determinados regulatoriamente.

• El multiplicador de pérdidas internas o *Internal Loss Multiplier* (ILM), que es un factor escalonado que se basa en las pérdidas históricas promedio del banco y el BIC.

Actualmente, en México aún no se ha implementado el uso del indicador emitido por el Comité, siendo los métodos de Basilea III previos a las reformas modificatorias los que se mantienen vigentes.

Segundo pilar.

Requerimientos complementarios: en respuesta a la crisis de 2008, se tuvieron que fortalecer las normas en materia del buen gobierno y gestión del riesgo en el conjunto de la entidad, riesgo de las posiciones fuera de balance y actividades de titulización, gestión de las concentraciones de riesgos, incentivos a los bancos para gestionar mejor el riesgo y los rendimientos a largo plazo, prácticas adecuadas de remuneración, prácticas de valoración, pruebas de tensión, normas de contabilidad para instrumentos financieros, gobierno corporativo, colegios de supervisores.

Tercer Pilar.

Requerimientos revisados de divulgación: ante las lecciones aprendidas se establecieron nuevos requisitos que están relacionados con las posiciones de titulización y con el patrocinio de vehículos fuera de balance. Se exigió una divulgación más detallada de los componentes del capital regulador y su conciliación con las cuentas declaradas, así como una explicación pormenorizada sobre cómo calcula el banco sus coeficientes de capital regulador.

- Liquidez: adicional a las modificaciones que sufrieron los tres pilares, surgió la necesidad de contar con un estándar internacional de liquidez, a pesar de que los bancos contaban con niveles adecuados de capital, tuvieron dificultades para administrar su liquidez, esto derivado de la facilidad con la que se podía obtener fondeo a través de tasas bajas, los momentos de tensión económica ameritaron

que bancos centrales intervinieran para asegurar el funcionamiento de los mercados así como el rescate de instituciones.

Durante los momentos de crisis se dejó entrever, puntos de mejora a los marcos de Basilea es por eso por lo que en 2008 el Comité publicó: “Los principios para la adecuada gestión y supervisión del riesgo de liquidez”, una de las características principales de dicha publicación consiste en la introducción de dos indicadores: el coeficiente de cobertura de liquidez y el coeficiente de financiación estable neta.

En México como lo menciona (Haro, Medición y control de riesgos financieros, 2018) El Coeficiente de Cobertura de Liquidez (CCL) es un indicador cuyo objetivo es garantizar que las instituciones no se vean afectadas por un período de 30 días, que en caso de tensiones los bancos cuenten con activos líquidos y de alta calidad.

El CCL se calcula de la siguiente manera:

$$CCL = \frac{Activos\ líquidos}{Salidas\ netas\ de\ efectivo\ bajo\ escenario\ de\ estrés\ de\ 30\ días} \qquad 2.2$$

El nivel requerido debe de ser mayor o igual al 100%
El coeficiente de financiación estable neta (CFEN) es un indicador cuya función es promover que los bancos cuenten con liquidez en un periodo de por lo menos de un año.

$$CFEN = \frac{Fondeo\ Estable\ disponible}{Fondeo\ Estable\ disponible\ requerido} \qquad 2.3$$

El nivel requerido debe de ser mayor o igual al 100%.

2.1.4 Evolución de los acuerdos de Basilea.

Tabla 1 Evolución de los acuerdos de Basilea.

Basilea I	***Basilea II***	***Basilea III***
Requerimiento de Capital de riesgo de crédito de un mínimo del 8%	Se establecen tres Pilares	Se mantienen tres Pilares
También consideraba al riesgo de mercado	I Pilar Requerimiento de Capital: el cual consideraba la calidad crediticia, al riesgo de mercado y al riesgo operacional, se introdujeron métodos internos como incentivos para mejorar la cultura de riesgo en los bancos.	I Pilar Requerimiento de Capital: se vuelven más estrictos los modelos internos, es obligatorio contar con "colchones de capital" y "colchón anticíclico de capital" para poder enfrentar procesos de alta tensión.
	II Pilar Proceso de examen supervisor: lineamientos para que los supervisores nacionales implementen mejores prácticas. Se esperaba que los bancos operasen por arriba de los límites permitidos.	II Pilar Proceso de examen supervisor: lineamientos para que los supervisores nacionales implementen mejores prácticas. Se esperaba que los bancos operasen por arriba de los límites permitidos.
	III Pilar Disciplina del mercado: con la finalidad de garantizar la calidad y confiabilidad de la información que los bancos publican.	III Pilar Disciplina del mercado: con la finalidad de garantizar la calidad y confiabilidad de la información que los bancos publican.
		Liquidez, se establecen dos indicadores para garantizar la liquidez de los bancos: CCL cuyo objetivo es garantizar que las instituciones no se vean afectadas por un período de 30 días y CFEN cuya función es promover que los bancos cuenten con un periodo de por lo menos un año.

Elaboración propia con información emitida por el Comité de Basilea (Comité de Supervisión Bancaria de Basilea, 2003), (Comité de Supervisión Bancaria de Basilea, 2010), (Comité de Supervisión Bancaria de Basilea, 2015) y (Comité de Supervisión Bancaria de Basilea, 2017)

2.1 *COSO*

Adicional al Comité de Basilea, existen otros organismos que tienen la misma finalidad como lo es el *Commite of Sporing Organizations of the Treading* mejor conocido como COSO la cual es una organización que fue creada en 1985 por los representantes de cinco organizaciones privadas cuyo objetivo principal es la gestión del riesgo empresarial, el control interno y la disuasión del fraude. (COSO, 2019)

Fundada en 1985 en EE. UU., promovida por malas prácticas empresariales de los años anteriores, COSO estudia los factores que pueden dar lugar a información financiera fraudulenta, y elabora textos y recomendaciones para todo tipo de organizaciones y entidades reguladoras como el SEC (Agencia Federal de Supervisión de Mercados Financieros).

A continuación, se enuncian las cinco organizaciones patrocinadoras de COSO.

- La Asociación Americana de Contabilidad (*AAA)* por sus siglas en inglés[4].
- El Instituto Americano de Contadores Públicos Certificados[5] (*AICPA*) por sus siglas en inglés.
- Ejecutivos de Finanzas Internacionales [6](*FEI*) por sus siglas en inglés.
- Instituto Americano de Auditores Internos[7] (*IIA*) por sus siglas en inglés.
- La Asociación Nacional de Contadores Administrativos[8] (*IMA*) por sus siglas en inglés.

2.2.1 COSO I Marco Interno Control Interno.

Las organizaciones preocupadas por resolver sus problemáticas internas y externas establecieron mecanismos de control bajo sus propios criterios, esto originó que existiera

[4] Asociación Americana de Contabilidad: es una organización que apoya la educación contable, la investigación y la práctica.
[5] Instituto Americano de Contadores Públicos Certificados: es una organización que se encarga de establecer estándares éticos para ejercer la profesión de contabilidad y de la auditoría.
[6] Ejecutivos de Finanzas Internacionales: su principal función es la gestión financiera corporativa de altos ejecutivos de instituciones financieras.
[7] Instituto Americano de Auditores Internos: es una organización especializada, en la formación y actualización continua para el desarrollo profesional de sus miembros.
[8] Asociación Nacional de Contadores Administrativos: la misión de la asociación es la educación y el desarrollo en la contabilidad y finanzas de gestión.

una divergencia de conceptos entre organizaciones y esto ocasionaba confusiones. Ante estas problemáticas en 1992 COSO publicó el primer informe llamado "*International of Control Integrated*" mayormente conocido como COSO I, este documento estaba enfocado principalmente a establecer un marco conceptual para el control interno y evitar así divergencias.

En COSO I se definió al control interno como *"un proceso, ejecutado por la junta directiva o consejo de administración de una entidad, por su grupo directivo (gerencial) y por el resto del personal, diseñado específicamente para proporcionarles seguridad razonable de conseguir en la empresa las tres siguientes categorías de objetivos*

1) *Efectividad y eficiencia de las operaciones*
2) *Suficiencia y confiabilidad de la información financiera*
3) *Cumplimiento de las leyes y regulaciones aplicables"* (Gaitán, 2015, pág. 27)

El proceso de control interno se debe de entender como intrínseco a los sistemas y procesos de la organización, y no separados de estos, el cual se encuentra alineado a los objetivos que en sí mismos se buscan como institución. Es decir, se debe de considerar al control interno como parte de la operatividad y no como un mero formalismo para el cumplimiento de la normativa interna y externa.

Componentes del Sistema de Control Interno.

El sistema de control interno está compuesto por cinco componentes que son: Ambiente de Control, Evaluación de Riesgos, Actividades de Control, Información y Comunicación, Supervisión y Seguimiento. Para el correcto funcionamiento del sistema de control interno, es indispensable que se garantice que todos sus componentes funcionen efectivamente, así como el involucramiento de todos los miembros de la organización.

Ambiente de Control.

Este componente de control se refiere a las actividades que la empresa realiza para estimular el control en las actividades que todo el personal ejecuta. La importancia de este componente es esencial para que el resto de los componentes de control puedan ejecutarse, pues en él se plantea el sustento de cada uno de éstos, además en él se provee de disciplina y estructura para que el sistema de control funcione como lo son:

- La estructura de las actividades del negocio
- La asignación de autoridades y responsabilidades
- La organización y el desarrollo de las personas
- Se comparten y se comunican los valores
- Se concientiza al personal de la importancia del control

El consejo y la alta dirección son los responsables de establecer dicho ambiente de control, a través de la importancia del control interno y los estándares de conducta que se esperan de los empleados.

El ambiente de control a su vez cuenta con elementos que coadyuvan a su cumplimiento como lo son:

- La integridad y los valores éticos, en él se establecen los valores éticos y el comportamiento bajo el cual se conducirán todos los miembros de la organización.
- El compromiso a ser competente: se refiere a todos los conocimientos y habilidades con el que debe de contar el personal en él también se busca el crecimiento y el desarrollo humano, manteniendo al personal capacitado, motivado y comprometido con la organización.
- Las actividades de la junta directiva y el comité de auditoría: estos órganos son quienes definen los criterios del ambiente de control, es indispensable que la alta gerencia se encuentre altamente comprometida con el control y su ejercicio en la organización.
- La mentalidad y estilo de la operación de la gerencia: los factores más relevantes son las actitudes mostradas hacia la información financiera, el procesamiento de la información, los principios y los criterios contables.

- La estructura de la organización: se refiere a la naturaleza, objetivos y necesidades de la organización.

Una manera para asegurarse de que se cuenta con un ambiente de control efectivo es que se están alcanzando los objetivos que ha definido la organización, y que además sí es ejecutado por todos los niveles de la organización.

Evaluación de riesgos.

La identificación y análisis de los riesgos de una organización, es fundamental para determinar qué situaciones adversas pudieran ocurrir que impidan que los objetivos sean alcanzados.

Previo a la evaluación de riesgos es de suma importancia la definición de objetivos que tiene la institución, para que se conozca qué es lo que se pretende identificar y evaluar agentes que impidan la consecución de los objetivos.

"En toda entidad, es indispensable el establecimiento de objetivos tanto globales como de la organización como de actividades relevantes, obteniendo con ello una base sobre la cual sean identificados y analizados los factores de riesgo que amenazan su oportuno cumplimiento" (Gaitán, 2015, pág. 31).

El manejo de los riesgos debe ser planteado como una responsabilidad de los miembros de la organización, pues de ello depende el logro de los objetivos específicos y, por consiguiente, de los globales.

Existen diversas categorías de objetivos, los cuales son:

- *Objetivos de cumplimiento:* se refiere a todos aquellos objetivos que se adhieren a leyes, reglamentos e incluso políticas internas emitidas por la organización.
- *Objetivos de la información financiera*: son todos aquellos donde su propósito es la consecución de la información financiera.

- *Objetivos de operación: este* tipo de objetivos son establecidos para asegurar la eficacia y efectividad de los procesos de la organización.

El logro de los objetivos de cumplimiento y de información financiera pueden asegurarse de una manera razonable, con el establecimiento de controles internos efectivos, no así para el alcance de los objetivos de operación, pues en estos pueden ocurrir eventos fuera del ente de control.

El manejo para el análisis de riesgos por lo menos debe de incluir:

- La estimación y la importancia del riesgo y sus efectos
- La evaluación de la probabilidad de ocurrencia
- El establecimiento de controles o en su defecto las acciones de mitigación
- Una evaluación periódica y permanente del manejo de los riesgos

El manejo de riesgos inicia por la alta gerencia, para que todas las áreas operativas puedan manejarlas, y el papel del auditor ayuda al cumplimiento.

En la evaluación de riesgos, COSO plantea que las Instituciones deben de considerar que se encuentran expuestas a riesgos tanto internos como externos, dichos riesgos pueden ser políticos, económicos, sociales, tecnológicos y ambientales.

Actividades de control.

Las actividades de control a las que COSO se refiere son realizadas por la alta gerencia y todas las demás personas responsables de la ejecución de las actividades a realizar.

Estas actividades son llevadas a cabo a través del establecimiento de políticas y procedimientos, bajo los cuales deberán de ejecutarse todas las actividades de la organización garantizando de esa manera que se estén realizando de acuerdo a esos lineamientos, que los riesgos se están administrando y como consecuencia, que los objetivos se puedan cumplir.

Es decir, todas las actividades de control son ejecutadas con la finalidad de administrar los riesgos, y por ende en beneficio de la organización. "*Las actividades de control son importantes no sólo porque en sí mismas implican la manera correcta de hacer las cosas,*

sino debido a que son el medio idóneo de asegurar en mayor grado el logro de los objetivos" (Gaitán, 2015).

Existen diversos tipos de control de acuerdo al momento en el que se ejecutan o por su propósito a continuación se enuncian algunos de ellos:

- *Controles Detectivos*: este tipo de controles tienen como propósito detectar eventos antes de que ocurran. Las características de este tipo de controles es que detienen el proceso porque aíslan la causa del riesgo, pero no las evitan, es decir, ayudan a vigilar al proceso. El uso de este tipo de controles para las organizaciones resulta costoso pues implica el reproceso de las actividades.

- *Controles Preventivos*: este tipo de controles están diseñados para prevenir los eventos y con ello se reduce la probabilidad de que estos ocurran. A diferencia de los controles detectivos evitan las causas y como su uso es prevenir que los eventos ocurran, estos controles resultan menos costosos porque reduce el reproceso de actividades.

- *Controles Correctivos*: este tipo de controles son diseñados para una vez que los eventos ocurran estos se puedan corregir a través de su ejecución, el uso de estos controles normalmente se usa por la carencia de controles detectivos, ayudando a identificar las causas de los eventos, así como su corrección. De todos los tipos de controles este es el más costoso, pues implica destinar recursos para lograr identificar las causas de los eventos, para poder corregirlo y en muchos casos realizar reprocesos.

Sistemas de información y comunicación.

Este componente de control interno se encuentra en toda la organización, está conformado a su vez por dos tipos de control que son los controles generales y los controles de aplicación. (Gaitán, 2015)

- *Controles generales:* este tipo de controles tienen como finalidad asegurar la continuidad de las operaciones de la organización, como lo son el control sobre el centro de procesamiento del hardware y del software, así como la operación propia.

- *Controles de aplicación:* este tipo de controles están dirigidos principalmente al interior de cada sistema y su finalidad es garantizar el procesamiento, integridad y confiabilidad, mediante la autorización y validación correspondiente. Estos controles también abarcan las aplicaciones destinadas a las interfaces con otros sistemas de los que reciben o entregan información.

Esta información normalmente es conformada por información financiera, y aunque es útil no deben de basarse las decisiones de la organización sólo en ella, pues si bien la información contable puede dar un panorama claro de lo sucedido en la organización, no es suficiente para anticipar lo que sucederá en el futuro.

“Los sistemas producen reportes que contienen información operacional, financiera y de cumplimiento que hace posible conducir y controlar la organización. Todo el personal debe recibir un claro mensaje de la alta gerencia de sus responsabilidades sobre el control”. (Gaitán, 2015, pág. 37)

Los elementos que a su vez conforman al componente de la información son:

- *Sistemas integrados a la estructura*: se refiere a que los sistemas se encuentran inmersos en las operaciones de las organizaciones, además de que a través de ellos surgen estrategias de negocio, así como su uso como herramientas de control.
- *Sistemas integrados a las operaciones*: a través de ellos se realiza la ejecución de las operaciones.
- *Calidad de la información*: la información para que pueda utilizarse como un control, es indispensable que esta sea oportuna, actualizada, razonable y

accesible, si se cumple con estas características la información puede resultar útil para la toma de decisiones.

En lo que se refiere a la comunicación, es indispensable que se definan los canales de comunicación en todos los niveles de la organización, así como comunicar a la alta dirección para que esta conozca los aspectos relevantes del sistema de control, y también los eventos críticos. La comunicación no debe de limitarse al interior de la organización, sino también al exterior como lo es a entidades reguladoras, ya sea para obtener o proporcionar información relacionada con eventos, clientes, proveedores entre otros. (Gaitán, 2015)

Existen diversos tipos de comunicación:

- *Comunicación formal*: se refiere a las políticas procesos y procedimientos, suelen utilizarse manuales, circulares, instructivos, entre otros.
- *Comunicación informal*: se refiere a la coordinación de actividades de asuntos relevantes de acuerdo con el perfil de riesgos de la institución. .
- *Canales de comunicación:* este tipo de canales pueden ser abiertos o cerrados, tanto internos como externos, lo que se pretende con el uso de este tipo de comunicación es saber cuál es la imagen corporativa de la organización, así como el clima laboral.

La información y comunicación se refiere a que se debe de identificar, recopilar y comunicar la información que deberá de ser informada al Consejo de Administración, esto con la finalidad de poder controlar la organización, y así tomar decisiones adecuadas, respecto al uso y aplicación de los recursos, para ello es preciso contar con información adecuada y oportuna.

Supervisión y monitoreo.

Las organizaciones se encuentran en constante cambio, tanto por factores internos como externos, pudiendo ocasionar que un control que inicialmente se había identificado como

eficiente al paso del tiempo puede considerarse como ineficiente, es por ello por lo que los controles requieren ser supervisados de manera constante.

Por controlar se entiende como un proceso que compara lo ejecutado con lo programado, con la finalidad de identificar posibles desviaciones y con base en ello establecer medidas correctivas. El propósito de los controles es asegurar el cumplimiento de objetivos organizacionales.

Con la finalidad de garantizar que el sistema de control interno de una organización está funcionando correctamente, deben de someterse a revisiones los componentes y los elementos que forman parte del sistema de control interno. Las evaluaciones pueden llevarse a cabo dentro de las operaciones diarias por las personas que las ejecutan o por personal independiente a ellas, o bien, en la combinación de esas dos.

Las evaluaciones a los componentes de control pueden ser realizadas por personal de la organización, normalmente suele ser Auditoría Interna, por externos a través de Auditores Externos, ambos emiten el resultado de evaluación por medio de informes o seguimiento a eventos previamente identificados. También suelen desarrollarse a través del sistema de información gerencial por medio de autoevaluaciones. Con independencia del medio que la organización haya optado de la evaluación del sistema de control, la información que se obtenga en términos de hallazgos debe de ser siempre informada a niveles superiores ya sea comités o la junta directiva, así como a los propietarios de los controles con la finalidad de que estos implementen las acciones necesarias.

Los sistemas de control interno requieren supervisión, es decir, establecer un proceso que compruebe que se está realizando el mantenimiento adecuado al sistema de control interno, esto se consigue mediante actividades de supervisión continua, evaluación periódica o una combinación de ambas cosas.

Las actividades de monitoreo: Rodrigo Estupiñán (2015) lo define como “la evaluación continua y periódica que hace la gerencia de la eficacia del diseño y operación de la

estructura de control interno para determinar si está funcionando de acuerdo a lo planeado y que se modifica cuando es necesario" (pág. 42).

El monitoreo se puede realizar durante la ejecución de las operaciones, realizándose actividades de supervisión o administración permanente.

Para que se pueda garantizar que el sistema de control interno está funcionando adecuadamente se deben de garantizar al menos que:

- Se cuenta con evidencia de que el personal que participa en la ejecución de control lo realiza.
- La información que el personal menciona es consistente con la de la información externa.
- Asegurar que se hayan implementado controles derivado de hallazgos identificados por auditores internos o auditores externos.
- Si las revisiones que ejecutan los auditores internos son adecuadas, efectivas y confiables.

2.2.2 COSO II ERM.

En 2004 se creó el *"Enterprise Risk Management-Integrated Framework*" en español conocido como Marco Integrado de Gestión de Riesgos, lo que se conoce más comúnmente como COSO II. En este marco se amplía el concepto de control interno a la gestión de riesgos, involucrando necesariamente a todo el personal, incluyendo a los directores y a los administradores. Cabe aclarar que este marco no sustituye a COSO I Marco Integrado, sino que lo complementa.

La irregularidad que salió a relucir en la primera década de los dos miles por el caso *Enron*, que como es conocido esta empresa cometió fraude al maquillar sus estados financieros aprovechando lagunas en las leyes contables, esto con la finalidad de ocultar pérdidas de la compañía. Este fraude se logró llevar a cabo con la colusión entre los auditores externos de la empresa *Arthur Andersen* y los contadores de *Enron*. La

gravedad del evento viene dada porque no sólo se ocultaron pérdidas, sino que se agregaron supuestas ganancias con subsidiarias de Enron, colocando acciones en la bolsa con precios sobrevalorados ocasionando que el público inversionista comprara acciones, que tras la revelación del fraude su precio se desplomó drásticamente, generando enormes pérdidas para sus compradores. Esto dio lugar a que los sistemas de control interno fueran todavía más relevantes y estrictos, pues estos eventos dejaron al descubierto deficiencias en los controles internos y externos, pues permitió que se maquillasen los balances.

Las irregularidades antes mencionadas dieron origen a que los gobiernos interpusieran normas más estrictas, en Estados Unidos el presidente *Bush* solicitó al congreso la promulgación de la ley “Sarbanaes-Osley”, en esta ley se establece de manera formal el control gubernamental, tanto interno como externo, así como la responsabilidad del control interno.

> *La Ley Sarbanes-Oxley, conocida también como SarOx o SOA (por sus siglas en inglés Sarbanes Oxley Act), es la ley que regula las funciones financieras contables y de auditoría y penaliza en una forma severa, el crimen corporativo y de cuello blanco. Debido a los múltiples fraudes, la corrupción administrativa, los conflictos de interés, la negligencia y la mala práctica de algunos profesionales y ejecutivos que conociendo los códigos de ética, sucumbieron ante el atractivo de ganar dinero fácil y a través de empresas y corporaciones engañando a socios, empleados y grupos de interés, entre ellos sus clientes y proveedores* (interamerican-usa.com, 2002).

El ERM del COSO II es conocido como el estándar para cumplir con la sección 404 de la ley *Sarbanes–Oxley*, que hace referencia entre otros, a la responsabilidad de la gerencia para establecer y mantener una estructura de control interno adecuado y procedimientos para los informes financieros, y tener una evaluación, a la fecha del cierre del año fiscal, de la efectividad de la estructura de control interno adecuado y de los procedimientos de los informes financieros. (Castro, 2004)

Rodrigo Estupiñán define a la Gestión de Riesgos Empresariales como (Gaitán, 2015, pág. 74):

> “un proceso efectuado por la junta de directores, la administración y otro personal de la entidad, aplicado en la definición de la estrategia y a través del emprendimiento, diseñado para identificar los eventos potenciales que pueden afectar a la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, para proveer seguridad razonable en relación con el logro del objetivo de la entidad”

Como se puede apreciar en esta definición, se define al ERM como un proceso que coadyuva a lograr el fin de la organización y no un objetivo en sí mismo, el cual debe de ser ejecutado por todo el personal, tomando como eje a la estrategia organizacional. Este sistema se encuentra diseñado principalmente para identificar aquellos eventos que pudieran afectar o impedir el logro de los objetivos de la entidad, cuando se menciona una seguridad razonable sobre los riesgos se refiere a no tener un exceso de controles, pero tampoco a asumir riesgos innecesarios, de ahí radica que estos eventos potenciales se mantengan dentro del apetito al riesgo que la organización haya establecido.

La metodología ERM se encuentra orientada a la generación de valor para los dueños o accionistas, lo cual tiene como finalidad garantizar la vigencia de la organización, así como de su imagen en el largo plazo, para mantener su solidez y atracción del público inversionista.

> “Gobierno Corporativo es un medio por el cual la sociedad puede estar segura de que las grandes corporaciones son instituciones que operan bien y en las cuales los inversionistas y prestamistas pueden confiar sus fondos”. (Mantilla, 2005, pág. 180)

El Gobierno Corporativo y el ERM se encuentran en la misma línea enfocada al control operativo, legal, financiero y logístico. Para evitar caer en los errores del pasado este debe de mantenerse independiente de la Junta Directiva o Consejo de Administración no

teniendo relación con los controles administrativos y contables evitando de esa manera el conflicto de interés.

En esta publicación también se complementa la manera en cómo se planean y evalúan los controles dando prioridad a la administración de riesgos, en ella se mantienen los cinco componentes de control interno de COSO I y se agregaron tres nuevos componentes, quedando finalmente: Ambiente de Control, Evaluación de Riesgos, Actividades de Control, Información y Comunicación, Supervisión, Establecimiento de objetivos, Identificación de eventos y Respuesta a los riesgos.

La adición de tres componentes identificación de eventos, valoración de riesgos y respuesta a los riesgos, hacen hincapié en la importancia en la gestión del riesgo dentro de una organización.

Establecimiento de objetivos.

Al realizar la definición de la misión y visión de una organización, inherentemente se hace el establecimiento de los objetivos estratégicos, bajo el cual como su nombre lo sugiere se eligen las estrategias y los objetivos para lograrlas, estos también se encuentran vinculados con la operatividad de la organización y cuya finalidad es garantizar la efectividad y la eficiencia de las actividades.

Identificación de eventos.

Ante la incertidumbre de no conocer los eventos que pudieran ocurrir, dónde, cómo y cuándo sucederán, así como los factores internos y externos que influyen para que estos sucedan, resulta indispensable realizar una identificación de eventos potenciales que pudieran afectar a la organización.

Existen diferentes metodologías para identificar esos eventos potenciales los cuales están basados en eventos pasados o bien, la anticipación de eventos futuros, que pudieran afectar positiva o negativamente a la organización representando así los riesgos inmediatos, mediatos o de largo plazo.

Estas metodologías se desarrollarán a detalle en el Capítulo 3.

Respuesta a los riesgos.

Este componente de control interno identifica y evalúa las actividades que se realicen como respuesta a los posibles riesgos, considerando los factores probabilidad e impacto. Todas las actividades que se ejecuten como respuesta al riesgo deberán de ser contemplando el apetito al riesgo que la organización definió.

Las respuestas a los riesgos van enfocadas a evitar, reducir, compartir y aceptar el riesgo.

Monitoreo.

Si bien este componente de control interno no fue adicionado de las cinco iniciales que COSO I planteaba, COSO II planteó las siguientes reglas para un correcto monitoreo (Gaitán, 2015, pág. 79):

- Obtención de evidencia de que existe una cultura a la identificación del riesgo
- Si las comunicaciones externas corroboran las internas
- Si se realizan comparaciones periódicas
- Si se revisan y se hacen cumplir las recomendaciones de los auditores
- Si las capacitaciones proporcionan realidad de lograr una cultura del riesgo
- Si el personal cumple las normas y procedimientos y es cuestionado
- Si son confiables y efectivas las actividades de la auditoría interna y externa

A continuación, se muestra la comparación entre COSO I y COSO II.

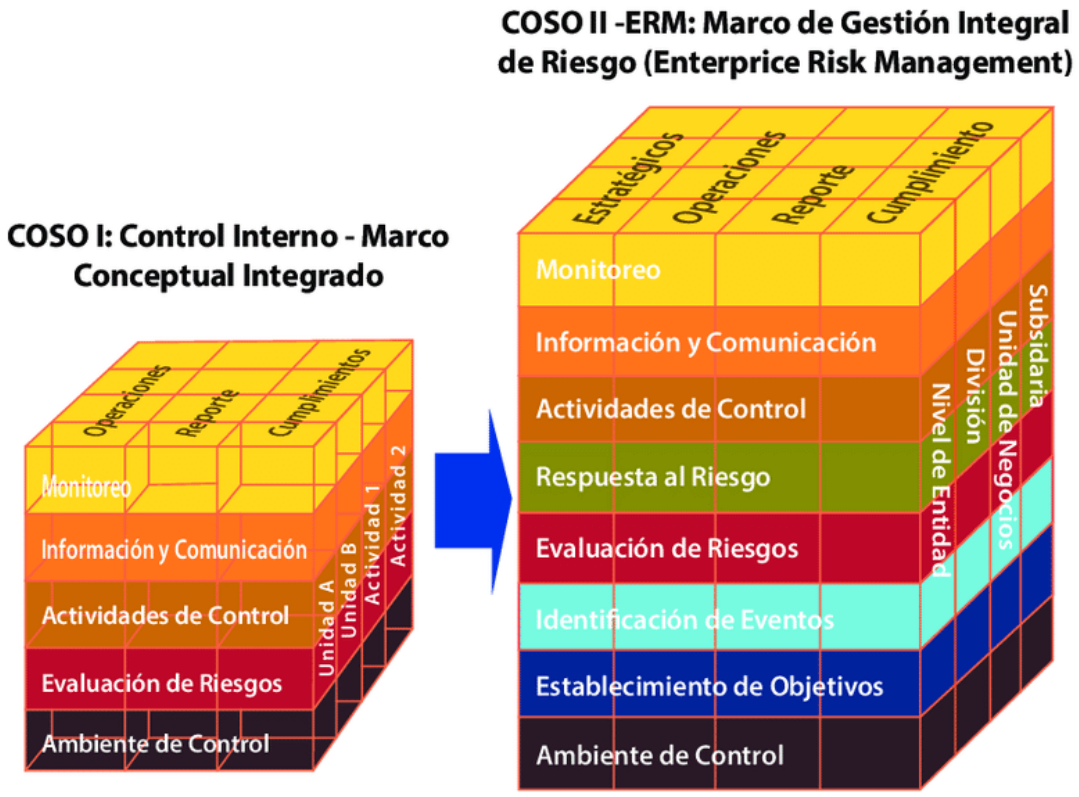

Figura 1. (Vega, 2017) Se muestra de manera visual comparación entre COSO I y COSOII, si bien ambos están basados en principios el enfoque es diferente, el primero busca asegurar un adecuado funcionamiento de las actividades de la organización bajo el sistema de control interno, mientras que el segundo está enfocado principalmente a la consecución del valor de la organización.

En la cara superior del cubo o columnas se muestran los objetivos de operaciones, reporte y de cumplimiento, mientras que los cinco componentes son representados por las filas, y por último la estructura organizacional que está en la tercera dimensión. Por lo tanto, todos los componentes de control interno se encuentran relacionados a los objetivos para poder alcanzarlos, mismos que requieren ser ejecutados por las unidades o áreas de la organización, es decir, para garantizar el correcto funcionamiento ninguno de esos tres elementos puede ser ejecutado aisladamente.

2.2.3 COSO III Marco Integrado de Control Interno.

La variación de los tipos de negocio ante un mundo globalizado, el incremento de la normatividad y su complejidad, el aumento en las expectativas de los inversionistas y reguladores para la prevención y detección de fraudes, así como el mayor uso de tecnologías y su constante desarrollo derivaron en la necesidad de realizar una actualización del Marco de Control Interno Integrado COSO I.

El 14 de mayo de 2013 el “nuevo” COSO Marco Integrado de Control Interno o COSO III fue publicado, reemplazando así a COSO I de 1992. La publicación de COSO II “Gestión de riesgos corporativos y la publicación Control Interno – Marco Integrado son publicaciones complementarias y una no sustituye a la otra aún cuando se mencionan partes de control interno y de riesgos en ellas, y si bien abordan áreas comunes el enfoque es distinto. Un sistema de control interno ayuda a que las entidades puedan lograr sus objetivos, así como a mantener e incluso mejorar su rendimiento.

El Marco se enfoca en grupos de interés tanto internos a través del consejo y la dirección, como de externos que interactúan con la entidad con sus respectivas funciones.

Para los grupos de interés internos, el Marco cuenta con un enfoque basado en principios flexibles, es decir, que van más allá del cumplimiento de políticas y procedimientos, para ello es indispensable el criterio y juicio profesional, tanto de los dueños de los riesgos mismos como de las áreas de control.

Una de las principales características de COSO III es el reconocimiento de la importancia de los objetivos, para ello los componentes de control interno expresan lo que se necesita para alcanzarlos y la estructura organizacional de la entidad que se requiere.

Más allá de los cinco componentes de control interno, COSO III estableció 17 principios, mismos que asoció a cada uno de los cinco componentes con la finalidad de asegurar que sean empleados adecuadamente.

A continuación, se muestran los principios asociados a cada uno de ellos:

Entorno de control.

1. La organización demuestra un compromiso con la integridad y valores éticos.
2. El Directorio demuestra independencia en la Administración y supervisa el desarrollo y cumplimiento del control interno.
3. La Administración establece con el Directorio la supervisión de las estructuras, las líneas de reportes y los sistemas de autoridad y responsabilidad para el logro de los objetivos.
4. La Organización demuestra un compromiso para apoyar a la Administración en la utilización de recursos suficientes para lograr reportes financieros externos confiables.
5. La Organización tiene personas responsables para el control interno en este proceso y el logro de los objetivos contemplados en los reportes financieros externos.

Evaluación de riesgos.

6. La organización especifica los objetivos con la suficiente claridad para permitir la identificación y evaluación de los riesgos en relación con los objetivos.
7. La Organización identifica los riesgos para el logro de los objetivos a través de toda la empresa y analiza los riesgos como una base para determinar cómo estos deberían de ser administrados.
8. La Organización considera el potencial de fraude en la evaluación en los riesgos para el logro de los objetivos.
9. La Organización identifica y mide los cambios que podrían impactar significativamente el sistema de control interno *(SCI).*

Actividades de control.

10. La Organización selecciona y desarrolla el control de actividades que contribuyen a la mitigación de los riesgos para el logro de los objetivos a niveles aceptables.
11. La Organización selecciona y desarrolla controles generales para actividades de tecnología para soportar el logro de objetivos.
12. La Organización despliega control de actividades por medio de políticas que establecen lo que se espera y procedimientos que componen las políticas de acción.

Información y comunicación.

13. La Organización obtiene o genera y usa información relevante y de calidad para soportar el funcionamiento de control interno.
14. La Organización internamente comunica la información, incluyendo objetivos y responsabilidades para el control interno.
15. La Organización comunica a partes externas materias relativas al Control Interno.
16. La Organización selecciona, desarrolla y ejecuta tanto monitoreo en línea como posteriores para evaluar si los componentes del COSO están presentes y funcionando.
17. La Organización evalúa y comunica las deficiencias de control interno en forma oportuna a quienes son responsables de hacer las correcciones, incluyendo a la Alta Administración y al Directorio

En lo que se refiere al Marco de control interno COSO III es la publicación vigente para asegurar el correcto funcionamiento de los sistemas de control interno de las organizaciones.

2.2.4 COSO IV ERM- Integrando Estrategia y Desempeño.

La última crisis económica y financiera de 2009, es un claro ejemplo de la importancia de la gestión del riesgo empresarial y de las consecuencias de tener o no, un buen gobierno corporativo en la gestión de riesgos dentro de las empresas que garantice su adecuado

funcionamiento, ya que ante la presencia de eventos críticos una organización que cuenta con una correcta gestión de riesgos, tiene mejor capacidad de respuesta porque conoce sus riesgos y por tanto, sabe qué hacer ante su ocurrencia y facilita la toma de decisiones, reduciendo así los impactos negativos, por el contrario de una institución que carezca de una gestión de riesgos o bien, que no cuente con la más adecuada, puede tener una respuesta tardía o inadecuada y por ende, el impacto podría ser mayor.

Los riesgos cada vez más complejos tanto internos como externos entrelazados y conjugados con el cambio en el mercado y el entorno político, nuevas y cada vez más exigencias regulatorias además de los riesgos que surgen con la incorporación de nuevas tecnologías, se suman a las incertidumbres de las empresas, lo cual exige una respuesta estratégica como reacción a eventos previstos y a crisis.

Todo esto dio como consecuencia la actualización del documento de 2004 el Marco Integrado de la Gestión del Riesgo Empresarial también conocido como ERM, el cual lleva por título Gestión del Riesgo Empresarial-Integrando Estrategia y Desempeño publicado en 2017, este marco hace énfasis en la importancia del riesgo además del proceso, en la estrategia, y la ejecución del desempeño.

Las principales características de la actualización del Marco son las siguientes:

- Mayor compresión de la generación de valor en la gestión del riesgo empresarial al momento de definir y ejecutar la estrategia.
- Presenta diferentes maneras de concebir el riesgo para definir y alcanzar objetivos.
- Es adaptable a la evolución de las tecnologías y a la proliferación de datos y análisis para facilitar la toma de decisiones.
- Proporciona definiciones, componentes y principios básicos para que todos los niveles que participan en la gestión del riesgo ya sea en su diseño, implementación y ejecución de técnicas de gestión del riesgo empresarial.

La importancia de la gestión del riesgo empresarial en la planificación estratégica es la consideración de los eventos que pudieran impedir alcanzar los objetivos, para ello es

imperativa su integración en todos y cada uno de los niveles de la organización para garantizar el correcto desempeño en todos los departamentos y funciones.

A diferencia de COSO II, los componentes ya no se muestran en un cubo, sino en una cadena que entrelaza cinco componentes y sus principios asociados, los cuales se mantienen en todo el flujo de la operación.

Gestión del Riesgo Empresarial ERM COSO IV

Figura 2 Imagen obtenida de (*Committee of Sporing Organizations of the Treadway Comission*, 2007, pág. 6)

El marco está constituido por cinco componentes que se encuentran interrelacionados en todo el flujo de la gestión del riesgo empresarial.

A continuación, se muestra cada uno de los cinco componentes y a qué se refieren:

- Gobierno y cultura: El Gobierno refuerza la importancia de la gestión del riesgo empresarial y establece responsabilidades de supervisión al respecto. En lo que respecta a la cultura hace referencia a los valores éticos de la institución, a los comportamientos deseados y a la comprensión del riesgo en la entidad.

- Estrategia y establecimiento de objetivos: bajo este enfoque, la estrategia y el establecimiento de objetivos funcionan juntos en el proceso de planificación estratégica, es aquí también donde se establece un apetito al riesgo, es decir, en este punto se define qué tanto riesgo la institución estaría dispuesta a asumir, y este se alinea con la estrategia; los objetivos del negocio ponen en práctica a la

estrategia al tiempo que sirven de base para identificar, evaluar y responder ante el riesgo.

- Desempeño: para garantizar el buen desempeño es necesario identificar y evaluar aquellos riesgos que puedan afectar a la consecución de los objetivos estratégicos y de negocio de la institución, una vez que se identificaron es necesario priorizarlos en función de su gravedad en el contexto del apetito al riesgo que la entidad estableció y posteriormente, decidir las respuestas ante los riesgos, el resultado de este proceso debe de ser comunicado a las principales partes interesadas en el riesgo.

- Revisión y monitorización: Una vez establecido el proceso de definición de estrategia y de negocio, así como de la identificación y priorización de los riesgos, la respuesta ante ellos, se requiere examinar el desempeño de la entidad, una organización puede determinar el desempeño de los componentes de gestión del riesgo empresarial en el tiempo en un entorno de cambios sustanciales, y qué aspectos son susceptibles de revisar y modificar para mejorar la gestión, lo anterior para garantizar que se cuenta con herramientas vigentes de la administración.

- Información, comunicación y reporte: La gestión del riesgo empresarial requiere ser un proceso continuo y permanente de obtención e intercambio de la información necesaria, tanto de fuentes internas como son las áreas operativas y de control de la entidad, fuentes externas, por ejemplo, auditores externos, entidades reguladoras, de tal manera que la información fluya hacia arriba, hacia abajo y de manera vertical a lo largo de todos los niveles de la organización. Contar con información oportuna y confiable puede ayudar a la toma de decisiones.

Los cinco componentes establecidos en el marco actualizado se encuentran respaldados por un conjunto de principios, la adhesión a estos principios puede proporcionar, a la dirección y al consejo, una expectativa razonable de que la organización entiende y se

esfuerza por gestionar los riesgos asociados con su estrategia y los objetivos de la empresa.

A continuación, se presentan los principios que respaldan cada uno de los componentes:

Principios asociados al componente de Gobierno y Cultura.

- Ejerce la supervisión de riesgos a través del consejo de administración: Se refiere a que el consejo de administración supervisa la estrategia para apoyar a la dirección en la consecución de los objetivos estratégicos y de negocio.
- Establece estructuras operativas: La organización establece estructuras operativas que permitan alcanzar los objetivos estratégicos y de negocio que la entidad haya establecido, es decir, todas y cada una de las personas que integren a la institución, así como las actividades que estas desempeñen serán en función de la consecución de esos objetivos.
- Define la cultura deseada: La organización define los comportamientos deseados que caracterizan la cultura a la que aspira la entidad, dicho de otra manera, se establece el comportamiento que deben de tener los empleados de la institución.
- Demuestra compromiso con los valores clave: La organización demuestra su compromiso con los valores clave de la entidad, es decir las acciones que la entidad realiza deben de cumplir siempre con los valores de la entidad.
- Atrae, desarrolla y retiene a profesionales capacitados: la organización está comprometida a contar con el capital humano adecuado el cual debe de estar alineado con los objetivos estratégicos y de negocio, así mismo es capaz de retener a los más capaces.

Principios asociados al componente de Estrategia y Establecimiento de Objetivos.

- Analiza el contexto empresarial: La organización tiene en consideración los efectos potenciales del contexto empresarial sobre el perfil de riesgo que la entidad ha asumido, es decir, se mantiene en constante análisis de las circunstancias de las empresas que le pudieran ayudar a evitar o reducir impactos negativos, aprovechar oportunidades, lo cual pudiera modificar su perfil al riesgo.

- Define el apetito al riesgo: La organización define el apetito al riesgo bajo el contexto de la creación, preservación y materialización del valor.
- Evalúa estrategias alternativas: La organización evalúa las estrategias alternativas y el impacto potencial en el perfil de riesgos.
- Formula objetivos de negocio: La organización considera el riesgo, así como el establecimiento de los objetivos de negocio en los distintos niveles, alineados y apoyados en la estrategia.

Principios asociados al componente de desempeño.

- Identifica el riesgo: La organización identifica el riesgo que pudiera impactar en la consecución de los objetivos estratégicos y de negocio.
- Evalúa la gravedad del riesgo: La entidad evalúa la gravedad que el riesgo pudiera tener.
- Prioriza riesgos: La organización prioriza los riesgos para tomarlo como base a la hora de seleccionar las respuestas a adoptar ante los riesgos.
- Implementa respuestas ante los riesgos: La organización identifica y selecciona las respuestas ante los riesgos con base en su apetito al riesgo.
- Desarrolla una visión a nivel de cartera: La organización desarrolla y evalúa una visión del riesgo a nivel de cartera.

Principios asociados al componente de Revisión y Monitorización.

- Evalúa los cambios significativos: La organización de manera constante identifica y evalúa los cambios que pueden afectar significativamente el alcance de los objetivos estratégicos y de negocio.
- Revisa el riesgo y el desempeño: La organización revisa el desempeño de la entidad a través de que se hayan alcanzado los objetivos, teniendo en consideración el riesgo en todo momento.
- Persigue la mejora de la gestión del riesgo empresarial: La organización se encuentra en una constante lucha por mejorar la gestión del riesgo empresarial, esto porque entiende que los riesgos a los que se expone no son estáticos y que pueden aparecer nuevos.

Principios asociados al componente de Información, Comunicación y Reporte.

- Aprovecha los sistemas de información y la tecnología: La organización utiliza los sistemas de información y tecnología con los que cuenta la entidad para lograr una adecuada gestión del riesgo empresarial.
- Comunica información sobre riesgos: La organización utiliza los canales de comunicación como soporte a la gestión del riesgo empresarial.
- Informa sobre el riesgo, la cultura y el desempeño: La organización comunica sobre el riesgo, la cultura y el desempeño a múltiples niveles y a través de toda la entidad.

2.2.5 Comparación entre las publicaciones COSO I, COSO II, COSO III y COSO IV.

A continuación, se presenta la comparativa de las cuatro publicaciones de COSO a lo largo del tiempo, así como sus principales características para una mejor compresión.

Tabla 2 Comparación de COSO a través del tiempo

COSO I Marco Integrado 1992	COSO II ERM 2004	COSO III Marco Integrado 2013	COSO IV ERM 2017
Cinco componentes: 1. Ambiente de control 2. Evaluación de riesgos 3. Sistemas de información y comunicación 4. Actividades de control 5. Supervisión y monitoreo	**Complementa a COSO I** **Ocho componentes:** 1. Ambiente de control 2. Evaluación de riesgos 3. Eventos 4. Valoración de riesgos 5. Respuesta al riesgo. 6. Sistemas de información y comunicación 7. Actividades de control 8. Supervisión y monitoreo	**Sustituye a COSO I y Complementa COSO II ERM** **Cinco componentes:** 1. Ambiente de control 2. Evaluación de riesgos 3. Sistemas de información y comunicación 4. Actividades de control 5. Supervisión y monitoreo **Inclusión de 17 principios COSO**	**Complementa a COSO II** **Cinco componentes** 1. Gobierno y cultura 2. Estrategia y objetivos 3. Desempeño 4. Revisión y monitorización 5. Información, comunicación y reporte **Se incluyeron 20 principios**

Tabla 2 Elaboración propia con información de COSO (2019)

2.3 Otras metodologías especializadas

La Organización Internacional para la Estandarización de ahora en adelante se referirá a esta como ISO, "*comenzó en 1946 cuando delegados de 25 países se reunieron en el Instituto de Ingenieros Civiles de Londres y decidieron crear una nueva organización internacional "para facilitar la coordinación internacional y la unificación de estándares industriales". El 23 de febrero de 1947, la nueva organización, ISO, comenzó oficialmente sus operaciones*" (ISO) en Ginebra, Suiza. Actualmente, cuenta con una membresía de 164 países, este es un organismo que define las normas y regulaciones para la fabricación, comercio y la comunicación, con lo cual se busca garantizar la calidad y seguridad de los productos que se fabrican.

ISO cubre la mayoría de los sectores y cuenta con vastos estándares, dentro de los más populares se encuentran: la Gestión de Calidad (serie ISO 9000), la Gestión del medio ambiente (serie ISO 14000), la Gestión de responsabilidad social (norma ISO 26000) y la Gestión de riesgos (serie ISO 31000)**.**

Por otro lado, Objetivos de Control para las Tecnologías de la Información y Relacionadas "*COBIT*" por sus siglas en inglés *Control Objectives for Information and related Technology* es una guía de mejores prácticas presentada como marco de referencia, que se encuentra dirigida al control y supervisión de tecnología de la información, esta guía cuenta con una serie de recursos que pueden servir de modelo de referencia para la gestión de Tecnologías de la Información, incluyendo un resumen ejecutivo, un *framework,* objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

"El objetivo de *COBIT* es brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentar las actividades de una manera manejable y lógica." (Asociación Española para la Calidad)

Estas prácticas están enfocadas más al control que a la ejecución, gestores, auditores, y usuarios que se benefician del desarrollo de *COBIT* porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

Conocer las diversas instituciones que fueron creadas con la intención de gestionar el riesgo y el entorno de control de diferentes organizaciones ya sea través de mejores prácticas internacionales o por medio de leyes, normas y regulaciones, es fundamental, en primera instancia para conocer cuáles son elementos mínimos con los que se deben de cumplir para evitar sanciones e incluso la imposibilidad de realizar operaciones y por otro lado tener en consideración los lineamientos con los cuales se debe de realizar la administración de los riesgos.

Capítulo III Modelo de gestión

Una vez definidos los diferentes tipos de riesgos, sus categorías y diferentes metodologías, enfoques y autoridades reguladoras, se toman los elementos de cada una de ellas para realizar una propuesta de la gestión del riesgo operacional la cual busca más allá del cumplimiento normativo el alcance de objetivos de una institución a través de una robusta gestión del riesgo que lleve a la reducción de pérdidas, optimización de procesos e incremento de beneficios.

3.1 Líneas de defensa

En la actualidad, es común que las organizaciones cuenten con equipos cuya finalidad es gestionar el riesgo, tales como lo son los auditores internos, especialistas en riesgo y de control, oficiales de cumplimiento e investigadores de fraude, cada uno de estos equipos tienen habilidades y enfoques únicos. Por ello, es indispensable sentar las bases de las responsabilidades que tienen estas figuras en el papel de la administración de riesgos, pues el más grande desafío es lograr sinergia entre cada una de ellas, esto con la finalidad de asegurar de que no se están omitiendo riesgos importantes para la organización así como que no existe duplicidades, todo esto en el sentido de lo que busca el control interno que es la eficacia y la eficiencia de la operaciones, lo mismo sucede para las áreas encargadas del control. Las responsabilidades deben de ser claras y específicas, de modo que cada grupo de profesionales entienda los límites de sus responsabilidades y conocer el rol que tienen dentro de la estructura general de riesgos y control de la organización.

El desarrollo de una RAS[9] eficaz debe ser guiado por el liderazgo, es decir, verticalmente «de arriba a abajo» por parte del Consejo y de la participación «de abajo a arriba» de la Gerencia. Si bien la Alta Dirección puede iniciar la definición del apetito por el riesgo, su correcta aplicación depende de la interacción entre el Consejo, la Alta Dirección, la gestión del riesgo y las unidades operativas.

Con la finalidad de evitar esa incorrecta segregación de funciones el Comité de Basilea ha establecido los principios del gobierno corporativo para los bancos, y en estos (Comité de Supervisión Bancaria de Basilea, 2015) se plantea el modelo de tres líneas de defensa, todas ellas desempeñando en el ámbito de sus funciones la gestión del riesgo.

- La primera línea de defensa: las unidades de negocio son consideradas la primera línea de defensa ya que estas son quienes asumen los riesgos y son responsables de su gestión continua, así como de identificar, evaluar y notificar las exposiciones al riesgo, teniendo en cuenta el apetito por el riesgo del banco, sus políticas, procedimientos y controles. La manera en que la primera línea de negocio ejecuta sus responsabilidades debe reflejar la cultura de riesgo[10] que el banco haya definido.
- La segunda línea de defensa: incluye una función de gestión del riesgo independiente de la primera línea de defensa la cual complementa las actividades de riesgo de las líneas de negocio mediante las responsabilidades de seguimiento y notificación. Entre otras cosas, es responsable de vigilar las actividades que implican asunción de riesgos en el banco, así como evaluar los riesgos y problemas independientemente de la línea de negocio, divulgar el riesgo a nivel de empresa, dentro de esta línea también se encuentra cumplimiento. La función debe realzar la importancia de la Alta Dirección y de los jefes de las líneas de negocio en la identificación y evaluación críticas de los riesgos, y no depender únicamente de la vigilancia realizada por la función de gestión del riesgo. La función de financiación desempeña un papel fundamental a la hora de garantizar

[9] RAS se refiere al escrito del nivel agregado y de los tipos de riesgo que una Institución está dispuesta a asumir a fin de lograr sus objetivos de negocio.
[10] Se refiere al conjunto de normas, actitud y comportamiento de un banco relativos a la concienciación, asunción y gestión del riesgo.

que el rendimiento y los resultados empresariales se reflejan y comuniquen con precisión al Consejo, la Gerencia y las líneas de negocio que utilizarán dicha información como base de sus decisiones sobre riesgo y negocio.

- La tercera línea de defensa: esta función es llevada a cabo por Auditoría Interna, con acciones como son las propias auditorías internas, dichas revisiones deben ser basadas en riesgos, todo ello para garantizar al Consejo que el marco de gobierno y riesgos con el que cuenta la institución funciona adecuadamente, y de esa manera asegurar que son aplicadas tanto las políticas como los procesos.

La importancia de las auditorías internas es que proporcionan una revisión independiente y objetiva sobre la calidad y eficacia del sistema de control interno del banco, la primera y segunda línea de defensa, así como del marco de gobierno del riesgo, incluidos los vínculos a la cultura organizativa, la planificación estratégica y empresarial, retribución y procesos de toma de decisiones. Los auditores internos deben ser competentes y estar adecuadamente formados y no participar en el desarrollo, implementación u operatividad de la función de gestión del riesgo u otras funciones de la primera o segunda línea de defensa para evitar conflicto de interés.

El Consejo tiene la obligación de garantizar que las funciones de gestión del riesgo, cumplimiento y auditoría interna están adecuadamente posicionadas, que cuentan con los recursos suficientes y que desempeñan sus responsabilidades de forma independiente, objetiva y eficaz. Todo esto al vigilar el marco de gobierno del riesgo, bajo la revisión periódica de sus principales políticas y funciones con la Alta Dirección y con los jefes de las funciones de gestión del riesgo, cumplimiento y auditoría interna para identificar y abordar riesgos y asuntos significativos, así como determinar áreas de mejora.

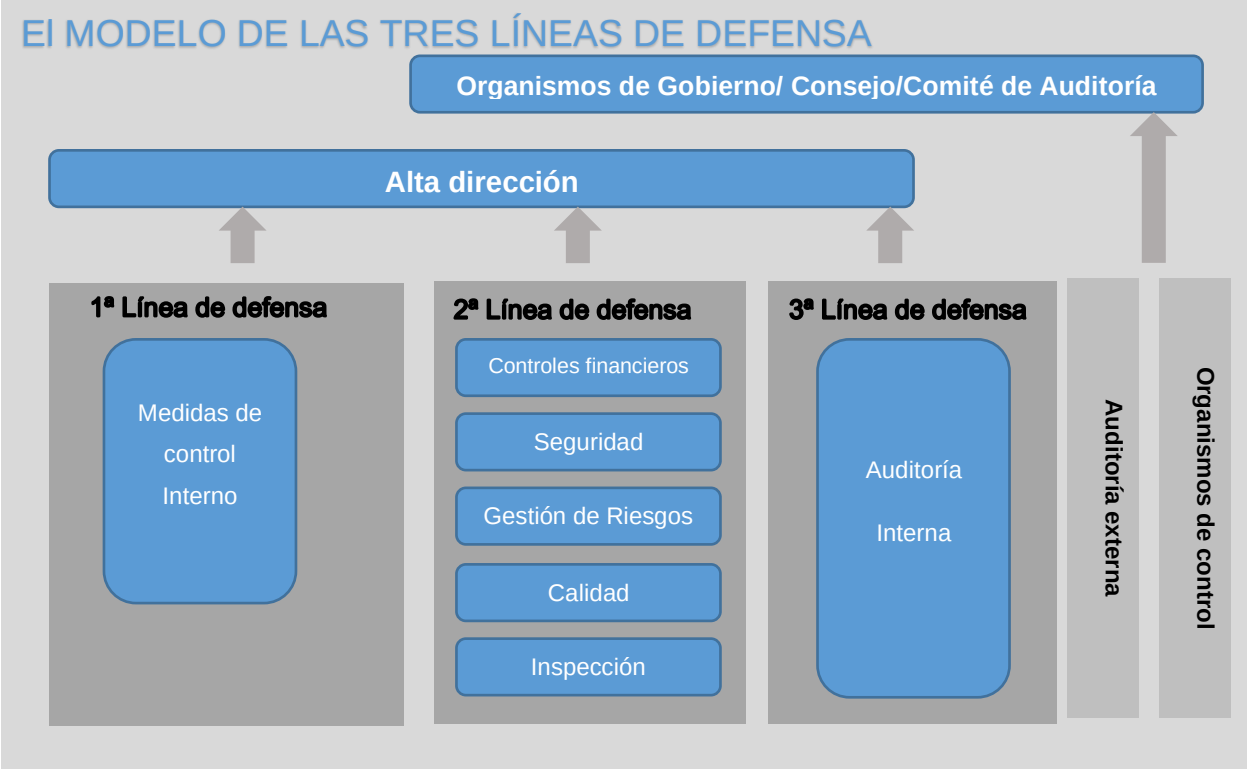

Figura 3 Modelo de las tres líneas de defensa. Tomado del documento emitido por la IIA: IIA Declaración de posición: las tres líneas de defensa para una efectiva gestión de riesgos y control.

3.2 Flujo de gestión del riesgo operacional

Una vez definido el modelo de tres líneas de defensa para la gestión de riesgo, se precisarán las etapas para llevar a cabo la administración del riesgo operacional, del cual se propone que se realice en seis fases o etapas que son: identificación de riesgos, evaluación de riesgos, monitoreo de riesgos, mitigación a los riesgos identificados, registro de eventos y retroalimentación de diferentes fuentes de información.

Para mantener un modelo de administración de riesgo operacional el flujo o ciclo de gestión debe ser dinámico, es decir, tiene que estar en constante actualización, porque el contexto en el que una institución se encuentra es cambiante, en sus procesos, productos, clientes, tecnología y el entorno externo; por ello, las instituciones pueden

estar expuestas a nuevos riesgos o bien, permanecer con los mismos riesgos a un mayor o menor impacto.

El flujo de administración del riesgo operacional propuesto responde a los elementos para el cumplimiento de la publicación de COSO IV ERM y de los acuerdos de Basilea, este último a su vez, a la adecuación de la Comisión Nacional Bancaria y de Valores por medio de la Circular Única de Bancos (2019), todo ello complementado con diversos métodos para contar con elementos suficientes que garanticen que cada una de las herramientas utilizadas en las etapas del flujo son adecuadas para la administración del riesgo operacional.

Figura 4: Flujo de administración del riesgo operacional. Elaboración propia

3.2.1 Identificación de riesgos.

La definición de la estrategia como se ha mencionado es la parte fundamental para identificar eventos potenciales que pudieran impedir que se lleve a cabo y, por ende, que no se alcancen los objetivos de la institución.

Para realizar la identificación de esos eventos se propone realizarla por medio de la utilización del método FODA o DAFO. Esta metodología fue diseñada para facilitar la toma de decisiones, inventada por el *Ingeniero Químico Albert S. Humphrey* de la

Universidad de *Illinois* y MBA por *Harvard* en la Universidad de *Stanford* (EE. UU.) en los años 70. (Huerta D. S., 2017)

El análisis DAFO o FODA, como se le conoce en países hispanohablantes y SWOT en los países angloparlantes el acrónimo inglés de *Strengths, Weaknesses, Opportunities* y *Threats*, fue desarrollado en una investigación de *Stanford*, ésta consistía en conocer las fallas de la planificación corporativa.

Durante el proceso de la investigación y a la pregunta de ¿qué es bueno y malo para cumplir los objetivos organizacionales?, se llegó a la conclusión de lo que es bueno en el presente es Satisfactorio, lo que es bueno en el futuro es una Oportunidad, lo que es malo en el presente es una Debilidad y lo que es malo en el futuro es una Amenaza, de la inicial de cada una de esas respuestas tomó el nombre de SWOT, en español se denomina FODA, este, al igual que en inglés cada una de las letras de su nombre corresponde a un atributo de la herramienta: Fortalezas, Oportunidades, Debilidades y Amenazas.

El análisis a través del método FODA indica la situación actual que una organización o que una persona tiene, este método puede utilizarse antes de crear una empresa, desarrollar un nuevo proyecto, ante cambios internos o externos a la organización.

Para poder realizar un análisis FODA de manera completa se emplean otros métodos que permitan contar con un panorama integral de todas las exposiciones al riesgo a las que el banco pudiera estar, en primer lugar, se identificarán las oportunidades y amenazas, fortalezas y debilidades, a través del estudio del microentorno y macroentorno, y un profundo análisis interno de la Institución. Con la información obtenida se construiría la Matriz FODA o DAFO, en tercer lugar, se realizará el Análisis CAME [11] y, por último, se definirán y planificarán las acciones a implementar en función de la estrategia de la compañía. (Huerta D. S., 2017)

[11] CAME: metodología complementaria del análisis FODA que se refiere a Corregir, Afrontar, Mantener y Explotar

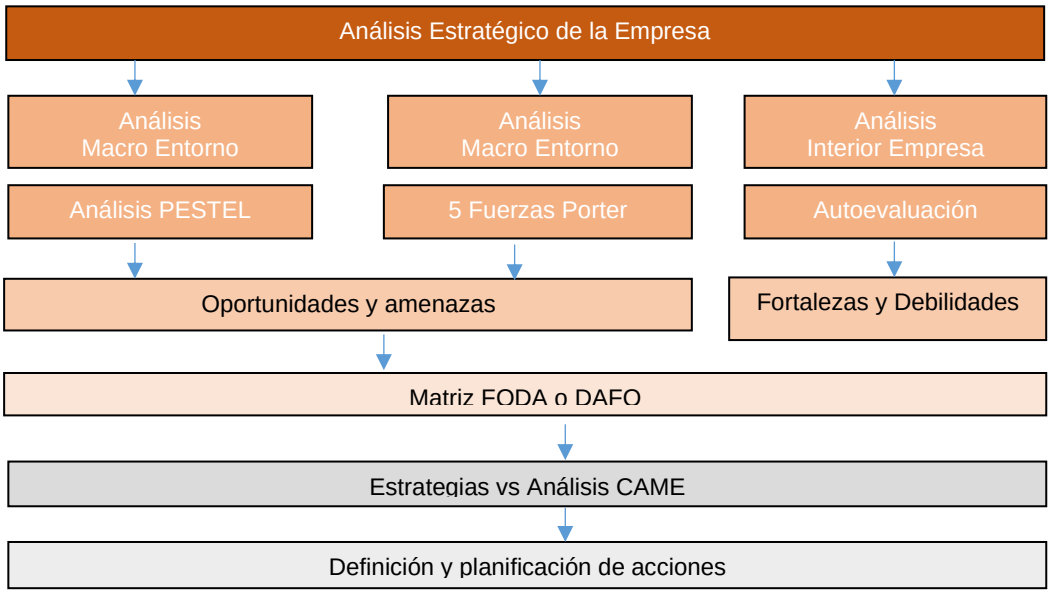

Figura 5: Fases proceso Análisis FODA o DAFO y pasos posteriores (Huerta D. S., 2017) recuperado de https://foda-dafo.com/

Identificación de Oportunidades y Amenazas.

Como se mencionó, para realizar el análisis externo es necesario englobar tanto el análisis de microentorno como del macroentorno con el fin de buscar oportunidades y amenazas que el banco podría tener en el panorama más amplio, para llevar a cabo la identificación de los factores internos que son las oportunidades y las amenazas a través de los entornos antes mencionados, se utilizarán la herramienta PESTEL para el primero y el segundo por medio de la utilización del método de las 5 fuerzas de Porter.

Análisis Externo: Macroentorno (PESTEL).

Para realizar el análisis de las amenazas y oportunidades del macroentorno, el cual consiste en el estudio de aquellas variables políticas, económicas, sociales, tecnológicas, ecológicas y legales que pudieran afectar a una empresa fuera de su entorno a esto se le conoce como análisis **PESTEL.**

> *Por primera vez el término PEST fue utilizado por Francisco Aguilar en su libro de 1967 «Análisis del entorno empresarial». El acrónimo PEST hace referencia a los*

Factores Políticos, a los Factores Económicos, a los Factores Sociológicos y a los Factores Tecnológicos que afectan a una compañía desde su macro-entorno.

El «EL» a el término PEST, dando lugar al término PESTEL, se añadió por Liam Fahey y V.K. Narayanan en su libro, publicado en 1986, «Análisis Macro-ambiental en Gestión Estratégica». El «EL» añadido a hace referencia a los Factores Ecológicos y a los Factores Legales, ambos de creciente importancia en los últimos tiempos. (Huerta, 2017)

Algunos ejemplos de factores que se pueden convertir en amenazas y oportunidades vinculadas al macroentorno serían:

- Políticas: Las diferentes políticas de los gobiernos nacionales y locales, la política fiscal de los diferentes países, modificaciones de los tratados comerciales, cambios de partidos políticos en los gobiernos y sus ideas sobre la sociedad y la empresa.
- Económicas: Ciclos económicos, la política económica del gobierno, la inflación y la tasa de desempleo.
- Sociales: Estructura de edades cambiantes de la población, la estructura familiar en permanente transformación, cambios geográficos de la población, población con mejor preparación y mayor diversidad (racial, discapacidad, opción sexual, religión).
- Tecnológicos: realidad virtual y realidad aumentada, impresiones en 3D, IOT (*Internet of Things* o internet de las cosas) y vehículos autónomos.
- Ecológicos: escasez de materias primas, aumento de la contaminación, intervención del gobierno, leyes de protección medioambiental, regulación sobre el consumo de energía, conciencia social ecológica actual y futura.
- Legales: leyes sobre el empleo, derechos de propiedad intelectual, leyes de salud y seguridad laboral, sectores protegidos o regulados, certificaciones y acreditaciones necesarias para ejercer y privacidad de los usuarios.

Análisis Externo: Microentorno

Para poder realizar un análisis del entorno más cercano a la empresa para la que se realiza el análisis DAFO o FODA, se puede utilizar una herramienta para *determinar las Amenazas y Oportunidades del microentorno que son las 5 fuerzas de Porter. Este método fue desarrollado por Michael Porter en 1979, Porter fue graduado en Ingeniería Aeroespacial por la Universidad de Princeton y obtuvo un* MBA con distinción por la Harvard Business School, seguido por un *Ph.D*. en Economía Empresarial por la Universidad de *Harvard* (Harvard Bussines School, 2020), el consideraba que la rivalidad con los competidores viene dada por cuatro elementos o fuerzas que son: las amenazas de nuevos competidores, el poder negociador de los clientes, la amenaza de nuevos productos o servicios, y el poder negociador de los proveedores.

Porter (2008) en su publicación “Las cinco fuerzas competitivas que le dan a la estrategia” define a las 5 fuerzas como sigue:

Fuerza 1: Poder de negociación de los clientes o compradores.

Esta fuerza se refiere a las amenazas y oportunidades que los clientes representan para la empresa, como lo es la alta concentración de compradores, el control de precios que están dispuestos a pagar por los bienes y servicios, también ante la facilidad con la que los clientes cambiarían por un proveedor de mayor y mejor calidad.

Fuerza 2 Poder de negociación de los proveedores o vendedores.

Este se refiere a una amenaza impuesta sobre la industria por parte de los proveedores, a causa del poder que estos disponen, ya sea por su grado de participación en el mercado, por las características de los insumos que proveen, por el impacto de estos insumos en el costo de la industria, entre otros. Dado de que es (Porter, 2008) natural de que los proveedores deseen cobrar los precios más altos por sus productos, surge una lucha de poder entre las empresas y sus proveedores. La ventaja va hacia el lado que tiene más opciones y menos que perder si la relación termina.

Fuerza 3: Amenaza de nuevos competidores entrantes.

Este punto se refiere a las barreras de entrada de nuevos productos y/o competidores, es decir la facilidad o dificultad que un nuevo competidor puede experimentar cuando quiere empezar a operar en una industria. Cuanto más fácil sea entrar, mayor será la amenaza.

Fuerza 4: Amenaza de productos sustitutos.

La competencia depende de la medida en que los productos de una industria sean reemplazables, esto puede surgir por diversos factores como lo son: la propensión del comprador a sustituir, precios relativos de los productos sustitutos, costo o facilidad de comprador por cambiar de proveedor, nivel percibido de diferenciación de producto o servicio, disponibilidad de sustitutos cercanos, así como suficientes proveedores, por mencionar algunos.

Fuerza 5: Rivalidad entre los competidores.

Esta fuerza se considera como el resultado de las cuatro fuerzas anteriores. La rivalidad define la rentabilidad de un sector: cuántos menos competidores se encuentren en un sector, normalmente será más rentable económicamente y viceversa.

Todos los factores anteriores convergen en la rivalidad, que para Porter es un cruce entre la guerra activa y la diplomacia pacífica. Pueden atacarse mutuamente, o tácitamente acordar coexistir, tal vez incluso formar alianzas.

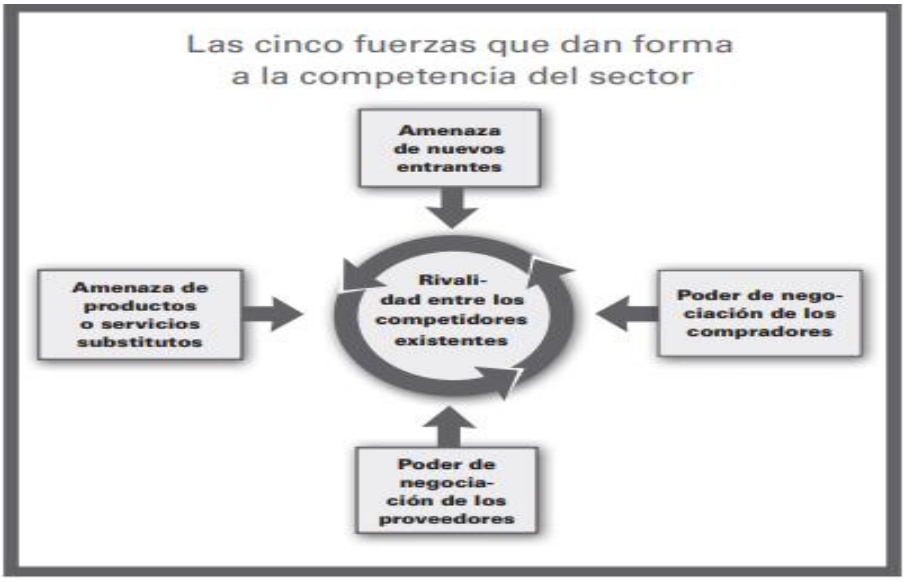

Figura 6 Las cinco fuerzas que dan forma a la competencia del sector (Porter, 2008)

Una vez analizado el macroentorno y el microentorno, es importante que se seleccione sólo aquellas oportunidades y amenazas que se consideren más relevantes a la hora de generar ventajas o desventajas competitivas para el negocio con la finalidad de tratar a los más relevantes.

Debilidades y Fortalezas (Análisis Interno).

Para la realización del análisis interno de una empresa se propone realizarse con la identificación de las debilidades y fortalezas, que generen ventajas o desventajas competitivas y que atañen a aspectos organizativos, de recursos, activos, calidad y/o percepción de los consumidores, lo ideal es que este proceso se lidere por personal interno, pues es quien mejor conoce el contexto de la organización y que no sea una única persona la que llegue a estas conclusiones, sino que se rodee y pida opinión a otras personas involucradas en la situación para contar con un panorama más amplio, como puede ser otros miembros de comité de dirección, compañeros, empleados, proveedores, clientes o incluso a una pareja o amigos cercanos en caso de un análisis FODA o DAFO personal.

- Fortalezas: se trata de aquellos puntos donde la empresa se encuentra bien o incluso mejor que los competidores, como puede ser poseer propiedad, tecnología

principal, capacidad de fabricación, capacidad de financiación, habilidades y recursos superiores, instalaciones modernas, costes unitarios bajos y buena rentabilidad por mencionar algunos.

- Debilidades: son los aspectos que limitan o reducen la capacidad de desarrollo efectivo de la estrategia de la empresa y que por tanto constituyen un serio problema para la organización que debe ser superado, ejemplos de ello es que no exista una dirección estratégica clara, incapacidad de financiación, falta habilidades o capacidades clave, atraso, exceso de problemas operativos internos, instalaciones obsoletas, costes unitarios elevados y rentabilidad insuficiente.

Completar la Matriz FODA o DAFO.

Otro investigador que también aportó fue *Heinz Weihrich Heinz Weihrich* (1982), el creador de la famosa Matriz de 4 cuadrantes que se utiliza cada vez que realiza un análisis FODA y que enfrenta los factores internos (fortalezas y debilidades) con los factores externos (oportunidades y amenazas).

Una vez que se cuenta con todas las debilidades, fortalezas, oportunidades y amenazas seleccionadas se recomienda que el siguiente paso sea asignar prioridades para eliminar aquellas con menor intensidad de cara a centrarse en aquellas más importantes, es decir cuáles generarían más valor o bien, las que pudieran tener un mayor impacto negativo en el banco. Posteriormente cumplimentamos la matriz FODA o DAFO.

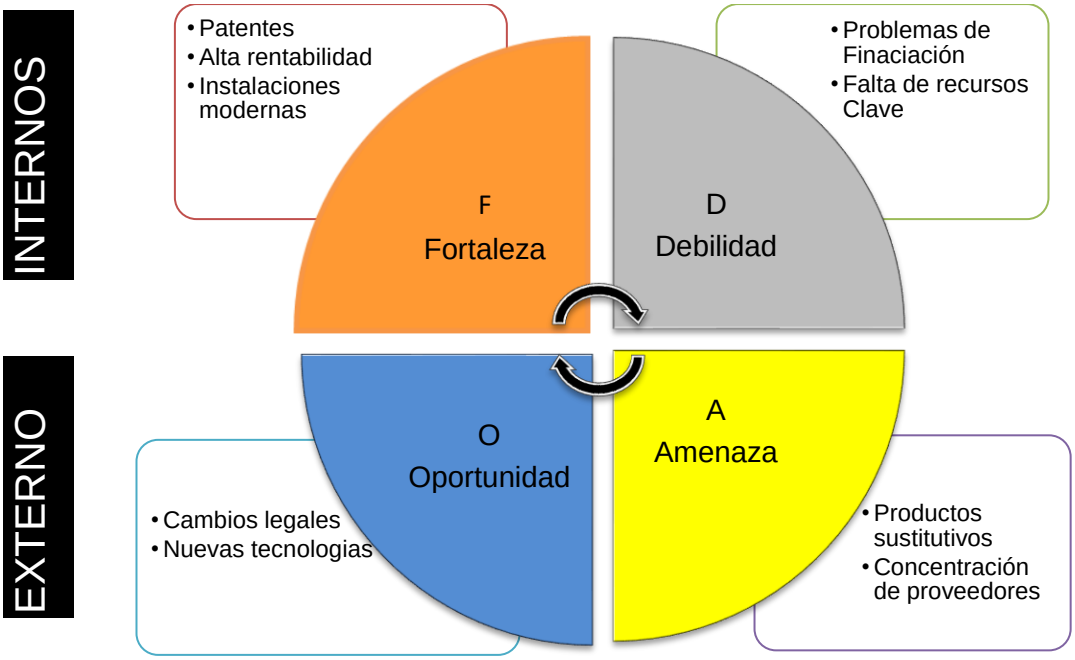

Figura 7 Matriz FODA o DAFO por sus siglas en inglés (Huerta D. S., 2017)

Como se ha repetido a lo largo del documento, la columna vertebral de la identificación de los riesgos operacionales es conocer el objetivo de la empresa, y la estrategia a utilizar para poder alcanzarlo, y una vez expuestos los métodos que ayudan a identificar las oportunidades y amenazas, fortalezas y debilidades, y dado el objetivo de esta investigación es el análisis de los riesgos operacionales, sólo se deberán identificar aquellas que provengan de fallos en los procesos, sistemas, personas, eventos externos y legales.

Para la identificación de riesgos operacionales es recomendado al menos realizarlo para los procesos más relevantes de la institución, con la finalidad de que se garantice que se están considerando los riesgos que pudieran afectar en mayor manera a la organización para ello como se mencionó en el apartado de “Líneas de defensa” esta responsabilidad recae en la primera línea, ya que ellos son quienes “conviven” con el riesgo y por tanto, quienes mejor lo conocen, en este proceso es fundamental asignar responsables de los riesgos, ya que de ellos dependerá también su gestión.

El análisis mencionado se debe de realizar a través de grupos de trabajo en los que participan todos los involucrados, es decir, los responsables de la gestión del riesgo

(primera línea de defensa), así como la segunda línea de defensa y, en su caso, cualquier otra unidad de negocio que se considere necesaria para poder llevar a cabo de mejor manera el ejercicio.

En esta fase la responsabilidad de la primera línea de defensa, como se ha mencionado, es la identificación de los riesgos, mientras que la segunda línea de defensa tiene la responsabilidad de validar que sean los riesgos mínimos que deben estar incluidos.

Análisis CAME (Corregir, Afrontar, Mantener y Explorar)

Una vez que se cuenta con el análisis de las variables tanto internas como externas que pudieran afectar al banco, es necesario definir la respuesta que se tendrá a ellas, esto consiste en realizar el Análisis CAME, este funciona como un complemento del análisis FODA. Este análisis es fundamental para saber cómo actuar ante las debilidades, fortalezas, oportunidades y amenazas identificadas. Lo que dice el Análisis CAME es qué debilidades hay que corregirlas, qué amenazas hay que afrontarlas, qué fortalezas hay que mantenerlas y qué oportunidades hay que explotarlas.

Figura 8: Análisis CAME (Huerta D. S., 2017)

Antes de definir y priorizar qué acciones se implementarán es fundamental como se ha hecho hincapié a lo largo del escrito que se necesita tener claro cuál es la estrategia y el apetito al riesgo que el banco ha definido, ya que en función de esto se priorizará cómo se realizará la corrección de debilidades, de qué manera se van a afrontar las amenazas, cómo se van a mantener las fortalezas y cómo se van a explotar las oportunidades.

A continuación, se enumeran las principales estrategias:

- Estrategias defensivas: este tipo de estrategias buscan evitar que empeore la situación actual. En este tipo de estrategias predominarán las acciones enfocadas en afrontar amenazas y mantener fortalezas.

- Estrategias ofensivas: Esta estrategia busca mejorar la situación actual, en este tipo de estrategias predominarán las acciones enfocadas a explotar las oportunidades y mantener o reforzar las fortalezas.

- Estrategias de reorientación: Esta estrategia busca trasformar la situación actual haciendo cambios que eliminen las debilidades y creen nuevas fortalezas. En este tipo de estrategias predominarán las acciones enfocadas a corregir debilidades y explotar oportunidades.

- Estrategia de supervivencia: Busca eliminar los aspectos negativos que nos perjudican. En este tipo de estrategias predominarán las acciones enfocadas a corregir las debilidades y a afrontar amenazas.

Figura 9 Análisis CAME (Huerta D. S., 2017)

Una vez realizados todos los pasos anteriores se tiene que definir un listado de acciones en detalle para cada fortaleza, debilidad, oportunidad y amenaza listada, para priorizar en función de la estrategia y el perfil de riesgo del banco.

Así como queda calendarizar, unidad responsable, coste, fecha, objetivo a cumplir y métricas a medir, todas las acciones a implementar para el periodo a cuya finalización volverá a realizar el análisis FODA o DAFO, esos últimos elementos se analizarán a detalle en las herramientas de mitigación e indicadores de riesgo.

3.2.2 Evaluación de riesgos y controles.

Una vez que los riesgos son identificados, es necesario realizar su evaluación, esto con la finalidad de conocer el impacto que pudieran tener en la institución.

Un banco puede experimentar diversos impactos ante la ocurrencia de un riesgo no discrecional, entre los más relevantes se encuentran:

a) Impacto financiero: es el impacto relacionado con una pérdida económica determinada por la frecuencia y las consecuencias monetarias de la

materialización del riesgo y que, por lo tanto, pudiera tener una afectación patrimonial del banco.

b) Impacto al cliente o reputacional: es el impacto relacionado con la percepción negativa que el cliente y demás partes interesadas pudieran tener por la materialización del riesgo.
c) Impactos regulatorios: es el impacto relacionado por la falta del cumplimiento de las normas y que las autoridades financieras interponen sanciones e incluso, restricciones en la operación.

Es importante comentar, que estos impactos no son excluyentes, es decir, un riesgo puede provocar más de un impacto en el banco.

La evaluación de riesgos considerará tres momentos que son: evaluación del riesgo inherente, evaluación de controles y, por último, evaluación del riesgo residual.

Medir los impactos mencionados se recomienda sea realizado por la primera línea de defensa o bien, de quienes son los dueños de los riesgos, ya que ellos poseen mayor sensibilidad del impacto que pudieran tener ante su ocurrencia.

- Evaluación de riesgo inherente: se refiere a la evaluación de la materialidad del riesgo inicial, es decir, sin considerar los controles que mitigan al riesgo, en esta etapa se conoce la exposición inicial que tiene el Banco.

Para poder determinar el impacto financiero, se consideran las variables de frecuencia e impacto:

a) Frecuencia: es el número de sucesos de riesgo que se producirían, es decir, es el número de veces que se estima la ocurrencia del evento que pudiera tener una pérdida, ligado a la periodicidad, es decir, si estos sucesos pasarían de manera diaria, semanal, mensual, anual o más de un año.
b) Impacto: es el importe que se estima se tendría ante la materialización del riesgo

c) La segunda línea de defensa tiene la responsabilidad de definir los niveles de frecuencia y severidad, así como de darlos a conocer a todos los involucrados.

Para efectos de la propuesta de investigación, se proponen las siguientes tablas de impacto y de severidad.

Tabla 3 Propuesta de niveles de tipo de impacto por tipo de riesgo

Nivel	Impacto Financiero	Impacto cliente/reputacional	Impacto regulatorio
1-Bajo	Bajo impacto financiero que el banco puede asumir sin consecuencias relevantes	Clientes afectados a nivel estatal	Observaciones por parte de autoridades financieras
2-Medio	Medio impacto financiero que si bien el banco puede asumir se debe contener para evitar incrementar su impacto	Afectación de clientes a nivel nacional conocimiento del público inversionista	Solicitud de visita extraordinaria por parte de alguna autoridad financiera
3- Alto	Alto impacto financiero	Difusión en medios de comunicación	Retiro de autorizaciones para operar productos o servicios

Tabla 4 Propuesta de niveles de probabilidad por tipo de riesgo

Nivel	Frecuencia de eventos
1-Bajo	Al menos 1 vez cada 12 meses
2-Medio	Al menos 1 vez cada 6 meses
3-Alto	Al menos 1 vez al mes

La combinación de estos dos factores suele representarse en las llamadas gráficas de calor para dar una visión de la exposición a este tipo de riesgos, la Comisión Nacional Bancaria y de Valores, ha emitido un estándar de tres niveles para su evaluación:

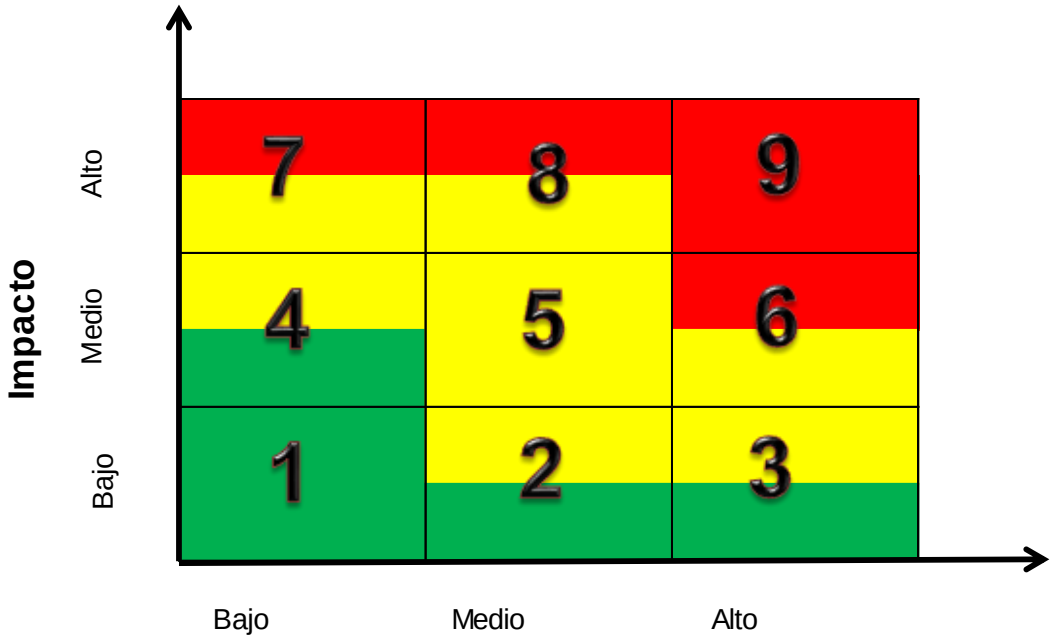

Figura 9 Calificación de riesgo. Tomado del documento emitido por la Comisión Nacional Bancaria y de Valores: Instructivo Del Reporte R28 Información De Riesgo Operacional (2019).

- Evaluación de controles: consiste en valorar el efecto mitigante que tienen los controles en el riesgo identificado. Para efectos de la propuesta, y en concordancia con la evaluación de riesgos se determinarán con base en tres niveles del control, utilizando en todo momento el análisis y resultados que realice la segunda línea de defensa en cuanto a efectividad y no efectividad del control:

  a) Fuerte: se refiere a que el control se encuentra correctamente diseñado y se ejecuta de acuerdo con lo establecido;
  b) Necesita mejorar: en este caso el control necesita mejorar en su diseño y/o en su ejecución; y

c) Débil: corresponde cuando el control es deficiente en su diseño, o bien, el control no es ejecutado adecuadamente.

- Evaluación de riesgo residual: corresponde al resultado obtenido de la evaluación inherente del riesgo y de la mitigación que tengan los controles sobre este, después de haber obtenido esta evaluación el Banco deberá de decidir cuál será su respuesta al riesgo, pudiendo ser reducirlo a través de la implementación de controles más robustos en cuanto a su diseño y/o ejecución, aceptarlo al no implementar ninguna medida adicional a las identificadas, o bien, ceder el riesgo a través de la contratación de seguros.

La matriz o inventario de riesgo: es el resultado de la identificación de los riesgos y de su evaluación, suele registrarse en lo que se le conoce como matriz o inventario de riesgos, en él se sugiere que al menos contenga lo siguiente:

a) Identificador de riesgo: corresponde a la clave con la que se hará referencia al riesgo, su importancia radica en que pueden existir riesgos con la misma descripción en otros procesos, además de que facilita su manejo dentro de la matriz o inventario.
b) Proceso o actividad en la que se identificó el riesgo: se refiere a la actividad en la que fue identificado el riesgo.
c) La descripción del riesgo operacional identificado: representa a lo que se refiere el riesgo, en esta se recomienda que sea clara y precisa, con la finalidad de que sea comprensible para los involucrados
d) Responsable del riesgo: corresponde a la unidad de negocio dónde se identificó el riesgo, de esta manera se asigna la responsabilidad de su gestión
e) Causa del riesgo: se refiere a la naturaleza del riesgo, su identificación es sustancial para realizar un tratamiento de riesgo de manera puntual
f) Tipo de riesgo operacional: se refiere a la clasificación del riesgo operacional identificado de acuerdo con las siete categorías definidas por el Comité de Basilea

definidas previamente en Capítulo 1 apartado 1.4 Categorías de Riesgo Operacional.

g) Línea de negocio: se refiere a la línea de negocio que afecta el riesgo operacional identificado de acuerdo con las ocho líneas de negocio definidas por el Comité de Basilea mencionadas en el capítulo II Organizaciones y normas para la gestión de riesgos, aparatado 2.1.2 Basilea II.
h) Producto: corresponde al tipo de producto que el riesgo afectaría de materializarse
i) Tipo de impacto (financiero, regulatorio y/o reputacional): corresponde al tipo o tipos de impacto que pudieran generar el riesgo
j) Impacto: se refiere al nivel del 1 al 3 que tendría el riesgo identificado
k) Frecuencia: se refiere a la frecuencia del 1 al 3 con la que se esperaría que el riesgo ocurriera
l) Evaluación de Riesgo inherente: corresponde a la evaluación del riesgo obtenida considerando a los dos factores tipo de impacto y frecuencia
m) Identificador de control asociado al riesgo: al igual que el riesgo es recomendable que se asigne una clave al control, sobre todo porque pueden existir controles que mitiguen a más de un riesgo o bien, que se hayan establecido controles institucionales
n) Descripción del control: se requiere incorporar la manera en cómo se mitigaría el riesgo
o) Clasificación del control: se requiere indicar el tipo de control con el que se cuenta
p) Responsable del control: al igual que el riesgo es importante asignar a la unidad de negocio que se encargará del control, ya que esta recaerá la responsabilidad del desempeño del control
q) Nivel de ejecución: corresponde a qué tan bien o que tan mal se ejecuta el control (fuerte, necesita mejorar y débil)
r) Nivel de diseño: se refiere al nivel de diseño del control (fuerte, necesita mejorar y débil)
s) Evaluación del control: corresponde a la evaluación del control con base en su nivel de diseño y ejecución

t) Riesgo residual: corresponde a la evaluación del riesgo después del efecto mitigante de los controles

u) En su caso, planes de mitigación y área responsable de su mitigación: corresponde a los casos en los que el nivel de riesgo residual se encuentre fuera del perfil de riesgo que el banco haya definido, para lo cual se requerirá que se establezcan medidas correctivas para que el riesgo se encuentre en niveles aceptables, ya sea a través de la mejora del control o bien, que se haya optado por ceder el riesgo.

La clasificación de los riesgos operacionales de acuerdo con su tipo suele ser la actividad más complicada por su subjetividad para ello se cuenta con un flujo que sirve como guía para realizar una clasificación más adecuada.

Clasificación de los riesgos y eventos por riesgo operacional

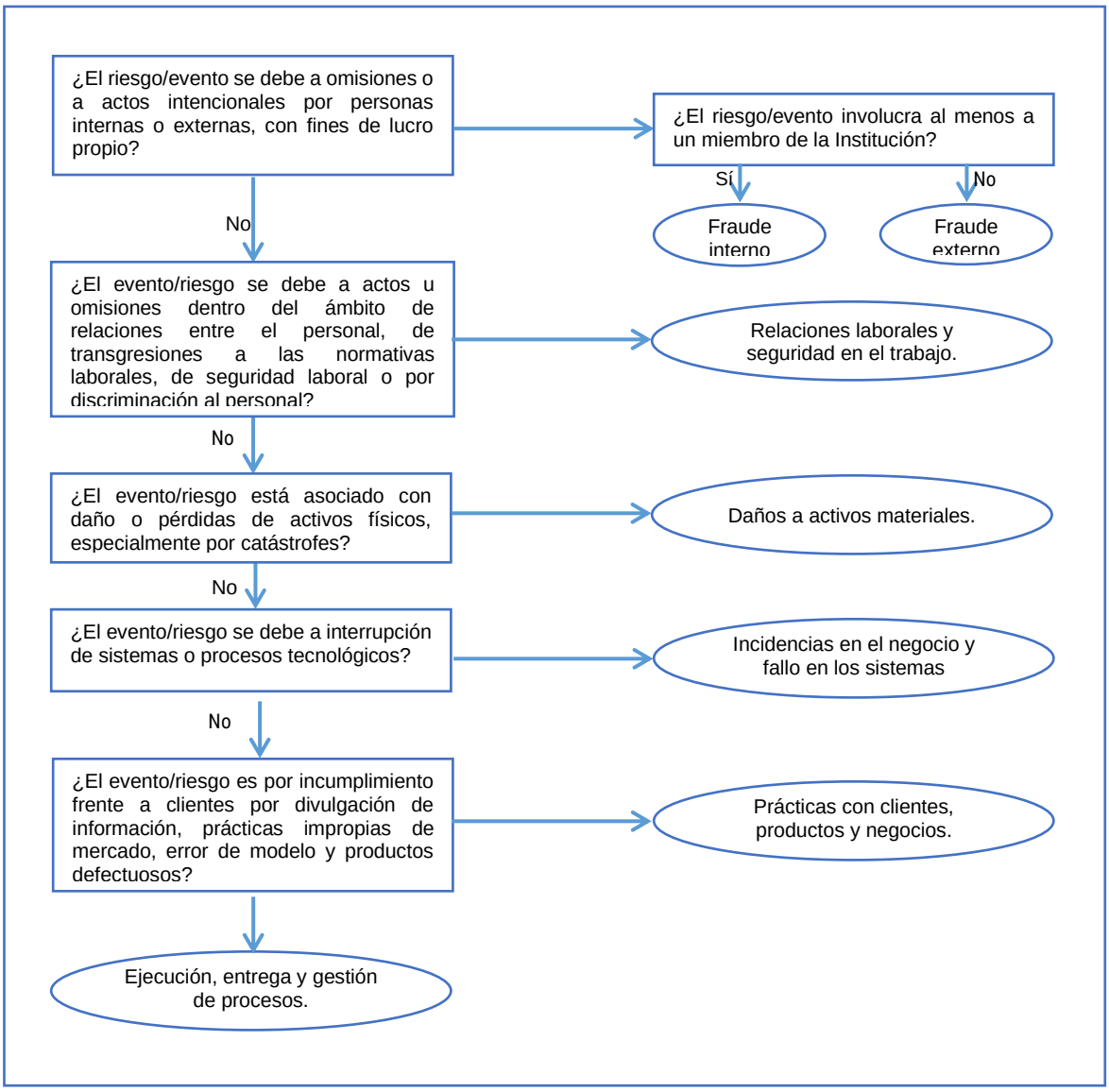

Figura 10 Elaboración realizada con base en información de los acuerdos de Basilea (Comité de Supervisión Bancaria de Basilea, 2003)

3.2.3 Monitoreo.

Una vez que se concluyó la etapa de identificación y evaluación de riesgos, es necesario conocer cuál es el comportamiento, es decir si mantiene su nivel de riesgo o bien, si ha deteriorado. Para ello el monitoreo de riesgos se realiza a través de indicadores clave de riesgo o bien KRI por sus siglas en inglés *Key Risk Indicator* los cuales permiten contar

con métricas de apoyo para dar seguimiento y alertar riesgos en el banco, de tal forma que se tomen medidas que impidan la materialización del riesgo.

Por lo tanto, los indicadores, pretenden actuar como alertas tempranas a los niveles de riesgo, así como medir continuamente la eficacia de los controles y procesos, para poder establecer mejoras en los mismos.

Con el fin de llevar un adecuado diseño, seguimiento y control de los indicadores de riesgo operacional, se proponen las siguientes fases como elementales para el diseño y mantenimiento de KRI's

Identificación y definición de indicadores.

Esta fase se basa en utilizar la matriz de riesgos y controles que se conformó previamente, para seleccionar aquellos riesgos que se encuentran con riesgo residual alto, así como el impacto cliente/reputacional y regulatorio.

Siguiendo el modelo de responsabilidades definido, la primera línea de defensa es la responsable de definir los indicadores y proponer a la segunda línea de defensa para su validación y cuestionamiento.

Definición de nivel de tolerancia, límite o umbral.

Una vez que se encuentran definidos los Indicadores resulta indispensable establecer el nivel de tolerancia o límite a partir del cual se dará seguimiento la posible alerta o deterioro que pueda estar sufriendo el riesgo.

Cálculo, seguimiento y monitoreo.

Al momento de definir los indicadores en conjunto con su nivel, se propone por lo menos establecer lo siguiente:

- Unidades responsables de cálculo y seguimiento
- Periodicidad de cálculo

- Definición de niveles de cumplimiento del indicador y concordancia con los tres niveles propuestos, es decir:
    a) Aceptable: se encuentra dentro de los niveles establecidos
    b) Preventivo: se encuentra por encima del nivel mínimo y por debajo del nivel crítico
    c) Crítico: el indicador está por arriba del nivel de tolerancia-límite-umbral definido

En caso de que exista alguna desviación preventiva o crítica es responsabilidad de la primera línea de defensa establecer el plan de corrección respectivo. En consecuencia, de ser necesaria la redefinición de los umbrales para un indicador, esta modificación debe ser propuesta a la segunda línea de defensa para su aprobación.

3.3.3 Mitigación.

Como se mencionó anteriormente, el inventario o la matriz de riesgos debe contener los controles asociados a cada uno de ellos, si es que el riesgo no contara con un control o bien, que no sea suficiente para mitigar el riesgo, este debe contar en su defecto con un plan de acción, esto con la finalidad de mitigarlo y que se encuentre en concordancia con el perfil de riesgo.

Los planes o medidas de mitigación tienen como objetivo el reducir la exposición a riesgos operacionales y es la consecuencia natural de que la administración del riesgo operacional cumple su función, pues al realizar la evaluación de riesgos y controles, monitorear los indicadores y ver los eventos ocurridos, permite establecer de manera oportuna aquellos casos donde se requieren acciones para reducir el riesgo.

Se propone el flujo para asegurar que el funcionamiento de los planes de mitigación sea homogéneo y cuente con la adecuada validación, supervisión y monitoreo por parte tanto de la primera línea de defensa, como de la segunda línea de defensa, el cual es el siguiente:

Identificación del riesgo a mitigar

Para poder establecer qué riesgos ameritan el establecimiento de medidas correctivas o mitigantes se requiere hacer uso de distintas fuentes de información cuyo resultado es la implantación de las herramientas previamente descritas como son:

- Proceso de evaluación de riesgos y controles, cuyo resultante indique la necesidad de establecer una medida mitigante (resultado de evaluación alta o fuera del perfil establecido por el banco)
- Tendencia o comportamiento de los indicadores de riesgo operacional que se encuentran excediendo los límites o umbrales permitidos
- Informes de otras fuentes como son auditores internos, reguladores, o bien, otras áreas del banco.
- Análisis de eventos de riesgo operacional de la base de datos de riesgo operacional

Definición del plan o medida para mitigar el riesgo.

Una vez analizadas las fuentes de información la primera línea de defensa definirá cuáles son los diversos planes y/o medidas mitigantes que establecerá para reducir la exposición al riesgo.

La definición de la medida deberá contar al menos con:

- Descripción del riesgo
- Descripción de la medida a implementar
- Descripción del beneficio estimado en la implementación y ejecución de la medida. El análisis o descripción del beneficio debe estar ligado al costo que tendrá a la institución si se aplica la medida
- Tiempo en que estará implementada
- Responsable de la implementación

Es importante que en todo momento la segunda línea de defensa apoye a la primera línea en la definición del plan de mitigación, así como de hacer los cuestionamientos que

considere necesarios, con el fin de que se cuente con la medida que mejor mitigue la exposición al riesgo.

Validación y seguimiento del plan o medida.

Una vez definido el plan o medida a establecer, ésta deberá quedar debidamente documentada y estará aprobada la primera línea y la segunda línea de defensa, con la finalidad de que quede constancia entre las partes involucradas de que se ejecutaron las acciones pertinentes para la corrección del riesgo.

Implementación y monitoreo.

Como última parte del flujo definido, la primera línea de defensa deberá implementar, en el tiempo establecido, la medida de mitigación. Durante este período la segunda línea deberá vigilar el cumplimiento al plan establecido.

Una vez implementada la medida de mitigación será necesario realizar la reevaluación del riesgo y/o controles correspondientes, de tal forma que la matriz de riesgos y controles quede debidamente actualizada por parte de la segunda línea de defensa, con la nueva evaluación del riesgo residual y en su caso, con la evaluación del control respectivo.

3.3.4 Eventos de riesgo operacional.

Un evento de riesgo operacional corresponde a la materialización de un riesgo operacional, como se mencionó en la parte de la identificación, este pudiera tener diversos efectos como lo son:

- Pérdida económica bruta: se refiere al importe de pérdida económica que ha tenido el banco por eventos de riesgo operacional como pueden ser:
    a) Pérdida directa en la cuenta de resultados
    b) Intereses devengados de demandas legales, fraudes, errores fiscales
    c) Multas y sanciones
- Ingreso no percibido, no se incluyen pérdidas o no ingresos por decisiones comerciales como el no cobro de comisiones.

- Gasto: se refiere a los gastos en lo que el banco incurrió como consecuencia de una pérdida económica.
- Cuasi-pérdida: se refiere a aquellos eventos de riesgo operacional que no tienen impacto económico para el banco y que en todos los casos se refiere a “impactos potenciales” ya sean directos o indirectos.
- Recuperaciones: se refiere a los importes que el banco con sus procesos y mecanismos de mitigación puede recuperar de algún evento de riesgo operacional. Es importante mencionar, que la recuperación por sí misma es un hecho independiente del impacto de pérdida y que puede ser en un tiempo totalmente distinto a la realización y materialización del evento, razón por la cual se debe registrar en la base de eventos de pérdida como un hecho independiente y sólo tener una clara relación con el evento operacional con el que esté ligado.

Se debe de considerar que el registro de la totalidad de los eventos es importante para tener una completa gestión y control del riesgo operacional, para ello se propone el siguiente modelo, proceso o fases para la adecuada gestión y control de la base de datos de riesgo operacional, de tal forma que pueda contar con los elementos de control suficientes y necesarios que permita la completitud e integridad de la información.

Fuentes de información y focos de riesgo operacional.

Es necesario realizar la identificación de las diferentes fuentes de información que tiene el Banco y cómo estas se encuentran relacionadas con sus focos de riesgo, previamente establecidos en su matriz de riesgos y controles.

Por lo anterior, la segunda línea de defensa es la responsable de realizar en conjunto con la primera línea de defensa un mapa de fuentes de información y focos de riesgos, de esta forma se tendrá de manera clara las diferentes unidades de negocio responsables de reportar los eventos de riesgo operacional relacionados con los principales focos de riesgo. Para lograr este mapa, al menos se deberán realizar las siguientes actividades:

- Análisis de cuentas contables del banco

- Análisis de bases de datos no contables
- Análisis de categorías de riesgo y líneas de negocio relacionadas con los focos de riesgo.

Captura y análisis de eventos de Riesgo Operacional.

Una vez que se han definido las fuentes de información y los responsables de reportar un evento de riesgo operacional, cada unidad de negocio será responsable de reportar los eventos.

Los eventos de riesgo operacional se pueden componer de uno o varios impactos, por lo cual cada uno de los impactos debe evaluarse y registrarse de manera individual.

Cada evento de riesgo operacional debe contar con elementos mínimos en su registro y que se hace necesario para tener un modelo integral de gestión y control de riesgo operacional. La Comisión Nacional Bancaria y de Valores por medio del Anexo 12-A establece los requisitos mínimos con los que deben de contar los eventos de pérdida, tomándolo como base se recomienda recopilar lo siguiente:

- Categoría de riesgo
- Línea de negocio
- Causa raíz
- Proceso
- Producto
- Control

Se deberá de establecer la periodicidad con la que la primera línea de defensa del banco realizará el registro de los eventos de riesgo operacional, mismos que deberán de ser informados a la segunda línea de defensa.

Reporte y comunicación del ROp.

Como está definido en el modelo de gestión y control de riesgo operacional, en la descripción de responsabilidades, y se ha descrito que la primera línea de defensa será responsable de reportar y comunicar los eventos de riesgo operacional.

Por otro lado, la segunda línea de defensa es la responsable de monitorear y asegurar el cumplimiento de reporte y comunicación de riesgo operacional.

Eventos frontera.

Uno de los elementos críticos en el modelo de gestión y control de riesgo operacional, es el poder identificar aquellos casos que un evento de riesgo operacional ha afectado otro tipo de riesgo, como es el riesgo de crédito y de mercado, e inclusive algunos casos de riesgo legal; y que por tanto, ya se encuentra reconocida la materialización del impacto del evento de riesgo operacional, dentro del propio modelo de gestión de riesgo de crédito o de mercado, este tipo de eventos se les conoce como frontera y la línea que los separa es muy delgada y por ello difícil de percibir.
Con el fin de establecer criterios generales para el tratamiento de estos eventos se definen como sigue:

- Relativos a Riesgo Legal: al ser un riesgo que no sólo afecta una categoría de riesgo en específico, deberá clasificarse de acuerdo con la categoría que se desprenda de la demanda.

- Relativos a Riesgo de Crédito: para poder diferenciar entre los eventos de riesgo de crédito puro sólo deben de integrarse aquellos cuyo origen haya sido el riesgo operacional, por ejemplo:

  a) Los eventos de fraude cometidos por empleados o terceros
  b) Dar préstamos basándose en documentos falsos
  c) Uso fraudulento de fondos
  d) Eventos que imposibilitan parcial o totalmente la gestión de recuperación por parte del banco

Es importante aclarar que los criterios que se han definido para incluir en la base de datos de riesgo operacional, es sólo para gestión y nunca podrán tomarse en cuenta para cálculos de capital, según lo señalado en la Circular Única de Bancos (2019).

Relativos a Riesgo de Mercado: para poder diferenciar entre los eventos de riesgo de mercado puro sólo deben de integrarse aquellos cuyo origen haya sido el riesgo operacional, por ejemplo:

- Eventos causados por calidad de información o indisponibilidad de sistemas informáticos
- Errores en la introducción de órdenes o especificación de operaciones
- Pérdidas de datos en la conciliación entre *el negocio* y *el área de control*
- Imposibilidad de acceder a mercados
- Toma de posiciones por arriba de límites de manera intencional
- Errores al valuar el *Mark-to-market* [12]o calcular el valor en, por errores en las operaciones o ejecución del modelo.

Es importante mencionar que las pérdidas operacionales relacionadas con el riesgo de mercado se consideran como riesgo operacional a efectos de cálculo de capital regulatorio, por lo que estarán sujetas a la exigencia de capital por riesgo operacional.

3.4.5 Retroalimentación de revisiones.

Con el objeto de reforzar la evaluación del perfil de riesgo operacional del banco, es necesario recopilar toda la información que esté disponible. Es por eso, que los informes de auditoría interna y de los diferentes reguladores son fuente de información relevante y se consideran indicadores de posibles debilidades en la gestión y control del riesgo operacional en las diferentes áreas del banco. Lo anterior ayuda a mantener un modelo de gestión vigente, en donde con base en la información se actualizarían las herramientas

[12] Mark-to-market: se refiere al registro de la liquidación diaria que existe de las pérdidas y ganancias de una operación de una cartera de inversión.

de riesgo operacional como lo son las matrices o inventarios de riesgo en donde los informes de auditores internos u observaciones de los reguladores revelen eventos que no tenían contemplados, lo cual es un proceso natural ante un contexto interno y externo dinámico, la evaluación de los controles ante el incremento de exposición al riesgo, la implementación de nuevos indicadores de riesgo como resultado de nuevos riesgos o la revaluación de controles.

El desarrollo e implementación de las herramientas antes descritas pueden ayudar a llevar una gestión de riesgos operacionales holística ya que recoge diversas perspectivas de los diferentes especialistas de riesgos y controles, así como la experiencia de los dueños de los procesos y de los riesgos, lo cual hace que se tenga un marco de gestión sólido. Ahora bien, este flujo de gestión y las herramientas que en él se utilizan no se limita a que las instituciones puedan optar por adicionar alguna herramienta o incrementar las etapas del flujo que consideren puedan fortalecer la administración de este tipo de riesgo.

Capítulo IV Requerimiento de Capital de Riesgo Operacional

En México, de acuerdo con lo estipulado en la CUB las instituciones de Crédito para realizar el cálculo de requerimiento de capital por riesgo operacional podrán optar por cuatro metodologías que son el método básico, método estándar, método estándar alternativo y método avanzado. El uso de esas metodologías es a discreción de la Institución de la que se trate en consideración con su tamaño y el beneficio que se obtenga de utilizar un método u otro.

4.1 Método básico

El método del indicador básico como su nombre lo sugiere, no requiere alguna autorización de la autoridad para su utilización. Las instituciones de crédito que opten por esta metodología de cálculo de acuerdo con la CUB que emite la CNBV (2019) deberán de cumplir sin excepción alguna con lo siguiente:

- Cubrir el Riesgo Operacional con un capital mínimo equivalente al 15 por ciento del promedio de los tres últimos años de sus ingresos netos anuales positivos.

- Los ingresos netos serán los que resulten de sumar de los ingresos netos por concepto de intereses más otros ingresos netos ajenos a intereses. El ingreso neto deberá ser calculado antes de cualquier deducción de reservas y gastos operativos.

- Para el cálculo de los ingresos netos se deberán considerar los importes de estos correspondientes a los 36 meses anteriores al mes para el cual se está calculando el requerimiento de capital, los cuales se deberán agrupar en tres periodos de doce meses para determinar los ingresos netos anuales, conforme a las fórmulas que se expresan a continuación. Para tal efecto, se considerará al mes t-1, como el anterior para el cual se está calculando el requerimiento de capital. Los ingresos netos para cada periodo de 12 meses deberán determinarse conforme a la fórmula siguiente:

$$INA_1 = \sum_{l=t-1}^{t=12} IN_t \qquad INA_2 = \sum_{l=t-13}^{t=24} IN_t \qquad INA_3 = \sum_{l=t-25}^{t=36} IN_t$$

4.1.1

En donde:

INA_1, INA_2, INA_3, representan la suma de los ingresos netos anuales para cada uno de los tres periodos

t - k para k=1, 2,36 representa el k-ésimo mes anterior al periodo para el cual se están calculado los ingresos netos.

- Una vez calculados los ingresos netos anuales el requerimiento de capital por concepto de Riesgo Operacional se define como:

$$RCRO = \left[\frac{\sum_{j=1}^{3} \max\left(INA_j, 0\right)}{n}\right] \alpha \qquad 4.1.2$$

Colocar símbolo correcto

En donde:

$RCRO$ = requerimiento de capital por Riesgo Operacional

INA_j= ingresos netos anuales, para cada uno de los tres periodos (INA_1, INA_2, INA_3) conforme a la información de los últimos 36 meses.

n = número de años (de los tres últimos) en los que los ingresos netos fueron positivos.

α = 15 por ciento.

El método básico si bien no exige una autorización para su cálculo establece los requisitos mínimos con los que debería de cumplir una institución bancaria, operar bajo este método puede representar altos costos, sobre todo para instituciones pequeñas o bien, que su exposición por riesgo operacional se encuentra distante del resultado que este cálculo sugiere.

4.2 Método estándar

Para calcular el requerimiento de capital por Riesgo Operacional bajo el Método Estándar de Riesgo Operacional, a diferencia del método del indicador básico, requiere previa autorización del regulador.

Las instituciones que opten por este método de cálculo de acuerdo a lo establecido por la CNBV (2019) deberán de contar sin excepción alguna con lo siguiente:

- Cubrir el Riesgo Operacional con un capital mínimo equivalente al promedio de los últimos tres años de la suma simple de los requerimientos de capital por riesgo operacional para cada una de las ocho líneas de negocio de cada año, conforme se señala en la fracción siguiente.
- El requerimiento de capital por riesgo operacional de cada línea de negocio será el monto que resulte de multiplicar el porcentaje que corresponda a cada línea de negocio conforme a la tabla 5 “Porcentaje aplicable por la línea de negocio” y los ingresos netos anuales de la línea de negocio correspondiente. Tomando los conceptos que apliquen para cada línea de negocio para los últimos 12 meses de cada año.
- En ningún caso, la suma de los ingresos netos anuales por línea de negocio podrá ser menor a los ingresos netos reportados bajo el Método del Indicador Básico.

Tabla 5 Porcentaje aplicable por línea de negocio

Líneas de Negocio	Porcentaje aplicable a cada línea de negocio (l)
Finanzas corporativas	18
Negociación y ventas	18
Banca minorista	12
Banca comercial	15
Pagos y liquidación	18
Servicios de agencia	15
Administración de activos	12
Intermediación minorista / operaciones de corretaje al menudeo	12

Tabla 5 Tomada de la Comisión Nacional Bancaria y de Valores, Circular Única de Bancos (2019)

En caso de que existieran requerimientos de capital negativos resultantes de ingresos netos negativos, en cualquiera de las líneas de negocio, se podrán compensar con los requerimientos positivos en otras líneas de negocio sin límite alguno. No obstante, cuando el requerimiento de capital agregado para todas las líneas de negocio dentro de un año en concreto sea negativo, dicho año se considerará como cero.

De esta forma, el requerimiento de capital por Riesgo Operacional bajo el Método Estándar de Riesgo Operacional puede expresarse como:

$$RCRO = \frac{[\sum_{\alpha=1}^{3} max[\sum_{t=1}^{8}(INA_{\alpha t}\beta_t), 0]]}{3} \qquad 4.1.3$$

En donde:

RCRO = Requerimiento de capital por Riesgo Operacional.

$INA\alpha$= Ingresos netos anuales (con α=1, 2 y 3) de cada línea de negocio *l*, como se define en la Tabla 5 Porcentaje aplicable por la línea de negocio.

β_t=Porcentaje fijo, que relaciona la cantidad de capital requerido con el ingreso neto de la línea de negocio *l*, conforme a la Tabla 5 Porcentaje aplicable por la línea de negocio

4.3 Método estándar alternativo

Las Instituciones, para utilizar el Método Estándar Alternativo para calcular el requerimiento de capital por su exposición al Riesgo Operacional, deberán obtener previamente la autorización de la Comisión.

Para calcular el requerimiento de capital por Riesgo Operacional bajo el Método Estándar Alternativo de Riesgo Operacional, las Instituciones deberán seguir la metodología que se describe a continuación:

- Apegarse a la metodología del Método Estándar de Riesgo Operacional, salvo cuando se trate del cálculo de los requerimientos de capital por riesgo operacional de las líneas de negocio de banca minorista y banca comercial, para las cuales el requerimiento de capital se calculará de acuerdo con el siguiente punto.
- Para calcular el requerimiento de capital por Riesgo Operacional de las líneas de negocio de banca minorista y banca comercial, las Instituciones sustituirán el ingreso neto mensual de cada una de estas líneas de negocio, por la cantidad ejercida de préstamos y el monto total dispuesto de la línea de crédito mensuales correspondiente a cada línea de negocio, multiplicado por un factor fijo “m” el cual será de 0.035.
- Tratándose de los préstamos y del monto total dispuesto de la línea de crédito de la línea de negocio de banca minorista, las Instituciones utilizarán las cantidades ejercidas de las carteras crediticias asociadas al menudeo, pequeñas y medianas empresas tratadas como minorista y derechos de cobro adquiridos frente a menudeo.
- En el caso de la línea de negocio de banca comercial, las Instituciones utilizarán las cantidades ejercidas de las carteras crediticias asociadas a empresas, gobiernos extranjeros, bancos, financiamiento especializado, pequeñas y medianas empresas, derechos de cobro adquiridos frente a empresas y el valor contable de los títulos conservados a vencimiento.

- El requerimiento de capital en los casos de la banca al menudeo y la banca comercial puede expresarse como:

$$RC_{LN} = \beta_{LN\beta}\ x\ m\ x\ LA_{LN} \qquad 4.2.1$$

Donde:

RC_{LN} = requerimiento de capital para la línea de negocio correspondiente

$\beta_{LN\beta}$= factor beta de la línea de negocio

LA_{LN} = saldo insoluto de los préstamos y del monto total dispuesto de la línea de crédito (no ponderados por riesgo y brutos de provisiones), promediado durante los tres últimos años. Para determinar el promedio anual, se tomará en consideración el saldo de los últimos 12 meses hasta el mes *t* de cada año; siendo el mes *t*, el mes para el cual se está calculando el requerimiento de capital por Riesgo Operacional de acuerdo con lo indicado en la fórmula 4.1.1.

Al igual que en el Método Estándar, el requerimiento total de capital en el Método Estándar Alternativo se calculará como el promedio de los últimos 3 años de la suma simple de los requerimientos de capital para cada una de las ocho líneas de negocio de cada año.

4.4 Método avanzado

Las Instituciones, para utilizar el Método Avanzado para calcular el requerimiento de capital por Riesgo Operacional, deberán obtener previamente la autorización de la CNBV.

- El requerimiento de capital por Riesgo Operacional bajo los Métodos Avanzados será igual a la medida de riesgo generada por el modelo de evaluación del riesgo operacional de la Institución, para dicho cálculo del riesgo operacional se deben de utilizar los criterios cuantitativos considerando el cálculo de la pérdida esperada y no esperada, así como los cualitativos que demuestren una correcta gestión del riesgo operacional.

- La medida de riesgo generada por el modelo de evaluación del riesgo operacional de la Institución deberá basarse en un periodo mínimo de observación de cinco años de datos internos de pérdida, ya sea para estimar directamente la pérdida o para validar dicha estimación. Cuando el banco desee utilizar por vez primera el Método Avanzado, se aceptará un periodo de observación de datos de tres años por parte de la CNBV.
- Llevar a cabo una autoevaluación, misma que será responsabilidad del director general quien, para su elaboración, deberá apoyarse en el área de Auditoría Interna, la cual será responsable de vigilar que los procesos de validación hayan sido aplicados correctamente y que cumplan los propósitos para los cuales fueron diseñados.
- Calcular su requerimiento de capital por Riesgo Operacional mediante el uso del Método Estándar de Riesgo Operacional o Estándar Alternativo y, de manera paralela, mediante el uso del Método Avanzado para el que soliciten autorización, presentando a la Comisión ambos resultados respecto de un periodo de por lo menos un año previo a la fecha en que se solicite la autorización del uso del Método Avanzado. No obstante, lo anterior, la Comisión podrá, en todo momento, ordenar que el cálculo paralelo del capital se realice durante un plazo mayor al establecido.

El plazo en que las Instituciones efectúen los cálculos paralelos de los requerimientos de capital podrá ser considerado, siempre y cuando la metodología empleada cumpla al inicio de dichas corridas paralelas.

Una vez que la Comisión haya autorizado el uso de algún Método Avanzado, las Instituciones deberán calcular el requerimiento de capital por Riesgo Operacional por un periodo de dos años contados a partir de la citada autorización. Durante este periodo las Instituciones simultáneamente deberán calcular el requerimiento de capital por Riesgo Operacional mediante el uso, tanto del Método Avanzado autorizado, como del Método Estándar o Estándar Alternativo, según corresponda.

Si durante dicho periodo, el requerimiento de capital por Riesgo Operacional obtenido al utilizar el Método Avanzado, resulta inferior al de la aplicación del Método Estándar o

Estándar Alternativo, según corresponda, las Instituciones deberán mantener en cada uno de los años posteriores a la autorización del Método Avanzado, un capital por Riesgo Operacional no menor al equivalente al porcentaje que se indica en la siguiente tabla, respecto del requerimiento de capital por Riesgo Operacional obtenido mediante la aplicación del Método Estándar o Estándar Alternativo, según corresponda.

Tabla 6 Requerimiento inferior del Método Estándar o Estándar Alternativo

	Año t- 1	Año + 1	Año +2
Método Avanzado	Cálculo paralelo	90%	80%

Tabla 6 Tomado de la Circular Única de Bancos emitida por la CNBV (2019)

Si, por el contrario, el requerimiento de capital por Riesgo Operacional obtenido mediante el uso del Método Avanzado es superior al que se obtenga al utilizar el Método Estándar o Estándar Alternativo, se deberá mantener aquél.

Una vez concluido este periodo de cálculos paralelos, las Instituciones deberán mantener el capital resultante del Método Avanzado, sin estar obligadas a estimar el requerimiento de capital por Riesgo Operacional con el Método Estándar o Estándar Alternativo.

Asimismo, la Comisión podrá requerir que las Instituciones mantengan un capital por Riesgo Operacional equivalente a un porcentaje del Método Estándar o Estándar Alternativo por un plazo mayor.

- La Comisión, cuando así lo requiera, podrá contratar los servicios de un tercero independiente que le auxilie en la validación de una parte o la totalidad del método en proceso de autorización.
- Aun una vez autorizado el Método Avanzado estará sujeto a un proceso de evaluación que permita determinar a esta Comisión si el método continúa siendo viable.

La adopción de cualquiera de los tres métodos tiene que ser elegido de acuerdo con las necesidades y el beneficio que se tiene al usar cualquiera de ellos, ya sea por costos

operativos que representan, ya que entre más avanzado sea se requiere una gestión más robusta, lo cual se puede compensar con el ahorro de capital, por lo anterior es necesario realizar este análisis costo-beneficio.

Conclusiones

Se conceptualizó la gestión de riesgos a través del uso de marcos de referencia como las publicaciones de COSO, las diversas publicaciones de Basilea y se exploraron otras metodologías específicas para el control de tecnologías de la información como es COBIT. Así como se mostró la evolución al paso del tiempo de esas metodologías y se realizó una comparación entre ellas para conocer qué tanto han cambiado como consecuencia de la evolución de los riesgos.

Se definieron los diferentes tipos de riesgos a los que una institución bancaria se encuentra expuesta, tanto para los riesgos discrecionales los cuales son tomados para la generación de negocio de la organización, y también de los riesgos no discrecionales los cuales no son tomados para tener una ganancia, sino que son inherentes a las actividades mismas.

Una vez que se definió al riesgo operacional se conceptualizó las diferentes categorías de riesgo operacional bajo los cuales deben de ser clasificados todos los riesgos que se hayan identificado.

Posteriormente se realizó una propuesta del flujo de gestión operacional bajo el cual se pretende garantizar que se cuenta con un modelo dinámico, cíclico y vigente, todo ello a través del uso de herramientas a utilizar en cada una de las etapas de gestión de riesgo operacional y garantizar una seguridad razonable del marco de control.

Por último, se mencionaron los métodos de cálculo del requerimiento de capital por riesgo operacional, así como las obligaciones que tienen los bancos para su uso. Este elemento es uno de los más relevantes para las instituciones, pues la metodología que habría de utilizarse está en función de qué tan robustos sean los procesos de gestión del riesgo operacional, es decir el uso de métodos avanzados de requerimiento de capital que permiten que este sea menor requerirán procesos más precisos en su gestión por el contrario de la metodología básica lo cual se traduce en un requerimiento de capital mayor.

Referencias

1. Asociación Española para la Calidad. (s.f.). Recuperado el 16 de Marzo de 2020, de https://www.aec.es/web/guest/centro-conocimiento/cobit
2. Bank for International Settlements. (s.f.). Recuperado el 14 de abril de 2020, de BIS: https://www.bis.org/about/chronology.htm?m=1%7C4%7C550
3. Castro, R. M. (Diciembre de 2004). Recuperado el 16 de marzo de 2020, de http://legal.legis.com.co/document/Index?obra=rcontador&document=rcontador_7680752a7d96404ce0430a010151404c
4. Comisión Nacional Bancaria y de Valores. (s.f.). *Circular Única de Bancos*. Recuperado el 1 de enero de 2019, de https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/BANCA-MULTIPLE/Paginas/Normatividad.aspx
5. Comisión Nacional Bancario y de Valores. (s.f.). Recuperado el 10 de diciembre de 2019, de SITI CNBV: https://www.cnbv.gob.mx/TR%C3%81MITES-Y-SERVICIOS/SITI/Documents/R28%20A-2811%20al%202814%20Informaci%C3%B3n%20de%20Riesgo%20Operacional%20(Instituciones%20de%20Cr%C3%A9dito)%20desde%20201601.pdf
6. Comité de Supervisión Bancaria de Basilea. (2003). *Buenas prácticas para la gestión y supervisión del riesgo operativo.* Basilea (Suiza).
7. Comité de Supervisión Bancaria de Basilea. (2010). *Basilea III: Marco regulador global para reforzar los bancos y sistemas bancarios.* Basilea (Suiza).
8. Comité de Supervisión Bancaria de Basilea. (2015). *Orientaciones Principios de gobierno corporativos .* Suiza.
9. Comité de Supervisión Bancaria de Basilea. (2017). *Basilea III Finalización de las Reformas poscrisis.* Basilea (Suiza).
10. Committee of Sporing Organizations of the Treadway Comission. (2007). *Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño Resumen Ejecutivo.* España.

11. COSO. (s.f.). Recuperado el 03 de 05 de 2020, de https://www.coso.org/Pages/aboutus.aspx

12. Gaitán, R. E. (2015). *Control Interno y fraudes Análisis de Informe COSO I, II y III con base en los ciclos transaccionales.* Bogotá: Ecoe Ediciones.

13. Haro, A. d. (2005). *Medición y Control de Riesgos Financieros.* México: Limusa.

14. Haro, A. d. (2018). *Medición y control de riesgos financieros.* México: Limusa.

15. Harvard Bussines School. (02 de 03 de 2020). *Harvard Bussines School*. Obtenido de https://www.hbs.edu/faculty/Pages/profile.aspx?facId=6532&facInfo=pub

16. Huerta. (2 de 11 de 2017). *Historia del Análisis PEST-Pestel*. Recuperado el 10 de enero de 2020, de https://foda-dafo.com/historia-del-analisis-pest-pestel/

17. Huerta, D. S. (2 de 11 de 2017). *Historia del análisis FODA o DAFO*. Recuperado el 15 de enero de 2020, de http://www.foda-dafo.com

18. Instituto de Auditores Interno. (s.f.). Recuperado el 10 de febrero de 2020, de https://na.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Spanish.pdf

19. interamerican-usa.com. (30 de julio de 2002). *Nuevaley frente a los fraudes contables (Ley Sarbanes-Oxley)*. Obtenido de http://interamerican-usa.com/articulos/Leyes/Ley-Sar-Oxley.htm

20. ISO. (s.f.). Recuperado el 3 de marzo de 2020, de ISO sitio web: https://www.iso.org/about-us.html

21. Mantilla, S. A. (2005). *Auditoría.* Pontificia Universidad Javeriana y Ecoe Ediciones.

22. Porter, M. E. (enero de 2008). Las cinco fuerzas competitivas que le dan a la estrategia. *Harvard Bussines Review América Látina*, 18. Recuperado el 02 de 03 de 2020, de

https://utecno.files.wordpress.com/2014/05/las_5_fuerzas_competitivas-_michael_porter-libre.pdf

23. Superintendencia de Bancos e Instituciones Financieras de Chile. (2009). *Riesgo Operacional: Conceptos y Mediciones.* Chile.

24. Vega, V. (Semptiembre de 2017). *Researchgate.net*. Recuperado el 15 de diciembre de 2019, de https://www.researchgate.net/figure/Figura-3-Cubos-de-gestion-de-riesgo-de-COSO-I-y-COSO-II_fig1_329323970

25. Zurita González, J., Martínez Pérez, J. F., & Rodríguez Montoya, F. (2009). La crisis financiera y económica del 2008. Origen y consecuencias en los Estados Unidos y México. *El Cotidiano*(157), 17-27. doi:https://www.redalyc.org/pdf/325/32512739003.pdf