

3. Marco Teórico de la Metodología

3.1. Identificación de las Necesidades y Expectativas de la Administración

Antecedentes del Proyecto

Como antecedente del proyecto, es necesario que se declaren las razones operativas, económicas y legales o de cumplimiento. A continuación se indican las razones por las cuales es indispensable la implementación de la gestión del riesgo operacional en una entidad del sector financiero, (las siguientes razones son anunciativas más no limitativas).

Razones Operativas
<input type="checkbox"/> Identificar riesgos asociados a las operaciones que ponga en peligro la continuidad del negocio.
<input type="checkbox"/> Establecer estándares de control para efectos de mitigar los riesgos en relación a los objetivos y estrategia del negocio.
<input type="checkbox"/> Establecer lineamientos y procedimientos operativos y administrativos que permita la efectividad de procesos, empleados y flujo información.
<input type="checkbox"/> Contar con una infraestructura y procedimientos que permita la continuidad de procesos.
<input type="checkbox"/> Prevención del fraude interno: Robos de empleados, mal uso de información confidencial.
<input type="checkbox"/> Prevención del fraude externo: Atraco, falsificación, daños por intrusión indebida en los sistemas informáticos.
<input type="checkbox"/> Establecer relaciones laborales saludables y seguridad en el puesto de trabajo.
<input type="checkbox"/> Procurar sanas prácticas con clientes, productos y negocios, previniendo blanqueo de capitales, abusos, negociación fraudulenta, ventas no autorizadas ,etc.
Razones Económicas
<input type="checkbox"/> Fortalecer la apreciación de oportunidades de negocio.
<input type="checkbox"/> Mejorar la imagen al público inversionista, clientes y proveedores.
<input type="checkbox"/> Evitar sanciones o multas económicas por no cumplir con la regulación local o internacional.
<input type="checkbox"/> Prevenir daños a los activos materiales por terrorismo, vandalismo, terremotos, incendios, inundaciones, etc.
Razones Legales
<input type="checkbox"/> Mejorar el manejo de la información jurídica con clientes y empleados procurando su integridad y validez.
<input type="checkbox"/> Eficientar la administración de colaterales / garantías.
<input type="checkbox"/> Prevenir prácticas inadecuadas de contrapartes distintas de clientes, litigios con proveedores y distribuidores.
<input type="checkbox"/> Cumplir con los requerimientos legales de entidades regulatorias o supervisores locales (incluida la generación de información financiera).

Declaración de Expectativas de la Administración

Una vez que se ha reconocido la necesidad y razones fundamentales de la Administración del Riesgo Operacional que son la base para determinar posteriormente el objetivo y alcance del proyecto, es necesario que la administración anuncie las expectativas mínimas del proyecto a los diversos Responsables de área o de función para concientizar a los empleados de la necesidad de contar con una Administración del Riesgo Operacional.

Así mismo se deben proporcionar las instrucciones a seguir en relación con el marco de referencia y estructura de documentación y responsabilidades.

Para dar inicio a las instrucciones se declara los requisitos a cumplir con el marco de referencia, que se refiere a la documentación o en su caso a la adecuación de la estructura del marco de control interno existente, con respecto a objetivos estratégicos, operativos y legales (incluidos los de generación de información financiera).

El reconocimiento y la documentación del marco de referencia de control interno anunciado por la Administración y el Consejo de Administración deben contener al menos lo siguiente:

- Identificar y documentar los Procesos críticos vinculados con objetivos operativos, estratégicos, de cumplimiento y de generación de información financiera.
- Identificar riesgos.
 - Riesgos asociados con cada proceso de negocio crítico que afecta el logro de los objetivos que persigue ese proceso, unidad o ciclo de negocio.
- Identificar y en su caso implementar controles para mitigar esos riesgos.
- Realizar evaluaciones a los controles establecidos.
- Definir y poner en marcha los planes de acción en caso de detectar deficiencias en controles.
- Presentar programas de monitoreo y de mantenimiento de tal modo que pueda ser auditado, mejorado y actualizado.

Una vez dadas las instrucciones con los requisitos mínimos de la administración para los empleados y demás funcionarios de la compañía, toca el turno de aclarar la estructura de documentación del marco de referencia, en la cual se debe de tomar en cuenta lo siguiente:

- La existencia de manuales de políticas y procedimientos, así como de flujogramas para la administración efectiva del riesgo operacional como parte de la identificación, documentación y validación de los procesos de la compañía.

- La existencia de evidencia documental o soporte de la realización de las actividades inherentes a cada proceso en especial la de los controles internos establecidos.
- Diseño de un modelo de documentación soporte, referente a la evaluación y de cumplimiento con auditorías.
- Diseño y documentación de procedimientos de monitoreo, supervisión y comunicación de cambios, planes de acción / remediación, etc, a lo largo de los diferentes ciclos de negocio y procesos de la compañía.
- La posibilidad adquirir o desarrollar aplicativos o sistemas informáticos para la administración central del programa de administración del riesgo operacional.

Como en todo proyecto se busca optimizar los recursos de la compañía es necesario instruir la constitución de una coordinación o equipo encargado, así como a un líder de proyecto cuyo objetivo sea centralizar y eficientar al máximo el proceso de administración del riesgo operacional. Así mismo se deben asignar responsabilidades para los empleados y funcionarios de la entidad como coordinadores de área con el fin realizar la implementación y documentación del marco de referencia y del cumplimiento de las instrucciones mínimas de la administración. Los coordinadores pueden ser a nivel de ciclo de negocio, proceso, unidad o área funcional, según convenga.

En la figura 3.1 resume en fases las instrucciones a seguir por parte de la administración así mismo indica los plazos a cumplir.

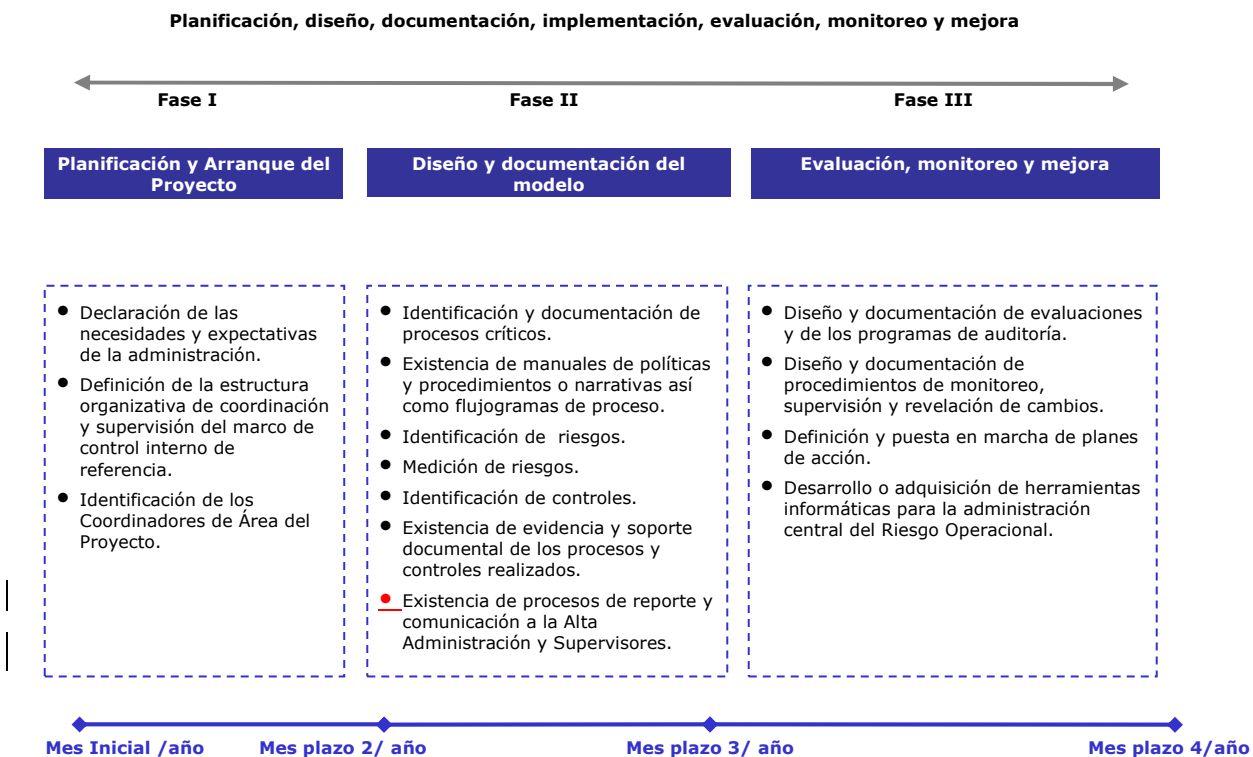


Figura 3.1 Fases con las instrucciones a seguir por parte de la Administración.

Planteamiento de Objetivos y Alcance

El planteamiento de objetivos que fundamentalmente persigue la administración incluye al menos lo siguiente:

- El desarrollo de políticas y procedimientos que proporcionen la seguridad razonable respecto al logro de los objetivos del negocio, vinculados a la estrategia, operaciones y cumplimiento (incluido la generación de información financiera) a lo largo y en todos los niveles de la compañía.
- El desarrollo de políticas y procedimientos que permitan el cumplimiento de los requerimientos regulatorios locales referentes a la administración del riesgo operacional y del marco de control interno.

El alcance planteado es el entendimiento, diseño, implementación y documentación de los procesos y subprocesos críticos que permitan el cumplimiento de los objetivos, incluido el proceso de generación de información financiera.

3.2. Análisis y Entendimiento de Ciclo(s) y Procesos de Negocio

Estructura de Gobierno y Administración

Estructura Organizacional

Inicialmente se debe de conocer el estado que guarda actualmente la compañía, en cuanto a la forma en como esta organizada, haciendo énfasis en los procesos de negocios que operan en la compañía.

La forma más recomendable es realizar inicialmente un desglose a nivel Grupo o entidad ya que hay que definir si a nivel grupo la entidad financiera posee subsidiarias ubicadas en diferentes regiones (países).

Luego de haber realizado la identificación de las subsidiarias a los cuales se tiene contemplado por la naturaleza misma del negocio, se prosigue a definir los ciclos de negocios, unidades funcionales que caen dentro de cada entidad o subsidiaria.

De acuerdo con el enfoque de procesos, que es necesario para realizar la administración del riesgo operacional es indispensable ubicar los procesos críticos de negocio relativos al logro de los objetivos y estrategia de la compañía por cada ciclo de negocio, en este punto es muy importante que cada proceso crítico sea asociado con su ciclo de negocio.

Para cada proceso crítico hallado y asociado es necesario realizar un desglose de éste para comprender las partes que lo integran, a estas partes las llamaremos subproceso, es vital que cada proceso este correctamente segregado por sus diferentes subprocesos ya que es posible que un subproceso puede estar presente o estar interconectado con más de

un proceso de negocio, como por ejemplo el subproceso de Liquidación de Cuentas Interbancarias que esta asociado al proceso de captación vista o plazo, así como con el proceso de Cámara de Compensación.

Para lograr un adecuado entendimiento de la estructura organizacional de la entidad es necesario paralelamente a esta, definir un esquema de responsabilidades de alto nivel, es decir aquellos funcionarios que reconocen la propiedad para la administración de los ciclos de negocio, procesos y subprocesos dentro de la entidad o inclusive si aplica a nivel Grupo.

Definición de ciclos de negocio

Normalmente se tiene que definir los ciclos de negocio en función de su incidencia o contribución con el logro de los objetivos del negocio y en especial con su incidencia en el cumplimiento regulatorio. También se puede considerar la clasificación de estos como de negocio o de soporte, por ejemplo un ciclo de negocio en una entidad de banca múltiple es la Tesorería, mientras una de soporte sería la Administración de Nómina y Personal.

El desglose de la estructura organizacional y de responsabilidades se puede resumir como se indica en la figura 3.2.

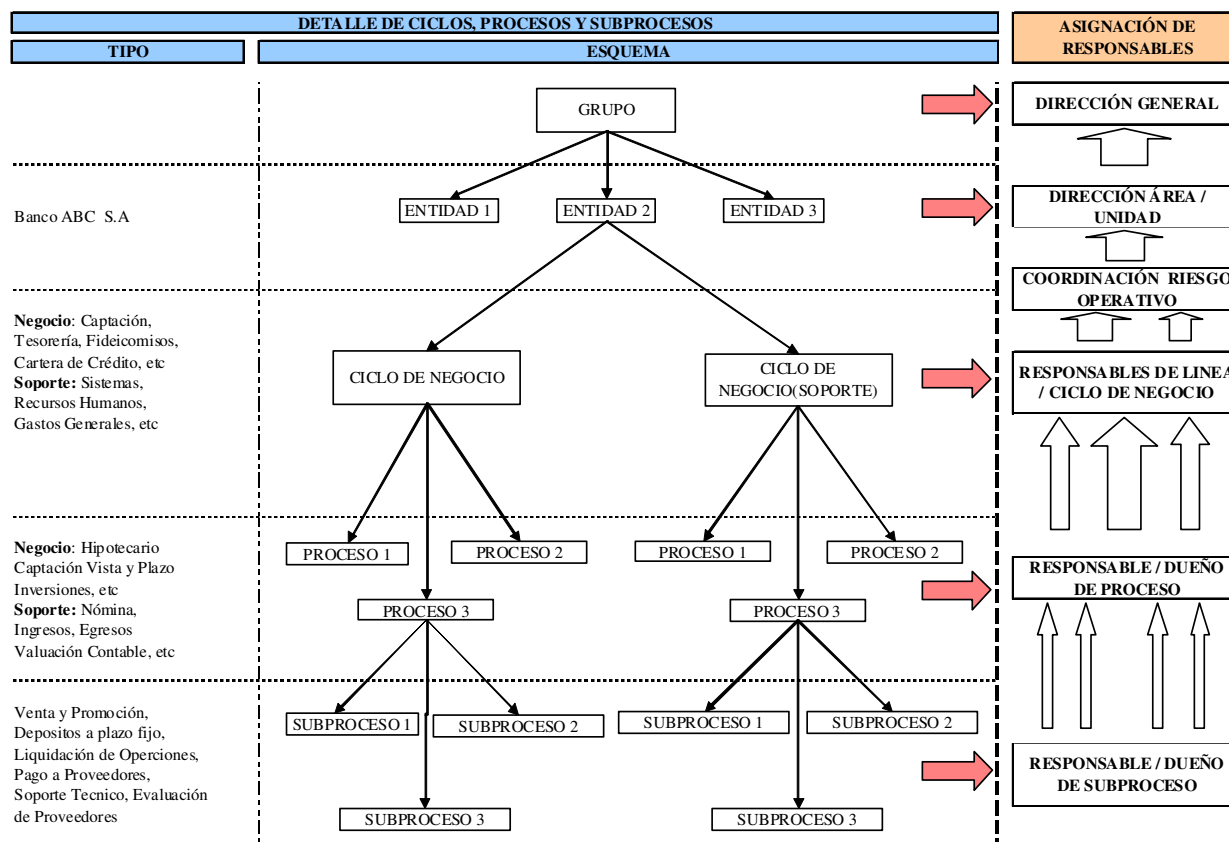


Figura 3.2: Ejemplo del desglose de la estructura organizacional y de responsabilidades.

Diseño organizacional

La clave en el diseño organizacional radica en la definición de roles y responsabilidades. Para el caso de la administración del riesgo operacional se hace mediante la identificación de las competencias y capacidades así como de las necesidades de cada integrante de la entidad para el correcto desempeño de funciones y responsabilidades que inciden en el funcionamiento del sistema de administración del riesgo operacional.

En nuestro modelo de administración del riesgo operacional se realiza una asignación de responsabilidades de acuerdo al esquema de la figura 3.3.

Director Área / Unidad : _____
 Coordinador de Administración Riesgo Operativo: _____

Ciclo de Negocio	Responsable del Ciclo de Negocio	Dueño del Proceso	Dueño del Subproceso

Figura 3.3: Asignación de responsabilidades.

Elaboración del plan de trabajo

El equipo coordinador o encargado de la Administración del Riesgo Operacional es el designado para la elaboración del plan de trabajo. Una vez que se hayan definido las responsabilidades, se esta en posición de elaborar el plan de trabajo cuyo objetivo es el documentar y estructurar la planeación del proyecto de diseño e implementación del Sistema de Administración del Riesgo Operacional, evaluación al diseño e implementación, evaluación sobre los resultados así como del monitoreo y mejora continua del Sistema para lo cual el contenido de dicho plan es el siguiente:

- Organizar un programa de actividades o tareas por parte del responsable del equipo coordinador o facilitador del proyecto y de los responsables directos de ciclos, procesos y subprocesos vs tareas o responsabilidades asignadas.
- Planear los recursos: Asignar Personal, Recursos Informáticos o Sistemas y fechas o plazos de término por cada ciclo / proceso / subproceso.
- Pactar o agendar juntas de arranque con los líderes de cada área funcional o dueños de procesos.
- Registrar y dar seguimiento a un calendario de juntas de avance.

Lo anterior puede ser complementado con un programa de aseguramiento de calidad mediante el establecimiento de las siguientes actividades:

- Establecer procedimientos de atención a conflictos.
- Administrar los cambios al programa de trabajo original.
- Monitoreo y reporte de avances.
- Control en el presupuesto del proyecto: Personal, Sistemas y fechas o plazos de término.
- Programar revisiones continuas o intermedias y finales de los avances y entregables de los responsables de los subprocesos y facilitadores o equipo coordinador de la Administración del Riesgo Operacional.

3.3. Diseño e Implementación del Sistema de Administración del Riesgo Operacional

El coordinador o el equipo encargado de la Administración del Riesgo Operacional definirá los criterios para el diseño e implementación del Sistema, así mismo de la administración de todo lo relativo a la documentación generada, y coordinará las acciones de validación de esta con la Dirección, de igual modo los recursos y plazos para la evaluación y monitoreo tal y como se menciona en el plan de trabajo.

Como condición necesaria inicial para la documentación de procesos específicos que forman parte del sistema de administración del riesgo operacional, esta la de diferenciar los ciclos, procesos y subprocesos.

Mapeo de Procesos

El esquema se visualiza en la documentación de cada uno de los procesos que se identifiquen conforme a una estructura que se describe a continuación.

Nombre de la entidad o grupo.
Nombre del ciclo de negocio o soporte.
Nombre del proceso.
Tipología de proceso.
Dueño o responsable del proceso.

Nombre del subproceso.
Descripción del subproceso.
Dueño o responsable del subproceso.

Es importante que una vez realizado el llenado de esta tabla cada coordinador o responsable asignado por la administración de la unidad de negocio correspondiente, valide que la información contenida sea la correcta.

Ciclos de negocio y soporte

Es de suma importancia clasificar a los procesos con base en el ciclo al cual pertenecen asignándolos como de soporte o de negocios es decir los de negocio son aquellos que afectan de modo directo la prestación del servicio o producto así también aquellos que permiten desarrollar o implantar la estrategia de la administración. A su vez los ciclos de soporte son aquellos que permiten a la Administración de la entidad, dar continuidad a las operaciones. A continuación se muestra un ejemplo de esta clasificación donde se recomienda asignar a cada ciclo un código o clave para efectos de administración y seguimiento.

Ciclos de negocio	Código del Ciclo
Tesorería e Inversiones	
Cartera de Crédito	
Captación	
Administración de Activos	
Fideicomisos	
Administración de Riesgos	
Atención al cliente	

Ciclos de Soporte	Código del Ciclo
Nómina y personal	
Servicios Generales	

Sistemas	
Contabilidad y Finanzas	
Legal y Cumplimiento	
Auditoría Interna	

Nota: Los ciclos indicados no pretenden ser limitativos, los ciclos de negocio varían de entidad en entidad en función del tamaño y complejidad de la compañía, solo se pretende ejemplificar algunos ciclos.

Tipología del proceso

Es posible categorizar cada proceso de acuerdo a su función y periodicidad y se muestra como sigue:

Tipología	Descripción
Rutinario	Son aquellos que son recurrentes.
No rutinario	Son procesos que ocurren de forma periódica es decir no están asociados con actividades recurrentes.
Negocio	Son aquellos que inciden directamente en la prestación del servicio u ofrecimiento de un producto y por lo tanto en la satisfacción del cliente.
Soporte	Son procesos que permiten la continuidad de las operaciones y la operación misma de la entidad.

Nombre y descripción del subproceso

La siguiente categoría y por ende sujeto a la diagramación del flujo de operaciones y de elaboración de guías, manuales o narrativas de acuerdo con las necesidades de la compañía, es el subproceso, al menos un subproceso, esta incluido dentro de un proceso, el nombre del subproceso esta influenciado por el objetivo y fin último del mismo, ya sea como etapa inicial, intermedia o final para el logro del objetivo del proceso, realización del producto o prestación del servicio.

Para describir el subproceso se debe hacer una introducción o presentación, luego de una breve indicación de la función e importancia de éste dentro del proceso, declarar el alcance o limitaciones que tiene y finalmente el fundamento regulatorio o legal que lo norma.

Diagramación y documentación del proceso y subproceso

Previo al inicio de la documentación del subproceso, los dueños o responsables del proceso y subproceso deben de tomar en cuenta los siguientes aspectos:

- La documentación (manuales de procedimientos, guías operativas, narrativas, flujos de proceso) debe quedar claramente descritos los aspectos relacionados con el inicio, autorización, registro, procesamiento y contabilización de las transacciones u operaciones.
- Se hará referencia a cada una de las diferentes áreas, unidades de negocio de la entidad que estén involucrados.
- La descripción deberá tener el suficiente detalle como para servir de soporte para la posterior identificación de los riesgos y controles internos para mitigar tales riesgos.
- Se deberá identificar los sistemas o aplicativos que intervienen en el desarrollo del subproceso y en general del proceso, así como de la documentación, insumos y entregables asociados.
- Se hará la identificación de todos los clientes internos y externos, proveedores u otros participantes (entidades gubernamentales o regulatorias).
- Los responsables o dueños del subproceso y proceso deben definir con precisión las entradas y salidas al subproceso que puede ser otro subproceso o proceso, cliente, proveedor, entidad regulatoria o gubernamental, área funcional, departamento, así como sistemas o aplicativos.

En el anexo 3 se muestra un formato sugerido para la diagramación del subproceso⁸.

Para realizar un efectivo diagramado o mapeo de procesos es recomendable seguir con las siguientes reglas:

- No se debe de incluir dentro del subproceso a otro subproceso en todo caso es posible nombrar a otro subproceso como entrada o salida, denominado como subproceso precedente o consecuente según corresponda.
- Las entradas o salidas al subproceso específico debe estar asociado a un producto, insumo (información o documentación relevante), sistema u aplicativo, área u unidad funcional, entidad regulatoria o subproceso según sea el caso.
- Los rombos o decisiones siempre deben estar conectados a una actividad, tarea o paso del subproceso.
- El flujo del proceso debe empezar de arriba hacia abajo o de izquierda a derecha.

⁸ Para el diseño del formato sugerido se tomaron en cuenta las recomendaciones presentadas en el libro “Implementación de la ISO 9000:2000”, Seaver Matt, Editorial Panorama Editorial, México 2003, pp. 23 - 24.

- Todo subproceso debe especificar su objetivo, área o unidad funcional así como al proceso y ciclo de negocio o soporte al cual pertenece.

Mapeo de Riesgos

Es indispensable que los responsables del proceso y subproceso declaren los riesgos asociados con el desarrollo de las actividades o tareas diarias; estos riesgos deben estar identificados en la documentación (narrativas del proceso, guías operativas o manuales de procedimientos, así como en los flujos de proceso).

Descripción del riesgo

Para cada subproceso se debe detallar el paso o tarea, así como todos aquellos puntos que potencialmente pudieran ocasionar o producir error (intencional o no intencional) durante el inicio, registro, procesamiento, autorización o liquidación de transacciones como parte de las operaciones rutinarias o no rutinarias, como antecedente a la descripción del riesgo. Lo más importante en esta etapa es identificar y documentar todos los riesgos relevantes que afecten al logro de los objetivos que sean inherentes al proceso.

Tipología del riesgo

Una vez identificados y descritos los riesgos es posible categorizarlos con base en los criterios u especificaciones del Comité de Supervisión Bancaria de Basilea, en el anexo 2 se muestran las tipologías hasta en un tercer nivel de detalle especificadas por el citado Comité y que también cumplen con la tipología indicada en las disposiciones de carácter general aplicables a las Instituciones de Crédito, emitidas por la CNBV⁹. Esta categorización se basa en el origen o procedencia del riesgo o sea de las causas que lo originan, así mismo, clasifica las fuentes de error potencial tales como fraude interno, fraude externo, relaciones laborales y seguridad en el puesto de trabajo, clientes, productos y prácticas empresariales, daños a activos materiales, incidencias en el negocio y fallos en los sistemas, ejecución, entrega y gestión de procesos.

Errores potenciales asociados a los riesgos

Es recomendable asociar a cada uno de los riesgos existentes e identificados en la descripción del subproceso su correspondiente error (o errores) potenciales con los que se asocia de acuerdo a las descripciones de errores que se especifican a continuación:

⁹ Anexo 12 A: Requisitos para la elaboración y actualización de la base de datos histórica a que contenga el registro sistemático de los diferentes tipos de pérdida asociada al riesgo operacional de las instituciones de crédito, emitido por la CNBV en su más reciente publicación del 12 de Agosto del 2011 como parte de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito, <http://www.cnbv.gob.mx/Paginas/Normatividad.aspx?an=37&c=27#is37>.

Error	Descripción
Integridad	Error producido por existir operaciones que no se han registrado. Transacciones, saldos y/o cualquier otro tipo de operaciones que no han sido registrados.
Validez	Error producido porque se hayan registrado operaciones que no son válidas y que no hayan existido como tal un evento.
Corte	Error por existir operaciones u eventos que no se encuentren registradas en el período correcto, es decir extemporáneas.
Registro	Error por existir operaciones u eventos registrados por un monto, concepto, cuenta contable u operativa o contrato incorrecto.
Valuación	Error por existir activos, pasivos, derechos o deudas calculados o determinados incorrectamente.
Presentación	Error por no estar correctamente clasificados u presentados en la cuenta o rubro de los estados financieros.

Impacto y probabilidad de ocurrencia del riesgo

La evaluación del riesgo se refiere a la magnitud del impacto del riesgo en la efectividad del proceso, pérdidas económicas derivadas del incumplimiento normativo, gastos no presupuestados, reducción en el valor de los activos, reducción de ingresos, costo de oportunidad, robos o fraudes. A la par de esta consideración se acompaña de la medición de la probabilidad de ocurrencia, que se refiere a la posibilidad de que un evento de riesgo dada su magnitud, tipo o categoría se presente durante el desarrollo o flujo de las operaciones en el proceso. A continuación se presenta una matriz con la evaluación del riesgo dada su impacto / magnitud y su probabilidad de ocurrencia.

Probabilidad de ocurrencia	Impacto / Magnitud					
	Imperceptible	Marginal	Moderado	Substancial	Severo	Desastroso
Alta probabilidad						
Probable						
Algo probable						
No probable						
Muy improbable						
Extremadamente improbable						

Intolerable	Indeseable	Marginalmente aceptable	Aceptable	Imperceptible
-------------	------------	-------------------------	-----------	---------------

La evaluación de los riesgos debe ser realizada para cada proceso y subproceso perteneciente a cada ciclo de negocio previamente considerado por la administración. En función de esta evaluación de los riesgos los responsables de cada proceso deben de determinar la respuesta que se tomara ante los riesgos y son cuatro: mitigar, compartir, aceptar o evitar. La decisión que tome la administración y los responsables de cada proceso influirá en el establecimiento del tipo de controles internos. En la figura 3.4 se muestra la relación entre el tipo de respuesta al riesgo con la evaluación.



Figura 3.4: Matriz de relación respuesta al riesgo vs evaluación.

Medición de riesgos

Una vez que se han identificado, descrito, categorizado y tipificado los riesgos, es importante analizar los componentes que todos los riesgos poseen, independientemente si es fraude interno, fraude externo, relaciones laborales y seguridad en el puesto de trabajo, clientes, productos y prácticas empresariales, daños a activos materiales, incidencias en el negocio y fallos en los sistemas, ejecución, entrega y gestión de proceso, si su impacto es mayor o menor o si su probabilidad de ocurrencia es alta o baja, en general todo los riesgos se componen de incertidumbre y exposición.

El asumir riesgos depende del grado de conocimiento que se tenga del negocio, de la experiencia en determinada actividad de negocios o por elementos de juicio (conocimiento de eventos relevantes de determinada industria, etc.), en suma la decisión de asumir riesgos descansa fundamentalmente en el juicio profesional y la experiencia.

Las compañías son las entidades que a través de diferentes procesos, productos, servicios y relaciones con empleados, clientes y autoridades, asumen riesgos, esos riesgos están presentes en todos los niveles de la organización, recaen en personas tales como accionistas / socios, acreedores, proveedores, empleados, clientes, consultores, auditores y supervisores.

La medición de riesgos pretende estimar las consecuencias esperadas de la materialización de los eventos de riesgos identificados y supone asignar un valor a la probabilidad de ocurrencia de un evento de riesgo y la magnitud o impacto (consecuencias tales como pérdidas económicas derivadas de conflictos legales, laborales, daño de imagen o fraudes).

Como parte esencial de la medición de los riesgos se sugiere diseñar y alimentar de una base de datos consolidada de pérdidas operacionales históricas que es el requisito fundamental para la cuantificación de riesgos; este proceso de elaboración de bases de datos debe ser una recolección de pérdidas y la asignación de éstas a los diversos ciclos de negocios, procesos, subprocesos y productos; no solo es registrar las pérdidas a causa de la materialización de riesgos operativos sino también entender sus causas. La metodología presentada en este trabajo solo se concreta a los requisitos para la consolidación de la base de datos de pérdidas, así como el análisis de las causas de las pérdidas y de los impactos y magnitud en cuanto a la pérdida potencial o real; así mismo, se hará mención a la determinación inicial cuantitativa de la probabilidad de ocurrencia de los eventos de pérdida, no se hará mención a la modelación probabilística para la obtención de la frecuencia de eventos o probabilidad de ocurrencia ni a la determinación de la magnitud de eventos de pérdida dado la escasez y confiabilidad de datos, la medición de riesgos aquí presentada es más bien la base para la posterior cuantificación de la frecuencia de pérdidas operacionales, la magnitud o severidad, así como del valor en riesgo “VaR” por riesgo operacional.

A continuación se propone una serie de pasos para medir los riesgos presentes en cada ciclo de negocio, proceso, subproceso, éstos pasos tienen el fin de concentrar una base de datos inicial relativa al impacto o intensidad de la pérdida y de la frecuencia en la ocurrencia de los eventos de riesgo (probabilidad de ocurrencia), y se detallan como sigue:

- Para determinar la frecuencia con lo que se presenta un determinado evento de riesgo, y así obtener una estimación inicial de la probabilidad de ocurrencia se realiza lo siguiente:
 - La coordinación o los encargados de la Administración del Riesgo Operacional realizan reuniones de trabajo con los responsables de cada proceso (o producto), así como con los responsables directos de la ejecución del subproceso, estas reuniones tienen el objeto de describir y consolidar todos los riesgos asociados con la ejecución del proceso (considerando condiciones normales de ejecución o situaciones de contingencia por fallos en la continuidad de sistemas o por incumplimiento de contrapartes o proveedores internos o externos relativa a la calidad y oportunidad en la entrega de información). Es importante señalar que en esta actividad es indispensable describir a detalle todos los eventos de riesgos presentes en cada proceso / subproceso o producto por cada ciclo de negocios, detallando la causa y el efecto del evento, así mismo se recomienda tomar como referencia la categorización de riesgo que propone el Comité de Supervisión Bancaria de Basilea en sus siete categorías¹⁰, para efectos de determinar el origen del riesgo indicadas en el anexo 2.

La determinación de la frecuencia inicial de la ocurrencia de los eventos de pérdida descansa fundamentalmente en la experiencia y juicio profesional que tengan los involucrados en la ejecución o puesta en marcha del proceso / subproceso y del grado de conocimiento que se tenga del ambiente de control, estilo operativo, nivel de experiencia y capacitación del personal, así como de la confiabilidad de los sistemas de información y de la calidad y oportunidad en la entrega de información y gestión del proceso. Se puede iniciar con una serie de aproximaciones tomando en cuenta la experiencia y del conocimiento de los eventos de pérdida reconocidos por cada área funcional de la entidad, estas aproximaciones pueden darse en función del tiempo (día, semana, mes, año) dependiendo de la frecuencia y exposición de la actividad asociada con el riesgo.

Una vez determinada esa aproximación se define una escala que indique la probabilidad de que se materialicen esos eventos de riesgos, en esta probabilidad se categorizan de acuerdo con la frecuencia, a continuación se sugiere una clasificación para la determinación inicial de la probabilidad de ocurrencia en función de una aproximación en la frecuencia con la que se presenta un evento de riesgo en determinado proceso / subproceso o producto.

¹⁰ Convergencia internacional de medidas y normas de capital, Comité de Supervisión Bancaria de Basilea, Banco de Pagos Internacionales, Junio de 2006, pp. 339 – 343, http://www.bis.org/publ/bcbs128_es.pdf.

Ocurrencia	Frecuencia
6 Alta probabilidad	1 vez por semana
5 Probable	1 vez por mes
4 Algo probable	1 vez por trimestre
3 No probable	1 vez por año
2 Muy improbable	1 vez cada cinco años
1 Extramadamente improbable	1 vez cada diez años

Descripción	Frecuencia	Probabilidad de ocurrencia					
		Alta probabilidad	Probable	Algo probable	No probable	Muy improbable	Extramadamente improbable
Causa - Efecto	Veces X día, semana, mes, año						

- Para determinar el tipo de impacto y la estimación de la magnitud de la pérdida dada la materialización de un evento de riesgo por proceso / subproceso o producto se realiza lo siguiente:
 - Una vez que se han identificado y consolidado todos los eventos de riesgos, los responsables del proceso y todos aquellos que intervienen en la ejecución o puesta en marcha de las actividades de los procesos y subprocesos, deberán definir el impacto que tiene cada uno de los riesgos identificados, el impacto puede ser en la generación de información financiera, en el cumplimiento de disposiciones legales, en la efectividad de operaciones (rentabilidad), cumplimiento de objetivos estratégicos u operativos, en la imagen pública de la compañía, y en las relaciones con el cliente y / o proveedores.
 - Para el caso de la determinación de la magnitud del impacto se realiza con base en el estudio de las disposiciones legales aplicables tales como sanciones por parte de la autoridad, o con base en criterios internos los cuales pueden ser establecidos por cada área funcional en relación con el tipo de operación / producto. A continuación se sugiere una tabla con una categorización de la magnitud del impacto, así como su pérdida potencial. Vale la pena mencionar que esta estimación en la magnitud del impacto (severidad) y su cuantificación (\$) depende de la experiencia y conocimiento del responsable del proceso o subproceso sobre las pérdidas que generarían por el riesgo operacional durante la realización de las actividades, así mismo esta estimación descansa en el juicio profesional de los responsables del proceso mediante el conocimiento que se tenga de las multas o sanciones de la autoridad en caso de

incumplimientos legales o por incumplimientos en las metas operativas o estándares de calidad, producción, rentabilidad o de servicio al cliente.

Impacto	Pérdida Potencial (\$)
Imperceptible	<\$M1
Marginal	\$M1 <= \$M2
Moderado	\$M2 <= \$M3
Substancial	\$M3 <= \$M4
Severo	\$M4 <= \$M5
Desastroso	> \$M5

Finalmente en el anexo 4 se muestra un formato de documentación para el mapeo y medición de riesgos, el cual es la base inicial para la elaboración de una base de datos de pérdidas, la cual es indispensable para la construcción o desarrollo de cualquier modelo de cuantificación, que por razones de insuficiencia de información en el presente trabajo no es posible realizar, sin embargo se sientan las bases para la administración y evaluación cualitativa que representa el antecedente para una fase posterior de cuantificación del riesgo operacional y de la determinación del capital mínimo por riesgo operacional.

Esta base de datos de pérdidas debe ser administrada por el equipo encargado de la administración del riesgo operacional.

Mapeo de Controles

Ya que se han identificado, descrito, tipificado y evaluado los riesgos para cada proceso y subproceso crítico ahora es posible identificar y describir los controles que mitiguen a esos riesgos. La documentación de tales controles también se realiza con el apoyo de los flujos de proceso (véase anexo 3), narrativas, manuales de políticas y procedimientos o guías operativas de la entidad.

Cada responsable de proceso o subproceso deberá de asignar a un responsable de control, asimismo se sugiere la clasificación de los controles como se indica a continuación:

Control mediante autorización. Implantación y monitoreo de límites de autorización en función del facultamiento del personal asignado.
Control mediante autorización. Aprobación de transacciones /

operaciones inusuales o emergentes.
Control mediante autorización. Autorización mediante segregación de funciones (prevención de fraudes).
Control mediante verificación. Validaciones de saldos, análisis y resolución de diferencias.
Control mediante verificación. Conciliaciones de datos u saldos.
Control mediante verificación. Recálculos.
Control mediante verificación. Seguimiento de indicadores o parámetros relevantes de desempeño.
Control mediante verificación. Seguimiento estándares de calidad del producto y / o prestación del servicio.
Control mediante monitoreo y supervisión. Seguimiento de las operaciones con el fin de vigilar el cumplimiento de políticas y procedimientos.
Control mediante monitoreo y supervisión. Seguimiento de las relaciones comerciales con el cliente / proveedores.
Control mediante monitoreo y supervisión. Seguimiento de las relaciones legales con entidades regulatorias.

Nota: La clasificación de controles aquí presentada no es limitativa ya que pueden existir más categorías de controles, ya que estos dependen de la magnitud y complejidad de la entidad.

Tipología de controles

Cada actividad de control se catalogará en función de sus características específicas como se indica:

Tipología	Descripción
Detectivo	Aquellas actividades de control que tienen como objetivo detectar errores que ya han ocurrido.
Preventivo	Aquellas actividades de control que tienen como objetivo prevenir errores antes de que sucedan.
Correctivo	Aquellas actividades de control que tienen como objetivo corregir o solucionar una vez detectada la falla o desviación.

Naturaleza del control

Cada actividad de control se catalogará en función de su naturaleza como se indica:

Tipología	Descripción
Automática	Actividades de control ejecutadas a través de algún aplicativo y no implica la voluntad o ingerencia de persona alguna.
Manual	Son actividades de control que requiere la participación de al menos una persona y está acompañada normalmente por el juicio o valoración de la persona que realiza el control.

Frecuencia del control

Se recomienda especificar la frecuencia según la realización de cada actividad de control dentro de cada subproceso:

En cada operación/actuación
Diaria
Semanal
Quincenal
Mensual
Trimestral
Semestral
Al cierre del ejercicio

Alcance de la actividad de control

Como parte del mapeo de controles es indispensable tipificar a los controles en función del alcance o grado de penetración que tiene a través de la organización ya sea en los diversos niveles de mando como en las diferentes áreas funcionales, para este caso de acuerdo con la metodología COSO¹¹ se han definido dos tipos y son:

Tipología	Descripción
Nivel Entidad	Aplican y permean a toda la empresa.
Nivel Transacción	Operan a nivel proceso (s) específico (s) / definido (s).

Documentación de los Procedimientos, Políticas o Actividades de Control

Todas las actividades de control significativas (políticas y procedimientos así como otros lineamientos de la entidad que dan las respuestas a los riesgos) deben estar documentadas, no obstante si se puede demostrar a través de pruebas que el control opera eficazmente. El problema radica en que sin documentación no se puede evidenciar el diseño, implementación y operación de los controles.

La documentación de los controles debe ser auditable incluyendo un mínimo de elementos que también son requeridos para propósitos de autoevaluación, a continuación se presentan algunas cuestiones a considerar en la documentación de las actividades de control y son:

- ¿Quién realiza o desempeña la actividad de control?
- ¿Cómo se realiza la actividad de control? (método, política o procedimiento asociado)

¹¹The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Framework, 2004, http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp.

- ¿Para qué o con qué fin se realiza la actividad de control? (cual es el objetivo del control)
- ¿Con qué periodicidad se realiza o desempeña la actividad de control? (frecuencia de ejecución)
- ¿Existe o interviene en la realización o ejecución de la actividad de control algún aplicativo o sistema?
- ¿Cómo y quién monitorea / revisa la actividad de control?
- ¿Cuál es la evidencia de la realización de la actividad de control?
- ¿Cuáles son los casos en los cuales se evade o pasa por alto los controles?
- ¿Qué procedimientos o documentos existen como parte del plan de acción en caso de interrupción de los sistemas?
- ¿Qué procedimientos existen en caso de ausencia del responsable de la realización y revisión de la actividad de control?
- ¿Cuál el procedimiento a seguir en caso de incumplimiento de contrapartes, proveedores internos u otras entidades con las cuales se comparten operaciones críticas para el negocio?
- ¿Existe evidencia de la realización de la actividad de control dentro de los horarios establecidos (internos y con contrapartes, clientes, entidades regulatorias)?

Es necesario indicar el grado de funcionamiento del control tal y como fue planeado es decir la adherencia de la documentación del control (políticas o procedimientos) contra la evidencia que es la documentación soporte resultado de la realización de la actividad de control, la evidencia debe de responder lo siguiente:

- ¿Es actualmente ejecutado el control tal como fue documentado y por la persona correcta?
- ¿Existe la evidencia suficiente de que funciona consistentemente?
- ¿Se monitorea y se revisa tal como está documentado?

Capacitación y Concienciación a Empleados

Cursos de capacitación a la gerencia y personal

El programa de entrenamiento o capacitación tiene que estar orientado a cumplir con las responsabilidades que el personal tiene a cargo, tomando en consideración políticas y procedimientos de control que se le han asignado al personal, sobretodo en la forma en como se tiene que documentar y preservar la evidencia de la realización de la actividad de control. Asimismo es importante que los empleados y la administración tengan bien en claro cuales son

sus límites de responsabilidad y de autoridad y más aún la concienciación de empleados y administración sobre el impacto o repercusiones que su comportamiento y desempeño tiene en el área funcional, entidad, clientes, socios o accionistas, proveedores y sociedad.

Los cursos de capacitación y actualización también deben de considerar la normatividad externa necesaria para aquellas áreas que así lo requieran, existen otras necesidades básicas que deben considerarse en la aplicación de cursos que entre otros destacan los siguientes:

- Cursos sobre el funcionamiento del aplicativo / herramientas informáticas residentes o indispensables para ejecución, monitoreo o evaluación de los controles.
- Trato con clientes, accionistas, proveedores, contrapartes financieras o legales así como con entidades regulatorias (SHCP, CNBV, CONSAR, IMSS, etc.).
- Continuidad de negocio, procedimientos de contingencia.
- Ética y comportamiento profesional.
- Cursos de especialización tendientes a eficientar el desempeño de las funciones según el puesto.

Cumplimiento y ética profesional

El objetivo es difundir a los empleados y a la administración prácticas que refuercen la integridad y los valores éticos así como el cumplimiento con la normatividad aplicable, para efectos de esta difusión se debe considerar lo siguiente:

- Existencia e implementación de códigos de conducta y otras políticas sobre prácticas de negocio apropiadas, conflictos de interés o estándares de comportamiento ético y profesional.
- Reforzar sanas prácticas en el trato con empleados, proveedores, clientes, inversionistas, competidores, auditores y supervisores.
- Canales de denuncia, los cuales deben estar dirigidos a todos empleados de la entidad, cuya finalidad es que se permita reportar o denunciar comportamientos indebidos o contrarios a la ética profesional y sanas practicas y el establecer sanciones, así como la toma de acciones correctivas a procesos o procedimientos mal diseñados o en su caso para la implementación de controles para la prevención o detección oportuna, preservando el trato anónimo del denunciante.

Retroalimentación y Validación de la Administración

Una vez culminado el mapeo de procesos, riesgos y controles es necesario realizar reuniones con los responsables de proceso y / o responsables de las diversas unidades funcionales con la coordinación o equipo encargado de la Administración del Riesgo Operacional con el objeto de conocer el grado de documentación logrado, es decir, el nivel de detalle y de especificaciones, y que toda la documentación preparada refleje las operaciones tal y como estas se desempeñan.

La retroalimentación y validación de la administración descansa fundamentalmente en la participación de los empleados de la entidad por medio de sesiones de trabajo mediante procedimientos de facilitación (puede ser liderada la sesión por expertos en riesgos y por líderes o cabezas de áreas con la suficiente autoridad para incentivar y patrocinar los cambios), con la finalidad de promover la participación de los principales involucrados en la operación o puesta en marcha de los procesos, subprocesos y demás actividades que están en posibilidad de transmitir la información relevante acerca del detalle de sus funciones, riesgos y controles.

3.4. Evaluación del Diseño del Sistema de Administración del Riesgo Operacional

La evaluación al sistema de administración del riesgo operacional se basa en el cumplimiento en el desempeño de los empleados a cargo de funciones de acuerdo a sus límites de autoridad y responsabilidad, desempeño del proceso, funcionamiento y continuidad de los sistemas u aplicativos así como de la agilidad del flujo y calidad de la información interna y externa de la compañía.

La evaluación del sistema de administración del riesgo es preferible que sea realizado por personas independientes al proceso, que no tengan injerencia en la puesta en marcha y mantenimiento de los controles por lo que es indispensable que la evaluación se efectúe en un contexto de independencia. La evaluación sin embargo puede ser realizada por el auditor interno o algún puesto con funciones similares o en su caso por un externo, así mismo la evaluación puede ser coordinada por el equipo encargado del Sistema de Administración del Riesgo Operacional para efectos de documentar y revelar a los Responsables o dueños de procesos de los posibles hallazgos o cambios en el diseño del Sistema de Administración del Riesgo Operacional.

Evaluación de los Componentes del Sistema de Administración del Riesgo Operacional

La evaluación se realiza tomando en consideración los componentes sobre los que descansa el sistema de administración del riesgo operacional y se refiere a los procesos, empleados, sistemas o aplicativos e información (interna y externa). Estos cuatro elementos se interrelacionan uno con el otro y el funcionamiento de uno afecta el funcionamiento de los demás. Las actividades de control descansan sobre estos cuatro elementos es decir, que para tener la seguridad razonable de que el control está operando con efectividad debemos tener la certeza de que estos cuatro elementos están funcionando eficazmente. En la figura 3.4 se muestra esta interrelación.

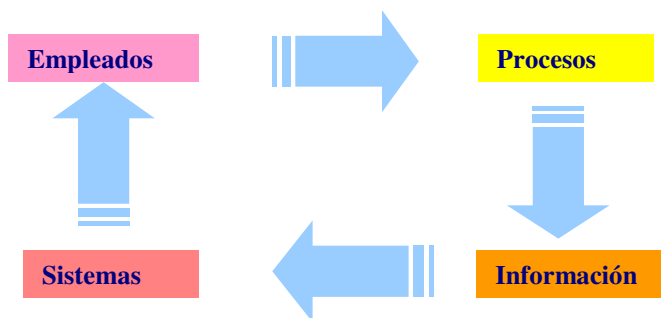


Figura 3.4: Componentes del sistema de administración del riesgo operacional

En la tabla 3.5 se muestran ciertos factores a considerar relativo al funcionamiento de cada uno de los componentes que permiten la evaluación del sistema de administración del riesgo operacional.

Empleados	Procesos
Grado de capacitación, especialización y demás competencias. Experiencia. Delegación de autoridad y responsabilidad. Comportamiento y valores éticos. Estilo operativo y filosofía de la administración. Relaciones laborales y seguridad en el puesto de trabajo.	Segregación de Funciones. Suficiencia de actividades de control (cobertura de riesgos). Fraude Interno / Externo. Cobertura de los riesgos a través de los controles establecidos. Errores de procesamiento de transacciones / operaciones. Relaciones con contrapartes comerciales y proveedores.
Sistemas o aplicativos	Información
Confiabilidad. Facultamiento y control de accesos. Delimitación de privilegios. Continuidad. Soporte y respaldos. Protección contra ataques.	Claridad y suficiencia de la información (interna y externa). Precisión y oportunidad en la transmisión de la información. Protección y resguardo de información. Uso confidencial y restringido de información privilegiada.

Tabla 3.5: Factores de los componentes del sistema de administración del riesgo operacional.

Evaluación al Diseño del Sistema de Administración del Riesgo Operacional y de la Estructura de Control

Evaluación de riesgo / control

Como comienzo se propone realizar una evaluación inicial del Sistema de Administración del Riesgo Operacional de la entidad tomando como base los procesos, personal, sistemas e información para luego compararlos contra un marco de referencia tales como criterios normativos (disposiciones de la CNBV, Banxico, SHCP, ley de instituciones de crédito, etc.), marco conceptual (COSO por ejemplo), recomendaciones u mejores prácticas del nuevo acuerdo de capital de Basilea¹².

La estructura que se sugiere para efectuar la evaluación del sistema de administración de riesgos tiene tres etapas como se indican en la figura 3.6.

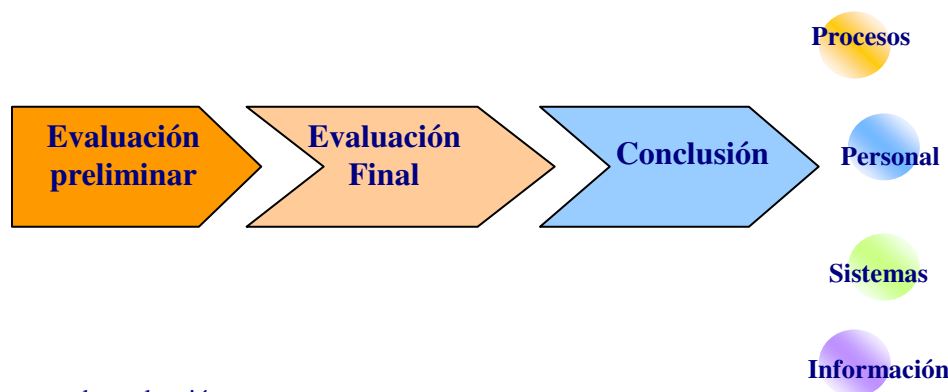


Figura 3.6: Estructura de evaluación.

¹² Se refiere al Comité de Supervisión Bancaria de Basilea que en Febrero del 2003 emitió el documento titulado Sound Practices for the Management and Supervision of Operational Risk (Sound Practices) que contiene las mejores prácticas y recomendaciones para la administración del riesgo operacional en la industria de servicios financieros, el cual puede ser consultado en la página electrónica www.bis.org/publ/.

El programa de evaluación como se indica en la figura 3.6 esta subdividido en tres etapas las cuales se desglosan de la siguiente manera:

- Evaluación preliminar.
 - Revisión de la documentación relativa al proceso, riesgos y controles. Se refiere a la revisión del flujo del proceso, manuales de políticas y procedimientos o narrativas del proceso.
 - Entrevistas preliminares con los dueños o responsables de proceso y controles. Se sugiere levantamiento de minutas con los acuerdos y declaraciones relevantes para la evaluación del proceso, riesgos y controles.

- Evaluación final.
 - Recorridos a través del proceso, identificando las transacciones u operaciones desde su inicio u origen hasta su registro en los sistemas contables, verificando que los controles establecidos ya sea manuales o automáticos o bien que residen en el sistema estén operando y que todos los riesgos hayan sido identificados.
 - Examen a la evidencia documental, se refiere al análisis detallado de la documentación proveniente o no de los sistemas u aplicativos, que soporta la realización de la actividad de control con el fin de concluir acerca del desempeño del control, esta información puede ser interna o externa es decir proveniente de otra entidad privada, gubernamental o regulatoria así como de clientes o proveedores.
 - Aplicación de cuestionarios al personal, con el objetivo de corroborar la competencia, experiencia, conocimiento de los lineamientos normativos u operativos y del código de ética o estándares de conducta profesional; en el anexo 5 se muestra un ejemplo de cuestionario realizado durante la entrevista con el personal clave o responsable de la realización de la actividad de control.

- Conclusión.
 - Evaluación acerca de los riesgos identificados; se han detectados todos y su clasificación o tipología es la correcta.
 - El proceso se ejecuta con fluidez y efectividad para el logro de los objetivos; existencia de deficiencias en el desempeño del proceso.

- Evaluación de los controles implementados ya sea manuales u automáticos o residentes en el sistema u aplicativos en cuanto a su puesta en marcha y correcta operación; existencia de evidencia suficiente en cuanto al correcto diseño y funcionamiento de los controles.
- Cumplimiento con los objetivos establecidos para cada proceso.
- El personal asociado con la puesta en marcha del proceso y de la realización de la actividad de control, posee las habilidades, conocimientos, competencias y experiencia adecuada para el desempeño de sus funciones.
- El personal conoce los lineamientos normativos o regulatorios que afectan o influyen en la realización o ejecución de las operaciones, las cuales tiene a cargo.
- El personal conoce el código de ética interno.

Documentación de la evaluación al sistema de administración del riesgo operacional

La evaluación realizada al sistema de administración del riesgo operacional debe quedar documentada de acuerdo con ciertas características que a continuación se detallan:

- Documentación relativa al desempeño del proceso, sistemas, personal así como suficiencia y calidad de la información.
- Documentación referente a la identificación, categorización y respuesta a los riesgos así como su probabilidad de ocurrencia y posible impacto.
- Documentación concerniente a la implementación de controles internos, verificando su operación y cumplimiento con los objetivos planteados para cada proceso.

En general como resultado de la evaluación al sistema de administración del riesgo operacional se debe de tener la seguridad razonable de que los riesgos identificados en el flujo del proceso y transacciones sean mitigados y que los objetivos de cada proceso son alcanzados. Esta seguridad es razonable si es posible determinar lo siguiente:

- Si la información relativa a la evidencia de realización de la actividad de control es completa, suficiente y refleja con precisión el procedimiento de control diseñado por el responsable del control y / o dueño del proceso.
- Que no se hayan identificado riesgos adicionales sin que no se hayan registrado cambios en el desarrollo de las operaciones o flujo del proceso, cambios en la plataforma o sistemas, productos o normativa.

- Que existen procedimientos de segregación de funciones, prevención de conflictos de interés y comportamiento no ético, así como de contingencia o interrupción de sistemas, ausencia de personal e incumplimiento de contrapartes (clientes, proveedores, entidades regulatorias o contrapartes financieras).

3.5. Resultado de la Evaluación del Diseño del Sistema de Administración del Riesgo Operacional

Evaluación de Deficiencias

Una vez realizada la evaluación al diseño del sistema de administración del riesgo operacional, y en caso de presentarse observaciones, estas deben de describir las desviaciones u hallazgos acerca del comportamiento de los controles internos previamente diseñados e implementados, luego se procede a evaluar esas “excepciones ” en función del comportamiento esperado en cuanto a la efectividad de la actividad de control, es decir el grado en el cual el riesgo asociado se puede materializar (ocurrencia) y el impacto o severidad en caso de presentarse. Las deficiencias de control dependen pues del grado de severidad y probabilidad de ocurrencia de que el riesgo se materialice por ausencia o mal diseño o desempeño de los controles internos.

Es importante mencionar que las deficiencias son resultado de la ausencia o escasez de evidencia o soporte documental de que el riesgo ha sido plenamente identificado y de la implementación y operación de controles internos que mitiguen esos riesgos.

La existencia y suficiencia de la documentación de controles internos radica en la posibilidad de reflejar con precisión los procedimientos de control previamente implementados y que demuestre que el error potencial asociado al riesgo esta cubierto, dando evidencia de documentación soporte ya sea impresa o electrónica (incluye filmaciones, grabaciones telefónicas o documentos digitalizados).

Esta evaluación de deficiencias incluye la evaluación a los procedimientos de control es decir, que las actividades o pasos asociados con los procedimientos relativos a los controles internos sean entendibles y que contemple todas las posibilidades de excepciones en caso de que el flujo de operaciones del proceso no sea realizado en condiciones normales por fallas en sistemas o equipos, ausencias de personal o incumplimientos en la oportunidad y calidad en la entrega y recepción de información por parte de contrapartes y proveedores estratégicos al proceso.

Calificación de las deficiencias

Una vez descrita la observación y la evaluación de la deficiencia, se procede a calificar la deficiencia es decir el grado de importancia que esa deficiencia tiene en el sistema de administración del riesgo operacional, de acuerdo a la metodología COSO¹³, una deficiencia de control es definida como: “un defecto percibido, potencial o real, o una oportunidad para fortalecer el sistema a efectos de que provea una mayor probabilidad de que los objetivos de la entidad serán logrados”, ahora el grado de importancia o “significancia” de la deficiencia de control depende de lo siguiente:

¹³ The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Framework, 2004, http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp.

- Probabilidad de ocurrencia.
 - Para determinar el grado de ocurrencia de las deficiencias hay que basarse en el conocimiento que se tenga del proceso y del error asociado a los riesgos presentes en la ejecución del proceso, en general la probabilidad de ocurrencia del riesgo, se basa en lo siguiente:
 - 1.- Nivel de automatización: A mayor automatización disminuye la frecuencia u ocurrencia pero aumenta el impacto asociado al riesgo.
 - 2.- Competencia del personal: Aumenta la probabilidad de ocurrencia cuando el responsable del control no cuenta con la experiencia necesaria, la capacitación es incipiente o si el puesto o función ha presentado alta rotación, o si el personal no conoce los lineamientos normativos u operativos necesarios para desempeñar su función así mismo si no cuenta o no conoce los estándares de conducta y ética profesional.
 - 3.- Diseño del proceso: Si se cuenta con procesos y procedimientos documentados y que sean aplicados de forma continua por el personal, así mismo si en estos se consideran todas las situaciones especiales u excepciones para los casos de interrupción o fallos en sistemas, ausencias de personal, incumplimiento en información de contrapartes y proveedores.
 - 4.-Confiabilidad en los sistemas: Existencia de manuales y cursos de entrenamiento por parte del proveedor o desarrollador, confiabilidad en el almacenamiento y registro de información, seguridad en accesos, perfiles de accesos, existencia de segregación de funciones en el registro, confirmación, autorización y liberación de operaciones.
 - 5.-Información: Disponibilidad, validez de la fuente, oportunidad en la entrega o recepción de información, existencia de facultamiento o restricción en el acceso / uso de información confidencial o privilegiada, resguardo y almacenamiento de información.
 - 6.-Frecuencia: A mayor frecuencia en la realización de un control que mitigue determinado(s) riesgo (s) se espera que sea mayor la frecuencia del error asociado al riesgo.
- Impacto del error.
 - El impacto se considera tomando en cuenta el monto del flujo de las transacciones que pasan por el control que no esta operando como se había diseñado.
- Acumulación de deficiencias.
 - En la medida en que se presenten en el horizonte del tiempo, las deficiencias serán cada vez más significativas.

Elaboración del informe sobre hallazgos y recomendaciones

Informe a los dueños del proceso o responsables de área funcional

Se procede a informar a los responsables del proceso y subproceso sobre los hallazgos detectados durante la evaluación al sistema de administración del riesgo operacional. El evaluador (auditor interno o puesto con funciones similares o en su caso por algún externo), deberá realizar los siguientes pasos:

- Presentación de las deficiencias de control a los dueños del proceso o responsables de área funcional, en esta presentación se debe indicar con claridad la observación (descripción del hallazgo), la causa de la desviación, la evaluación de la deficiencia de control (frecuencia, impacto, acumulación) en cuanto si es o no es significativa, el posible efecto o impacto de la deficiencia de control y las recomendaciones de mejora.
- Recepción de la retroalimentación por parte de los dueños del proceso o responsables del área funcional, en este paso es posible acordar el plan de acción o remediación y de las fechas compromiso de la puesta en marcha de los planes de acción o remediación pertinentes y de la liberación de los mismos.

Diseño del Plan de Acción o de Remediación

Definición del plan de acción / remediación

Posterior a la comunicación y comentarios de los hallazgos a los responsables del proceso o área funcional, se debe de formular un plan de remediación o de acción para todas aquellas deficiencias de control detectadas y documentadas por cada proceso, en este plan de acción se tiene que detallar el método o procedimiento que resolverá la deficiencia de control así mismo como el tipo de acción de mejora a implementar ya sea detectivo, preventivo o correctivo según corresponda.

Plan de trabajo

El equipo coordinador o a cargo de la administración del riesgo operacional, será el que administre y en colaboración con los responsables del proceso u área funcional participen en la elaboración del plan de trabajo, este deberá contener al menos la siguiente información:

- Definir los responsables (áreas) de la implementación, seguimiento de la implementación y evaluación de los planes de acción o remediación.
- Definir los requerimientos en el o los sistemas u aplicativos, de personal especializado (interno o externo), información (interna o externa), así como de posibles requerimientos regulatorios / legales o normativos indispensables para puesta en marcha del plan de acción.

- Detallar la documentación soporte y evidencias de los resultados derivados de la puesta en marcha del plan de acción o remediación tales como políticas, procedimientos, diseño de procesos (flujos de procesos), desarrollos en los aplicativos o sistemas que generen algún tipo de reporteria o registros así como comprobantes de entrenamiento o capacitación al personal.
- Establecimiento de las fechas compromiso para la evaluación durante y a la culminación de la implantación y operación del plan de acción y remediación, así como de los resultados alcanzados.

Evaluación de resultados

Un tercero independiente ya sea el auditor interno (o algún otro puesto con funciones semejantes) o en su caso el auditor externo, realizará la evaluación de los resultados alcanzados derivados de la culminación del plan de acción, la evaluación se realizara mediante indagaciones corroborativas con base en lo siguiente:

- Entrevistas con los funcionarios a cargo del proceso y de los controles internos.
- Monitoreo de las operaciones.
- Examinación a la evidencia documental (políticas, procedimientos, flujos de proceso, reportería interna o externa).
- Pruebas a los sistemas u aplicativos en cuanto a su funcionalidad, seguridad y confiabilidad.

3.6. Monitoreo y Mejora Continua del Sistema de Administración del Riesgo Operacional

Monitoreo Continuo

Las actividades de monitoreo continuo al sistema de administración del riesgo son todas aquellas actividades realizadas por los mismos responsables del proceso, personas independientes a la ejecución del proceso tales como auditores internos, etc., efectuadas en el transcurso ordinario de las operaciones, entre estas actividades se pueden mencionar las actividades regulares de supervisión de la dirección, comparaciones, conciliaciones y otras tareas de verificación de rutina (sistemas, activos físicos, validación con terceros o clientes).

El empleo de actividades de monitoreo continuo tiene la ventaja de que las desviaciones o deficiencias en los controles internos pueden ser reportadas y solventadas con mayor oportunidad que las que se han detectado posterior a la realización del hecho.

Definición de plan y alcance del monitoreo

Inicialmente se tienen que definir los procesos, subprocesos o controles a monitorear de forma continua, para lo cual se debe de tomar en cuenta lo siguiente:

- Dependiendo de la importancia de los riesgos que se están controlando y de la importancia de los controles en la reducción de dichos riesgos. Los controles que encaran riesgos de más alta prioridad y aquellos más críticos para reducir un riesgo dado tendrán a ser evaluados más frecuentemente.
- Frecuencia en los cambios en las operaciones o métodos de procesamiento de información contable u operativa.
- Experiencia del personal a cargo, entre menos experimentado y capacitado sea el personal a cargo, el monitoreo tiene que ser continuo hasta que el personal adquiera el nivel de experiencia y aprendizaje de acuerdo con las exigencias y responsabilidades del puesto.
- Resultados de auditorías previas, para los controles reportados como deficientes se tendrá que realizar un seguimiento continuo de las mejoras en los controles.

Evaluación y documentación de hallazgos

Una vez definido el alcance del monitoreo continuo, se procederá realizar la evaluación de los hallazgos para lo cual se recomienda efectuar una evaluación / calificación de los hallazgos como se indicó en la sección 3.5 Resultado de la evaluación al diseño del Sistema de Administración del Riesgo Operacional, donde se propone calificar los hallazgos y determinar el grado de deficiencia de control (significativa / NO significativa) con base en la frecuencia del error y del impacto así como de la posible acumulación de errores.

Comunicación de hallazgos

- En caso de haber encontrado deficiencias en el funcionamiento o desempeño de los controles internos, se procede a informar a los responsables del proceso, subproceso o área funcional sobre los hallazgos detectados durante la evaluación al sistema de administración del riesgo operacional. El evaluador (auditor interno o puesto con funciones similares o en su caso por algún externo), deberá realizar los mismos pasos indicados en el apartado “Elaboración del Informe sobre hallazgos y recomendaciones” de la sección 3.5 Resultado de la evaluación al diseño del Sistema de Administración del Riesgo Operacional.

Seguimiento a los planes de acción / remediación

Posterior a la comunicación y comentarios de las hallazgos se debe de proponer un plan de remediación o de acción para todas aquellas deficiencias de control detectadas y documentadas por proceso, en este plan de acción se tiene

que detallar el método o procedimiento que resolverá o solventara la deficiencia de control así mismo el tipo de acción a implementar ya sea detectivo, preventivo o correctivo según corresponda.

Evaluaciones Separadas

Las evaluaciones separadas tienen el objetivo de proveer una oportunidad para considerar si los procedimientos de monitoreo continuo siguen siendo eficaces, así mismo son útiles cuando se requiere realizar evaluaciones esporádicas a ciertos controles internos cuyos riesgos no son de alta criticidad, que sin embargo merecen ser evaluados debido a que su posible incumplimiento podría alterar el funcionamiento del Sistema de Administración de riesgos, así como su posible repercusión en el cumplimiento de los objetivos de cada proceso (objetivos de cumplimiento, efectividad de operaciones, de generación de información financiera).

Se recomienda que estas evaluaciones sean realizadas por un tercero independiente al área evaluada, los cuales pueden ser auditores internos o externos u otro personal que no participe en la ejecución del proceso.

Planeación de las evaluaciones separadas

Inicialmente se tiene que acordar con el revisor los controles internos a revisar dada su criticidad o impacto en la mitigación o prevención de riesgos, posteriormente acordar las fechas de la realización de la evaluación y la fecha de entrega de los resultados de la evaluación. La evaluación se basará en indagaciones corroborativas mediante entrevistas al personal encargado, revisiones a la ejecución en tiempo real de las operaciones, examinación de la documentación (manuales de políticas y procedimientos, flujos de proceso, narrativas de proceso) y evidencias de la realización de los controles internos (registros).

Así mismo se debe definir el horizonte de tiempo a evaluar el cual depende de la vigencia y de los cambios hechos en los procesos entre los que se mencionan los siguientes:

- Cambios en la estructura del proceso: Modificaciones en tareas, métodos, procedimientos o políticas.
- Cambios Normativos que afectan al proceso.
- Cambios en los sistemas, aplicativos y plataformas.
- Cambios en el personal o responsables.
- Cambios en el diseño de los controles internos del proceso.

También se recomienda realizar evaluaciones a ciertas transacciones u operaciones realizadas en el intervalo de tiempo previamente definido, la selección de dichas transacciones puede ser aleatoria.

Alcance de las evaluaciones separadas

Inicialmente el alcance de las evaluaciones separadas serán todos aquellos procesos / controles internos que no hayan sido contemplados en el proceso de monitoreo continuo, sin embargo es posible incluir los controles y procesos que de acuerdo a su probabilidad de ocurrencia e impacto económico deban ser considerados.

Evaluación y documentación de los hallazgos

Una vez definido el alcance del monitoreo continuo, se procederá a realizar la evaluación de los hallazgos para lo cual se recomienda efectuar una evaluación / calificación de los hallazgos como se indicó en la sección 3.5, en cual se propone calificar los hallazgos y determinar el grado de deficiencia de control (significativa / NO significativa) con base en la frecuencia del error y del impacto así como de la posible acumulación de errores.

Comunicación de los hallazgos

- En caso de haber encontrado deficiencias en el funcionamiento o desempeño de los controles internos, se procede a informar a los responsables del proceso y subproceso los hallazgos detectados durante la evaluación al sistema de administración del riesgo operacional. El evaluador (auditor interno o puesto con funciones similares o en su caso por algún externo), deberá realizar los mismos pasos indicados en el apartado “Elaboración del Informe sobre hallazgos y recomendaciones” de la sección 3.5 Resultado de la evaluación al diseño del Sistema de Administración del Riesgo Operacional.

Seguimiento a los planes de acción / remediación

Posterior a la comunicación y comentarios de las hallazgos se debe de proponer un plan de remediación o de acción para todas aquellas deficiencias de control detectadas y documentadas por cada proceso, en este plan de acción se tiene que detallar el método o procedimiento que resolverá o solventara la deficiencia de control así mismo como este método o procedimiento estará acorde con el tipo de acción a implementar ya sea detectivo, preventivo o correctivo según corresponda.

Programa de Mejora Continua

De acuerdo con la norma de calidad ISO 9001: 2000 “Sistemas de Gestión de Calidad – Requisitos”, establece que la organización debe mejorar continuamente la efectividad del sistema de gestión de calidad, mediante el uso de la política de calidad, los objetivos de calidad, los resultados de las auditorías, el análisis de datos, las acciones correctivas y preventivas y la revisión por la Dirección.

Para nuestro caso se define el programa de auditoría una vez realizada la evaluación al sistema de Administración del riesgo operacional, el monitoreo continuo y las evaluaciones separadas que son propiamente auditorías al proceso y controles internos (evaluación del cumplimiento de los objetivos del proceso y mitigación de los riesgos por parte de los controles internos y análisis del impacto o probabilidad de ocurrencia en la materialización de los

riesgos), así mismo una vez definidos los planes de acción / remediación a las deficiencias de control, también realizada la comunicación y revisión de los hallazgos y recomendaciones a la administración o responsables del proceso, estamos en posibilidad de desarrollar un programa de mejora continua el cual debe contener al menos lo siguiente:

- Detección de hallazgos.
 - Ubicación en el proceso y en controles internos de excepciones, desviaciones operativas o de desempeño.
- Evaluación de hallazgos.
 - Determinar el impacto, la probabilidad de ocurrencia del error o desviación y acumulación de fallas, errores o desviaciones.
 - Calificar los hallazgos en función de la severidad del impacto, probabilidad de ocurrencia o acumulación de errores, fallas, desviaciones (deficiencias significativas / Deficiencias NO significativas).
- Asignar responsabilidades.
 - Responsables del diseño e implementación del plan de acción / remediación.
 - Responsables del monitoreo a la implementación del plan de acción / remediación.
 - Responsables de la evaluación y comunicación de los resultados del plan de acción / remediación.
- Diseño del plan de acción / remediación.
 - Desarrollo del método / procedimiento / objetivos / políticas, referentes a la mejora o corrección de las deficiencias.
 - Determinación de requerimientos tales como modificaciones o desarrollos en sistemas.
 - Requerimientos de información normativa, legal u operativa.
 - Determinación de personal especializado (interno o externo).
 - Requerimientos de capacitación o entrenamiento específico a los encargados del proceso / controles internos.

- Evaluación de los resultados.
 - Evaluación intermedia de los resultados del plan de acción / remediación.
 - Evaluación final y pruebas de efectividad a la acción implementada.

- Comunicación a la dirección.
 - Presentación de los resultados alcanzados.
 - Validación de la dirección de los resultados alcanzados.
 - Cierre del estado del proyecto.

Referencias

- 1.- Anexo 12 A: Requisitos para la elaboración y actualización de la base de datos histórica a que contenga el registro sistemático de los diferentes tipos de pérdida asociada al riesgo operacional de las instituciones de crédito, emitido por la CNBV en su más reciente publicación del 12 de Agosto del 2011, <http://www.cnbv.gob.mx/Paginas/Normatividad.aspx?an=37&c=27#is37>.
- 2.- Buenas prácticas para la gestión y supervisión del riesgo operativo, Comité de Supervisión Bancaria de Basilea, Banco de Pagos Internacionales, Febrero de 2003, <http://www.bis.org/publ/bcbs96esp.pdf>.
- 3.- Convergencia internacional de medidas y normas de capital, Comité de Supervisión Bancaria de Basilea, Banco de Pagos Internacionales, Junio de 2006, pp. 159 – 171, 339 – 343, http://www.bis.org/publ/bcbs128_es.pdf.
- 4.- De Lara Haro, Alfonso. Medición y Control de Riesgos Financieros, Editorial Limusa, 3er Edición, México 2005.
- 5.- Disposiciones de carácter general aplicables a las instituciones de crédito (CNBV), 2011, <http://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20carácter%20general%20aplicables%20a%20las%20instituciones%20de%20crédito.docx>.
- 6.- Frost, Chris, et al. Manual de Gestión de Riesgos Operativos, Editorial Deusto, España 2002.
- 7.- Hoffman, Douglas G, Managing Operational Risk: 20 Firmwide Best Practice Strategies, Editorial John Wiley & Sons, E.U 2002.
- 8.- Norma de calidad ISO 9001: 2000 “Sistemas de Gestión de Calidad – Requisitos”.
- 9.- The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Framework, 2004, http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp.
- 10.- Seaver Matt, Implementación de la ISO 9000:2000, Editorial Panorama Editorial, México 2003, pp. 23 - 24.