Proceso de implementación y supervisión de un modelo de control del riesgo operativo para una sofipo enmarcado en la metodología COSO

[1]Nelson Yamid Cely Salamanca, [2]Isabel Casares San José-Martí y [3]Misaela Francisco Márquez

1,3. Sección de Estudios de Posgrado e Investigación
Instituto Politécnico Nacional-UPIICSA
Av. Té 950, Col. Granjas México, C.P. 08400,
Ciudad de México, México.
2. Presidenta de CASARES, ASESORIA
ACTUARIAL Y DE RIESGOS, S.L.
C/ Edgar Neville, 9 - 4ºD (Esquina C/Hernani)
28020 Madrid

nelsoncelysalamanca@gmail.com,
mcasares@mcasares.es,
mfrancisco@ipn.mx

Resumen—En el desarrollo organizacional actual, el tema de riesgos está tomando gran relevancia debido a la volatilidad y dinámica de los mercados y las crisis financieras presentadas alrededor de los años 90 y luego entre el 2006 y 2008; para entender el origen de este modelo de gestión, también es necesario considerar que las entidades bancarias son las más sensibles y expuestas a riesgos, por ello es que desde allí surge un marco para mejorar el control y la evaluación de los riesgos, dentro de esta categoría se puede considerar el modelo desarrollado por el Committee of Sponsoring de la Commission Treadway (COSO) que en su última versión se presenta como un Enterprise Risk Managment (ERM). La presente investigación se centra en la implementación de un modelo que permita a una entidad del sector financiero mejorar el control de los riesgos y garantizar la eficacia y eficiencia en su desarrollo misional, la investigación actualmente presenta resultados sobre: los principales modelos y metodologías de control del riesgo operativo, el diagnóstico de los elementos del modelo de control de riesgos presente en la organización enmarcado en COSO III y la elaboración de una matriz de riesgos para evaluar los mismos. A futuro se espera pasar a desarrollar e implementar los elementos que permitan llevar a una madurez el modelo de control de riesgo operativo en la organización. La idea con el proyecto es extrapolar el modelo diseñado y dar uso a COSO ERM 2017, al nivel que se usa la ISO 31000, aplicándolo en empresas de cualquier sector, incluidas por supuesto las empresas del sector logístico.

Palabras Clave— riesgo operacional, comité de Basilea, COSO, SOFIPO, ISO 31000.

I. INTRODUCCIÓN

Considerando que el riesgo operacional empezó a tomar relevancia a partir de los años noventa, y que fue conocido gracias a noticias de fraude de compañías multinacionales, asociado a los falsos reportes de estados financieros ante los entes reguladores, lo que llevo a fuertes consecuencias de perdidas para el sector financiero y la economía en general. El riesgo operacional siempre ha sido inherente al sistema bancario por el tipo de recursos que maneja, consientes de ello el comité de Basilea en el año 2004 emite un acuerdo conocido como Basilea II donde da relevancia al riesgo operacional y lo pone al nivel del riesgo de crédito y el riesgo de mercado. Como se verá más adelante en este artículo, en este acuerdo y en publicaciones posteriores el comité de Basilea sienta las bases para la formulación de un modelo de control interno que permita mitigar el riesgo operativo.

Derivado de esto entidades consultoras y agremiaciones allegadas al sector financiero, empiezan a construir desde su amplia experiencia modelos que se pudieran implementar a las organizaciones financieras y que dieran respuesta a las regulaciones propuestas por el comité de Basilea. Es así que firmas como: KPMG quien diseño su esquema de consultoría, Deloitte y PWC que se asociaron con el comité de organizaciones patrocinadoras de la comisión Treadway y trabajan hoy por hoy en la actualización de COSO, que está en su versión 2017. El instituto de auditores internos trabajo en su propio modelo de gobierno diseñando el esquema de las tres líneas de defensa; y porque no una organización como la ISO al ver que los modelos de gestión de riesgos se estaban enfocando en un sector específico decide elaborar la ISO 31000 como norma no certificable, que ofrece un modelo para que empresas de todo tipo no solo financieras empiecen a tratar sus riesgos.

En este proyecto se parte de la revisión literaria de los principales modelos creados para el tratamiento de los riesgos operativos como lo son Acuerdo de Basilea, la norma ISO 31000, el modelo COSO III, para ello se partió de una consulta en bases de datos de amplia divulgación y haciendo uso también de informes de las firmas consultoras, esto último considerando que no se disponen de muchos artículos donde se publique específicamente la aplicación de los modelos y metodologías acá expuestos.

Luego se presenta un caso de estudio que ofrece como ventaja, acercar al lector al diagnóstico de un modelo de control del riesgo operativo enmarcado en COSO III así como a la elaboración de una matriz de riesgos para la evaluación de los mismos. Al final del artículo y derivado de la revisión bibliográfica, se hacen algunos planteamientos de aplicación de futuros avances en la investigación como lo es el desarrollo y la implementación de métodos cuantitativos para la definición de las reservas de capital por riesgo operativo y otra propuesta que plantea el uso de ISO 31000 a empresas del sector logístico.

II. EL MODELO DE LAS CUATRO LNEAS DE DEFENSA

Una guía revisada y que sirve para la definición de una estructura que ayude a la implementación y el mantenimiento de un sistema de control interno adecuado, es la que se encuentra en el paper “The four lines of defence model for financial institutions” [1] emitido por the Bank for International Settlements y que se resume en la Figura 1.

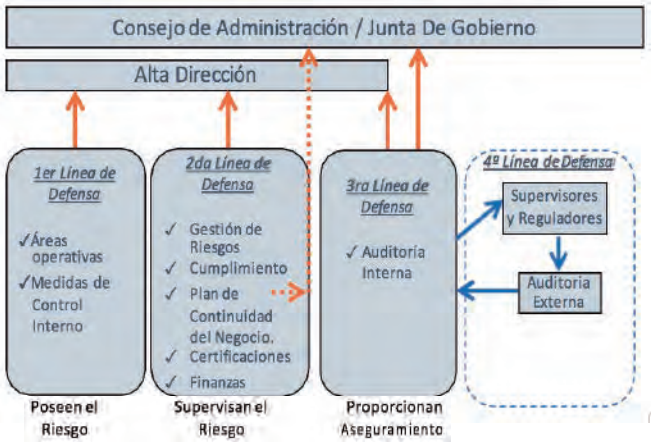

Figura 1. Modelo de las 4 lineas de defensa
Fuente: Elaboración propia

Se puede definir como lo contempla el libro rojo de la OCEG [2] que comprende, las unidades de negocio, áreas operativas con sus respectivas medidas de control interno en la primera línea de defensa, las cuales están respaldadas en la segunda línea de defensa, donde se encuentran las funciones de cumplimiento y gestión de riesgos que proveen el monitoreo de los controles implementados, la tercera línea de defensa está compuesta por los auditores internos que proveen el aseguramiento del gobierno corporativo, la gestión del riesgo y el cumplimiento o los controles y en la cuarta línea de defensa [1] se encontrarían para las entidades financieras los supervisores delegados por los organismos de regulación y los auditores externos de la firma, los cuales junto a los auditores internos deben generar una estrecha relación para garantizar la eficacia del sistema de control interno.

El garantizar que una organización cuente con una estructura claramente definida, como la expuesta en la de las 4 líneas de defensa, garantizara un mayor gado de eficacia del sistema de control interno, independiente del modelo que escoja de los que se mencionan y explican a continuación.

III. PRINCIPALES MODELOS PARA EL TRATAMIENTO DEL RIESGO OPERATIVO

Hace más de una década que el comité de Basilea [3], comité creado por las principales entidades financieras del mundo, para analizar y regular la operación financiera a nivel global y que toma su nombre por la ubicación de sus oficinas en la ciudad sueca que lleva este nombre, puso en evidencia la importancia de considerar al riesgo operacional en el mismo nivel de riesgo de crédito y del riesgo de mercado en el sector financiero [4]. Eventos como los ocurridos en los 90 en firmas como ENRON, SUMITOMO CORP, XEROX, entre otras que trataron el riesgo operacional de manera reactiva, impulsaron la definición y parametrización de este tipo de riesgo, es así como, el comité de Basilea menciona que la practica de tratar el riesgo operacional en una entidad financiera no es una práctica nueva, de hecho, siempre se ha tratado el riesgo de prevenir fraudes, mantener controles internos íntegros y reducir errores entre otras actividades. Sin embargo, era necesario brindar una guía de parte del banco de bancos centrales (Basilea) sobre el tratamiento del riesgo operacional con un enfoque anticipado y cuantitativo. Es entonces que se emite una nueva versión del acuerdo de Basilea conocido como Basilea II.

A. Basilea II

Esta propuesta del comité se fundamenta en tres pilares [3], en su primer pilar, establece los lineamientos para definir el requerimiento de capital de un banco y el nivel de riesgo en que este pueda incurrir. Lo que en esencia se puede traducir en que los bancos tengan el capital suficiente para protegerse de riesgo de crédito, riesgo operacional y el riesgo de mercado.

Basilea II presenta tres alternativas o modelos para el cálculo del capital requerido, a saber: Metodología del indicador básico, el método estándar, métodos de medición avanzados (AMA), no obstante la recomendación del comité es que cada entidad defina sus propios modelos de estimación, toda vez que serán más precisos y tendrán menores requerimientos de capital; el segundo pilar define la necesidad de ejercer una supervisión efectiva de las entidades financieras que permita a los supervisores un control solido y el mejoramiento de sus procesos; por ultimo el pilar tres busca que el comportamiento del mercado motive una buena administración que fomente la transparencia de los reportes públicos de los bancos y un nivel más alto de autodisciplina.

Sobre el manejo de riesgo operacional, el comité de Basilea publico un documento aclaratorio titulado “Sound Practices for the management and supervision of operational risk” [3]. En este documento el comité aclara que cada entidad tiene autonomía para identificar los generadores de riesgo operacional, sin embargo, suministra

una guía de posibles generadores de riesgo operacional con importantes impactos en la organización.

En este mismo documento se suministran diez principios agrupados en 4 niveles que las entidades deben tener en cuenta para dar un buen manejo a la administración de sus riesgos, el primer nivel corresponde al desarrollo de un apropiado ambiente de manejo de riesgos, asociado a tres principios que definen responsabilidades y deberes para la junta directiva y para el presidente de la entidad. El siguiente nivel corresponde a la administración de riesgos que está integrado por cuatro principios enfocados a la identificación, valoración, monitoreo, mitigación y control. El tercer nivel corresponde al papel de los supervisores que esta integrado por dos principios que asignan responsabilidad a los supervisores para exigir a los bancos un sistema efectivo de control de riesgo operacional, y la evaluación regular, directa o indirectamente de estos principios. El cuarto nivel de esta guía corresponde a la revelación de información asociado a un principio que es la definición de los bancos de tener una comunicación pública suficiente para que las partes involucradas puedan medir la exposición al riesgo operacional de la entidad financiera y la calidad de la administración de este riesgo.

B. ISO 31000

Posterior a la publicación del acuerdo de Basilea, empezaron a surgir modelos, por parte de organizaciones consultoras, asociaciones públicas y privadas, orientados a brindar a las organizaciones financieras (principalmente), herramientas para hacer una correcta administración de sus riesgos, un catalizador que permitió el surgimiento del estándar ISO 31000 fue el hecho de que los modelos que surgieron estaban enfocados a sectores específicos mayormente financieros y al sector tecnológico, es por ello que el objetivo general de esta norma es mostrar los principios y las directrices generales para la gestión del riesgo en cualquier tipo de organización [5]. Esta norma a pesar de ser la familia de las normas ISO es una norma no certificable, con este estándar se busca minimizar, gestionar, y controlar cualquier tipo de riesgo.

En el siguiente diagrama se ilustra de manera general la metodología propuesta por ISO 31000.

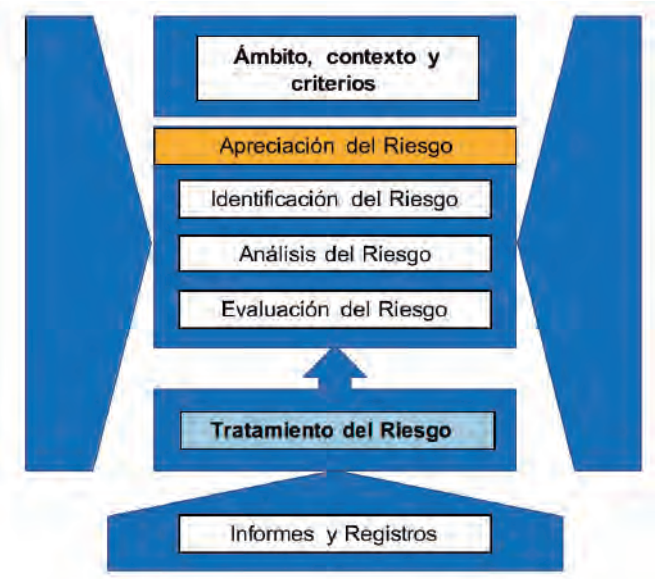

Figura 2. Esquema del modelo para la gestión del riesgo bajo ISO 31000

Como se puede apreciar, el modelo propuesto por ISO 31000, está enmarcado por una constante comunicación y consulta de las partes involucradas [5], el modelo de gestión del riesgo bajo esta norma parte de un establecimiento del contexto, donde se incluye la definición de objetivos, que respondan a lo que se busca con la implementación de este sistema de gestión, cual será el alcance de los mismos, el presupuesto y la asignación de recursos a la vez que se nombren los responsables de liderar y supervisar las políticas y elementos definidos [6].

Dentro del macroproceso de apreciación de riesgos se establece la identificación de los riesgos, su análisis y evaluación; tarea que se puede apoyar en los lideres de cada área, quienes pueden identificar los eventos que pueden sacar de control sus procesos. Espero sea claro para el lector que estos modelos tienen toda una estructura clara, sobre el deber hacer, pero no sobre el como hacerlo o que herramientas emplear.

Posterior a la valoración del riesgo se encuentra el tratamiento del riesgo en donde la organización

debe definir la respuesta que dará al riesgo en cada proceso, esta puede ser: suprimir el riesgo, lo cual puede ser muy raro teniendo en cuenta que la supresión involucraría no ejecutar la actividad o el objetivo organizacional, otra opción es trasferir el riesgo, mitigar su impacto o su probabilidad, aceptar el riesgo de buscar un resultado que sea positivo, considerando que se tenga una provisión para hacer frente a un resultado negativo, es importante también mantener informes y registros permanentes de este tratamiento.

Todo lo anterior, según el modelo de ISO debe estar enmarcado por un seguimiento y revisión constante, donde se supervise de manera crítica o de forma continua del estado, con el fin de identificar cambios con respecto al nivel de desempeño definido. La ISO 31000, se puede decir que por su carácter general contempla una definición de este tipo para los riesgos, que en este caso es: "la incertidumbre que surge en la consecución de un objetivo" [5].

C. COSO III

Uno de los métodos que mas se asemeja a los lineamientos definidos en Basilea II y que a su vez es uno de los modelos de mayor divulgación en las compañías financieras es el desarrollado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO). En su versión COSO III presenta un esquema de cubo que ilustra la manera como se deben administrar los riesgos [7].

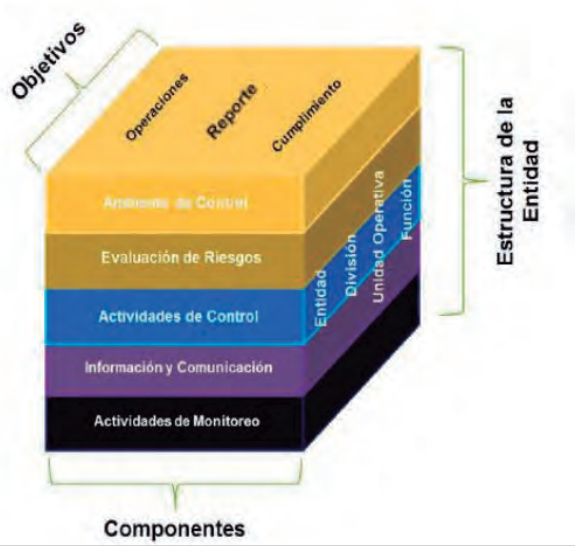

Figura 3. Modelo de control de Riesgos COSO

El cubo de COSO presenta cinco áreas estratégicas con los componentes y los principios que tienen una cobertura transversal [7], el primer componente está relacionado con el ambiente de control, es donde la organización debe establecer la estructura para que exista el compromiso con la integridad y los valores éticos de la empresa. Se debe garantizar, además el ejercicio de las responsabilidades de supervisión y sobre quien recaerán, es necesario establecer también una estructura que evidencie las líneas de autoridad y las responsabilidades y, en último, cerrar el entorno de control con la atracción, el desarrollo y la retención del personal clave [8].

Una vez definido el entorno de control, el siguiente nivel en el cubo es, realizar una evaluación de los riesgos. Para ello, la organización debe considerar que de acuerdo con los objetivos definidos de operación, es necesario hacer una evaluación y un reporte respecto al cumplimiento de estos, a tiempo que según los resultados de la evaluación es necesario identificar y evaluar los cambios relevantes, en este punto es donde se debe hacer la valoración del impacto y la frecuencia de los riesgos.

Posterior a la evaluación de los riesgos se deben realizar actividades de control de acuerdo a los resultados, dentro de estas actividades se tiene como ejemplo, la implementación de políticas y procedimientos, también existen la selección y el desarrollo de actividades de control sobre las personas o sobre las tecnologías, en resumen, estas actividades se deben contemplar en todos los niveles y funciones [7], las actividades de control deben contemplar las estrategias vistas en ISO 31000 como los son: evitar, asumir, mitigar, etc.

Definidas las actividades de control, se debe hacer la divulgación e implementación de las mismas a través del mecanismo que COSO III define como información y comunicación [9], donde se generan contenidos relevantes a todos los niveles de la organización, se establecen y se usan los canales de comunicación interna y se

tiene como premisa que el mensaje debe ser claro por parte de la alta dirección; también es importante la comunicación con accionistas, autoridades gubernamentales y analistas financieros.

El ultimo nivel está relacionado con las actividades de monitoreo, que es con las cuales se reinicia un ciclo de mejora continua, desde este nivel es donde se hacen evaluaciones continuas e individuales y se comunicaran las deficiencias, que permitan tomar las medidas correctivas.

Las actividades descritas anteriormente se consideran, son transversales pues contemplan todos los niveles de la entidad, iniciando con niveles de dirección general, luego se contemplan divisiones que pueda tener la entidad, dentro de cada división los controles diseñados también cubren a las unidades de operación, donde a su vez se definen medidas de control que se implementaran en la ejecución de las funciones (parte lateral del cubo). Los parámetros generales sobre los cuales se mantiene COSO III y que están en la parte superior del CUBO, incluyen la operación, la calidad de los reportes financieros y la conformidad.

En la versión COSO III, cada uno de los 5 niveles expuestos se encuentra conformado por un grupo respectivo de principios que en total por los 5 niveles suman 17 principios.

D. COSO ERM 2017

La última versión de COSO ERM [10], definida como: la gestión de riesgos empresariales o ERM (por sus siglas en inglés): Integración con estrategia y rendimiento, tiene dentro de sus avances proporcionar mayor valor a la gestión del riesgo articulándolo con la estrategia, y llevando a largo plazo a una mejora en el rendimiento y el cumplimiento de los objetivos; adicional facilita las expectativas para la gobernanza y la supervisión, presenta nuevas formas para hacer frente a la cultura de riesgos y lograr los objetivos en el contexto del negocio. Se ajusta mejor al panorama cambiante del riesgo y ayuda a comprender mejor la naturaleza del riesgo, tiene en cuenta que cada una de las elecciones que se hace en las organizaciones conlleva riesgos y aprovechando esto, tiene presente que, si se consideran los riesgos en la formulación de la estrategia y los objetivos empresariales de una organización, es la administración de riesgos empresariales la que ayudara a optimizar los resultados esperados [10] panorama cambiante del riesgo y ayuda a comprender mejor la naturaleza del riesgo, tiene en cuenta que cada una de las elecciones que se hace en las organizaciones conlleva riesgos y aprovechando esto, tiene presente que, si se consideran los riesgos en la formulación de la estrategia y los objetivos empresariales de una organización, es la administración de riesgos empresariales la que ayudara a optimizar los resultados esperados [10].

La nueva versión tiene en cuenta que las causas más significativas de la destrucción de valor están presentes en la posibilidad de que la estrategia no se alinee con la misión y la visión de la entidad. Considera que la administración de riesgos empresariales, redunda en una mejora de la selección de estrategias. La elección de una estrategia requiere una toma de decisiones estructurada que analice el riesgo y alinee los recursos con la misión y la visión de la organización. El nuevo marco de COSO incluye los siguientes cinco componentes interrelacionados:
1. Gobierno y cultura. 2. Estrategia y establecimiento de objetivos. 3. Desempeño (rendimiento). 4. Revisión 5. Información. En esta versión de COSO, se contemplan 20 principios distribuidos en los 5 principios. Sin embargo y, por motivos de alcance de la investigación, el presente trabajo se centra en la versión de COSO III en la sociedad financiera popular, SOFIPO de estudio.

Según lo definido por Basilea [3] “la mayoría de los tipos de riesgos operacionales implican fallas en los controles internos y en el gobierno corporativo”, en los países con sistemas bancarios de carácter multinacional, existen más modelos que están alineados con los requerimientos de Basilea II ejemplos de ellos son: el Control Objetives for Information and Related Tecnology (COBIT) estándar, publicado por la asociación de auditoria

y control de sistemas de información (ISACA), el Sarbanes Oxley Act., en Canadá cuentan con el Criteria of Control Comité (CoCo), en Gran Bretaña con el (FSA), entre otras naciones como Holanda y Alemania con regulaciones como: ROC y Kon TraG, respectivamente. Las regulaciones todas ellas orientadas al mejoramiento de los controles internos, la administración de riesgos y el fortalecimiento del gobierno corporativo.

IV. RIESGO OPERACIONAL

A. Definición

El comité de Basilea define al riesgo operacional como: "el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos, esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación" [3].

Teniendo en cuenta que las directrices que emite el comité de Basilea [4] dejan claro que corresponde a cada país definir los mecanismos de regulación sugeridos, es por ello que en un escenario más local y teniendo en cuenta que la entidad de regular la actividad financiera en México es la comisión nacional bancaria y de valores, en adelante CNBV, se debe considerar para la presente investigación la regulación dada por esta entidad dentro de la ley general de la comisión nacional bancaria y de valores de México (LCNBV) [11] que en su artículo 4 sección V establece las facultades para solicitar reportes de riesgo operacional que para el caso corresponde a la serie R28, y en su anexo dos presenta la clasificación del riesgo operacional por tipos, subtipos y clases de eventos; dentro de los tipos de eventos están: Fraude Interno, Fraude externo, relaciones laborales y seguridad en el puesto de trabajo, clientes productos y prácticas empresariales, desastres naturales y otros acontecimientos, incidencias en el negocio y fallos en los sistemas, ejecución entrega y gestión de procesos. Cada tipo de riesgo cuenta con subtipos así por ejemplo para el tipo de riesgo de fraude interno, los subtipos serán: actividades no autorizadas, hurto y fraude interno y seguridad de los sistemas, para cada subtipo la comisión también tiene dispuestas unas clases de eventos, para el caso anterior en el subtipo de seguridad de los sistemas, la CNBV establece cuatro clases de eventos a saber: Vulneración de sistemas de seguridad, daños por ataques informáticos, robos de información (con pérdidas pecuniarias), esquema que es muy similar al propuesto en el acuerdo de Basilea II. Teniendo en cuenta lo anterior, las organizaciones financieras usan esta información para el diseño de sus matrices de identificación de riesgo operacional.

B. Relación del riesgo inherente y riesgo residual

Cuando se procede a la valoración del riesgo operacional, es necesario considerar dos etapas en el tratamiento que se da al riesgo.

La primera etapa consiste en valorar el riesgo inherente que es tal cual el que presenta el evento y que de acuerdo con el procedimiento definido al interior de la organización en su procedimiento M1-MA-RO correspondiente a la metodología para la evaluación de riesgos operativos, debe ir asociado a una probabilidad y a un impacto. La segunda etapa corresponde a considerar que una vez definidos e implementados los controles, la nueva calificación del riesgo en cuanto a probabilidad e impacto corresponderá al riesgo residual. En la Figura 4, se explica esta relación.

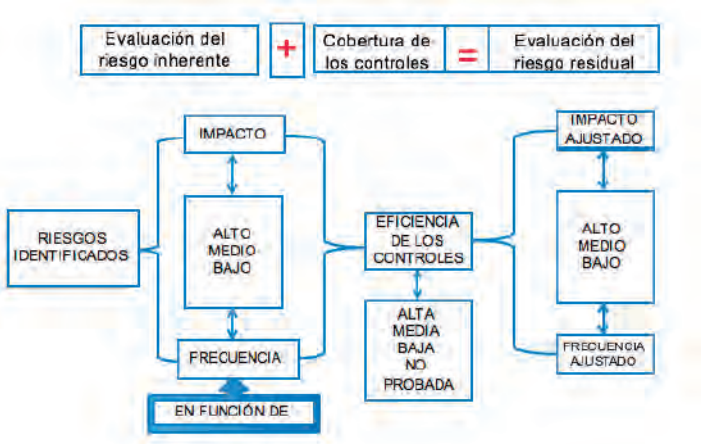

Figura 4. Relación riesgo inherente, riesgo residual y controles establecidos
Fuente: Elaboración propia

V.ANTECEDENTES DEL PROBLEMA DE INVESTIGACIÓN

El origen de regulaciones como la Sarbanes – Oxley Act [12], ley que fue aprobada por el congreso de los estados unidos en julio de 2002 e introdujo cambios legislativos relacionados con practicas financieras y con gobierno corporativo y cuyo objetivo principal fue proteger a los inversionistas por medio del mejoramiento de la precisión y confiabilidad de la información corporativa revelada y, evitar inconvenientes como los ya mencionados que tuvieron lugar en los años 90.

A nivel nacional, el gobierno de México a través de la CNBV ha emitido regulaciones que siguiendo los lineamientos establecidos por Basilea II exigen a las organizaciones definir buenas prácticas de gobierno corporativo, y un sistema de control interno y de riesgos adecuado.

En la SOFIPO de estudio, la necesidad más clara que fue planteada en las primeras entrevistas con el director de contraloría de la organización y tiene que ver con un evento que se presentó dos años atrás, donde por una problemática en particular se descubrió la necesidad de encontrar una mejor práctica de gobierno corporativo que articulara la comunicación y la gestión de los órganos de decisión de la entidad con los objetivos planteados desde la junta de gobierno de la organización.

Uno de los síntomas detonantes, se relacionó con una falla en la operación entre los diferentes niveles de la organización involucrados en los nuevos productos ofrecidos por la entidad, específicamente una línea de crédito diseñada por la junta de gobierno; luego de entrar en operación el producto, se empezaron a tener inconvenientes en la venta; lo anterior siguió creciendo con desconocimiento y falta de comunicación hacia el área de control interno; la consecuencia más grave fue un serio incremento en el índice de morosidad, esto llevo a un mayor requerimiento de capital por parte de los socios como medida de contingencia para disminuir el índice de riesgo crediticio. Los aportes extraordinarios requeridos a los socios ascendieron a la suma de $ 100.000.000 de pesos mexicanos. El problema, no solo se vio reflejado al interior de la organización, sino que de cara al ente regulador como la CNBV, la SOFIPO tuvo que responder y pactar planes de acción y sustentar los montos necesarios para mitigar el impacto de los riesgos mencionados y asegurar continuidad del negocio.

Hay serios indicios que demuestran las bondades que ofrece para una organización financiera el apoyar su modelo de control interno de acuerdo con el marco planteado por COSO III ver [13] donde se muestran los resultados de una encuesta aplicada por la Universidad del Estado de Carolina del Norte y refleja el logro de un buen desempeño de los sistemas de Control Interno asociados a la implementación del modelo COSO.

Desde el área de contraloría de la SOFIPO, y como parte de los planes de acción para hacer frente a la situación mencionada, sumado a los soportes que en la bibliografía se encuentran asociados a la implementación de COSO, [3] las guías emitidas por el comité de Basilea; se determina que se está fallando en el diseño y la ejecución adecuada del sistema de control interno, se sugiere que a los problemas presentados, pueden abordarse desde la solución planteada con la implementación de la metodología propuesta por COSO III, razón por la cual se presentó la oportunidad de desarrollar el trabajo de investigación en esta organización.

VI. METODOLOGIA

Teniendo en cuenta la revisión de la literatura [14], el presente proyecto aborda, desde una investigación cualitativa, descriptiva, exploratoria y propositiva.

Se considera que es exploratoria y descriptiva porque está orientada hacia el problema, describe sus elementos y a través de las herramientas de gestión COSO III las investigara a profundidad; es propositiva porque al finalizar la etapa exploratoria descriptiva se presentaran nuevos diseños para el sistema de control interno de la organización.

Para el diseño de la investigación se tuvo en cuenta las etapas de observación o diagnóstico inicial del Sistema de Control Interno, luego se evaluarán los elementos del sistema que sean necesarios; posterior a ello se implementará la propuesta y finalmente se hará un monitoreo de la efectividad de estos controles. Se puede decir que, para este enfoque de investigación se llega desde un método inductivo, donde se aplica un sistema de control interno diseñado bajo un marco específico, para llegar a unas conclusiones generales sobre el desempeño de la organización en cuanto a eficacia, eficiencia y continuidad.

VII. IMPLEMENTACIÓN DE LA HERRAMIENTA DE DIAGNOSTICO

Una vez revisadas las condiciones ideales para un sistema de control interno, para saber si está diseñado de acuerdo con las directrices sugeridas por el modelo COSO III se hace uso de una herramienta de diagnóstico del estado actual de implementación.

La herramienta de diagnóstico aplicada [15] mide el nivel de madurez del sistema de control interno, en su estructura presenta una clasificación de los cinco niveles de COSO III dentro de los cuales se encuentran contenidos los 17 principios del modelo, en esta herramienta por cada principio se encuentran definidas unas categorías denominadas puntos de enfoque, cada uno se califica según el nivel de madurez en: Inmaduro, Repetición, Definición, Maduro y Nivel Óptimo, definidos y asociados a un valor numérico como se describe a continuación:

Inmaduro:
Los controles están fragmentados y son específicos para cada caso; generalmente se gestionan en silos y de forma reactiva; falta de políticas y procedimientos formales; se depende de acciones individuales para que se realice el trabajo; existe una mayor posibilidad de cometer errores; y grandes costos ocasionados por ineficiencias operativas.
Se asigna valor numérico de 1.

Repetición:
Los controles se establecen con una determinada estructura política: aún falta documentación formal de procesos claves; existe cierta claridad de las funciones, responsabilidades y autoridad, pero no existe responsabilidad; existe una mayor disciplina y las pautas respaldan la repetición; y la gran confianza en el personal existente produce una gran resistencia al cambio. Se asigna calificación 2.

Definición:
Los controles están bien documentados y definidos, en consecuencia, existe coherencia incluso en tiempos de cambio; existe una conciencia general de la importancia de los controles internos; las brechas de control son detectadas y controladas de manera oportuna; la supervisión del desempeño es informal; depositando una gran confianza en la diligencia del personal. Calificado con 3.

Maduro:
Se utilizan indicadores claves de desempeño y técnicas de supervisión para medir el éxito; existe mayor confianza en los controles de prevención que en los controles de detección; una sólida autoevaluación de la eficiencia operativa es desarrollada por parte de los responsables de los procesos; y existe una cadena de responsabilidad bien definida. Se califica con 4.

Nivel Óptimo:
Se considera que los controles poseen un nivel óptimo, en función del benchmarking y las mejores prácticas; la estructura del control está altamente automatizada y se actualiza de forma automática; creando una ventaja competitiva; existe uso intensivo de supervisión en tiempo real y marcos o enfoques de control implementados. Se califica con 5.

La herramienta fue contestada por el director de contraloría de la entidad de estudio.

El siguiente paso fue, tomar las calificaciones de los puntos de enfoque dentro de cada principio de COSO y promediar para obtener una calificación global por cada principio, obteniendo la siguiente calificación que se muestra en la Figura 5.

Figura 5. Diagnostico por principios de acuerdo a COSO III en la SOFIPO de estudio

Tabla 1. Calificación por niveles de COSO III en SOFIPO de estudio

NIVELES DE COSO III	CALIFICACIÓN
Entorno /Ambiente de Control	2,92
Evaluación de Riesgos	3,48
Actividades de Control	2,75
Información y Comunicación	2,64
Actividades de Supervisión	2,20
SISTEMA EN GENERAL	**2,80**
VALOR ESPERADO	**5**

Como se puede apreciar el nivel de calificación oscila desde los valores correspondientes a repetición (2) y muy cercano al valor de calificación de maduro (4), teniendo los valores más bajos en la calificación que corresponde al principio 17 que en COSO III establece: "La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda".

Teniendo en cuenta que dentro de los antecedentes una de las falencias fue el no contar con un medio de control adecuado que permitiera detectar las fallas en los productos ofertados; las mayores fortalezas encontradas en este diagnóstico inicial se presentan en el principio 3 que corresponde a: "La dirección establece con la supervisión del consejo, las estructuras, líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos", y el principio 9: "La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno". Lo cual demuestra que la organización tiene una estructura claramente definida además de hacer un correcto monitoreo de los cambios en el entorno que pueden llegar a presentar una amenaza, al sistema de control interno.

A nivel general y luego de promediar las calificaciones de cada uno de los 17 principios en los 5 niveles de COSO se obtuvieron los siguientes resultados, que se contemplan en la Tabla 1.

Como se aprecia en estos resultados de la evaluación inicial, el área más fuerte de la compañía corresponde al nivel de evaluación de riesgos, como se ha mencionado en los párrafos anteriores, las entidades financieras por diseño hacen un control efectivo de sus riesgos por las exigencias de las entidades reguladoras, adicional el ambiente de control se percibe más desarrollado, pero las oportunidades de mejora se encuentran principalmente en actividades de supervisión, información y comunicación y en actividades de control; que son en parte las falencias que permitieron que situaciones como las de dos años atrás se materializaran, los resultados se resumen en la Figura 6.

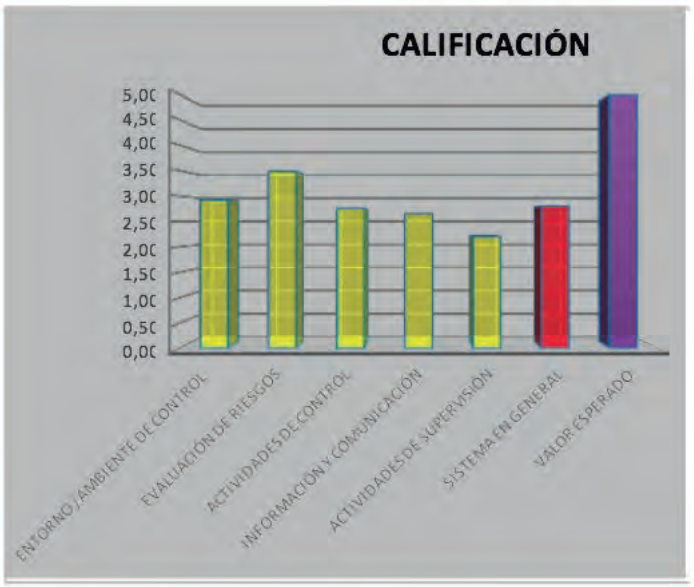

Figura 6. Calificación general en los cinco niveles definidos por COSO III

De los resultados anteriores y teniendo en cuenta metodologías como las definidas por COSO y adaptando las guías establecidas por el Comité de Basilea, el área de contraloría en conjunto con las actividades adelantadas por Auditoria y Riesgos de la SOFIPO de estudio, se inicia en el 2018 un trabajo más estricto de evaluación de sus riesgos operativos haciendo uso de una matriz de riesgos, de la cual se presenta una breve descripción.

VIII. ELABORACIÓN DE LA MATRIZ DE RIESGOS

Para la elaboración de esta matriz se parte de los conceptos revisados previamente en cuanto a la definición de riesgo operacional.

Las primeras columnas de la matriz parten de un ID de identificación del riesgo, la fecha de identificación, área donde se identificó, el producto de la compañía afectado, el proceso al que pertenece ese producto, la categoría, evento y subevento del riesgo según esta definido en el R28 de la CNBV la descripción de ese riesgo. Las columnas que siguen en la Tabla 2 van más aplicadas a la metodología descrita para la calificación del riesgo inherente, dependiente de la probabilidad y del impacto, donde se parte de una calificación de la probabilidad de ocurrencia que puede ser: raro con valor de 1, improbable con valor de 2 posible con valor de 3 probable con valor de 4 y casi cierto con valor de 5. Éstas probabilidades están relacionadas con las frecuencias de acuerdo con la Tabla 2 que se presenta a continuación:

Tabla 2. Escala de valoración de la frecuencia de los riesgos en la empresa de estudio

Frecuencia	Nivel	Áreas con volumen Moderado de Operación	Áreas con volúmenes grandes de operación
Casi Cierto	5	Mayor a 60 veces al año	<=40%
Probable	4	37 a 60 veces cada año	<=35%
Posible	3	12 a 36 veces cada año	<=25%
Improbable	2	4 a 8 veces cada año	<=20%
Raro	1	2 a 4 veces cada año	<=10%

Para la calificación del impacto se toman en cuenta los criterios de: Muy Alto con valor de 5, alto con valor de 4, moderado con valor de 3 leve con valor de 2 y muy leve con una calificación de 1. Valores que se asignan de acuerdo con el impacto monetario estimado en la entidad, sus cifras están en pesos mexicanos.

Tabla 3. Escala de valoración del impacto de los riesgos en la empresa de estudio

Impacto	Nivel	Descripción
Muy alto	5	Mayor $259,000.00
Alto	4	$150,000.20 - $259,00.00
Moderado	3	$100,000.20 - $150,000.20
Leve	2	$50,000.20 - $100,000.20
Muy leve	1	Hasta $50,000.20

De la calificación de la probabilidad y el impacto para cada riesgo se hace una multiplicación y su resultado nos da una calificación que constituirá la calificación del riesgo inherente y que permitirá clasificarlo en la matriz de calor, según la escala que se ilustra en la Tabla 5, se clasifican los riesgos así:

Tabla 4. Escala de valoración del impacto de los riesgos en la empresa de estudio

Score	Rating
> 20	Extremo
entre 10 y 19	Muy Alto
Entre 5 y 9	Alto
Entre 3 y 4	Moderado
Menor a 2	Bajo

Después de la calificación de los riesgos se da prioridad a los riesgos con calificación de Extremo, Muy Alto y Alto. Teniendo en cuenta lo definido en COSO, para el caso de la empresa de estudio se obtuvo un total de 253 riesgos identificados de los cuales en la categoría de Alto y Muy Alto existen 62 riesgos a los cuales se le debe dar prioridad posterior a la calificación de los riesgos se debe definir las actividades de control, que para el caso de la empresa son definidos por los dueños de cada proceso, posterior a ello y según la

organización estratégica seguida por la empresa para el control de sus riesgos teniendo como marco el modelo de las cuatro líneas de defensa, corresponde al área de contraloría pedir al encargado de cada proceso evidencia de las actividades de control adelantadas. Por ello, se agregó a la matriz una opción para la calificación de los controles que permite decidir el nuevo valor de la probabilidad y el impacto combinados para definir una calificación del riesgo residual.

La nueva calificación de riesgo, después de evaluar la efectividad de los controles está basada en los mismos valores definidos en la Tabla 4.

Hasta el momento, se presenta un avance parcial del proyecto con las actividades que se han hecho desde el diagnóstico hasta la implementación de la matriz de evaluación, calificación y definición de los controles a los riesgos de origen operacional.

IX. CONCLUSIONES Y FUTURO EN LA INVESTIGACIÓN

Como se pudo apreciar luego de aplicar la herramienta de diagnóstico, hay brechas que se pueden cerrar para mejorar el sistema de control interno de la organización dentro de las cuales están: actividades referentes al ambiente de control como la definición de procedimientos más estrictos de supervisión y en cuanto a comunicación se necesita formalizar y fortalecer los canales de comunicación para llevar el sistema de control interno desde la estructura de COSO y el modelo de las tres líneas de defensa que está actualmente, a un nivel que se apoye más en los entes externos como cuarta línea de defensa y que incluya a los supervisores y auditores.

Otra de las actividades que se recomienda luego de la aplicación del presente instrumento es el uso de una segunda herramienta de diagnóstico que esta vez será contestada por los directivos de las principales áreas de la organización, esto tiene como objetivo final dar más objetividad al diagnóstico inicial y definir de manera acertiva las actividades necesarias para implementar la metodología de control interno bajo el esquema de COSO III.

En cuanto al seguimiento de la implementación eficaz del sistema de control interno, la tarea siguiente consiste en calificar los controles e identificar cuáles de los 62 controles claves, correspondientes a los riesgos de mayor criticidad, son preventivos o detectivos y de cara buscar eficiencia en el sistema de control interno, evaluar y mejorar los controles manuales para llevarlos a semiautomáticos o automáticos [16].

Una de las etapas en el desarrollo de estos modelos y, por cumplimiento reglamentario, se deben cumplir y es lo referente a la cuantificación del capital a reservar por riesgos operativos, procedimiento que parte de los datos de frecuencia de cada riesgo y mediante el uso de herramientas estadísticas como la simulación de Montecarlo permite hacer reservas de capital más precisas en [17], se puede ver una descripción de los modelos generales.

A pesar de la justificación de la ISO 31000, donde los demás modelos de gestión del riesgo sólo se aplican a organizaciones específicas, existen publicaciones por parte de COSO [18] sobre la implementación de su modelo en empresas de diversas áreas.

En el área de Supply Chain, considerando la información como la suministrada en [19] donde se evidencia un creciente número de publicaciones en la evaluación de riesgos en esta área en los últimos años y adicionalmente viendo a proyectos desarrollados como el que se expone en [20] en el cual se empleó ISO 31000, consideramos que de acuerdo al desarrollo de esta investigación se puede en futuros trabajos hacer una aproximación de un modelo que contemple el uso de COSO III en la evaluación del riesgo en la cadena de suministros.

REFERENCIAS

[1] The Bank for International Settlements (2015), The Four Lines of Defence Model for Financial Institutions . Occasional Paper Nº11.

[2] GRC Capability Model (Red Book) Full Version Standard Filed in Integrated GRC , Free , Capability Model. Recuperado el 06 de abril de 2019 de https://go.oceg.org/grc-capability-model-red-book.

[3] BASEL COMITÉ ON BANKING SUPERVISION. Sound Practices for the Management and Supervision of Operational Risk. Bank for Internacional Settlenments. https:/www.bis.org.

[4] Leon, R. Nuevo Acuerdo de Basilea: Aspectos Critícos y Desafios para su Implantación. II Congreso de Riesgo Financiero. Cartagena , agosto 1 de 2003.

[5] ISO, 2018. "Risk management - Guidelines." ISO 31000:2018, Geneva. [6] IEC, 2009. Risk management - Risk assessment techniques: IEC 31010:2009.

[7] Miles. E, Stephen. E, Frank. J, Cara. B, Charles. H, Aaron. J, Jourdan. C, Posklenski. A, Sallie. J, (2015), COSO: ITERNAL CONTROL – INTEGRATED FRAMEWORK. Recuperado el día 20 de Octubre de 2018, de https://www.coso.org/Documents/990025P-Executive-Summary-Final-may20.pdf

[8] Galaz, Yamazaki, R, U (2015), COSO Enterprise Risk Services, Evaluación de Riesgos. Corporative Presentation, DELOITTE.

[9] Russell A (2005) There is no Shortcut to Good Controls, ABI/INFORM Collection 4, Pag 62.

[10] Miles. E, Stephen. E, Frank. J, Cara. B, Charles. H, Aaron. J, Jourdan. C, Posklenski. A, Sallie. J, (2015), COSO: ITERNAL CONTROL –INTEGRATED FRAMEWORK. Recuperado el día 20 de Octubre de 2018, de https://www.coso.org/Documents/990025P-Executive-Summary-Final-may20.pdf

[11] Secretaria de Hacienda y Crédito Público, Comisión Nacional Bancaria y de Valores, Disposiciones de Carácter General Aplicables a las Entidades de Ahorro y Crédito Popular, Organismos de Integración, Sociedades Financieras Comunitarias y Organismos de Integración Financiera Rural, a que se Refiere la Ley de Ahorro y Crédito Popular, 26 de Abril de 2018.

[12] www.sarbanes-oxley-forum.com/

[13] J. Moody (2011) Enterprise Risk Management COSO Framework Proves Efficacious.

[14] Sampieri R. H y otros (2014), Metodología de la Investigación 6 Ed.Capítulo 12, Pag 468 – 528.

[15] Casares, I y Lizarzaburu, E (2016), Introducción a la Gestión Integral de Riesgos Empresariales Enfoque: ISO 31000 Primera Ed. Capitulo 7, Pag 101.

[16] Herramientas para el Control Interno, https://www.auditool.org/herramientas. Consultada el día 28 de Octubre de 2018.

[17] Franco, L. Velazques, E (2009) Alternativas Fundamentales para Cuantificar el Riesgo Operacional, ECOS DE ECONOMIA, Nº 30 año 14, Abril de 2010.

[18] COSO Issues Guidance for Healthcare Providers, https://www.coso.org/Documents/COSO-CROWE-COSO-Internal- Control-Integrated-Framework.pdf. Consultada el día 02 de Mayo de 2019.

[19] Tsan-Ming, C. Chun-Hung, C, Hing-Kai, C (2016) . Risk Management of Logistics Systems, ELSEVIER, en prensa. Contents lists available at Science Direc Transportation Research Part E.

[20] Rébula de Oliveira,U. Silva,F. Martins, H. Pamplona, V. (2017) The ISO 31000 Standard in Supply Chain Risk Management. Journal of Cleaner Production "Articulo Aceptado".