UNIVERSIDAD TORCUATO DI TELLA

ESCUELA DE NEGOCIOS

EMBA-BCP 2016

EMBA BCP - 2016

Implementación de un sistema de gestión de riesgos operativos en una Banca Central

Alumno: Juan Asunción Riveros Limenza

Tutor: Dr. Carlos Loisi

Asunción – Paraguay

AGRADECIMIENTOS

A mis jefes y compañeros de área, por brindarme sus experiencias y conocimientos referentes a la importancia de la Gestión de Riesgo Operativo y por apoyarme para hacer el EMBA.

A los excelentes profesores que tuve durante el EMBA de la UTDT.

A mis padres y mi novia Jazmín, quienes siempre me apoyan en todos los proyectos que emprendo.

RESUMEN

El trabajo está elaborado con el fin de poder visualizar la importancia de la aplicación de la Gestión de Riesgos Operativos en una Institución de carácter tan relevante en las políticas económicas del país como lo es el Banco Central.

Toda actividad está sujeta a riesgos, ya sea en la vida cotidiana como laboral. Es por ello que se vuelve necesario conocer los beneficios que una buena gestión de riesgos operativos puede llegar a dar a la Institución.

Para poder implementar un Sistema de Gestión de Riesgos Operativos adecuado es necesario conocer sus principales conceptos, origen, naturaleza, tipologías, evolución como disciplina a través del tiempo y los roles fundamentales que actúan en ella.

Se hará una revisión de los principales estándares en la materia, de forma a poder ver cuales son aplicables a la Institución. Si bien es cierto que la mayor parte de los estándares internacionales están diseñados para bancos privados, se podrá ver cuales son aplicables a la Institución.

Una vez revisado todos los conceptos fundamentales de la Gestión de Riesgos Operativos, se describirán los avances realizados en la implementación desde el inicio, las herramientas utilizadas anteriormente y las que están vigentes.

Como ha ido avanzando el proceso de gestión de riesgos, cuales fueron las mejoras encontradas, así como los puntos que requerirán de un mayor trabajo para poder acercarse al objetivo de una adecuada gestión de riesgos.

Por último, se analizará sobre la Cultura de Riesgos que actualmente se presenta en la Institución a través de encuestas de carácter anónimos y que abarquen a diversos rangos dentro de la misma.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

PALABRAS CLAVE

Riesgo operativo, regulación bancaria (BasileaII), gestión riesgo operativo (identificación, evaluación, mitigación, información y control), COSO ERM.

INTRODUCCIÓN

Como bien sabemos toda actividad ya sea de la vida cotidiana o laboral puede estar sujeta a riesgos. Por ejemplo, en el día a día al salir uno a la calle está sujeto a numerosos riesgos que podrían ser: que lo choquen a uno por cruzar las calles sin respetar los lugares por donde debe cruzar; que uno sufra accidentes por manejar un vehículo de forma imprudente o no respetar las señales de tránsito o no usar cinturón de seguridad; que uno ocasione accidentes por las causas mencionadas anteriormente; que uno sufra algún asalto cuando uno va por un lugar un tanto marginado o desolado. Todos estos ejemplos nos muestran casos en los cuales hay una "pérdida" ya sea económica o física. En la vida laboral también acontece algo similar, pueden ocurrir eventos donde falle una máquina que no haya sido bien probada; un sistema colapse por falta de asignación de recursos; errores en la realización de algunas actividades por falta de capacitación o incluso actividades interrumpidas por eventos producidos por la naturaleza (lluvias, terremotos, etc.). En estos casos, los eventos dañarían los recursos de la empresa, pudiendo ser estos de forma económica, reputacional y/o alguna otra métrica.

Los *procesos*[1] de negocios de empresas, instituciones u otro organismo estarán siempre expuestos a riesgos en sus operativas de negocios aun cuando dichas actividades sean sencillas y con más razón sin son complejas. En el caso de grandes instituciones como en los bancos comerciales, el *Bank for International Settlements o BIS (Banco de Pagos Internacionales)* ha publicado a través del *Comité de Supervisión Bancaria de Basilea* las **"Buenas prácticas para la gestión y supervisión del riesgo operativo"**[2]**.** Si bien estas prácticas están más enfocadas a bancos comerciales y no las hay de dicha índole para instituciones como un Banco Central, como habíamos mencionado anteriormente, se vuelve más que necesario utilizar las prácticas que sean aplicables de dicha regulación para poder gestionar los riesgos operativos que pudieren existir en una institución de vital importancia.

Este trabajo se enfoca en la forma como deberían ser implementadas las herramientas que sean más útiles para buscar una adecuada gestión del riesgo operativo en el contexto de un Banco Central debido a que existen herramientas propuestas en las prácticas mencionadas anteriormente que se encuentran más orientadas para ser utilizadas en bancos comerciales.

Conseguir una adecuada gestión de riesgos operativos es proceso bastante complejo cuya implementación conlleva tiempo, esfuerzo, compromiso y conciencia de parte de todos quienes forman parte de una institución, desde el presidente, los miembros del consejo y autoridades de las altas gerencias hasta los empleados de más bajos rangos.

Sin lugar a duda una institución de la envergadura de un Banco Central no puede dejar de observar este aspecto que se vuelve fundamental a la hora de tomar decisiones y diseñar las estrategias de negocios.

[1] Según la norma ISO 9000:2000 un proceso es "un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados"

[2] https://www.bis.org/publ/bcbs96esp.pdf

MARCO TEÓRICO

EL RIESGO OPERATIVO.

Antes de ver los aspectos específicos del riesgo operativo es importante que podamos conocer algunos conceptos básicos que nos ayudarán a poder construir los conocimientos necesarios para entender la gestión de dicho riesgo como un proceso que se lleva a cabo en una institución.

¿Qué entendemos por riesgo?

Podría decirse que es la posibilidad de que ocurra algún evento que se traduzca en pérdidas. Como se sabe, en la mayoría de los casos está pérdida podría ser económica, lo cual puede ser constatado en el balance contable. Otras veces, estas pérdidas económicas no se constatan en el balance ya que son eventos que ocasionan que la empresa deje de ganar dinero (lucro cesante).

No existen actividades que estén libres de riesgo. El riesgo siempre estará presente en mayor o menor grado. Lo máximo que podemos hacer es mitigar el riesgo ya que, si se desea eliminarlo, se deberá también eliminar la actividad donde se genera dicho riesgo.

En el párrafo anterior mencionábamos la palabra mitigar, lo cual entendemos que es atenuar o reducir una pérdida. En la gestión de un riesgo es muy importante saber que "mitigar" es similar a "gasto" o "costo". Un ejemplo de mitigación son los seguros que uno contrata contra daños o accidentes para un vehículo. Este seguro "mitiga" la pérdida, en caso que lo hubiere, pero tiene un costo.

La gestión de riesgo siempre existió, por ejemplo, en algunas actividades cotidianas. Ejemplo de ellos son los cinturones de seguridad en un vehículo, las alarmas en un banco, las cámaras de seguridad, los guardias y otros innumerables ejemplos de gestión que se realiza de forma prácticamente implícita.

Lo nuevo en cuanto a la gestión de riesgos es que se está regulando y se está implementando de forma más sistemática en muchos lugares donde podrían afectar de forma notable las operaciones provocando por ende daños económicos y/o reputacionales.

Ahora que ya manejamos los conceptos de riesgo y pérdida, estamos listos para poder abordar los conceptos que se refieren a nuestro tema en particular.

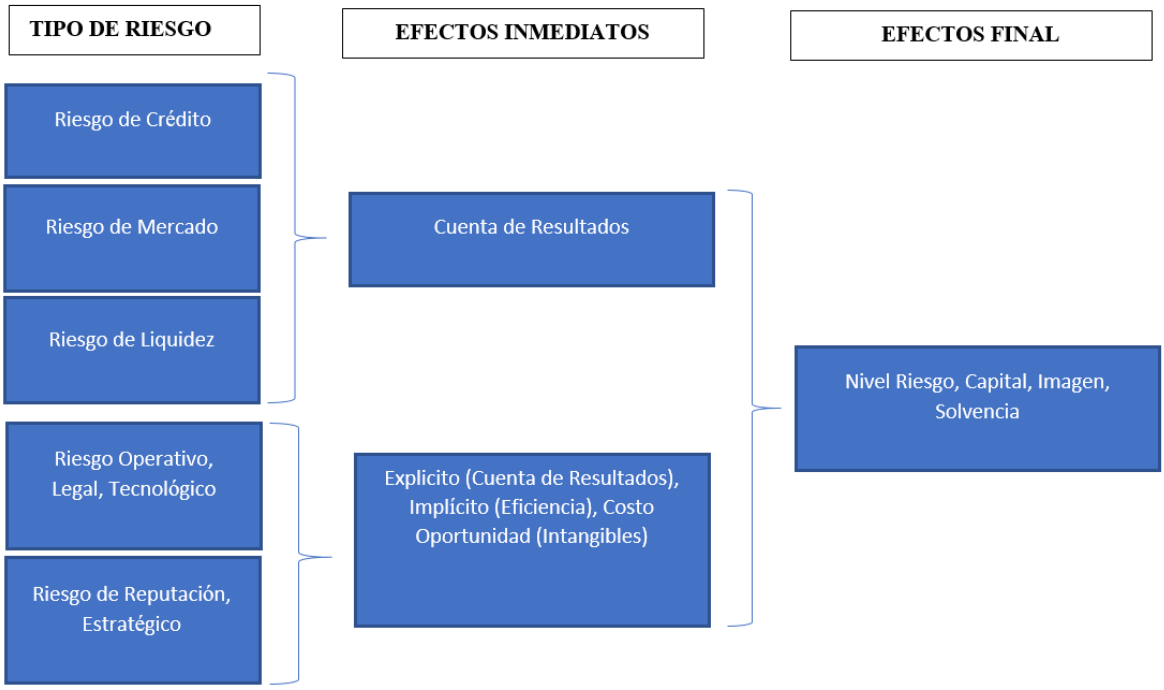
Riesgo operativo u operacional, *es el riesgo de pérdidas resultantes de la inadecuación o fallas en los procesos internos, las personas o los sistemas o por eventos externos. Esa definición incluye al riesgo legal, pero excluye el riesgo estratégico y reputacional*[3].

[3] Basel Committee on Banking Supervision: el Comité de Supervisión Bancaria de Basilea, hasta 1990 Comité de Regulación y Prácticas Supervisoras Bancarias, es uno de los diversos comités adscritos al Banco Internacional de Pagos (BIS); fue creado, a finales de 1974, por los gobernadores de los bancos centrales del G-10. Es conocido como Comité de Basilea, por la ciudad suiza donde se ubica, y tiene como objetivo garantizar una supervisión eficaz de las actividades bancarias en todo el mundo.

A diferencia de los otros riesgos no es tomado directamente a cambio de una retribución esperada, aun cuando existe en el transcurso normal de la actividad corporativa y tiene impacto en el proceso de gestión de riesgos.

En los bancos comerciales, desde tiempo atrás, la gestión de riesgos financieros se ha realizado como una actividad rutinaria junto a los riesgos de mercado y de liquidez. Los nuevos enfoques de supervisión bancaria enuncian la necesidad de implementar un sistema de gestión de riesgos operativos. El riesgo operativo es un tipo de riesgo que presenta muchas semejanzas en varias organizaciones de industrias y servicios.

Figura 1: Esquema básico de cómo puede llegar a afectar los riesgos a las entidades bancarias comerciales.



Los efectos de la materialización de los riesgos operativos pueden tener impactos que pueden ser reflejados en las cuentas de resultados de Contabilidad y otros que no, en los casos donde se genera costo de oportunidad, procesos ineficientes, duplicidad de funciones. En cuanto a evaluar el costo, pérdida de oportunidad y menores ingresos futuros son más complejos a la hora de evaluar. En cuanto a procesos ineficientes, duplicaciones o solapamientos se pueden detectar utilizando análisis de procesos, entre otras herramientas.

La evaluación de las estadísticas sobre eventos materializados es un factor muy importante pero insuficiente debido a que no contempla la posibilidad de evaluar nuevos procesos. Por ello, es importante utilizar otras fuentes externas similares y la realización de un análisis crítico y cualitativo de los procesos operativos.

Por lo mencionado anteriormente, se vuelve necesario que haya una gestión por procesos eficiente dentro de la institución.

En la actualidad, en muchas empresas e instituciones, tanto públicas como privadas, los procesos institucionales requieren de una definición clara. En el mundo de los negocios de hoy día la primera mitigante a riesgos es la definición adecuada de los procesos y que por ende haya una adecuada gestión por procesos.

Se hace necesario recurrir al conocimiento de las entidades y la utilización de análisis "subjetivo" para hacer una comparación con la gestión habitual del tipo de riesgo.

ORIGEN DEL RIESGO OPERACIONAL

En el año 1988, el Comité de Supervisión Bancaria de Basilea publicó el documento "Internacional Convergence of Capital Measurement and Capital Standards", el cual representa el primer Acuerdo de Capital y que es más se lo conoce con el nombre de Basilea I.

Esta recopilación de información fue elaborada con la misión de ser una guía para las entidades bancarias comerciales de forma tal a que los mismos tengan controlado sus riesgos de créditos. Para ello, este documento plantea que los bancos mantengan un capital mínimo de acuerdo al riesgo que asumen, de tal modo a que en casos en donde los deudores presenten insolvencia, las pérdidas sean absorbidas.

Así surgió el Ratio de Cook, que representa el coeficiente de solvencia y que básicamente especifica que los bancos comerciales deberían tener un capital mínimo del 8% de todos sus activos y ponderados de acuerdo al riesgo de crédito. Este Acuerdo de Capital solo contemplaba el riesgo de crédito, es por ello que posteriormente, en 1996, el Comité incluyó el riesgo de mercado.

Con el correr de los años, los procesos bancarios fueron adquiriendo mayores dificultades y por ende la gestión de sus riesgos bajo enfoques de supervisión y de mercados han hecho notar que Basilea I no es suficiente para mostrar los riesgos asumidos por los bancos. Básicamente, este acuerdo genera una utilización de recursos poco eficiente. Esto generaba una subvaloración en los riesgos y sobrevaloración del capital.

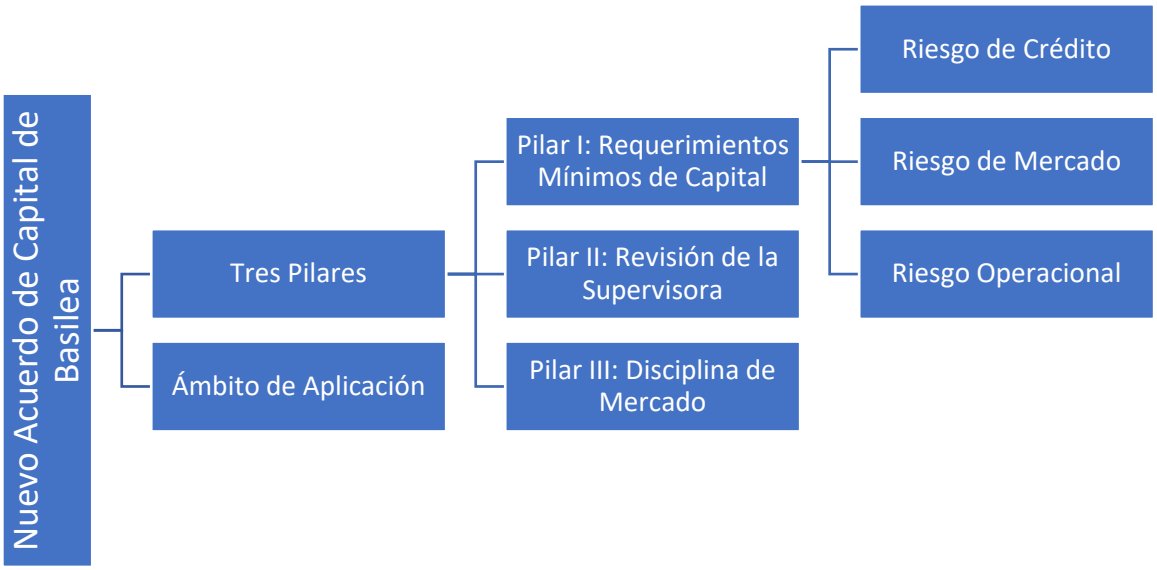
Es por ello que, en junio de 1999, se publica "A New Capital Adequacy Framework", el cual reemplaza a Basilea I. Luego de algunos ajustes realizados en el enero de 2001 y posteriormente en abril de 2003 se publica la versión definitiva del Nuevo Acuerdo de Capital, "Internacional Convergence of Capital Measurement and Capital Standards: A Revised Framework". Los ejes temáticos se centralizan en la solvencia y seguridad del Sistema Bancario, presentándose como una norma que busca adecuar el capital de forma más efectiva a los riesgos de las operaciones bancarias. Para ello propone mejorar la capacidad de gestión y el control de los riesgos.

Es en Basilea II, donde se da origen a la gestión del riesgo operacional como una nueva disciplina que ayuda a que las entidades puedan conocer los riesgos presentes en sus operaciones, y que permite identificar los controles con que se cuenta para hacer frente a dichos riesgos.

Las normativas de Basilea II se dividen en dos grupos (véase Figura 2): uno es el ámbito de aplicación, el cual especifica cuales entidades deberán satisfacer el coeficiente de solvencia. El otro grupo sería tres pilares (requerimientos mínimos de capital, revisión de la supervisora y disciplina de mercado).

El Pilar I expresa que los requerimientos mínimos de capital se establecen en base a los riesgos que la entidad está dispuesta a asumir, esto es el coeficiente de solvencia del 8%. El capital destinado no varía, pero si como se distribuye el coeficiente. En este sentido, se incluye que el 20% de los 8% del capital deberá ser destinado al riesgo operacional. Por otro lado, tanto el riesgo de crédito y de mercado mantienen la misma definición que se realizó en Basilea I.

Figura 2: Esquema del Nuevo Acuerdo de Capital de Basilea.



Pilar I (Requerimientos mínimos de capital)

Establece el nivel mínimo del capital para entidades de créditos de acuerdo a los niveles de riesgos dispuestos a ser asumidos (de crédito, mercado y operacional). Para ello se deberá distribuir utilizando metodologías estandarizadas (predefinidas en Basilea II) o metodologías avanzadas que desarrollan las propias entidades y son aprobadas por los entes reguladores. La entidad deberá prever un capital mínimo de 8% en total para los 3 tres riesgos. Tanto el riesgo de crédito y de mercado se preservan en base a lo expuesto en Basilea I, pero el operacional debe ser considerado, tratado y evaluado de forma particular previendo un costo del mencionado capital.

Pilar II (Supervisión bancaria)

Las entidades deberán someterse a otras entidades supervisoras (Bancos Centrales, Superintendencia de Bancos, etc.) encargadas de velar el cumplimiento de las normativas y regulaciones vigentes. Para ello, se sustentará en cuatro principios:

1. Cada entidad deberá estar preparada para evaluar sistemáticamente su requerimiento de capital de forma tal a poder mantener bajo control sus riesgos.
2. Los reguladores deberán evaluar los procesos que las entidades realizan para verificar que estos mantienen un seguimiento del control de sus riesgos. Estos reguladores deberán intervenir en caso que lo mencionado no es cumplido.
3. Los reguladores pueden exigir un cumplimiento mayor que el del capital mínimo.
4. En caso que el capital requerido este por debajo del mínimo, los reguladores deberán intervenir solicitando la implementación de soluciones para lograr el mínimo.

Pilar III (Disciplina de mercado)

La entidad deberá comunicar de una forma adecuada información sobre sus riesgos y gestiones de forma tal a que los interesados puedan conocer el perfil de riesgo de la misma.

NATURALEZA DEL RIESGO OPERACIONAL

El riesgo operacional presenta particularidades en relación a otros tipos de riesgos:

- ✓ Su materialización puede tener impactos cuantitativos y cualitativos.
- ✓ Las causas que lo materializan: los factores que lo originan.
- ✓ Presenta la necesidad de prever una variada gama de eventos en las diversas unidades organizacionales.
- ✓ La importancia de su gestión se basa en información cualitativa según los principios de BIS II
- ✓ No incluye al riesgo estratégico ni reputacional, pero tiene afectación directa tal como en los riesgos de crédito, mercado y liquidez.

GESTIÓN DEL RIESGO OPERATIVO TRADICIONAL Y MODERNA

Durante mucho tiempo, convencionalmente, se ha utilizado un **enfoque tradicional basado en la auditoría**, el cual también es conocido como **gestión del riesgo operativo tradicional**. Sus fundamentos generales fueron utilizados para generar un conjunto de normas llamados COSO ERM[4].

[4] El **COSO ERM** es un organismo de reconocimiento internacional donde se establecen los marcos reguladores básicos de riesgo y cumplimiento en temas de control interno.

Muchas importantes instituciones contables alrededor del mundo han sugerido la utilización de este enfoque. Empresas de consultoría, calificadoras de riesgos, industrias y consultores independientes también lo han recomendado. Asimismo, tanto reguladores nacionales como internacionales lo han apoyado.

El enfoque tradicional presenta muchas funciones de utilidad. Proporciona la estructura, norma de gobierno y un enfoque intuitivo de identificación y evaluación de riesgos.

Pero, también presenta algunas deficiencias. Una de las más importantes es que a la hora de determinar el riesgo, este es evaluado utilizando la pérdida media. En otros casos, se utiliza el peor escenario de pérdida que podría ocurrir. Entonces, la evaluación se centra en las amenazas habituales y las debilidades de los controles sobre estos quedando sin poderse identificar riesgos que podrían tener mayores impactos.

Otro inconveniente que suele presentar este enfoque es que las decisiones de optimización de riesgos y controles determinadas por una evaluación pueden caer en exceso de controles en áreas de las instituciones con bajo nivel de riesgo, que como bien se sabe representa gastos. Asimismo, podría haber áreas con alto nivel de riesgos y que se encuentren con un bajo nivel de controles.

El enfoque tradicional es muy eficaz para la prevención de pérdidas de forma táctica, pero esto representa sólo un aspecto del problema de negocio y claramente no es el más importante. Particularmente, este enfoque, deja un vacío en cuanto a la mitigación de las exposiciones a riesgos catastróficos, tales como violaciones de ventas y operaciones en las cuales hay una toma excesiva de riesgos. Estos ejemplos si representan factores claves de riesgos operacionales.

Uno de los riesgos operacionales más importantes es el riesgo del problema agente-principal[5]. El riesgo de agente-principal provoca situaciones en donde los agentes, que controlan o actúan en nombre de la organización, podrían emprender acciones para su beneficio propio y no para el interés de los stakeholders (los interesados) de la empresa. Este riesgo ha sido el factor principal de muchas de las mayores pérdidas.

En los últimos años, se ha desarrollado un nuevo enfoque en la gestión del riesgo operacional el cual se denomina **gestión del riesgo operativo moderna**. Es un enfoque de arriba abajo, es decir, se focaliza primeramente en los riesgos mayores dentro de una integral de riesgos y que son excluyentes. Es un enfoque holístico y sistemático que permite evaluar el proceso de gestión de riesgos. Utiliza menos recursos y evita que estén concentrados en riesgos inmateriales. Es lo más adecuado para mitigar el riesgo del problema agente-principal.

Las regulaciones de Solvencia II[6], que han sido programadas para entrar en vigor en Europa en 2012, utilizan un lenguaje que sea consistente con la gestión del riesgo operativo moderna. Estas regulaciones explican los riesgos

[5] En Economía, el **problema del agente-principal** designa un conjunto de situaciones que se originan cuando un actor económico (el principal o el jerarca), depende de la acción o de la naturaleza o de la moral de otro actor (el agente), sobre el cual no tiene perfecta información. En otras palabras, ese asunto concierne las dificultades que se presentan bajo condiciones de información asimétrica, cuando el actor principal contrata a un agente.

[6] La Directiva Solvencia II es una Directiva en derecho de la Unión Europea que codifica y armoniza la regulación de seguros de la UE. Principalmente, esto se refiere a la cantidad de capital que las compañías de seguros de la UE deben tener para reducir el riesgo de insolvencia.

como una magnitud de la incertidumbre (especificado a un nivel de confianza del 99,5% para un periodo de tiempo de un año). Estas regulaciones también tienen por requerimiento que los modelos de controles internos desempeñen un papel fundamental en el sistema de cualquier organización aportando gobernabilidad y la gestión de riesgos. Las compañías norteamericanas con operaciones internacionales ya lo utilizan y por ende se constituyen en un conjunto de regulaciones de americanas y canadienses.

Además de ayudar a las organizaciones a satisfacer los requisitos de cumplimiento, también puede producir un valor tangible. En concreto, aborda el problema de la empresa de gestión de riesgo más importante, que es la mitigación de la exposición a los eventos que tienen el mayor impacto en el rendimiento financiero y de solvencia.

Los principales objetivos de la gestión del riesgo operacional moderna son:

- Facilitar la gestión integral de los riesgos operacionales utilizando como base una clara definición arquitectura o taxonomía.
- Ser un proceso bien definido en cuanto a su estructura y transparencia de forma tal a que en caso de factorización de riesgos el proceso para toma de decisiones pueda ser eficiente tanto a nivel táctico como estratégico. Esto es, que permita a los ejecutivos, directivos y gerenciadores poseer las herramientas con la información necesaria para optimizar la gestión de riesgos y los beneficios que este ofrece a través de análisis de costos y beneficios.
- Instaurar una cultura de riesgo en la organización que busque el alineamiento entre los objetivos de la institución y los de los grupos de interés tanto internos como externos.
- Eliminar la falta de información tanto para gestionadores de riesgos y partes interesadas de forma tal a que los administradores puedan aplicar las estrategias de forma más flexible.

Un gran número de empresas han iniciado el camino para la migración del enfoque de la gestión del riesgo operativo tradicional a la moderna. Esta transición si es llevado a cabo de forma adecuada no solo hará que se gestione de manera eficaz los riesgos, sino que reducirá notablemente los costos.

A continuación, un comparativo de las diferencias más notables entre ambos enfoques:

Tabla 1: Diferencias más notables entre un enfoque de gestión de riesgo tradicional y uno moderno

Gestión del riesgo operacional tradicional	Gestión del riesgo operacional moderna
El riesgo es conceptuado como un evento no deseable, un fraude, fallo en sistemas. La pregunta habitual en este enfoque suele ser "qué/dónde se encuentran sus riesgos?"	El riesgo es considerado como una magnitud de cuanta pérdida podría haber en los eventos no deseables. La pregunta en este enfoque suele contestar a "cuanto riesgo tiene esta actividad/tarea/proceso?"
Se solicita a los administradores identificar sus principales riesgos, los riesgos incluyen factores de riesgos que son controlables y generalmente suelen solaparse ya que no hay distinción entre los riesgos y controles. Genera muchos riesgos y resulta más complicado gestionarlos.	Se define un universo de riesgos el cual se constituye en el conjunto definido de tipos de riesgos y que se encuentran bien diferenciados unos de otros. Se utilizan datos cuantitativos y cualitativos que ayudan a determinar las mayores pérdidas que podría haber.
El riesgo es calculado por multiplicación simple de impacto por probabilidad y esto ya limita el riesgo a cada evento.	Utiliza simulaciones científicas como Monte Carlo, distribución de frecuencias y gravedad para calcular una pérdida probable por tipos de eventos.
No permite adicionar datos de probabilidad, por lo que los resultados quedan rígidos.	Permite la adición de datos de frecuencia, haciendo que los resultados puedan variar de acuerdo a los datos adicionados.
Mide la probabilidad de pérdida de un incidente.	Mide la pérdida acumulativa por tipos o clases de riesgos, es decir la pérdida esperada y la inesperada que permite comparar al promedio y al peor caso de pérdida.
Es muy costoso en cuanto a recursos.	Costos más controlados.

DIFERENCIA ENTRE PROBABILIDAD Y FRECUENCIA

En el enfoque de gestión de riesgo tradicional, los términos de probabilidad y frecuencia se utilizan como sinónimos, pero en el enfoque de gestión del riesgo operativo moderno estos términos tienen significados muy diferentes. Probabilidad se refiere a la medida estadística y se utiliza generalmente en el contexto de un solo incidente o escenario (por ejemplo, la probabilidad de en un accidente de coche hoy en día es 9%). Probabilidad se mide en una escala de 0 a 1 (o 0 a 100%).

Frecuencia describe el número de eventos (por ejemplo, 25 eventos materializados por año). La frecuencia se mide en una escala de 0 a infinito. La media frecuencia es el número promedio de eventos que se han producido o se espera que tenga lugar durante un período de tiempo especificado. Nota: El número de eventos siempre es un

número entero (por ejemplo, 0, 1, 2, 3, 4, etc.), pero el valor de frecuencia puede ser un valor fraccionario (por ejemplo 1,75).

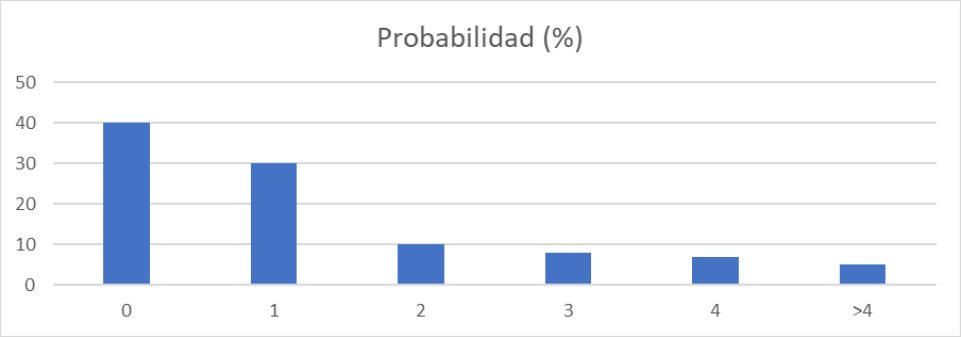
Una distribución de frecuencias es una distribución de probabilidad discreta para un período de tiempo, casi siempre un año. Una distribución de frecuencias especifica valores de probabilidad para cada posible número entero de eventos.

A continuación, analizaremos una distribución de frecuencias de Poisson de la probabilidad cada cantidad de veces que puede materializarse un evento a lo largo de un año.

Tabla 2: Probabilidad que tiene cada cantidad de veces que puede ocurrir un evento en un año.

Cantidad de eventos	Probabilidad (%)
0	40
1	30
2	10
3	8
4	7
>4	5

Figura 3: Distribución de frecuencias de la probabilidad que tiene cada cantidad de veces que puede ocurrir un evento en un año.



En el gráfico, observamos una muestra de distribución de frecuencias de Poisson de la probabilidad que tiene cada cantidad de eventos de presentarse por año: 0 eventos: 40%, 1 evento30%, 2 eventos: 10%; 3 eventos: 8%; 4 eventos: 7%, por encima de 4 de Eventos: 5%. El eje vertical de una distribución de frecuencias representa la probabilidad (probabilidad) y el eje horizontal representa el número correspondiente de eventos. En una distribución de frecuencia, como es el caso con cualquier distribución de probabilidad, la probabilidad total debe sumar 100%.

IMPORTANCIA DEL RIESGO OPERACIONAL EN LA ACTIVIDAD BANCARIA

La continua evolución y globalización de las prestaciones financieras acompañadas de avances tecnológicos han llevado la actividad bancaria a que estas estén inmersas en diversos riesgos. Surgen entonces la necesidad de una continua revisión de las normativas de regulación y supervisión a los efectos de poder tener controlados, no solo los tradicionales riesgos (de crédito, interés y mercado) sino también el riesgo operacional.

Argumentos que ayudan a visualizar la importancia de la gestión del riesgo operacional:

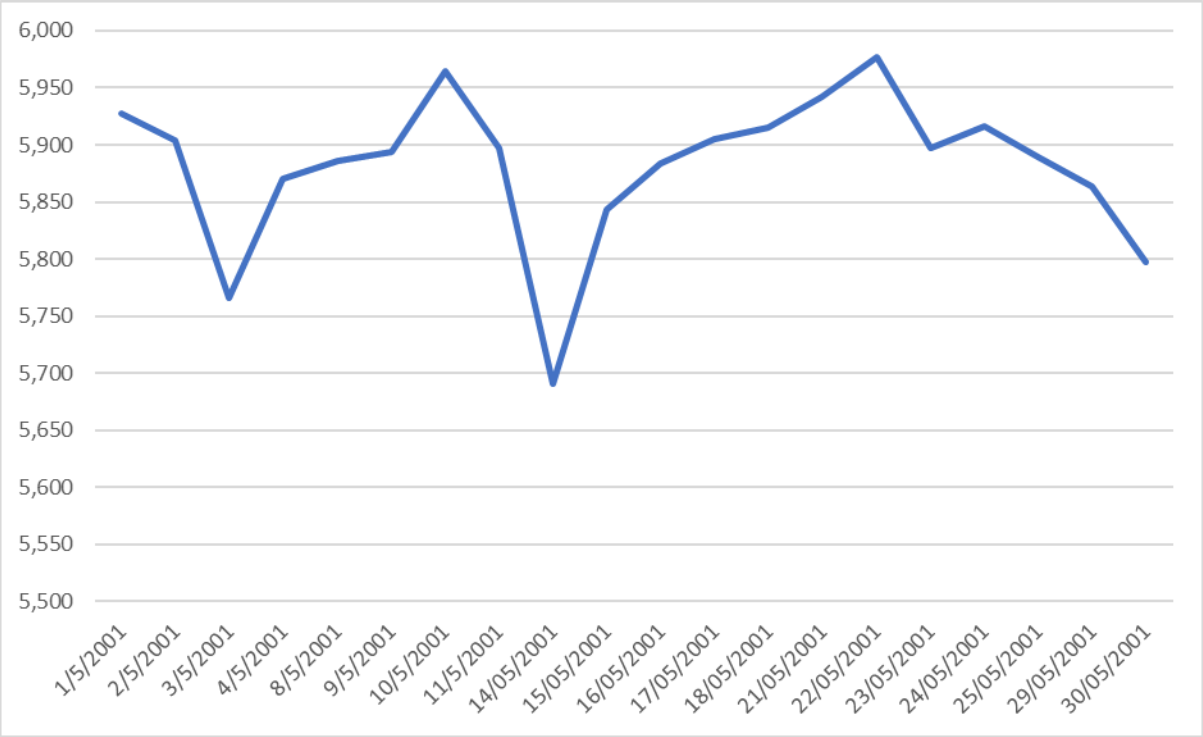
- Cuanto mayor es la tecnología y más automatizada se requiere de un mayor control ya que existe una mayor dependencia de estos en las actividades de la entidad. Los riesgos en los errores de operación de estas tecnologías podrían impactar de forma significativa a los objetivos del negocio.
- Las transacciones electrónicas poseen algunos riesgos intangibles para los clientes y que pueden afectar a la reputación de la entidad.
- La integración de una gran cantidad de sistemas y servicios en una entidad requiere de un sistema sofisticado de seguridad informática y que pueda ser manejado por gente técnica y calificada.
- La tercerización de algunos servicios se suele realizar con el fin de reducir ciertos riesgos, pero a la vez abre el camino a otros potenciales riesgos.

Si bien es cierto que el factor tecnológico genera la mayor cantidad de los riesgos por fallas técnicas, también la interacción humana con la tecnología representa un riesgo de errores humanos. Uno de los habituales errores en la interacción humana corresponde al mal ingreso de datos.

Un ejemplo materializado donde se produjo una gran pérdida cuantitativa fue el ocurrido en el año 2001 cuando un empleado al realizar una transacción de venta escribió un monto de 300 millones en lugar de 30 millones. Esta operación fue una venta de valores del índice FTSE 100[7] generando una baja de 120 puntos que equivalen a 40 mil millones de libras pérdidas. A continuación, se muestra como afecto la pérdida al FTSE 100 específicamente entre la caída entre el viernes 11/05/2001 y el lunes 14/05/2001.

[7] El FTSE 100 es el índice bursátil de referencia de la Bolsa de Valores de Londres. Está compuesto por las 100 compañías de mayor capitalización bursátil del Reino Unido y es indicador del rendimiento financiero de las empresas reguladas por la ley de empresas del Reino Unido.

Figura 4: Gráfico de variación del índice FTSE 100 en mayo de 2001. Puntos.



Fuente: http://www.expansion.com/mercados/cotizaciones/historicos/ftse100_I.LE.html. Gráfico de elaboración propia.

LA GESTIÓN DEL RIESGO OPERATIVO EN LAS ENTIDADES BANCARIAS

El riesgo operacional se encuentra de forma inherente a todas las actividades de las entidades bancarias y no hay forma de que sean eliminadas en su totalidad, en todo caso lo se puede hacer es gestionarlo intentado mitigarlo. Hasta antes del año 2003, en la mayoría de las entidades, la gestión y control del riesgo operacional era llevado a cabo por el área de Auditoría Interna.

En las recomendaciones hechas por el Comité, propone que la gestión de riesgo operativo sea desempeñada por las áreas de gestión de riesgos y que la Auditoría Interna se encargue de controlar que el marco general de la gestión de riesgos sea llevado de forma adecuada a través de los procesos institucionales.

A través de su publicación "Sound Practices for the Management and Supervision of Operational Risk", en el año 2003, el Comité de Supervisión Bancaria de Basilea fundamenta los principios que los bancos y entidades supervisoras deberán tener presente para poder afrontar una gestión y supervisión de riesgo operacional adecuada.

Tabla 3: Principios de Basilea II "Buenas prácticas para la gestión y supervisión del riesgo operativo"

Desarrollo de un marco adecuado para la gestión del riesgo
PRINCIPIO 1 El Directorio[8] se encargará de aprobar y revisar de forma periódica el marco general para la gestión de riesgo del banco. Este marco deberá establecer una definición del riesgo operativo que sea única para toda la empresa y los principios para identificar, evaluar, controlar y mitigar este tipo de riesgos. **PRINCIPIO 2** El Directorio deberá asegurar que el marco para la gestión del riesgo operativo esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser responsable de la gestión del riesgo operativo, solo de la revisión del cumplimiento del marco. **PRINCIPIO 3** La alta gerencia[9] deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el Directorio. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco.
Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control
PRINCIPIO 4 Los bancos deberán identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, también deberán comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente. **PRINCIPIO 5** Los bancos deberán vigilar periódicamente los perfiles de riesgo operativo y las exposiciones sustanciales a pérdidas. La alta gerencia y el Directorio deberán recibir información necesaria de forma periódica que complemente la gestión activa del riesgo operativo.

[8] Para fines prácticos, se denomina "Directorio" al "Consejo de Administración" de un banco. Este último fue la denominación utilizada en el documento "Buenas prácticas para la gestión y supervisión del riesgo operativo".

[9] Generalmente, alta gerencia, se refiere a la Dirección General o la Gerencia General.

PRINCIPIO 6 Los bancos deberán contar como herramientas, para la gestión de riesgos operativos, con políticas, procesos y procedimientos para controlar y mitigar los riesgos operativos más relevantes. Además, deberá revisar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operativo según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo. **PRINCIPIO 7** Los bancos deberán contar con planes de contingencia y de continuidad de forma tal a garantizar una capacidad operativa continua y que no generen pérdidas significativas para la Institución.
La función de los supervisores
PRINCIPIO 8 Los supervisores bancarios deberán exigir a los bancos, sin tener en cuenta su tamaño, el suministro de un marco eficaz y eficiente para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes, como parte de su aproximación general a la gestión de riesgos. **PRINCIPIO 9** Los supervisores deberán llevar a cabo, de manera directa o indirecta, una evaluación periódica independiente de las políticas, procedimientos y prácticas de un banco relacionadas con el riesgo operacional.
La función de la divulgación de información
PRINCIPIO 10 Los bancos deben realizar constante divulgación pública para permitir que los participantes del mercado evalúen su enfoque para la gestión del riesgo operacional.

Esta normativa fue diseña para que la gestión del riesgo operacional actué en conjunto con las gestiones de riesgo de crédito y de mercado, proveyendo a estas de otras disciplinas tales como:

Asignación eficiente de recursos financieros

El riesgo operativo requiere de una previsión de 8% del capital de la empresa. Se constituye en el recurso más costoso para las entidades y representa una medida para las pérdidas (no esperadas y esperadas) que deberán ser estimadas en calidad de gestión de riesgo operativo.

Esta disciplina genera un interés en las autoridades de la institución para establecer el control y la gestión del riesgo operacional como algo serio y estratégico. También hace que sea vista por los stakeholders como un seguro que permite creación de valor y seguridad.

Transparencia

Deberán existir canales de comunicación formales para mantener informado a los stakeholders, entre ellos al mercado. Esta información servirá al mercado para que pueda hacer un análisis, evaluación y comparación con las mejores prácticas a ser llevados a cabo por los bancos. Esto implica que deberá haber transparencia sobre la gestión de forma interna y externa. Para ello es necesario que la cultura de riesgos este ampliamente desarrollada.

Compromiso por parte los supervisores

Obliga a que los órganos de supervisión controlen de forma periódica la aplicación y adecuación de las normativas para gestión de riesgo operativo en los bancos. Por lo tanto, los supervisores, deberán controlar la estructura funcional, orgánica, los sistemas, modelos y metodologías relacionadas a la gestión de riesgo operativo de todas las entidades. Esto hace que la gestión de riesgo en los bancos se convierta en una función de constante aplicación y que se convertirá en un proceso de mejora continua.

Herramienta enfocada al manejo eficiente de las finanzas

La asignación de capital por riesgo operativo genera un interés en realizar una gestión adecuada de forma a que sea visto como una disciplina que crea un valor significativo para las empresas.

Competitividad en el mercado

La correcta aplicación de un marco adecuado de gestión de riesgos operativos generará beneficios y ventajas ante la competencia. La empresa creará una visión en el mercado de:

- Eficacia: costos más bajos, pérdidas menores y capital bien administrado.
- Reputación: seguridad, calidad, profesionalidad.
- Flexibilidad: para poder adaptarse a situaciones cambiantes.

Conciencia interna de la importancia de gestionar y controlar el riesgo operativo

Representa un compromiso para que todos los que interactúan con la institución se comprometan a mantener un comportamiento adecuado para la gestión de riesgo operativo. Las personas han de comprometerse a identificar, evaluar, gestionar y mitigar el riesgo operativo de forma eficiente para poder satisfacer las exigencias de los supervisores. Se deberán establecer canales adecuados para comunicar la ocurrencia de eventos que generen pérdidas a la institución de forma tal a que en el futuro está información pueda ser utilizada para mejorar la gestión. La correcta aplicación de esta disciplina también ayudará a que la cultura de gestión por procesos mejore, ya que las personas irán familiarizándose con los procesos institucionales y los objetivos de estos.

PERCEPCIÓN DEL RIESGO OPERACIONAL

La gestión del riesgo operacional en las entidades bancarias no se encontraba definidos desde una perspectiva normativa. El riesgo operacional era considerado todo aquello que no era riesgo de crédito, de mercado ni de interés. Recién cuando fue publicada la nueva propuesta de requerimientos de capital por Basilea II se pudo tener una definición del riesgo operacional.

La primera definición data del año 1999 cuando unas empresas, entre ellas Price Waterhouse Cooper, publicaron un artículo de investigación sobre las recomendaciones a seguir para gestionar el riesgo operacional. Así mismo, definían al riesgo como *"todo lo que representaba pérdidas directas o indirectas a consecuencia de procesos mal diseñados o con fallas, personas, sistemas o eventos externos"*. En el año 2000, el Institute of Internacional Finance, enriqueció la definición anterior excluyendo riesgos estratégicos, de liquidez y de reputación.

La definición madre y que perdura en la actualidad es la desarrollada por el Comité de Supervisión Bancaria de Basilea el cual es *"El riesgo operacional se define como el riesgo de pérdida resultante de una falta de adecuación o un fallo de procesos, el personal y los sistemas internos o bien de acontecimientos externos"*. La definición incluye al riesgo legal y tecnológico, pero excluye al riesgo estratégico y de reputación.

Tabla 4: Casos de eventos de pérdidas por riesgo operacional ocurridos en grandes instituciones.

AÑO	INSTITUCIÓN	IMPACTO ECÓNOMICO	DESCRIPCIÓN DEL EVENTO
1995	Barings Bank	1400 millones de dólares	Banco Barings, fundado en 1.762, era el banco más antiguo de Inglaterra y uno de los más antiguos del mundo en donde incluso tenía sus ahorros la Reina de Inglaterra. Nick Lesson, un trader de la institución, fue juntando pérdidas durante 2 años en una sucursal en Singapur. El Banco intentó un rescate de fin de semana, pero fue inútil. Barings fue declarado insolvente el 26 de febrero de 1995. El colapso fue dramático, los bonos de sus empleados en el mundo de manera instantánea.
1996	Sumitomo Bank	2600 millones de dólares	Yasuno Hamanaka, el trader principal de Sumitomo adulteró los precios mundiales del cobre en sus operaciones en el mercado de futuros en el Mercado de Metales de Londres entre 1991 y 1995. Posteriormente, a fines de 1995 los precios comenzaron a caer como consecuencia del una mayor producción del mencionado metal. En setiembre de

			1996 la propia empresa reportó una pérdida aproximada de 2600 millones de dólares.
1997	Natwest Bank	127 millones de dólares	Kyriacos Papouis, trader del mercado no organizado de swaptions, cubrió pérdidas subvaluando y sobrevaluando contratos para valorar swaps.
2002	Allied Irish Bank	691 millones de dólares	John Rusnak, cambista, ocultaba pérdidas de operaciones entre yen y dólar durante 3 años.
2002	Citigroup (caso WorldCom)	2650 millones de dólares	El presidente de WorldCom realizó fraudes contables que hicieron quebrar a la empresa. Citigrupo tuvo que pagar a los accionistas 2650 millones de dólares para evitar una demanda por parte de los mismos.
2005	Edificio Windsor	Incalculable	Misteriosamente el edificio Windsor de Madrid comenzó a arder a las 11 de la noche del 12 de febrero de 2005, esto generó pérdidas para comercios y bancos que se encontraban en las proximidades.

FACTORES DEL RIESGO OPERATIVO

Son las fuentes que generan los eventos en los se originan o pueden originar las pérdidas por riesgo operacional. Se dividen en factores internos y externos. Los factores internos se refieren a procesos, recursos humanos, tecnología e infraestructura. Los externos están relacionados a la naturaleza o por terceros ajenos a la entidad y que escapan a su control.

PROCESOS

Se refieren a una secuencia tares y actividades que transforman las entradas adicionándoles valor, para producir una salida para otro proceso o un producto o servicio para el cliente.

Generalmente los procesos pueden ser distinguidos en tres grandes categorías:

Procesos Estratégicos

Aquellos definidos por el directorio de una institución y que sirven para definir las estrategias y objetivos de la misma.

Procesos Operativos

Son aquellas actividades o tareas que producen servicios o productos para los clientes de la institución.

Procesos de Apoyo

Son el soporte de los anteriores procesos que están destinados a gestionar la institución, así como medir la calidad y satisfacción de los clientes.

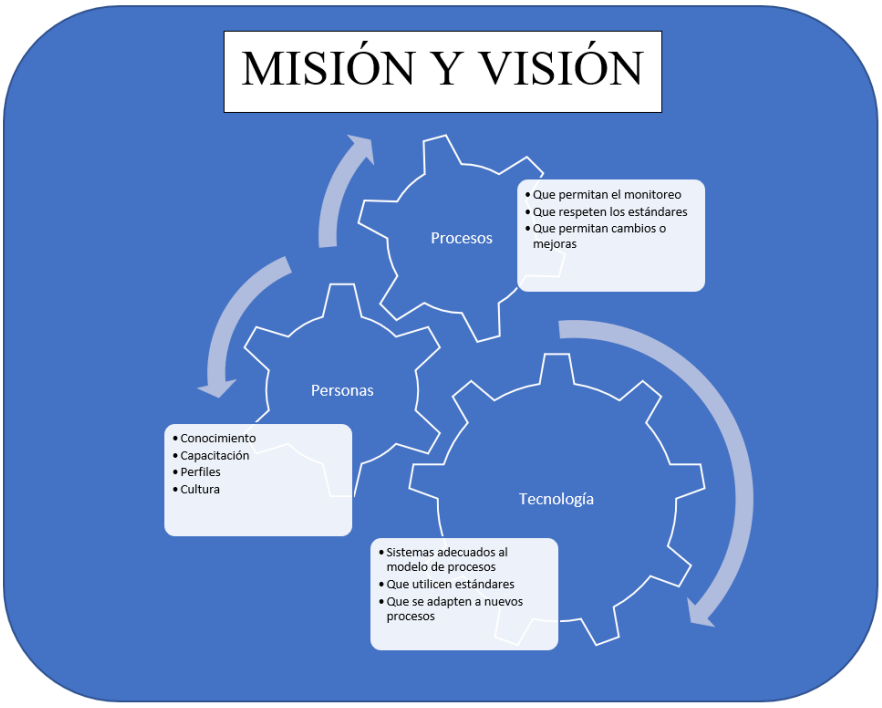
Tabla 5: Características Fundamentales de los Procesos Institucionales

✓ Deben tener una armonía con las características de la institución y estar alineados a su estrategia. ✓ Pueden abarcar a toda la institución, algunas dependencias o solo una. ✓ Es necesario combinar con otros factores (personas, sistemas, etc.) para poder ejecutarlos. ✓ Deben tener un dueño, quien deberá ser responsable de su correcto funcionamiento, mantenimiento y mejoramiento. ✓ Deben dar la posibilidad de construir indicadores. ✓ Permite identificar la gestión que corresponde al dueño de proceso (gestión por procesos).

Gestión por procesos

La gestión por procesos puede verse como un engranaje, el cual hace posible que los componentes fundamentales de la organización puedan trabajar de manera conjunta para lograr los objetivos que contribuyen a la misión y visión de una institución.

Figura 5: Esquema de la gestión por procesos



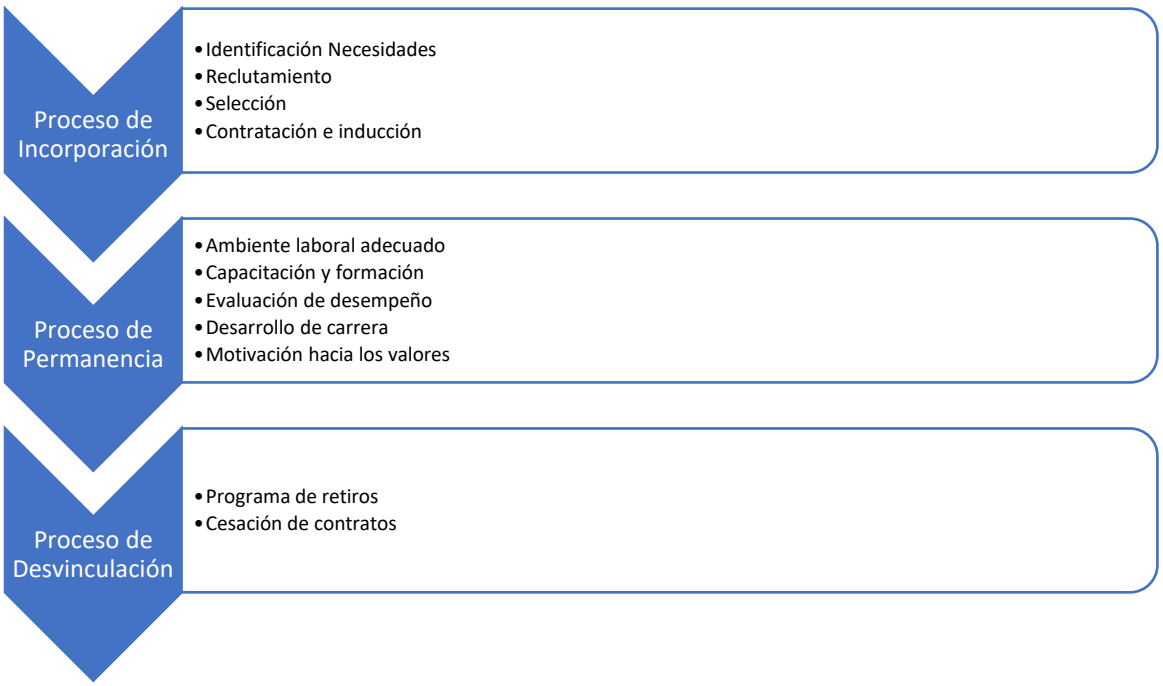
Este gráfico nos muestra la importancia de que los componentes funcionen de forma correcta, coordinada, adaptada. Mientras en mejor estado se encuentren los elementos que lo hacen funcionar (estándares, conocimientos, sistemas, cultura, etc.) mejor performance tendrá el Sistema.

RECURSOS HUMANOS

Son las personas que se encargarán de que se lleve a cabo la ejecución de los procesos ya sea de forma manual, semiautomática o automática. Ellas realizan sus tareas de diversas formas (como empleado, parte de un equipo o a través de la prestación de servicios) pero siempre enfocados en una gestión por procesos. Sus tareas están acotadas por manuales de funciones relacionados a una estructura organizacional.

En una institución las personas deberán atravesar tres procesos de recursos humanos los cuales garanticen la calidad de sus gestiones. Los estatutos y normativas que estuvieren vigentes en cuanto a recursos humanos deberán estar alineados, respetar y seguir estos esquemas de procesos.

Figura 6: Esquema de procesos en recursos humanos



TECNOLOGÍA

Representa un conjunto de elementos utilizados para ejecutar los procesos de la institución. Principalmente se refieren a Hardware, Software y Redes de comunicación. Permiten adquirir, producir, almacenar, tratar, manipular, comunicar, registrar informaciones en texto simple, imágenes, sonidos y otros.

Entre los elementos principales se encuentran los servidores, estaciones de trabajo, dispositivos de impresión, telecomunicación entre otros. Además de ser las herramientas para llevar a cabo procesos transversales de soporte

de la institución, son el soporte fundamental de los procesos institucionales ya sean estos de naturaleza estratégica, operativa o incluso otros de apoyo.

Arquitectura de la Tecnología

Conjunto de componentes, servicios y procedimientos destinados a dirigir y soportar el desarrollo y funcionamiento de soluciones a los negocios de la institución asegurando calidad, integridad y fácil operación. Es importante que esta arquitectura funcione con las siguientes características:

- ✓ Principalmente, aporte valor.
- ✓ Ofrecer operatividad, reusabilidad y escalabilidad.
- ✓ Sea ágil y eficaz para la implementación de nuevos procesos y formas de negocios para la institución.
- ✓ Que este diseñado en base a mejores prácticas y estándares que garanticen la calidad.
- ✓ Permita la alineación a las normativas, políticas y reglamentación de la institución.

Cuanto más sofisticada es la arquitectura utilizada, mayor es la dependencia de los procesos de esta. Es por ello que es importante que cumpla con todos los requisitos mencionados anteriormente. Por tanto, se vuelve fundamental la adopción de estándares de seguridad, tales como ISO/IEC 27001[10], COBIT[11], entre otros.

EVENTOS EXTERNOS

Desastres naturales

Son los eventos que podrían desembocar en una situación compleja debido a desastres naturales. Esta situación compleja podría representar pérdidas de vida, daños a la infraestructura, pérdidas de bienes que podrían afectar a la institución de manera crítica.

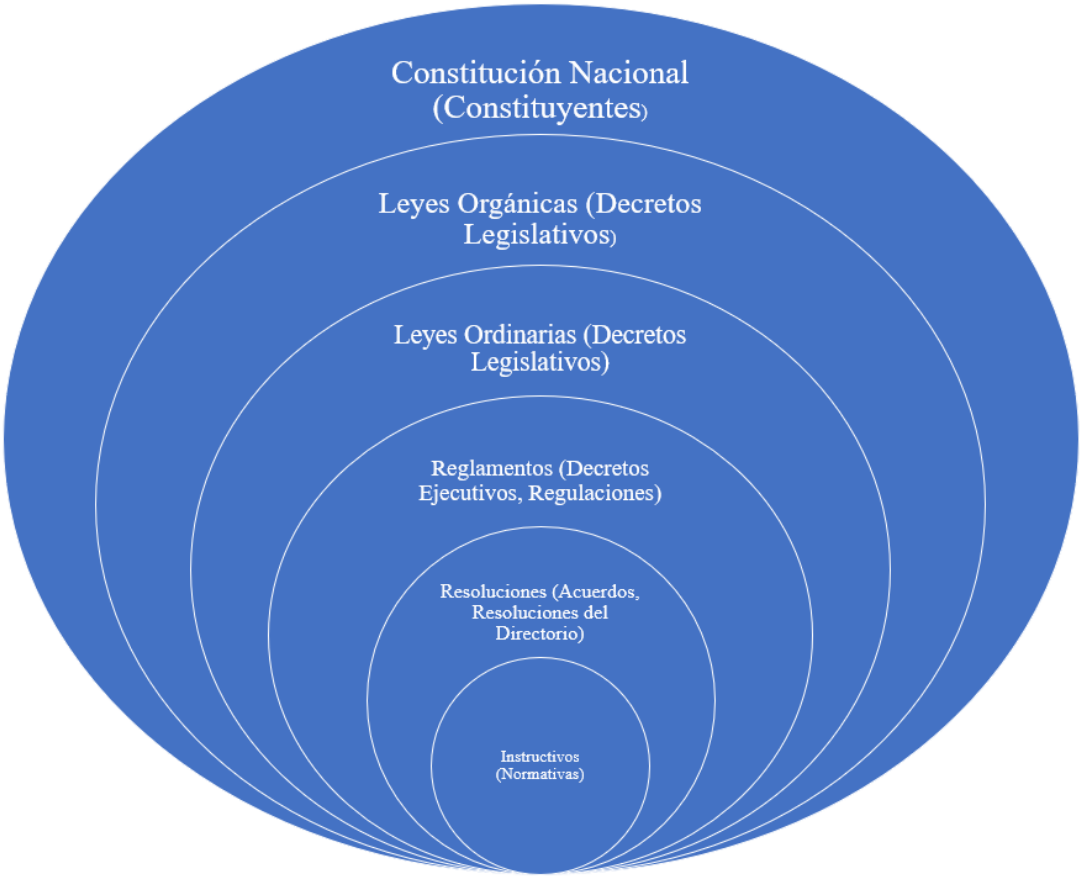
Leyes y normativas

Es un conjunto de disposiciones, leyes, reglamentos, acuerdos que deben ser respetados y que generan en la institución una dependencia y observancia mientras realiza sus actividades en busca de lograr sus objetivos.

[10] ISO/IEC 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

[11] Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI).

Figura 7: Dependencia normativa que generalmente poseen las instituciones



CAPTURA DE EVENTOS QUE GENERAN PÉRDIDAS

Representa una herramienta fundamental para poder realizar una gestión eficiente del riesgo operativo. En las empresas donde inician la implementación, habitualmente utilizan planillas electrónicas como base de datos para la recolección de los eventos que generan pérdidas, posteriormente, cuando la cultura y madurez se robustecen, se tiende a desarrollar o adquirir un software para realizar dicha actividad.

Se estila registrar el área afectada, el proceso institucional al cual afectó, la categoría del evento (falla en los procesos, falla en los sistemas, fallas en personas o eventos externos), la descripción del evento ocurrido y los impactos ocurridos (monetarios, en insumo de recursos humanos y la repercusión).

La buena calidad en el registro de los datos y que todos eventos sean comunicados/reportados a través de este sistema, permitirá contar con una poderosa herramienta que permita determinar la probabilidad de ocurrencia de los eventos. Se requiere de una base de datos de al menos 5 años (en bases de datos nuevas podrán utilizarse datos de 3 años) para poder calcular con cierto intervalo de confianza aceptable.

El desafío se encuentra en lograr que toda la institución adquiera la cultura de riesgos de forma tal a poder reportar responsablemente los eventos de pérdidas. El Acuerdo de Basilea II, recomienda para aquellas instituciones en las que se encuentran en inicio de la implementación de un sistema de gestión de riesgos, y que cuentan con pocos reportes de eventos aún, que consulten a bases de datos externas de empresas similares y se focalicen en aquellos eventos de baja frecuencia y mediano o alto impacto para poder realizar los cálculos de probabilidad de ocurrencia de los eventos. Estos representarían algunos de los riesgos a los que se encuentran expuestos la empresa.

En la Tabla 6 se detallan los principales aspectos que deberán ser tenidos en cuenta para que la base de datos represente una herramienta lo necesariamente útil.

Tabla 6: Características Fundamentales de los Procesos Institucionales

- ✓ Los eventos materializados deberán ser categorizados de acuerdo a una taxonomía estandarizada para la empresa y relacionarse a una de las líneas de negocio predefinidas a la cual hayan afectado.
- ✓ Todas las actividades esenciales en las cuales se produzcan pérdidas deberán comunicar los eventos. La entidad deberá definir un monto mínimo desde el cual se deban comunicar los eventos. Este monto mínimo también podrá adaptarse por tipo de evento y línea de negocio.
- ✓ Se deberán especificar detalles cualitativos, como ser los elementos que ocasionaron los eventos materializados.
- ✓ Aquellos eventos que afecten a diversas líneas de negocios deberán ser tratados como un único evento, para ello la entidad deberá definir un mecanismo particular de comunicación.
- ✓ Las pérdidas de riesgo operativo desencadenadas de riesgo de créditos que anteriormente eran incluidas en base de datos de esta, deberán seguir registrándose de la forma anterior de modo a que se pueda seguir definiendo el cálculo de su capital. En los casos donde las pérdidas representen una cantidad importante también deberán ser incluidas en las bases de datos de riesgo operacional de forma tal a que esta información este disponible para la toma de decisiones transcendentes respecto a las operaciones.
- ✓ Todas las pérdidas de riesgo operativo desencadenadas de riesgo de mercado deberán ser registradas en las bases de datos de riesgo operacional aún cuando estas presenten la dificultad para identificar dentro cuentas de pérdidas y ganancias que resultan de las operaciones financieras.
- ✓ Para poder contar con una base de datos relevante requiere de que está esté construida con datos de al menos 5 años. En los casos donde la base de datos sea relativamente nueva, podrán utilizarse datos de los últimos 3 años.

El Risk Management Group del Comité de Supervisión Bancaria de Basilea realizó un informe denominado ***Ejercicio de recolección de datos de pérdida de riesgo operacional*** en el marco de su ***Estudio de Impacto Cuantitativo*** sobre los eventos de pérdidas por riesgo operacional reportados en 89 distintos bancos internacionales durante el año 2001. Estas pérdidas fueron clasificadas por líneas de negocios y por categoría de riesgos. Las pérdidas incluyeron 50.000 eventos materializados que generaron pérdidas por un monto aproximado a los 7.800 millones de euros.

La Tabla 7 y 0 nos muestra la distribución de esas pérdidas en cuanto a impacto y frecuencia por categoría de eventos. Por ejemplo, nos permite ver que la categoría de eventos "Ejecución, entrega y gestión de procesos" representa la que mayor pérdida generó con un 29%, seguido de la categoría "Daños a activos físicos" con 24%. En cuanto a la frecuencia, la categoría "Fraude externo" fue la que ocurrió más frecuentemente con un 42% seguido de la categoría "Ejecución, entrega y gestión de procesos" con 35%.

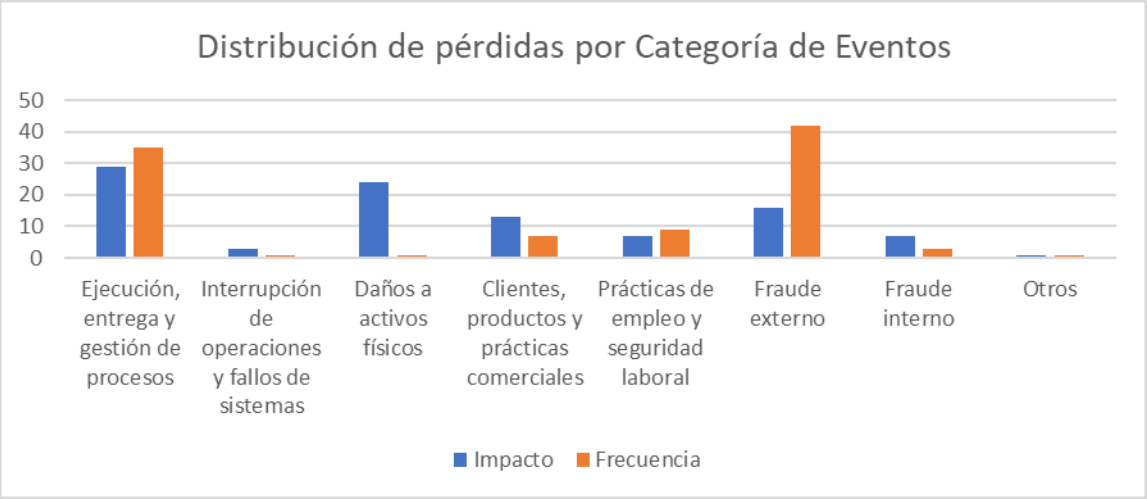
Si bien los eventos de la categoría "Fraude externo" fueron los más frecuentes, estos no representan los que ocasionaron mayor pérdida, un ejemplo de fraude externo frecuente, pero de impacto bajo, suelen ser las realizados con las tarjetas de créditos, los cuales no llegan a afectar notablemente el patrimonio de los bancos.

Así mismo, los eventos de la categoría "Daños a Activos Físicos", son los que con menor frecuencia ocurrieron, sólo 1%, pero tuvieron mucho impacto, con 24%. Esto es comprensible ya que en el 2001 se produjeron sendos acontecimientos como los ataques terroristas del 11 de setiembre entre otros.

Tabla 7: Pérdidas en el año 2001 por tipos de eventos en los 89 bancos analizados.

Categoría de Evento	Impacto (%)	Frecuencia (%)
Ejecución, entrega y gestión de procesos	29	35
Interrupción de operaciones y fallos de sistemas	3	1
Daños a activos físicos	24	1
Clientes, productos y prácticas comerciales	13	7
Prácticas de empleo y seguridad laboral	7	9
Fraude externo	16	42
Fraude interno	7	3
Otros	1	1

Figura 8: Comparativo de frecuencia e impacto por tipos de eventos.



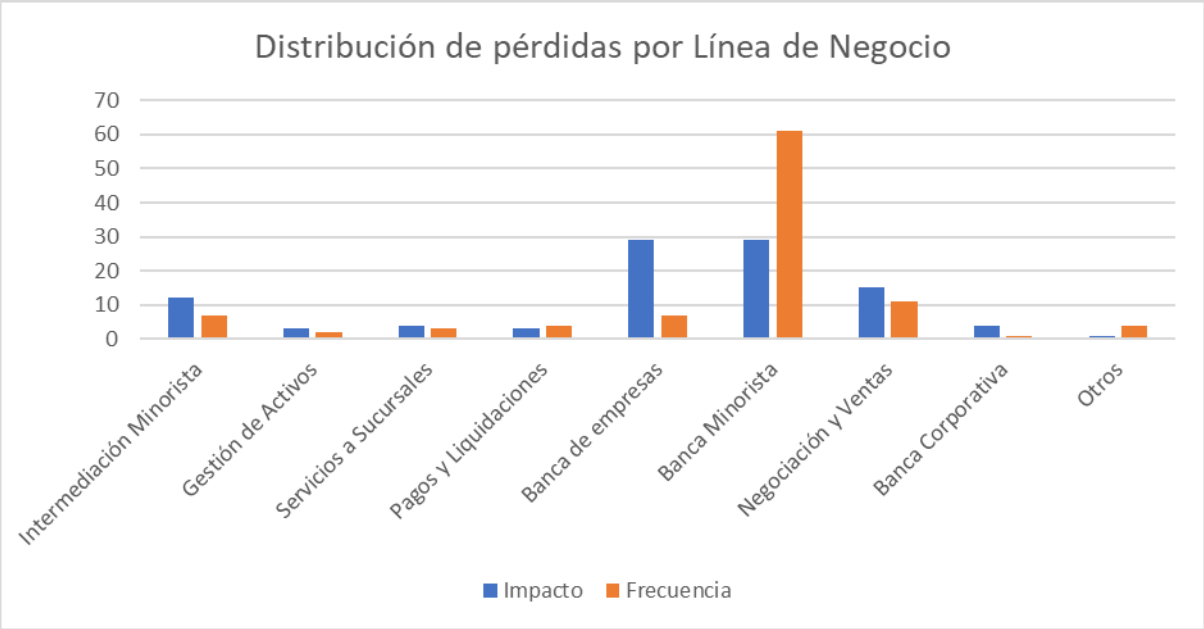
Fuente: https://www.bis.org/bcbs/qis/ldce2002.pdf. Gráfico de elaboración propia.

Respecto a las líneas de negocios, según la Tabla 8 y 0, podemos observar que los eventos que generaron mayor impacto se materializaron en "Banca de Empresas" y "Banca Minorista", aunque el porcentaje de frecuencia del primero es muy superior al del segundo. Esto es razonable debido a que en la línea "Banca Minorista" se realizan un mayor número de transacciones de forma habitual, pero con un monto menor al de la línea "Banca Mayorista" en donde las transacciones suelen ser por montos muchos mayores.

Tabla 8: Pérdidas en el año 2001 por línea de negocio en los 89 bancos analizados.

Línea de Negocio	Impacto (%)	Frecuencia (%)
Intermediación Minorista	12	7
Gestión de Activos	3	2
Servicios a Sucursales	4	3
Pagos y Liquidaciones	3	4
Banca de empresas	29	7
Banca Minorista	29	61
Negociación y Ventas	15	11
Banca Corporativa	4	1
Otros	1	4

Figura 9: Comparativo de frecuencia e impacto por línea de negocios.



El Comité de Basilea, a través de su documento *Buenas prácticas para la gestión y supervisión del riesgo operativo*, argumenta que el término *riesgo operativo* implica una amplia gama de eventos que pueden ocurrir dentro del sector bancario por lo que cada banco puede adoptar sus propias definiciones de forma interna. También definió un conjunto de tipos de eventos, en colaboración con diversas instituciones bancarias, que podrían ser fuentes de posibles pérdidas importantes.

Tabla 9: Eventos de pérdidas según el Comité de Basilea

Tipos de Eventos	Descripción
Fraude interno	Errores deliberados en beneficio propio, robos por parte de empleados o uso de información confidencial para obtener algún beneficio o de terceros.
Fraude externo	Robo, falsificación, creación de cheques falsos, daños por accesos no autorizados a sistemas informáticos.
Relaciones laborales y seguridad en el puesto de trabajo	Indemnizaciones por quejas, incumplimiento de normas laborales, discriminación, etc.
Prácticas con los clientes, productos y negocios	Abuso de confianza y de información sobre el cliente, ventas de productos no autorizados, negociaciones fraudulentas, entre otros.

Daños a activos materiales	Terrorismo, vandalismo, terremotos, fuegos e inundaciones.
Alteraciones en la actividad y fallos en los sistemas	Fallas en software, hardware, telecomunicaciones, interrupción en los suministros públicos.
Ejecución, entrega y procesamiento	Carga de datos erróneos, documentos incompletos, concesión de accesos no autorizados, entre otros.

La evaluación del riesgo operativo requiere de dos variables. La primera es la frecuencia o probabilidad, la cual se refiere a la regularidad con la ocurre el evento de riesgo operativo. La segunda es la severidad o impacto el cual afecta al patrimonio de la empresa. Ambas variables se utilizan para determinar el riesgo operativo a través de cuatro posibles zonas. Una vez definida la zona del riesgo se deberá tomar decisiones para "llevar" estos riesgos a una zona "aceptable", en donde en caso de materializarse no afecten al patrimonio de la empresa.

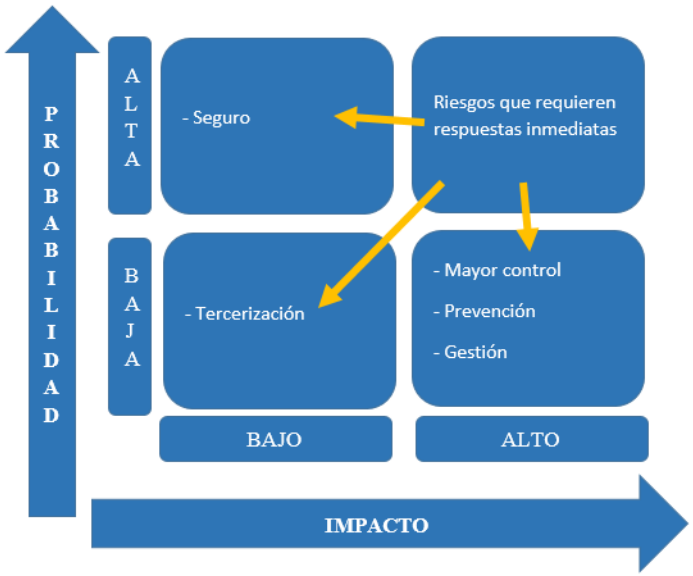
Dentro de estas zonas, la más peligrosa corresponde a aquella que posee tanto el impacto como la probabilidad altos, los cuales, en caso de ocurrir tendrían efectos irreversibles para la entidad. Los riesgos ubicados allí deberán tener un tratamiento inmediato a fin de mitigar y trasladar a una zona de probabilidad baja a través con controles preventivos o a una zona de impacto bajo a través de seguros entre otros. En situaciones extremas, en donde la actividad podría generar pérdidas significativas, habrá que analizarse la posibilidad de transferir la actividad a través de una venta, cesión o tercerización.

La zona representada por baja probabilidad y alto impacto también requiere de una atención especial. Si bien los controles mitigan la probabilidad, ya sea a través de gestión, control, prevención, entre otros, si llegará a materializarse el riesgo, tendría un impacto importante. Las medidas a implementar para estos casos son aseguramiento de activos contra eventos externos, incendios, catástrofes, entre otros.

En cuanto a la zona que presenta alta probabilidad, pero bajo impacto, estas son las que la gestión de riesgos operativos debe identificar de manera concreta y gestionar la implementación de planes de acción para disminuir la frecuencia de ocurrencia.

La zona objetivo de la entidad será la de baja probabilidad y bajo impacto. Esta es la zona permite ver nuevas alternativas de negocios de una forma más tranquila sin preocuparse por tener que gestionar los riesgos de las actividades ya existentes.

Figura 10: Prioridades para la mitigación de riesgos



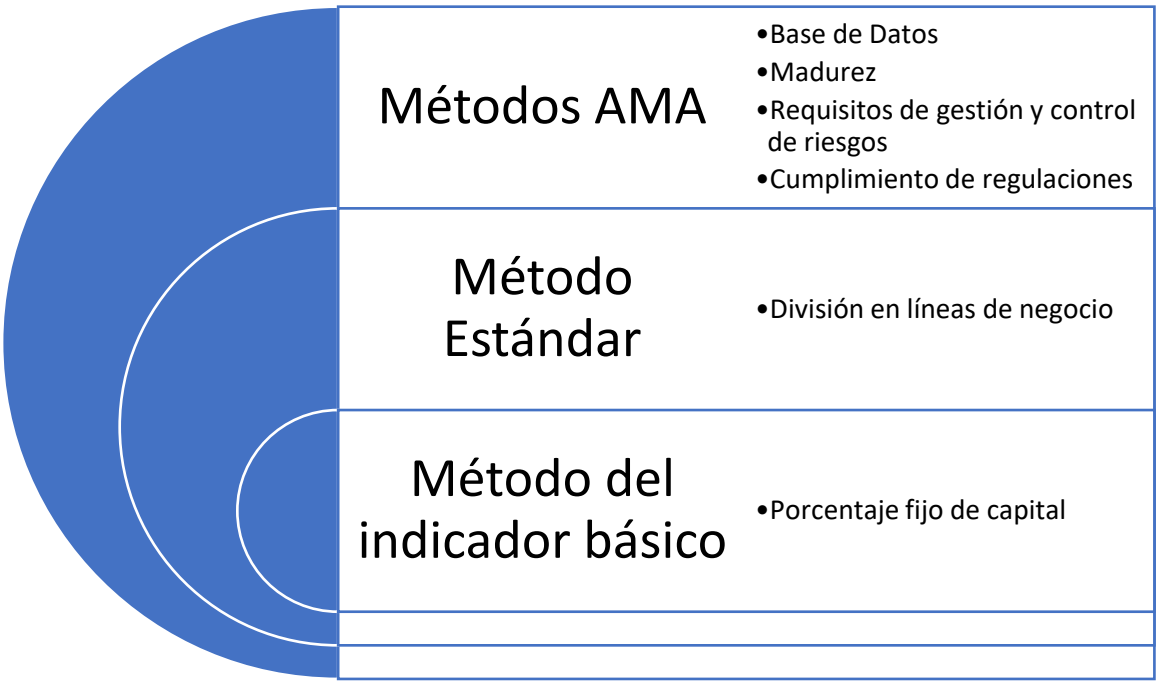
ENFOQUES PARA LA MEDICIÓN DEL RIESGO OPERACIONAL

El aspecto más importante para poder planificar la creación de una base y armar las estrategias para la gestión del riesgo operacional es la medición o cuantificación. Esto ayudará a determinar las medidas de mitigación o aseguramiento requerido para los diversos riesgos de la entidad. Basilea II propone 3 enfoques para que las entidades puedan medir el riesgo operacional de forma tal a poder utilizar eficientemente el capital destinado a este tipo de riesgo y con el perfeccionamiento en la medición poder reducir el mencionado capital.

La medición adecuada del riesgo operacional ayuda a poder determinar la rentabilidad ya adecuada a este tipo de riesgo necesaria para conocer el valor real de la compañía.

Los 3 enfoques diseñados por el Comité a través de Basilea II permiten calcular los requerimientos de capital por riesgo operacional. Estos enfoques son: el método del indicador básico (Basic Indicator Approach o BIA), el método estándar (Standardized Approach o SA) y las metodologías de medición avanzada (Advanced Measurement Approach o AMA). Estos enfoques varían en la medición del riesgo que realizan en cuanto a la exactitud, sofisticación y sensibilidad.

Figura 11: Enfoques de medición del riesgo operacional



Primeramente, para poder entender estos enfoques es necesario saber que los ingresos brutos son utilizados para poder obtener una aproximación al tamaño o el nivel de exposición del riesgo operacional en la entidad. Aunque el Comité reconoce que cada país podría tener una regulación que respecto al cálculos de dichos elementos. También es importante tener en cuenta que una entidad con ingresos brutos grandes podría tener mejores prácticas para gestionar el riesgo.

Tanto el método indicador básico como el estándar utilizan metodologías que sirven para cubrir el riesgo operacional de acuerdo a través de un capital equivalente que representa un porcentaje determinado de los ingresos brutos. El primer método está basado en un porcentaje fijo del capital por un indicador. El segundo divide el porcentaje fijo en 8 líneas de negocios y las multiplica por un indicador para cada línea de negocio definida por el Comité.

En cuanto a los enfoques AMA, estas tienen un diseño bottom-up (ascendente) en donde el requerimiento de capital es calculado en base a la sumatoria de pérdida registrada en un sistema interno que mide el riesgo operacional. El enfoque AMA se subdivide en 3 metodologías: los modelos de medición interna (Internal Measurement Approach o IMA), los modelos de distribución de pérdidas (Loss Distribution Approach o LDA) y los cuadros de mando (Scorecards). Los enfoques AMA presentan mayor flexibilidad para la medición del riesgo operacional, pero también requieren de mayor madurez, costo y complejidad. Entre los requisitos necesarios se

encuentra el de contar con una buena base de datos de las pérdidas, los cuales son necesarios para poder aproximar a las variables requeridas para utilizar en los modelos. Esto representa, muchas veces, la principal dificultad para poder implementar este enfoque ya que inicialmente no es posible contar con una base de datos que refleje la realidad de las pérdidas ocurridas.

Las entidades que deseen implementar el método estándar o una de las metodologías AMA deberán cumplir unos requisitos mínimos en cuanto a la gestión y control del riesgo operacional. En cuanto al enfoque indicador básico está diseñado de forma tal a que pueda ser utilizado por cualquier entidad independientemente de su tamaño y complejidad por lo cual se convierte en el modelo a utilizar cuando una entidad desea empezar a incursionar en la implementación de su gestión de riesgo operacional.

Método del Indicador Básico

Según Basilea II, para cubrir el riesgo operacional, los bancos que vayan a utilizar este enfoque deberán calcular un requerimiento de capital equivalente a la media de los últimos 3 años de un porcentaje fijo (15% y denotado por alfa) de sus ingresos brutos anuales que sean mayor a cero. Se excluyen tanto los ingresos brutos negativos o que son iguales a cero.

$$RC = (\sum (IB_{1-n} \times \alpha)) / n$$

RC: Requerimiento de capital

IB: Ingresos brutos anuales positivos

n: Número de años en los últimos 3 con IB positivos.

α : 15%

Método Estándar

Está enfocado a determinar el requerimiento de capital utilizando cada línea de negocio definida por Basilea II. A cada línea de negocio se le asigna un porcentaje fijo.

Tabla 10: Porcentajes que se asigna en el método estándar a cada línea de negocio.

Línea de negocio	Porcentaje asignado
Finanzas corporativas	18
Negociación y ventas	18
Banca minorista	12
Banca comercial	15
Liquidación y pagos	18
Servicios de agencia	15
Administración de activos	12
Intermediación minorista	12

$$RC = \sum_{años\ 1}^{año\ 3} \left(\sum \max(IB_{1-8} \times \beta_{1-8}), 0 \right) / 3$$

RC: Requerimiento de capital

IB: Ingresos brutos anuales positivos para cada línea de negocio

β : porcentaje fijo por cada línea de negocio

Método de medición avanzado (A.M.A.)

Para poder utilizar este método, las entidades deberán estar calificados con un conjunto de principios que el Comité de Supervisión consideró necesario.

1. El Directorio o la Gerencia deberán estar totalmente comprometidos en revisar periódicamente el cumplimiento de la Política de Gestión de Riesgos Operativos.
2. Tener implementado un Sistema de Gestión de Riesgos Operativos bien diseñado y que presente integridad.
3. Poseer los recursos necesarios que el Sistema necesita, así como áreas que control y auditoría.

Otras consideraciones que deberá contemplarse para utilizar este método son:

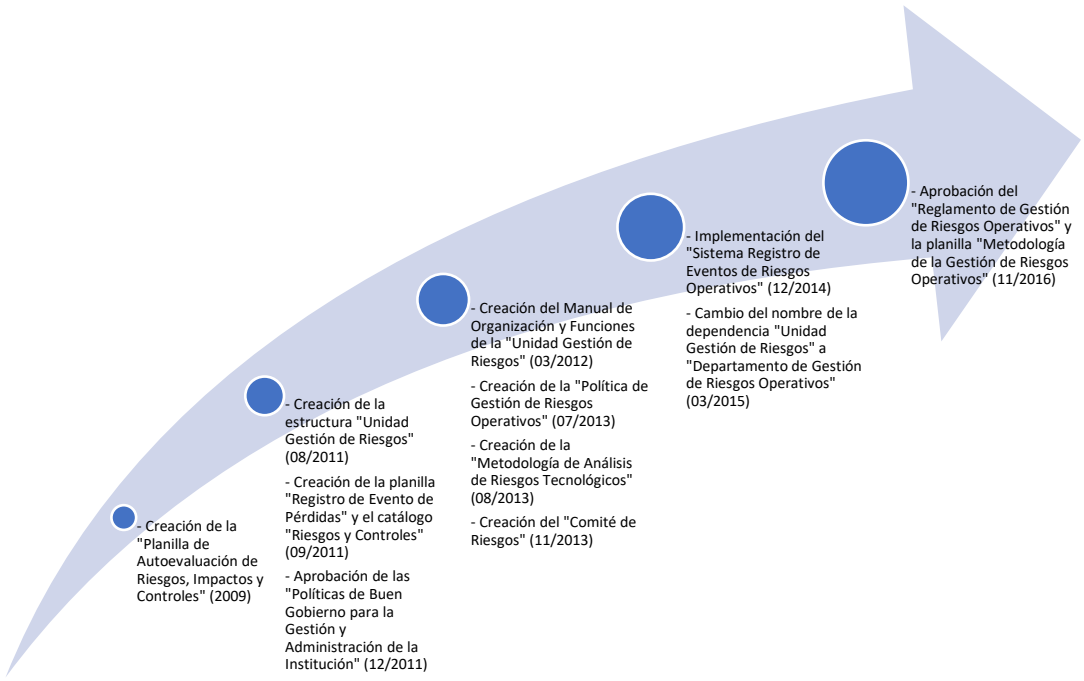
- El sistema deberá estar verificado por auditorías internas y externas. Así mismo, deberá contar con la aprobación del supervisor.
- Podrán ser utilizados seguros que reduzcan hasta 20% el requerimiento de capital, condicionados a que las aseguradoras tengan calificación A o mayor y que las mismas no estén relacionadas a la entidad.
- El supervisor, podrá disponer la utilización del AMA en algunas áreas, de forma parcial, y en otras el indicador básico o el estándar.
- Cuando en un banco ya esté completamente implementado un método más complejo que otro, no podrá volver a utilizarse el método menos complejo.

MARCO EMPÍRICO

Avances cronológicos en la implementación de la Gestión de Riesgos Operativos en la institución.

En la Institución, la necesidad de llevar adelante la especialidad de la gestión de riesgos operativos fue manifestada por el área de Auditoría Interna. En la Figura 12 puede observarse una cronología en la implementación del Sistema de Gestión de Riesgos Operativos hasta la creación del Manual de Organización y funciones de la dependencia que finalmente se encargaría de establecer el mencionado Sistema.

Figura 12: Cronología de las actividades realizadas para la implementación del Sistema de Gestión de Riesgos Operativos



Planilla “Autoevaluación de Riesgos, Impactos y Controles”

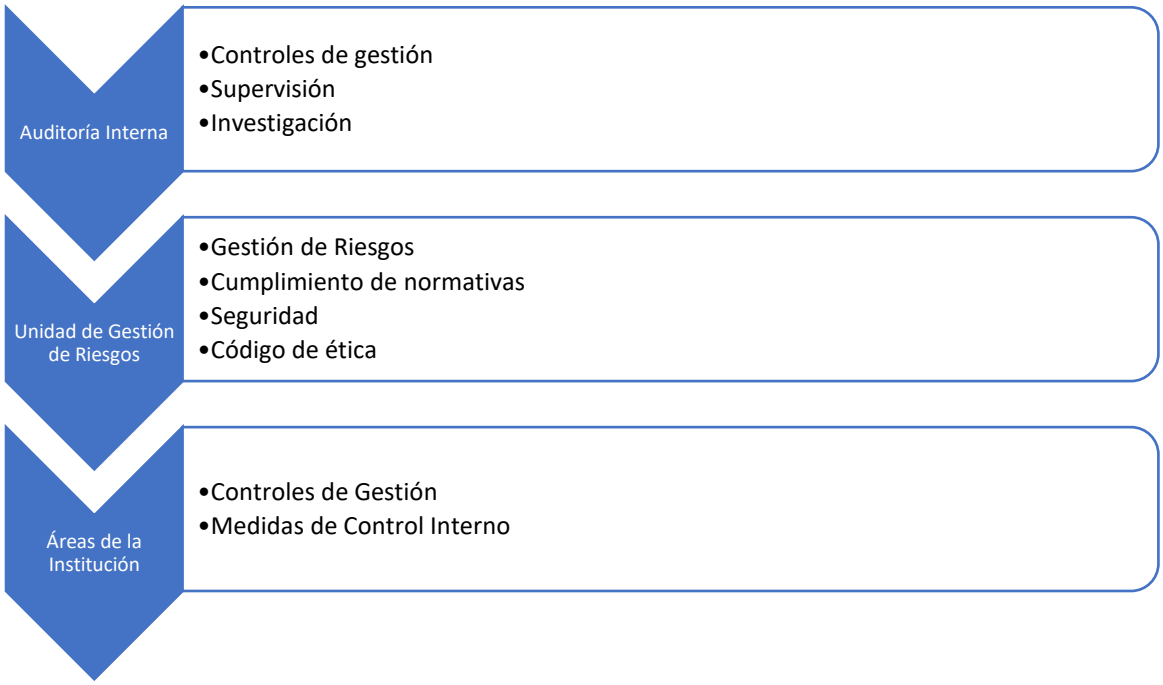
En el afán de poder implementar el Sistema de Gestión de Riesgos Operativos, inicialmente, la Auditoría Interna desarrolló la planilla “Autoevaluación de Riesgos, Impactos y Controles” y lo oficializaron en mayo de 2009. Una herramienta inicial que estaba diseñada con la idea de identificar y evaluar los riesgos y controles de las áreas de la Institución. La misma fue organizada en Categorías de Riesgos que a la vez se dividían Subcategorías de Riesgos. Las valoraciones de impactos y controles eran evaluadas por cada Subcategoría, siendo de carácter muy general y no individualizando el riesgo en particular que podrían sufrir los impactos valorados y tampoco

permitían tener una identificación adecuada de los controles. Sin lugar a dudas se trataba de un nivel inicial para la implementación de la gestión de riesgos operativos.

Creación de la Unidad Gestión de Riesgos

En agosto del año 2011, se crea la Unidad Gestión de Riesgos, tomando como referencia principal el **PRINCIPIO 2** mencionado Tabla 3 el cual establece que "*El Directorio deberá asegurar que el marco para la gestión del riesgo operativo esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser responsable de la gestión del riesgo operativo, solo de la revisión del cumplimiento del marco*". A la vez se toma en cuenta la estructura de gestión de riesgos operativos recomendada por el marco COSO ERM (ver Figura 13) en el cual la primera línea de defensa para la gestionar los riesgos operativos está representada por las propias áreas, quedando la segunda línea a cargo de la Unidad de Gestión de Riesgos y finalmente, en la tercera línea la Auditoría Interna, la cual evaluará la gestión realizada por las anteriores.

Figura 13: Estructura de la gestión de riesgos operativos recomendada por COSO ERM



Entre las principales funciones que esta área debía realizar se encontraban:

- Apoyar al Directorio en el cumplimiento los objetivos institucionales proponiendo la implementación de metodologías para la gestión de riesgos operativos.
- Orientar a las áreas en el proceso de identificación, análisis, evaluación y tratamiento de riesgos.
- Promover la cultura de gestión de riesgos operativos en la institución por medio de seminarios, talleres, capacitaciones, etc.

- Asesorar a las áreas en la aplicación de las metodologías para implementar la gestión de riesgos operativos.
- Desarrollar, de acuerdo a las mejores prácticas recomendadas, las metodologías y herramientas para la gestión de riesgos operativos.

Planilla "Registro de Evento de Pérdidas"

Unos días después de que se haya aprobado la creación de la Unidad Gestión de Riesgos, se oficializó la implementación de la planilla "Registro de Evento de Pérdidas" y el catálogo "Riesgos y Controles". La planilla "Registro de Evento de Pérdidas" era una herramienta construida a los efectos de recolectar los eventos de riesgos materializados de forma tal a alimentar una base de datos para la cuantificación del riesgo operativo. En caso de materializarse un evento de riesgos, el área afectada debía llenar la planilla y remitirla a la Unidad Gestión de Riesgos para que esta la incorpore a la base de datos. El catálogo “Riesgos y Controles” era un anexo de la planilla mencionada y servía de guía para la categorización de los eventos de riesgos y los controles.

La base de datos mencionada, sería utilizada en las evaluaciones de riesgos operativos, para poder determinar la probabilidad de ocurrencia de eventos, que al ser combinadas con las valoraciones de impactos obtenidos de la planilla “Autoevaluación de Riesgos, Impactos y Controles” permitirían las construcciones de mapas de riesgos.

Figura 14: Planilla “Registro de Eventos de Pérdidas”.

I. REGISTRO DE EVENTOS DE PERDIDAS								
I. INFORMACIÓN DEL EVENTO								
1. FECHA DEL EVENTO			3. FECHA DE CAPTURA			5. FUNCIONARIO QUE REALIZA EL REGISTRO		
			4. GERENCIA					
2. PROCESO			DPTO					
			DIVISIÓN					
PROCESO			SECCIÓN					
II. CLASIFICACIÓN DEL EVENTO POR FACTOR DE RIESGO								
6. CATEGORIA DE RIESGO				7. SUBCATEGORIA DE RIESGO				
Según Taxonomía de Riesgo Operativo				Según Taxonomía de Riesgo Operativo				
III. DESCRIPCION DEL EVENTO								
8. DESCRIPCIÓN DE LAS CIRCUNSTANCIAS QUE RODEARON AL EVENTO								
9. MECANISMO DE CONTROL RELACIONADO								
IV. IMPACTO DEL EVENTO								
10. TIPO DE PERDIDA			11. EVENTOS MATERIALIZADOS CON IMPLICACIONES CONTABLES			12. EVENTOS MATERIALIZADOS SIN IMPLICACIONES CONTABLES		
ECONOMICO			PERDIDA CONTABLE			HORAS-HOMBRE BASICAS		
REPUTACIONAL			RECUPERACIONES					
			COSTOS ASOCIADOS					
			PERDIDA NETA	0				
V. REVISIÓN DEL EVENTO								
13. COMUNICACIÓN EFECTUADA Y DATOS DE DOCUMENTACIÓN RESPALDATORIA								
	SI	NO						
COMUNICADO A ALTA GERENCIA?			FECHA DE COMUNICACIÓN:			COMUNICADO POR:		
DOCUMENTO DE COMUNICACIÓN								
	ACLARACIÓN Y FIRMA FUNCIONARIO RESPONSABLE DEL REGISTRO DE EVENTOS DE PÉRDIDAS				ACLARACIÓN Y FIRMA RESPONSABLE DEL AREA			

Aprobación de las "Políticas de Buen Gobierno para la Gestión y Administración de la Institución"

En diciembre del año 2011, el Directorio de la institución aprueba las "Políticas de Buen Gobierno para la Gestión y Administración de la Institución", documento con el que la institución se compromete y busca comprometer a todos los integrantes de la organización respecto a los ámbitos técnicos, operativos y sociales. En uno de sus capítulos, hace hincapié en las "Políticas sobre riesgos", mencionando el compromiso de la adopción de una Política de Administración de Riesgos adecuada a los procesos que la institución desarrolla.

Manual de organización y funciones de la Unidad Gestión de Riesgos

En marzo del año 2012, luego de aproximadamente 6 meses que se haya creado la Unidad Gestión de Riesgos, se aprobó su manual de organización y funciones. De este modo quedaba documentado, de forma oficial, las principales tareas que el área debía realizar.

Aprobación de la "Política de Gestión de Riesgos Operativos"

En julio de 2013, el Directorio aprueba la "Política de Gestión de Riesgos Operativos", el cual contiene los lineamientos generales relacionados a la gestión de riesgos operativos en la institución y que deberán ser observados por todos los integrantes de la organización.

Los principales aspectos que incluidos en la política son los siguientes:

- Definición del Riesgo Operativo.
- Objetivo de la Política.
- Alcance.
- Roles y responsabilidades.
    - Máxima Autoridad o Directorio
    - Alta Administración o Gerencia General
    - Gerencias de áreas
    - Unidad Gestión de Riesgos
    - Auditoría Interna
    - Funcionarios de la institución
- Cultura de riesgos operativos en la institución.
- Etapas de la gestión de riesgos.
- Glosario de términos.

Metodología de Análisis de Riesgos Tecnológicos

En agosto del año 2013, se oficializa la Metodología de Análisis de Riesgos Tecnológicos, herramienta diseñada con el objetivo de establecer un método sistemático para la evaluación de riesgos de sistemas informáticos y

activos de información. Estaba basado en varios estándares de tecnologías de la información, pero principalmente en el MAGERIT[12] (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). El alcance de la metodología era para todos los procesos que tengan de forma implícita riesgo tecnológico. A la vez definía el riesgo tecnológico como la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso, la propiedad, la operación, adopción de tecnologías de la información (software, hardware, sistemas, aplicaciones, redes) y otros canales de distribución de información que la institución pudiere disponer.

Comité de Riesgos

En noviembre de 2013, se aprueba la creación del Comité de Riesgos. Un órgano cuya principal función era asesorar al Directorio en la gestión de riesgos operativos. Estaba conformado por: un Miembro del Directorio (como Coordinador General), el Gerente General, los Sub Gerentes Generales, el Gerente de Desarrollo (del cual dependía la Unidad Gestión de Riesgos), el encargado de la Unidad Gestión de Riesgos y el secretario de este Comité, el cual debía ser un analista de riesgos correspondiente a esta última dependencia.

Reglamento del Comité de Riesgos

En mayo del año 2014, se aprueba el Reglamento del Comité de Riesgos. El objetivo del mencionado órgano sería, según el documento, el de realizar el monitoreo y seguimiento periódico de la exposición a riesgos de los procesos desarrollados por la institución, asegurando que se cumplan los perfiles de riesgos definidos en las Políticas de Gestión de Riesgos, el cual forma parte de las Políticas de Buen Gobierno de la institución.

Dicho documento, además, especifica que el Comité apoyará a la Unidad Gestión de Riesgos, el cual se encarga del asesoramiento a las unidades de la institución en lo referido a la gestión de riesgos operativos.

Otro aspecto importante, que recoge el documento, es que los responsables de los procesos de la institución deberán cumplir de forma obligatoria con las instrucciones que este Comité pueda solicitar y que todo lo resuelto en el mismo deberá ser comunicado al Directorio de la institución. Deberán sesionar al menos 3 veces al año o más si fuese necesario, pudiendo convocar a otros responsables de áreas para la revisión de los riesgos de sus procesos.

Tabla 11: Principales funciones del Comité de Riesgos según su reglamento

#	Funciones
1	Asesorar al Directorio en las estrategias a impulsar en la Gestión de Riesgos Operativos.
2	Monitorear por el cumplimiento de las Políticas de Gestión de Riesgos operativos.
3	Aprobar las herramientas propuestas por la Unidad Gestión de Riesgos Operativos.

[12] Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

4	Establecer los niveles de tolerancia al riesgo de los procesos institucionales.
5	Definir acciones para desviaciones respecto a la tolerancia.
6	Revisar los informes elevados por la Unidad Gestión de Riesgos a los efectos de tomar decisiones pertinentes.
7	Recibir información periódica de los eventos de riesgos ocurridos, mediante Informes de la Unidad Gestión de Riesgos y tratarlos en las sesiones del Comité.
8	Promover la Cultura de Riesgos.
9	Apoyar a la Unidad Gestión de Riesgos, en cuanto a la dotación necesaria para el cumplimiento de sus funciones.
10	Mantener informado al Directorio sobre las decisiones tomadas en las sesiones del Comité.

Modificación de los integrantes del Comité de Riesgos

En diciembre del año 2014, se modifica la conformación del Comité de Riesgos de forma tal a que el Miembro del Directorio deja de ser parte de él, quedando como Coordinador, el Gerente General. Posteriormente, en noviembre del año 2016, se modifica nuevamente el reglamento a los efectos de adicionar un nuevo integrante, el cual es el encargado del área de Seguridad de la Información.

Sistema Registro de Eventos de Riesgos Operativos

En diciembre del año 2014, se implementa el Sistema Registro de Eventos de Riesgos Operativos, el cual sustituye a la planilla "Registro de Evento de Pérdidas". El mencionado Sistema fue desarrollado para capturar las informaciones de los eventos de riesgos materializados de forma más dinámica a lo que era la planilla. También servirá para determinar la probabilidad de ocurrencia de los eventos de riesgos y una media de las pérdidas ocurridas por categorías de eventos y por procesos institucionales. Entre los beneficios que ofrece el mencionado Sistema se encuentran:

- La posibilidad de que cada dependencia pueda comunicar los eventos a través del acceso a este Sistema de sus usuarios designados para utilizarlo.
- La eliminación de papeles que surgían de la impresión de la planilla para remisión y comunicación de los eventos.
- Contar con una base de datos, más dinámica, de eventos de forma tal a poder obtener reportes para diversos grupos de interesados.
- La posibilidad de ofrecer niveles de validación de los eventos comunicados.
- La adecuación a los procesos institucionales y la taxonomía de riesgos vigentes.
- Auditoría informática sobre las modificaciones de los eventos comunicados.
- Guardar datos de forma confiable, consistente y en grandes cantidades.

Reglamento de Gestión de Riesgos Operativos

En noviembre del año 2016, se oficializa el Reglamento de Gestión de Riesgos Operativos, el cual busca orientar a los responsables de las dependencias y procesos, gerenciadores de riesgos en la adecuada identificación y gestión de sus riesgos.

Las principales especificaciones con que permite contar este documento son:

- El conjunto de las actividades a ser realizadas en las etapas de la gestión de riesgos.
- Los criterios de impacto (patrimonial y reputacional) y frecuencia.
- La tipología de y el grado de fortaleza de los controles.
- Una taxonomía actualizada de riesgos operativos.
- La estructura de la gestión de riesgos operativos.
- Roles y responsabilidades de los participantes.
- Aspectos generales de la gestión de riesgos relacionados a la Cultura de Riesgos y a la comunicación de los eventos.

Otro importante aspecto, contenido en este reglamento, es la planilla "Metodología de la Gestión de Riesgos Operativos", el cual sustituye a la planilla de "Autoevaluación de Riesgos, Impactos y Controles". Esta metodología fue desarrollada por los técnicos del Departamento de Riesgos mediante su experiencia, participación en diversos cursos y seminarios, así como la investigación en otras entidades similares con gestión de riesgos operativos más avanzadas.

Las principales ventajas con que cuenta la metodología más reciente respecto a la anterior son:

- La posibilidad de una mejor identificación de riesgos. En la metodología anterior no se podían describir riesgos, sino más bien era valorar los impactos por categorías de riesgos.
- Una taxonomía más actualizada y desarrollada tanto para las causas como para los eventos.
- Poder contar con un relacionamiento riesgo-causa-efecto.
- Realizar un listado y tipificación de los controles existentes para los riesgos identificados.
- Evaluar si los controles mitigan los impactos y la frecuencia.
- Calculo automático del riesgo residual a partir de haber completado el riesgo inherente y los controles.
- Generación automática, en hoja adicional de la planilla, por proceso institucional del mapa de calor de acuerdo al impacto y la frecuencia.
- Generación automática de mapa de calor a partir de varios procesos institucionales (por macroproceso).
- Generación automática, en hoja adicional, de hoja para plan de acción de riesgos a mitigar con datos para el análisis de viabilidad de las acciones, así como las fechas de implementación con sus respectivos responsables.

Avances cronológicos en la cantidad de procesos/áreas evaluadas en el inicio hasta la actualidad.

Desde la incorporación de la disciplina de gestión de riesgo operacional a las actividades de la institución, se han utilizado 2 herramientas para realizar la evaluación de riesgos operativos. Como se citó anteriormente, el primero fue en el año 2009 (Planilla "Autoevaluación de Riesgos, Impactos y Controles"), el segundo fue en el año 2016, el cual forma parte del documento "Reglamento de Gestión de Riesgos Operativos", y se trata de la Planilla "Metodología de la Gestión de Riesgos Operativos".

Las evaluaciones de riesgos, con ambas metodologías, fueron realizadas sobre los procesos institucionales. Inicialmente, hasta el año 2016, la distribución por tipos de procesos, en cuanto a cantidad, estaban compuestos de acuerdo al siguiente cuadro:

Tabla 12: Distribución por tipos de procesos hasta el año 2016.

TIPO DE PROCESOS	MACROPROCESO	PROCESO	SUBPROCESO
ESTRATÉGICOS	3	6	18
MISIONALES	13	36	131
APOYO	11	38	114

Posteriormente, los procesos fueron actualizados a través de una consultoría para relevamiento y rediseño de los tipos de procesos estratégicos y de apoyo, los cuales fueron finalizados a inicios del 2017. Con las herramientas brindadas por dicha consultoría, la institución, inicio el desafío de desarrollar a través de su área especializada en procesos en conjunto con las áreas, los procesos misionales, los cuales se encuentran en gran mayoría finalizados. Actualmente, la distribución por tipos de procesos, en cuanto a cantidad, está compuesto de acuerdo al siguiente cuadro:

Tabla 13: Distribución por tipos de procesos desde el año 2017.

TIPO DE PROCESOS	MACROPROCESO	PROCESO	SUBPROCESO
ESTRATÉGICOS	3	8	18
MISIONALES	7	30	
APOYO	11	34	98

En cuanto a la evaluación de riesgos operativos, realizadas con las metodologías citadas anteriormente tuvieron una distribución anual de acuerdo al siguiente cuadro:

Tabla 14: Distribución de cantidad de procesos evaluados de forma anual con las metodologías vigente y anterior.

Año	Cantidad evaluaciones		
	Macroprocesos	Procesos	Subprocesos
2011	0	0	0
2012	0	0	0
2013	0	0	2
2014	0	1	0
2015	0	2	1
2016	2	1	0
2017	6	0	0
2018	8	30	70

La tabla anterior nos permite observar un avance progresivo en cuanto a cantidad de procesos evaluados de forma anual. Existen varios factores que han determinado este avance de procesos que se van evaluando año tras año. A continuación, se listan las principales:

- Una mayor especialización del área encargada del asesoramiento en gestión de riesgos operativos.
- El desarrollo de herramientas más dinámicas para la evaluación.
- El crecimiento de la cultura de riesgos en la organización.
- El crecimiento en cuanto a una cultura de gestión por procesos.
- Un mayor por parte de las autoridades en cuanto tener identificados los riesgos a los que se encuentra expuesto la institución.

Evolución de la comunicación de eventos de riesgos operativos.

Como se había mencionado anteriormente, para comunicar eventos de riesgos operativos materializados, en setiembre del 2011, la institución, puso a disposición de las áreas la planilla "Registro de Evento de Pérdidas". Se solicitó, inicialmente, a las áreas que registren todos los eventos materializados de los que tenían conocimientos, incluso siendo estos de años anteriores. Por lo tanto, todos los eventos almacenados en la base de datos de riesgos operativos hasta el 2011 corresponden a eventos cuyos datos ya se encontraban almacenados en las áreas y que fueron incorporados con el fin de enriquecer la mencionada base.

Por lo expuesto anteriormente, los eventos que corresponden de los años 2012 a parte del 2015 (57 de los 93 del año 2015), corresponden a los eventos comunicados a través de la planilla “Registro de Evento de Pérdidas”. Es importante resaltar que la normativa de comunicación de eventos a través de la mencionada planilla solicitaba que los mismos sean acumulados en lotes y sean remitidos de forma bimestral y obligatoria, aun cuando en las áreas no hayan ocurridos eventos de riesgos materializados.

La comunicación de eventos, por parte de las áreas, a través del aplicativo "Sistema Registro de Eventos de Riesgos Operativos" inició en el año 2015, en total fueron comunicados 36 eventos a través de ese canal en ese año. De este modo, se reemplazó la forma de comunicación, el cual era a través de expedientes pasando

posteriormente a ser mediante un aplicativo informático interactivo. Este aplicativo, podía ser accedido a través de la red interna y el acceso al mismo fue instalado en las áreas de la institución, en cada área fue designado un registrador y dos verificadores. Los eventos ocurridos debían ser puestos a conocimientos de los registradores, quienes se encargarían de registrar en el aplicativo. Posteriormente, el registro debía ser validado por los verificadores. Representaba una forma más interactiva de comunicar los eventos y por lo tanto el reporte bimestral obligatorio fue suprimido.

A continuación, se expone un cuadro de resumen anual de los eventos comunicados con las herramientas destinadas para el efecto:

Tabla 15: Cantidad de eventos de riesgos operativos materializados comunicados de forma anual.

Eventos comunicados por año		
Año	**Total**	**Método de comunicación**
2001	5	Planilla “Registro de Evento de Pérdidas”
2002	1	
2003	1	
2006	1	
2007	7	
2008	12	
2009	25	
2010	14	
2011	31	
2012	91	
2013	215	
2014	166	
2015	57	
2015	36	Aplicativo "Sistema Registro de Eventos de Riesgos Operativos"
2016	57	
2017	29	
2018	49	
Total General	797	

La evolución de las herramientas que se han ido implementado.

En cuanto a las principales herramientas utilizadas para realizar la gestión de riesgos operativos, tanto la metodología de recolección de eventos de riesgos operativos como la metodología de evaluación de riesgos y controles han sido mejoradas debido a una mayor experiencia del área encargada del asesoramiento técnico en cuanto a la gestión de riesgos y una mayor cultura por parte de los empleados de la institución.

La planilla "Autoevaluación de Riesgos, Impactos y Controles" fue sustituida por la planilla "Metodología de la Gestión de Riesgos Operativos". La primera herramienta presentaba inconvenientes en cuanto a limitaciones para individualizar los riesgos; especificar la frecuencia de ocurrencia de los eventos; un alto grado de subjetividad en cuanto a la valoración de las categorías de riesgos; y dificultad para la construcción de los mapas de riesgos. La herramienta reemplazante, "Metodología de la Gestión de Riesgos Operativos", presentó mejoras sustanciales en todas las desventajas citadas de la herramienta anterior. Permitía identificar riesgos, causas y controles existentes asociados; la especificación de frecuencias para los riesgos de acuerdos a criterios predefinidos; una disminución (no desaparición) del grado de subjetividad; y la construcción de mapas obtenidos a través de la combinación de impacto y frecuencia.

En cuanto a la metodología utilizada para la evaluación de riesgos, la planilla "Registro de Evento de Pérdidas" fue sustituida por el aplicativo "Sistema Registro de Eventos de Riesgos Operativos". La primera herramienta contaba con una frecuencia fija y obligatoria para realizar la comunicación de los eventos por parte de las áreas, aun cuando no se hayan presentado eventos de riesgos materializados. La particularidad de ser obligatoria, ayudaba a que las áreas reporten sus eventos, aún cuando no hubiera tanto interés (en algunas áreas) de comunicar los eventos. En cuanto a la herramienta reemplazante, el aplicativo "Sistema Registro de Eventos de Riesgos Operativos", presentaba las ventajas de ser automatizada; poseer niveles de verificación; eliminación de impresiones para realizar las comunicaciones; y almacenar los datos en una base de datos. El mismo presentaba la debilidad de que ya no era de carácter obligatorio y por lo tanto dependía de la "Cultura de Riesgos" de las personas registradoras. Por lo anteriormente expuesto, se han llevado a cabo campañas dedicadas a la concientización de las áreas de la institución, a través de afiches, circulares, correos, y charlas de capacitación en las áreas.

Si bien es cierto que ambas herramientas corresponden a aspectos que son muy necesarias para una buena gestión de riesgos operativos y que un diseño adecuado, automatizado y amigable para los usuarios de ambas ayudará a las autoridades a realizar una gestión de riesgos operativos más eficiente, todo dependerá del grado de compromiso de los empleados de la institución y de su "Cultura de Riesgos".

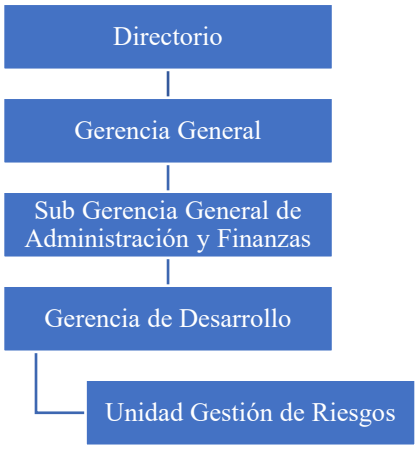
Evolución del área de riesgos operativos dentro de la estructura organizacional

Cuando las autoridades tomaron la decisión de implementar la Gestión de Riesgos Operativos en la institución, se la encargaron al área de Auditoría Interna. Esta estructura tuvo lugar desde el inicio, año 2007, al año 2011.

Figura 15: Dependencia en la estructura organizativa 2007-2011.

En agosto de 2011, tomando como base las sanas prácticas (entre ellas Basilea II), el Directorio de la institución determina que el área de gestión de riesgos debe ser independiente a la Auditoría Interna. Esta estructura permaneció vigente entre los años 2011 y 2015.

Figura 16: Dependencia en la estructura organizativa 2011-2015.

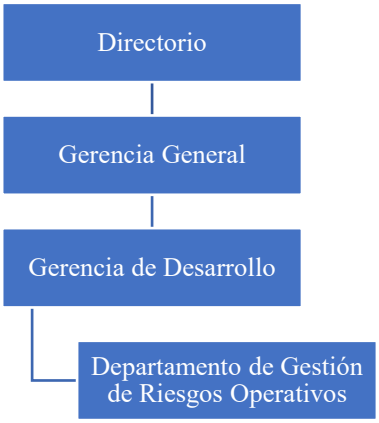


En marzo del 2015, las autoridades de la institución, con la predisposición de poder trabajar más directamente con las áreas estratégicas de Planificación Institucional, Organización y Procesos, y Gestión de Riesgos modifican la estructura pasando la Gerencia de Desarrollo a depender directamente del Directorio. Estructura vigente desde marzo de 2015 a setiembre de 2018.

Figura 17: Dependencia en la estructura organizativa 2015-2018.

Finalmente, las autoridades deciden delegar la gestión de riesgos, procesos y planificación a la Gerencia General con la idea de empoderar a esta para tomar decisiones a ser adoptadas de forma más dinámica para la estructura organizacional general.

Figura 18: Dependencia en la estructura organizativa 2018-Actualidad.



Diagnóstico sobre la permeabilidad de la Cultura de Gestión de Riegos en la Institución.

Con el propósito de poder medir la permeabilidad de la Cultura de Riesgos en la Institución, se ha realizado una encuesta a través de la plataforma Google Forms. La misma fue completada por 50 funcionarios[13] de diferentes áreas y distintos cargos dentro de la Institución entre las fechas 22/11/2018 al 27/11/2018. La encuesta consistió en 13 preguntas cuyas respuestas fueron realizadas a total criterio del encuestado sin asesoramiento técnico. Las preguntas estaban enfocadas en indagar sobre temas como Política de Gestión de Riesgos Operativos, Eventos de Riesgos Operativos, Sistema para comunicar Eventos, Identificación de Riesgos, conocimiento del área de Gestión de Riesgos.

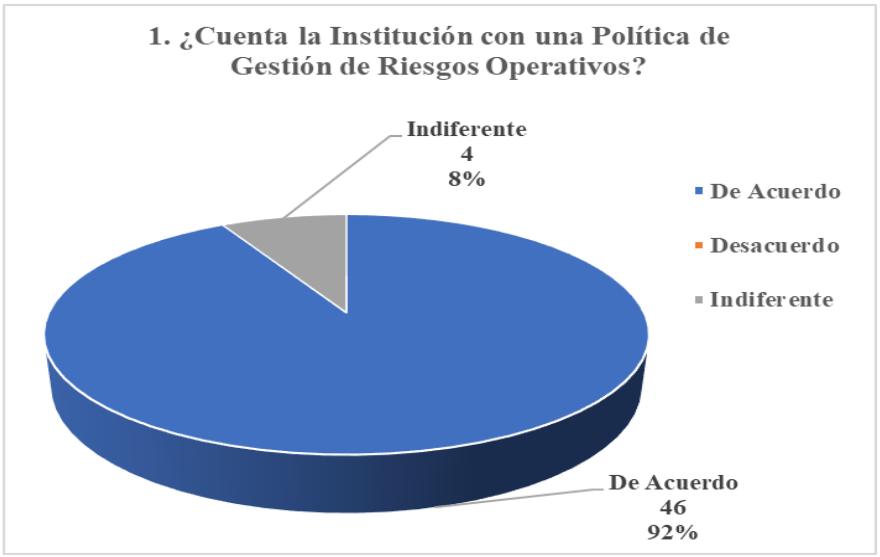
A continuación, se detalla un resumen de las respuestas recibidas por cada pregunta realizada:

Pregunta 1. ¿Cuenta la Institución con una Política de Gestión de Riesgos Operativos?

La Política de Gestión de Riesgos Operativos está vigente desde setiembre del año 2013. La Política debe ser conocida y observada por todos los integrantes de la institución (autoridades, gerentes, directores, jefes y funcionarios de los más bajos niveles).

De los 50 funcionarios encuestados, 46 (92%) han respondido afirmativamente en que la institución cuenta con el mencionado documento y 4 (8%) de forma indiferente. Esto nos da la pauta de que la mayor parte de los funcionarios está en conocimiento de que existe el mencionado documento, aún cuando no se conozca su contenido explicito.

Figura 19: Distribución de respuestas de la pregunta 1.



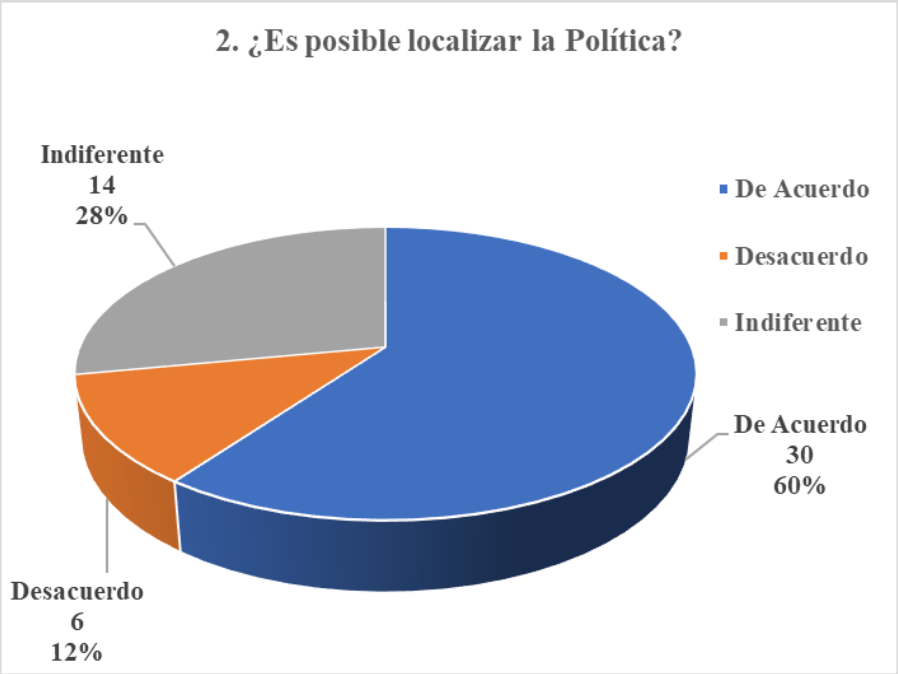
[13] La Institución cuenta con aproximadamente 900 funcionarios.

Pregunta 2. ¿Es posible localizar la Política?

La Institución ha realizado difusiones de forma periódica a través de charlas y correos sobre el contenido del documento referido y también la forma de localizarlo. El mencionado documento está siempre accesible en una sección correspondiente al Departamento de Riesgos dentro del portal interno institucional.

De los 50 funcionarios encuestados, 30 (60%) han respondido afirmativamente en que es posible localizar la Política, 14 (28%) de forma indiferente y 6 (12%) que no. Estos resultados demuestran que se vuelve pertinente buscar un método que genere un impacto mayor sobre como localizar el documento, debido a que solo un poco más de la mitad de los encuestados pudo afirmar que puede localizarlo.

Figura 20: Distribución de respuestas de la pregunta 2.

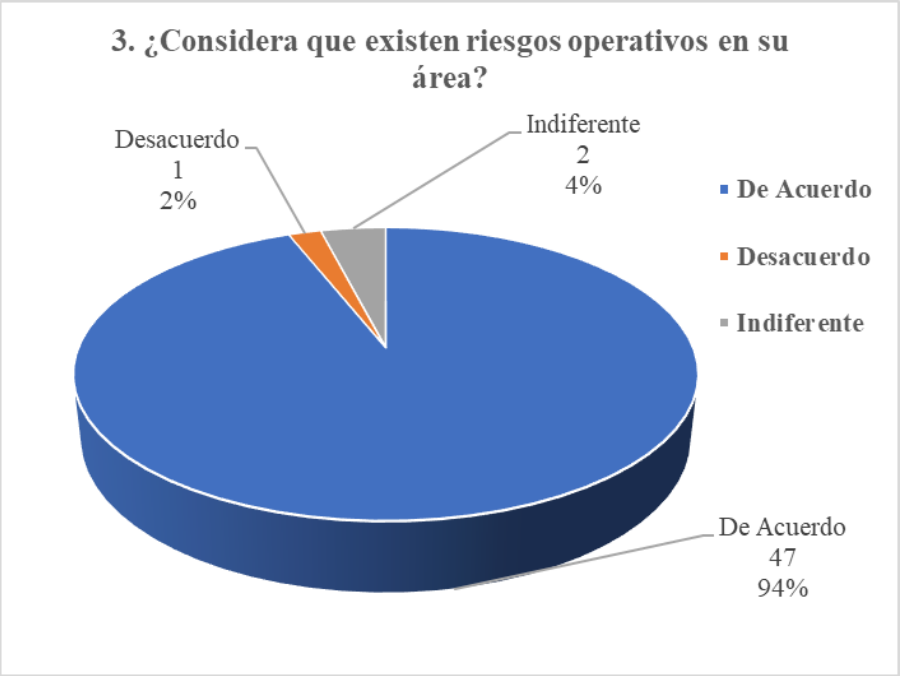


Pregunta 3. ¿Considera que existen riesgos operativos en su área?

Como habíamos mencionado anteriormente, el riesgo operativo ***es el riesgo de pérdidas resultantes de la inadecuación o fallas en los procesos internos, las personas o los sistemas o por eventos externos***. De esta definición, podemos inferir que, en todas las empresas, incluidas las bancarias, existen riesgos operativos ya sean altos, medios o bajos. Como habíamos mencionado anteriormente, la única forma de eliminar el riesgo completamente es eliminar la actividad que lo genera.

De los 50 funcionarios encuestados, 47 (94%) han respondido afirmativamente en que el área en la que se encuentran está expuesta a riesgos operativos, 2 (4%) de forma indiferente y 1 (2%) que no. Estos resultados nos permiten apreciar que la gran mayoría de los funcionarios es consciente de que las actividades que él o su área realiza están sujetos a la materialización de eventos que podrían ocasionar pérdidas a la institución.

Figura 21: Distribución de respuestas de la pregunta 3.

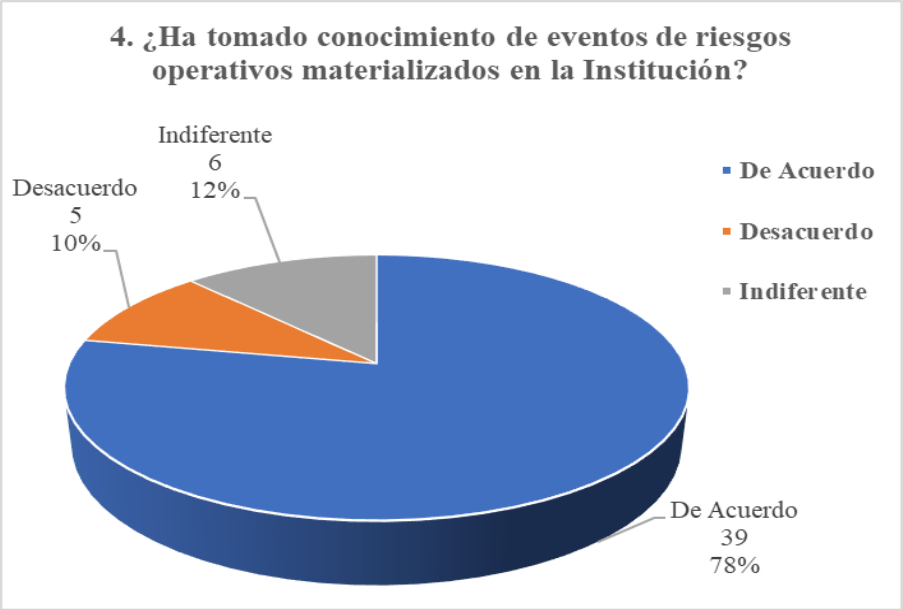


Pregunta 4. ¿Ha tomado conocimiento de eventos de riesgos operativos materializados en la Institución?

En la institución, se divulgado la vigencia de herramientas para la comunicación de eventos de riesgos operativos materializados, primeramente, en su oportunidad fue la planilla "Registro de Evento de Pérdidas" y luego el aplicativo "Sistema Registro de Eventos de Riesgos Operativos" (actualmente vigente). Así mismo, dentro de la Institución, han ocurrido eventos que han tenido repercusión en entidades supervisadas, en eventos organizados por la propia institución y en la prensa.

De los 50 funcionarios encuestados, 39 (78%) han respondido, 6 (12%) de forma indiferente y 5 (10%) que no. Estos resultados nos permiten apreciar que, aunque hay un número importante de funcionarios que tiene conocimientos de eventos de pérdidas ocurridos, también hay un porcentaje interesante que no se ha percatado de dichos eventos o no conciben de que se trata de eventos de riesgos operativos materializados.

Figura 22: Distribución de respuestas de la pregunta 4.

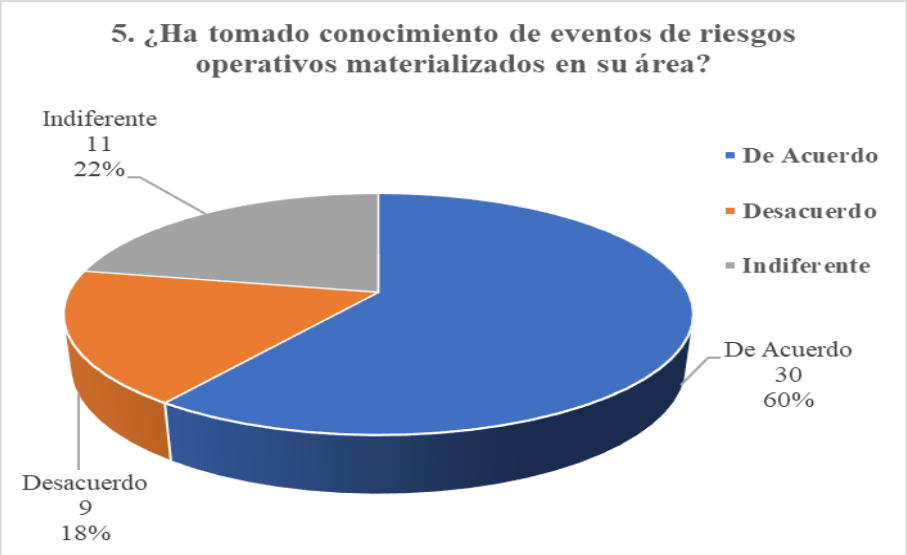


Pregunta 5. ¿Ha tomado conocimiento de eventos de riesgos operativos materializados en su área?

Esta pregunta corresponde a una parte del universo de la anterior, está diseñado de forma tal a que pueda distinguirse si han podido diferenciar la ocurrencia de eventos en la institución versus el área donde se desempeñan.

Los resultados obtenidos muestran que 30 (60%) de los encuestados manifiestan que han notado eventos de pérdidas, mientras que los restantes 20 (40%) están distribuidos entre encuestados con desconocimiento o negativa de ocurrencia de eventos.

Figura 23: Distribución de respuestas de la pregunta 5.

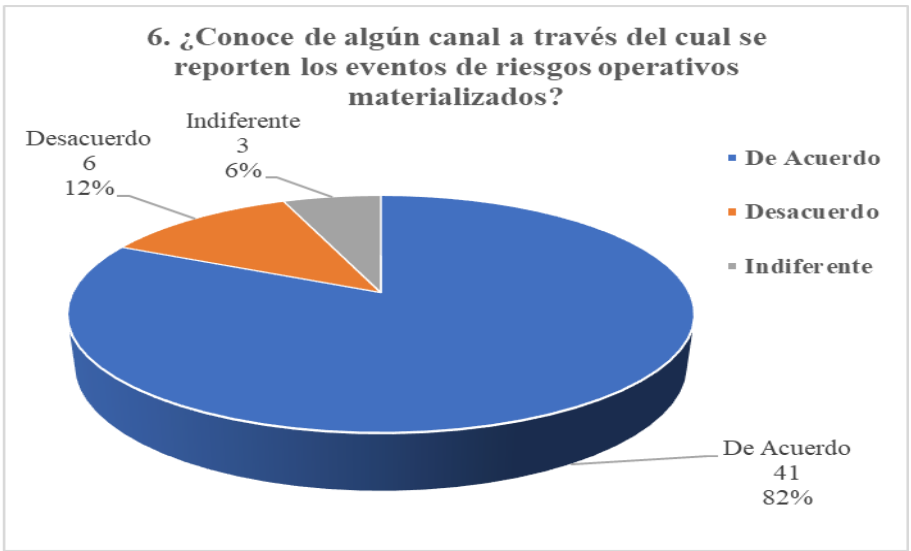


Pregunta 6. ¿Conoce de algún canal a través del cual se reporten los eventos de riesgos operativos materializados?

La pregunta busca determinar qué tan conocido es el actual aplicativo "Sistema Registro de Eventos de Riesgos Operativos".

Los resultados muestran que 41 (82%) encuestados han respondido afirmativamente, en tanto, 9 (18%) desconocen la mencionada herramienta.

Figura 24: Distribución de respuestas de la pregunta 6.

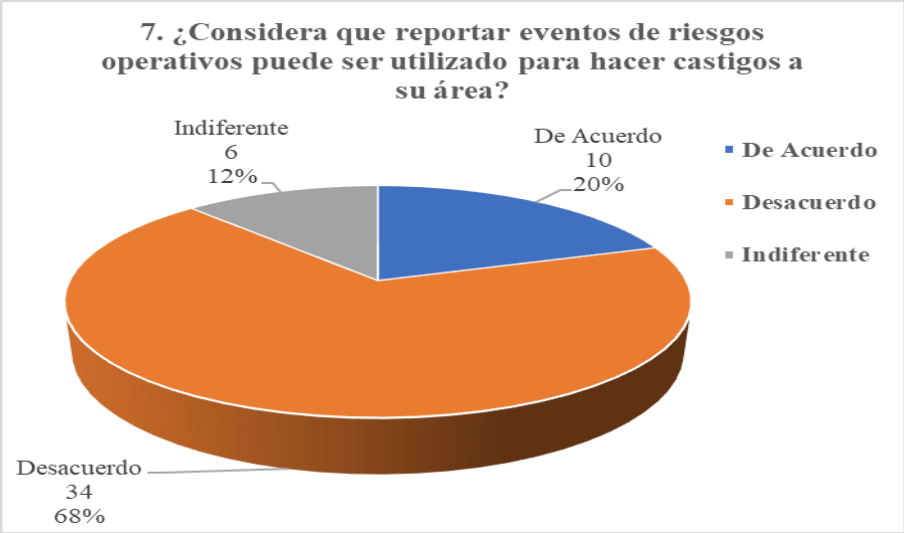


Pregunta 7. ¿Considera que reportar eventos de riesgos operativos puede ser utilizado para hacer castigos a su área?

En muchas ocasiones, la comunicación de eventos de riesgos operativos ha sido vista como una herramienta que podría ser utilizada a los efectos de buscar culpables a los eventos/errores acontecidos, lo cual es una apreciación errónea pues lo que se busca es mejorar la gestión con controles más eficientes.

En la encuesta, se pudo obtener que 34 (68%) considera que no es así, mientras que 6 (12%) no lo sabe y 10 (20%) considera que la herramienta podría ser utilizado para buscar culpables.

Figura 25: Distribución de respuestas de la pregunta 7.

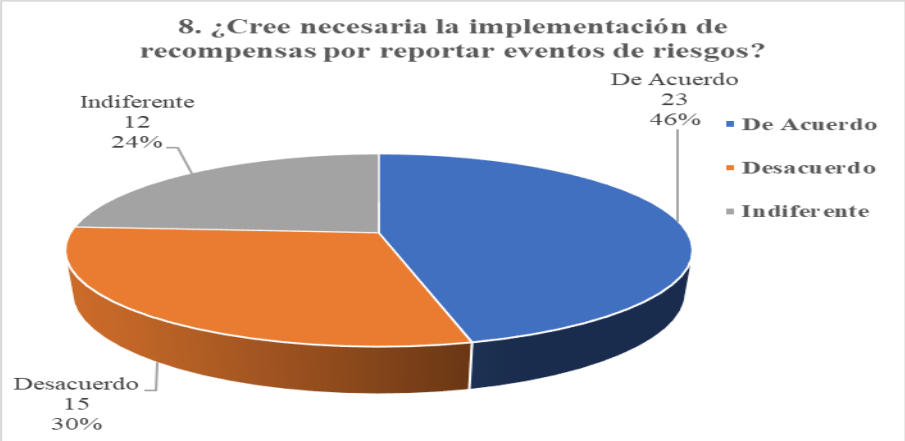


Pregunta 8. ¿Cree necesaria la implementación de recompensas por reportar eventos de riesgos?

Otra causa que, generalmente, suele ocasionar un bajo número de eventos comunicados es que dicha actividad es vista como una tarea extra que no agrega valor o no produce recompensa realizar. Esto muchas veces es entendible debido al volumen de trabajo que muchas veces suele haber en las áreas y otras veces por falta de conocimiento de las bondades de la gestión de riesgos.

Los resultados dieron que 23 (46%) de los encuestados cree que se necesitan recompensas para poder comunicar los eventos de forma eficiente y oportuna, 12 (24%) piensa que los resultados no variarán y 15 (30%) entiende que no es necesario.

Figura 26: Distribución de respuestas de la pregunta 8.

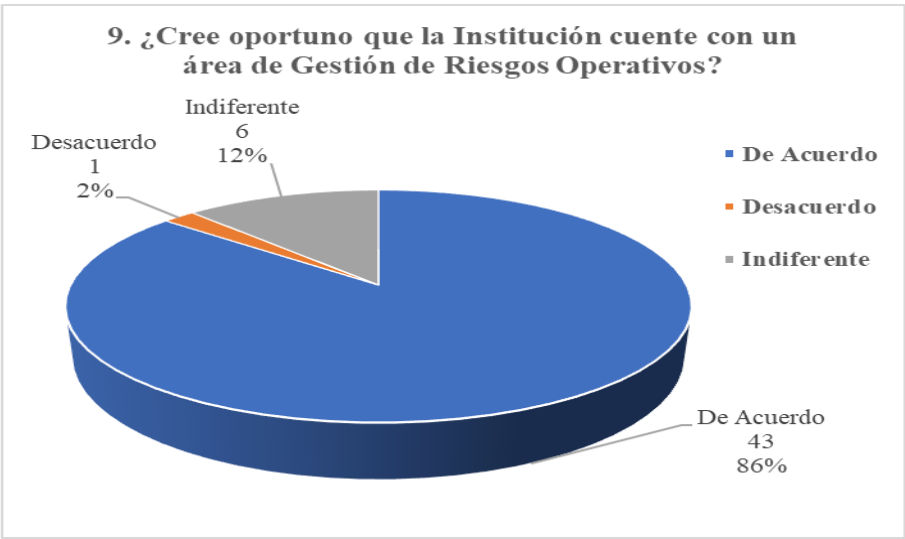


Pregunta 9. ¿Cree oportuno que la Institución cuente con un área de Gestión de Riesgos Operativos?

En muchas ocasiones, la creencia "No existen riesgos operativos" determina que los empleados piensen que no es necesario que la misma posea un área encargada de desarrollar herramientas y asesorar en cuanto al gestión de riesgos operativos.

De acuerdo a los resultados obtenidos, 43 (86%) de los encuestados cree que es necesario que haya un área de Gestión de Riesgos Operativos en la institución, 6 (12%) le es indiferente en que haya o no y 1 (2%) cree que no es necesario.

Figura 27: Distribución de respuestas de la pregunta 9.

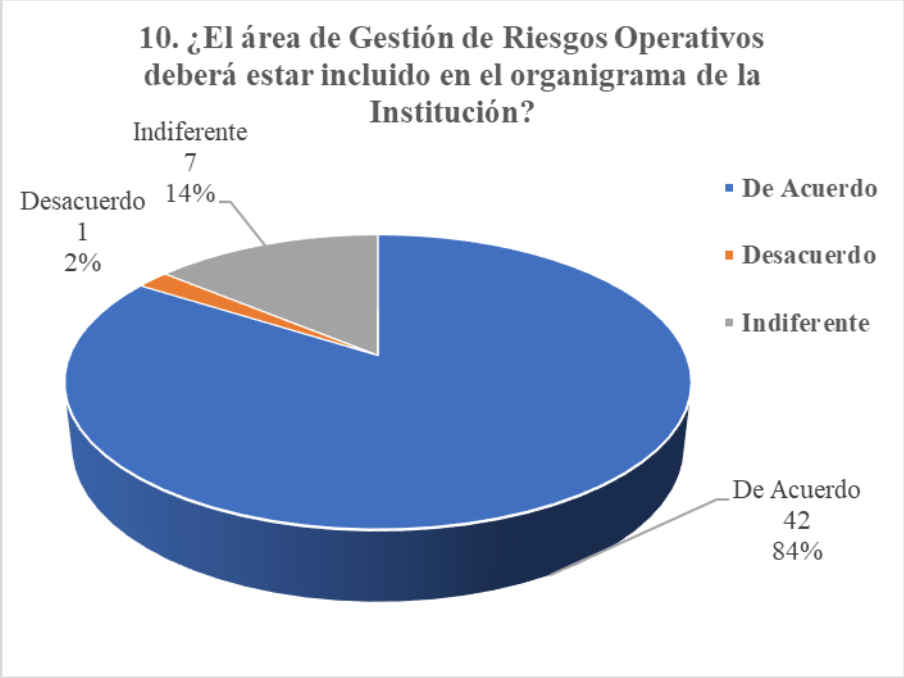


Pregunta 10. ¿El área de Gestión de Riesgos Operativos deberá estar incluido en el organigrama de la Institución?

Como habíamos visto, la Gestión de Riesgos, era emprendida, tradicionalmente, por el área de Auditoría Interna en la gran mayoría de las empresas. Lo mismo ocurrió en la institución en estudio. También muchas veces se da que ciertas actividades se tercerizan. Pero, los estándares recomiendan que el área de gestión de riesgos operativos sea un área dentro de la institución que asesore a las demás áreas del banco y que también sean objeto de Auditorías Internas y Externas.

Los resultados arrojaron que, 42 (84%) de los encuestados cree que es necesario que el área de Gestión de Riesgos Operativos sea un área más de la institución, 7 (14%) le es indiferente en que este o no en el organigrama y 1 (2%) cree que no es necesario.

Figura 28: Distribución de respuestas de la pregunta 10.

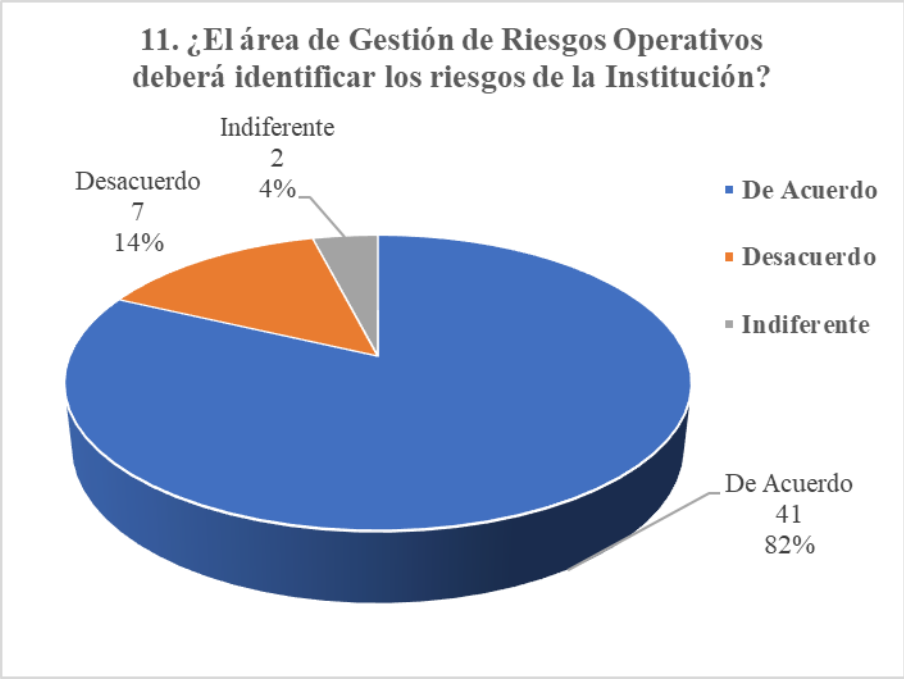


Pregunta 11. ¿El área de Gestión de Riesgos Operativos deberá identificar los riesgos de la Institución?

El área de gestión de riesgos operativos será la encargada de desarrollar políticas, reglamentos, herramientas, y generar una cultura de riesgos en la institución de forma tal a que las demás áreas puedan identificar y gestionar sus riesgos. Entiéndase que no deberá identificar riesgos, sino coadyuvar en dicha actividad a las áreas. Incluso las medidas mitigatorias deberán ser establecidas por las áreas.

Los resultados obtenidos son, 41 (82%) de los encuestados cree que el área de riesgos deberá identificar los riesgos, 2 (4%) piensa que no afecta quien identifique los riesgos y 7 (14%) piensa en que no.

Figura 29: Distribución de respuestas de la pregunta 11.

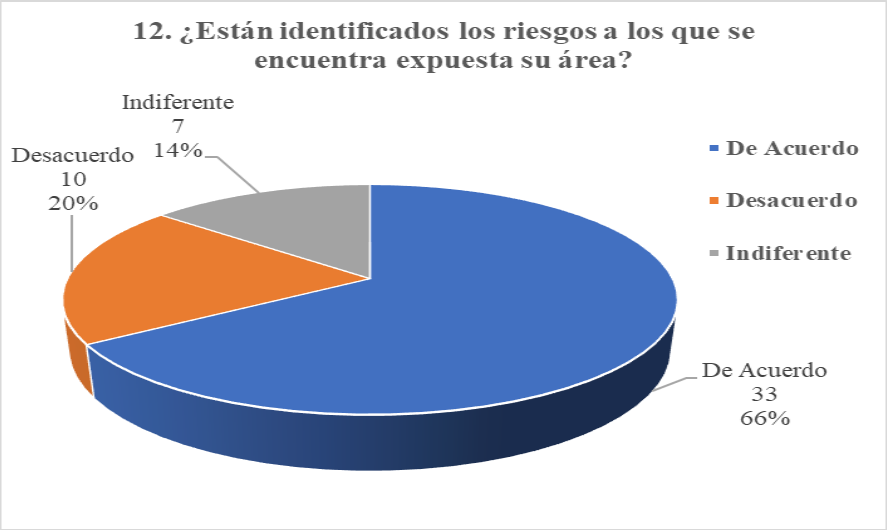


Pregunta 12. ¿Están identificados los riesgos a los que se encuentra expuesta su área?

Los riesgos operativos se identifican a través de la herramienta provista para el efecto por el área de riesgos. La mayor parte de los encuestados corresponden a áreas donde ya se realizó una evaluación e identificación de riesgos operativos. Por ello, se esperó que un importante número de encuestados responda afirmativamente a esta pregunta.

Los resultados obtenidos muestran que, 33 (66%) de los encuestados manifiestan que los riesgos a que se expone su área se encuentran identificados, 7 (14%) no lo sabe y 10 (20%) en que no lo están.

Figura 30: Distribución de respuestas de la pregunta 12.

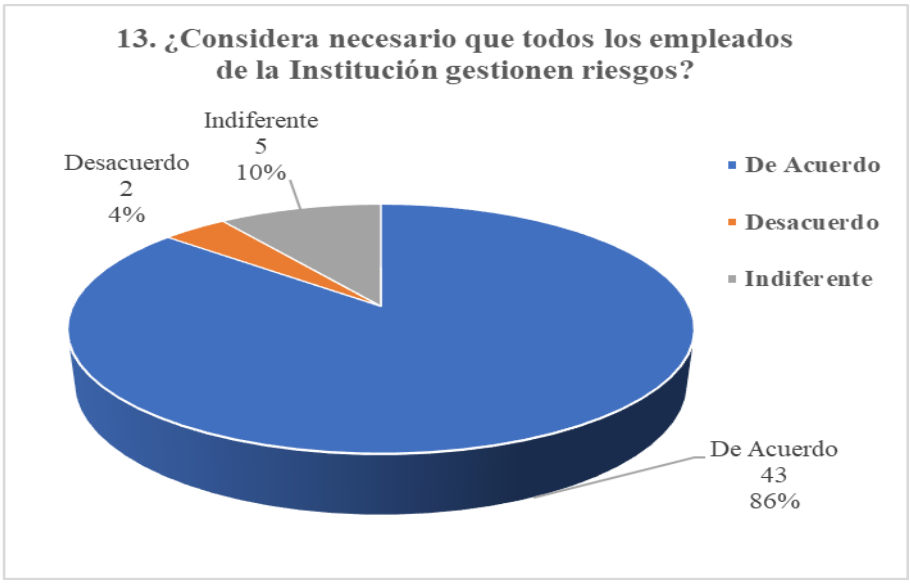


Pregunta 13. ¿Considera necesario que todos los empleados de la Institución gestionen riesgos?

La Política de Gestión de Riesgos Operativos establece que el alcance de la misma abarca a todos los funcionarios de la Institución independientemente de su rango. Todos los empleados deberán tener el compromiso de gestionar los riesgos que pudieren surgir en sus actividades y comunicar los que podrían afectar a otras.

De los 50 encuestados, 43 (86%) está de acuerdo con que todos los empleados deban gestionar riesgos, 5 (10%) cree que no afecta con que todos puedan o no gestionarlos y 2 (4%) piensan que no es necesario que todos gestionen.

Figura 31: Distribución de respuestas de la pregunta 13.



Conclusiones y recomendaciones

El presente trabajo nos permite ver que, si bien se ha avanzado bastante en la implementación del Sistema de Gestión de Riesgos Operativos, aún queda un largo camino por recorrer para lograr que el mismo sea sólido, óptimo y eficiente.

Aspectos tales como Reglamentos de Gestión Riesgos, Sistema de Registro de Eventos, Metodología de Evaluación de Riesgos, y Cultura de Riesgos aún deben ser perfeccionados.

En cuanto a la Política, la misma se encuentra bien estructurada y desarrollada, aunque se requiere de una mayor socialización sobre el contenido de la misma. Cabe recordar que la Política deberá ser observada por todos los integrantes de la institución.

El Sistema Registro de Eventos de Riesgos Operativos debe servir como el principal insumo para la Metodología de Gestión de Riesgos Operativos de forma tal a que se puedan generar datos de impacto y frecuencia de los eventos de riesgos operativos comunicados. De esta manera, se podrá construir mapas de riesgos que representen la situación real de los riesgos a los que se encuentra la Institución.

Es necesario la evolución del reglamento vigente, ya que enfoca a una Gestión de Riesgos Operativos Tradicional, en la cual se encuentra un alto grado de subjetividad cuando se realizan las evaluaciones y también genera un número alto de riesgos identificados que se vuelve muy difícil de manejar.

El enfoque tradicional, también muchas veces identifica riesgos cuya frecuencia e impacto son altos. Un riesgo cuyo impacto es alto, no puede tener una frecuencia alta, ya que esto si es realmente así, el negocio desaparecería muy pronto al estar sufriendo la materialización de riesgos de impactos altos de manera frecuente.

En otras ocasiones, este enfoque, lleva a identificar riesgos innecesarios que son por decirlo de alguna manera, el precio del funcionamiento del negocio. Por ejemplo, los riesgos de impacto bajo y frecuencia baja, al tener bajo impacto y producirse de manera muy fugaz, no representa un riesgo para la institución.

El enfoque de Gestión de Riesgos Moderno, elimina una gran parte de la subjetividad, debido a que el impacto y la frecuencia son calculados utilizando métodos estadísticos como simulación de Monte Carlo, distribución de frecuencias y severidad por tipos de eventos. Este enfoque también permitirá poder realizar un cálculo más preciso del capital necesario para gestionar los riesgos operacionales.

Pero, la implementación del enfoque moderno, requiere de una cultura de riesgos muy desarrollada en la Institución. Tal es así, de que los empleados puedan conocer las políticas, reglamentos y comunicar todos los eventos de riesgos operativos ocurridos a través del canal correspondiente.

El cimiento sobre el cual se deberá construir el Sistema requerido, es la comunicación de eventos. Deberán implementarse métodos que conviertan “el trabajo” (se la ve como una tarea más) de comunicar los eventos en “un hábito” que los personas realicen con confianza sin temor a recibir represalias. Quizás para lograr que las personas adquieran “el hábito”, sea necesaria la implementación de algún tipo de recompensas o incentivos, las

cuales por obvias razones no deberán ser monetarias ya que se tiene conocimiento de casos ocurridos, en otras instituciones, donde los riesgos eran generados para ser poseedor de las mencionadas recompensas. Los incentivos podrían ser, puntos para una evaluación de desempeño, diplomas de gestionador eficiente de riesgos, reconocimientos a la gestión, a la buena predisposición, a la identificación con el servicio público y un compromiso con la sociedad, entre otros.

Si bien todo lo mencionado requiere de proyectos ambiciosos con una planificación adecuada en tiempo y recursos, existe otro aspecto importante que debe ser observado con mucha atención, y el cual es la capacitación. Las personas del área de riesgos deberán estar suficientemente capacitados a fin de poder brindar la asistencia, asesoramiento y desarrollar las herramientas adecuadas para proveer a las áreas que gestionarán sus riesgos de forma adecuada. Así mismo, está área deberá contar con un importante apoyo tecnológico, debido a que en muchas ocasiones necesitará desarrollar sus propias herramientas automatizadas y también administrar el acceso y la confidencialidad.

Los próximos pasos, recomendados, a seguir son:

- Fomentar la utilización del Sistema para comunicar eventos de riesgos.
- La adaptación del reglamento de forma tal a disminuir la subjetividad y por lo tanto la cantidad enorme de riesgos que se identifican de esta manera en las evaluaciones periódicas que son desarrolladas sobre los procesos institucionales.
- También en el reglamento, definición de criterios más adecuados de forma tal a evitar que se puedan identificar riesgos de impacto y frecuencia ya sean ambas altas o ambas bajas.
- Buscar personas comprometidas de diversas áreas que puedan ser capacitadas para fomentar la cultura de riesgos en dichas áreas.
- Una vez implementado todo lo anterior, el desarrollo o la adquisición de una herramienta automatizada que pueda integrar el reporte de los eventos y la evaluación y que pueda ser utilizada de manera dinámica por las diversas áreas de la Institución.

BIBLIOGRAFÍA

- Banco Internacional de Pagos (2018). Retrieved from https://www.bis.org/publ/bcbs96esp.pdf
- FTSE 100. (2018). Retrieved from https://es.wikipedia.org/wiki/FTSE_100
- Problema del agente-principal. (2018). Retrieved from https://es.wikipedia.org/wiki/Problema_del_agente-principal
- Jiménez Rodríguez, E., & Martín Marín, J. (2005). El nuevo acuerdo de Basilea y la gestión del riesgo operacional. *UNIVERSIA BUSINESS REVIEW-ACTUALIDAD ECONÓMICA*, (TERCER TRIMESTRE 2005), 2-15.
- di Pietro, F., Irimia-Diéguez, A., & Oliver-Alfonso, M. (2013). Cuestiones abiertas en la modelización del riesgo operacional en los acuerdos de Basilea: el umbral de pérdidas y la distribución de severidad. *UNIVERSIA BUSINESS REVIEW*, (TERCER TRIMESTRE 2012), 78-92.
- LLAGUNO MUSONS, J. (2005). Gestión del riesgo operativo en las entidades de crédito: un camino sin retorno. *Cuadernos De Gestión*, *Vol. 5*(N.º 1), 53-77.
- Society of Actuaries. (2009). *A New Approach for Managing Operational Risk* (pp. 7-43). Towers Perrin & OpRisk Advisory.
- Roisenzvit, A. (2012). Nueva Normativa de Requerimiento de Capital por Riesgo Operacional (pp. 2-6). Buenos Aires.
- Bessis, J. (2009). *Risk management in banking* (2nd ed., pp. 26-114). New York [u.a]: Wiley.
- Asociación Española de Normalización y Certificación. (2011). *Gestión del riesgo - Técnicas de apreciación del riesgo* (pp. 10-24). AENOR.
- Organización Internacional de Normalización. (2015). *Sistemas de gestión de la calidad - Requisitos* (pp. 10-16). Ginebra: Secretaría Central de ISO.
- Asociación Española de Normalización y Certificación. (2012). *Sistema de Gestión de la Continuidad del Negocio (SGCN) - Especificaciones* (pp. 16-27). AENOR.
- Instituto Nacional de Normalización - INN. (2013). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos (pp. 2-12). INN.
- Bravo, D. (2018). Nick Leeson, el trader que hundió el Banco Barings. Retrieved from https://www.rankia.com/blog/bolsa-desde-cero/485936-nick-leeson-trader-que-hundio-banco-barings
- País, E. (2018). El gurú del mercado mundial del cobre deja un 'agujero' de 235.000 millones en Sumitomo. Retrieved from https://elpais.com/diario/1996/06/15/economia/834789625_850215.html
- (2018). Retrieved from http://www.bcr.com.ar/Publicaciones/serie%20de%20lecturas/2007_12.pdf
- País, E. (2018). Un 'broker' del mayor banco de Irlanda desaparece tras causar pérdidas gigantescas. Retrieved from https://elpais.com/diario/2002/02/07/economia/1013036410_850215.html
- País, E. (2018). El fundador de WorldCom, condenado a 25 años por fraude contable. Retrieved from https://elpais.com/diario/2005/07/14/economia/1121292003_850215.html

- Se cumplen 10 años del incendio del Windsor y muchas incógnitas siguen sin despejarse. (2018). Retrieved from https://www.20minutos.es/noticia/2375172/0/incendio-windsor/rascacielos-madrid/aniversario/
- (2018). Retrieved from https://www.bis.org/bcbs/qis/ldce2002.pdf
- MAGERIT versión 3. 0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. (2012). Madrid: Ministerio de Administraciones Públicas.

ANEXOS

Encuesta sobre la Cultura de la Gestión de Riesgos Operativos a nivel Institucional

Estimado Señor (a):

El presente cuestionario es a los efectos de diagnosticar sobre la permeabilidad de la cultura de Gestión de Riesgos Operativos en la Institución. Se solicita muy cordialmente responder a las siguientes preguntas.

1. ¿Cuenta la Institución con una Política de Gestión de Riesgos Operativos?

Desacuerdo	Indiferente	De Acuerdo

2. ¿Es posible localizar la Política?

Desacuerdo	Indiferente	De Acuerdo

3. ¿Considera que existen riesgos operativos en su área?

Desacuerdo	Indiferente	De Acuerdo

4. ¿Ha tomado conocimiento de eventos de riesgos operativos materializados en la Institución?

Desacuerdo	Indiferente	De Acuerdo

5. ¿Ha tomado conocimiento de eventos de riesgos operativos materializados en su área?

Desacuerdo	Indiferente	De Acuerdo

6. ¿Conoce de algún canal a través del cual se reporten los eventos de riesgos operativos materializados?

Desacuerdo	Indiferente	De Acuerdo

7. ¿Considera que reportar eventos de riesgos operativos puede ser utilizado para hacer castigos a su área?

Desacuerdo	Indiferente	De Acuerdo

8. ¿Cree necesaria la implementación de recompensas por reportar eventos de riesgos?

Desacuerdo	Indiferente	De Acuerdo

9. ¿Cree oportuno que la Institución cuente con un área de Gestión de Riesgos Operativos?

Desacuerdo	Indiferente	De Acuerdo

10. ¿El área de Gestión de Riesgos Operativos deberá estar incluido en el organigrama de la Institución?

Desacuerdo	Indiferente	De Acuerdo

11. ¿El área de Gestión de Riesgos Operativos deberá identificar los riesgos de las de la Institución?

Desacuerdo	Indiferente	De Acuerdo

12. ¿Están identificados los riesgos a los que se encuentra expuesta su área?

Desacuerdo	Indiferente	De Acuerdo

13. ¿Considera necesario que todos los empleados de la Institución gestionen riesgos?

Desacuerdo	Indiferente	De Acuerdo

Resumen de los resultados de la Encuesta sobre la Cultura de la Gestión de Riesgos Operativos a nivel Institucional

	De Acuerdo	Desacuerdo	Indiferente
1. ¿Cuenta la Institución con una Política de Gestión de Riesgos Operativos?	46	0	4
2. ¿Es posible localizar la Política?	30	6	14
3. ¿Considera que existen riesgos operativos en su área?	47	1	2
4. ¿Ha tomado conocimiento de eventos de riesgos operativos materializados en la Institución?	39	5	6
5. ¿Ha tomado conocimiento de eventos de riesgos operativos materializados en su área?	30	9	11
6. ¿Conoce de algún canal a través del cual se reporten los eventos de riesgos operativos materializados?	41	6	3
7. ¿Considera que reportar eventos de riesgos operativos puede ser utilizado para hacer castigos a su área?	10	34	6
8. ¿Cree necesaria la implementación de recompensas por reportar eventos de riesgos?	23	15	12
9. ¿Cree oportuno que la Institución cuente con un área de Gestión de Riesgos Operativos?	43	1	6
10. ¿El área de Gestión de Riesgos Operativos deberá estar incluido en el organigrama de la Institución?	42	1	7
11. ¿El área de Gestión de Riesgos Operativos deberá identificar los riesgos de la Institución?	41	7	2
12. ¿Están identificados los riesgos a los que se encuentra expuesta su área?	33	10	7
13. ¿Considera necesario que todos los empleados de la Institución gestionen riesgos?	43	2	5