UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

UNA METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS OPERACIONALES EN INSTITUCIONES BANCARIAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

A C T U A R I A

P R E S E N T A :

JACQUELINE ERIKA SIGRIST MARTOS

TUTOR: M. EN C. AGUSTÍN ROMÁN AGUILAR

MÉXICO, D. F. 2014

Hoja de Datos del Jurado

1. Datos del alumno
Sigrist
Martos
Jacqueline Erika
56 65 40 50
Universidad Nacional Autónoma de México
Facultad de Ciencias
Actuaría
085525430

2. Datos del tutor
M en C
Agustín
Román
Aguilar

3. Datos del sinodal 1
Dra
Nora
Gavira
Durón

4. Datos del sinodal 2
Act
Julio Irving
Aguilar
Galindo

5. Datos del sinodal 3
Mat
Margarita Elvira
Chávez
Cano

6. Datos del sinodal 4
M en C
Raúl
Álvarez del Castillo
Penna

7. Datos del trabajo escrito
Una metodología para la administración de riesgos operacionales en instituciones bancarias
83 p
2014

A Carlos, Jackie y Tania, por todo su cariño y creer en mí… hoy y siempre.

A mi madre, por su apoyo y amor incondicional.

A mi familia, por todo su amor.

A mi amada Regina, por el nuevo sentido que le dio a mi vida…

A Agustín Román, por su paciencia y apoyo durante tanto tiempo.

A Cristi y Mary, mi agradecimiento.

Í N D I C E

I N T R O D U C C I Ó N

Durante los últimos años, la administración y la mitigación del riesgo ha adquirido especial importancia en el ámbito financiero internacional. Las entidades financieras han venido realizando grandes esfuerzos por avanzar en materia de gestión del riesgo, enfocados principalmente en la medición e identificación de los riesgos más comunes, el de mercado y el de crédito.

La desregulación y globalización de los servicios financieros, junto con la creciente sofisticación de la tecnología financiera, están haciendo cada vez más diversas y complejas las actividades de los bancos y, por lo tanto, sus perfiles de riesgo.

A medida que los efectos de la globalización impactan la industria de los servicios financieros y ésta se adentra en nuevas líneas de negocios y regiones geográficas, las probabilidades de que ocurran fallas operativas generadas por errores en los procedimientos, en la administración, en los sistemas computacionales y en la calidad de un producto o servicio, aumentan significativamente.

Los riesgos relacionados con la continuidad del negocio, la diversificación y los recursos humanos, entre otros, saltaron repentinamente en magnitud. Éstos son riesgos operativos u operacionales y el manejo de ellos requiere un sistema para identificar, evaluar, controlar, supervisar y mitigar las exposiciones.

El riesgo operativo u operacional está presente en todas las actividades de una institución financiera y en cualquier empresa u organismo, desde el primer instante de su vida. Su nombre representa un conjunto de problemas e intereses, además de que interviene en la estructura interna de dichas entidades.

El proceso de desarrollo, implementación y supervisión de la gestión del riesgo operacional en las instituciones bancarias aún se encuentra en maduración, pero se ha dado el paso más difícil y decisivo, el crecimiento y la institucionalización de dicho riesgo como una categoría de atención reguladora y directiva.

El documento que rige la administración de riesgos operacionales emitido por la Comisión Nacional Bancaria y de Valores (CNBV) lo nombra riesgo operativo y contiene los principios que establece el Segundo Acuerdo de Basilea o Basilea II.

El Diccionario de la Lengua Española de la Real Academia Española define:

Riesgo m. Contingencia o proximidad de un daño/ Es cada una de las contingencias que puede ser objeto de un contrato de seguro.

Operacional (adj.). Relativo o perteneciente a las operaciones matemáticas, militares o comerciales.

Operativo, va (adj). Dícese de lo que obra y hace su efecto.

En el presente trabajo, se utiliza el término de *riesgo operacional* para hacer referencia a toda contingencia, real o potencial, propia de la realización de operaciones y por ser el término que mejor lo describe.

I. Antecedentes

En diciembre de 1974, se creó el Comité de Supervisión Bancaria de Basilea[1] para incrementar la colaboración entre los supervisores bancarios de los países integrantes del G-10. Su propósito es establecer un foro apropiado para la discusión de los problemas propios de esta actividad, así como coordinar la actuación de las autoridades encargadas de la supervisión y establecer estándares relacionados con la solvencia de la banca.

Las causas que pueden generar inestabilidad financiera deben ser tratadas de forma oportuna, por lo que en la actualidad, las autoridades supervisoras de las entidades bancarias están en alerta permanente. Por esta razón, en julio de 1988 el Comité de Supervisión Bancaria de Basilea (en adelante el Comité), publicó el documento "International Convergence of Capital Measurement and Capital Standards" (Basilea I) y establecía parámetros dirigidos a garantizar la solvencia adecuada de los bancos, con base en el riesgo crediticio.

El propósito del Comité era evitar que los bancos incurriesen en excesivos riesgos crediticios, requiriéndoles mantener un nivel mínimo de capital en función del riesgo asumido, de tal manera que, en caso de insolvencia de sus deudores, absorbieran las posibles pérdidas. El capital mínimo de los bancos debería ser el 8% de sus activos totales ponderados en función de su riesgo crediticio, lo cual no se debe ver como un mecanismo para evitar las quiebras o las crisis bancarias, sino para mitigar las mismas.

Originalmente, los requerimientos de capital sólo contemplaban el riesgo de crédito, pero en 1996, el Comité incluyó el riesgo de mercado para regular la exposición del sistema financiero en sus incursiones en el mercado público de valores, para nivelar la igualdad competitiva de los bancos y estar acorde con una economía sin barreras, más globalizadas y con instituciones con mayor presencia internacional.

A través de los años, la actividad bancaria se ha complicado. Las prácticas de gestión de riesgos, los enfoques de supervisión y los mercados financieros en general, sufrieron transformaciones significativas restándole eficacia al Acuerdo de Capital de Basilea I, evitando que se reflejara la verdadera naturaleza de los riesgos asumidos por algunas entidades, teniendo como consecuencia una asignación de recursos deficiente.

Por lo anterior, se considera que el Acuerdo de 1988 subvalúa los riesgos y sobrevalora la suficiencia de capital de las entidades financieras. El Comité, atento a esta situación, en junio de 1999 publicó un documento consultivo: "A New Capital Adequacy Framework"

[1] El Comité de Supervisión Bancaria de Basilea (el Comité de Basilea), es una organización formada por los supervisores (países del G-10) de Alemania, Canadá, Bélgica, España, Estados Unidos, Francia, Italia, Japón, Luxemburgo, Países Bajos, Reino Unido, Suecia y Suiza, siendo su principal misión el establecimiento de estándares de supervisión relacionados con la solvencia de las entidades financieras. Aunque sus recomendaciones no son vinculantes desde el punto de vista jurídico, tradicionalmente han sido asumidas con carácter general en el ámbito internacional.

para reemplazar al primero, presentando dos propuestas más desarrolladas en 2001 y 2003, dando como resultado la versión definitiva del Nuevo Acuerdo de Capital o Basilea II (junio de 2004). Posteriormente, se publicaron modificaciones que se integraron en el documento "International Convergence of Capital Measurement and Capital Standards: a Revised Framework" (2006).

I.1. Pérdidas históricas por riesgos operacionales

El riesgo operacional se genera por deficiencias directas o indirectas en los sistemas de información o en los controles internos de la institución, con un resultado adverso para la misma. Generalmente, está asociado a errores humanos, fallas en los sistemas e inadecuados sistemas de control, pero incluso puede ser producto de un factor externo, como un incendio, ataque terrorista o fraude. En el Nuevo Acuerdo también se incluye el riesgo legal.

Se empieza a considerar como un riesgo creciente, debido a factores como la globalización, el crecimiento de los medios electrónicos, las fusiones y adquisiciones a gran escala, una mayor automatización tecnológica, una mayor oferta en proveedores de servicios, el incremento del outsourcing, la complejidad y cobertura de productos, el crecimiento de los volúmenes de negocios y las regulaciones y normativas.

En la década de los 90, un gran número de entidades financieras y no financieras implementaron procesos de administración del riesgo, principalmente para la gestión de los riesgos de mercado y de crédito. En los últimos años, se han enfocado al manejo del riesgo operacional, el cual antes era considerado como un riesgo no cuantificable por muchas instituciones, pero que, a raíz de la importancia que le ha dado el Comité de Basilea y considerando algunos eventos de pérdida significativos asociados a este tipo de riesgo, se ha hecho evidente que puede representar grandes peligros para la seguridad y solidez del sistema bancario internacional.

A partir de este momento, se comienza a hablar del riesgo operacional como una categoría separada de riesgo, y que al igual que los riesgos de crédito y de mercado, se debe medir y controlar. Parece increíble que el riesgo que siempre ha existido, que mayores desastres y pérdidas ha ocasionado, es el que ha tardado en recibir un trato conceptual, una definición clara y una gestión activa y global.

En la historia reciente, algunos de los casos más sonados en donde riesgos operacionales han dado lugar a quebrantos multimillonarios en todo el mundo, destacan el de Barings Bank (1995), en donde el trader de derivados Nick Leeson de la sucursal de Singapur, acumuló pérdidas no reportadas durante dos años, ocasionando un quebranto por 1,300 millones de dólares, llevando como consecuencia a la quiebra de la institución.

En el Daiwa Bank (1995), el trader de bonos Toshihide Iguchi acumuló pérdidas durante once años en la sucursal de Estados Unidos, ocasionando pérdidas por 1,100 millones de dólares; en el All First (Allied Irish Bank – 2002), John Rusnak ocultó pérdidas por 691 millones de dólares durante tres años, en la negociación de divisas.

Algunos casos más recientes son, el que sufrió el banco francés Société Générale detectado a finales de enero de 2008, en el cual el operador de 30 años a cargo de

contratos a futuro, Jérôme Kerviel, comerció con futuros en los mercados europeos excediendo ampliamente sus competencias y encubriendo sus acciones mediante complejos negocios ficticios, ocasionándole a la institución pérdidas por 4,900 millones de euros. Otro caso similar se presentó en 2011 en el banco suizo UBS, donde el trader Kweku Adoboli de 31 años, perdió $2,000 millones de dólares al realizar operaciones no autorizadas.

I.2. Definición de riesgo operativo u operacional

Antes de construir el marco conceptual, primero es necesario aclarar y definir el concepto de riesgo operacional. Cada institución en el mundo puede tener su propia definición, lo cierto es que todas se apegan a lo establecido por el Comité de Basilea, el cual define al riesgo operativo u operacional como *el riesgo de pérdidas derivadas de fallas en los sistemas, en la actuación del personal, por eventos externos o por procesos internos no adecuados*.

En México, la Comisión Nacional Bancaria y de Valores (CNBV) es el órgano que se encarga de dictar las obligaciones de las instituciones financieras en lo que se refiere a la administración de riesgos basado en los requerimientos establecidos por el Comité de Basilea. Para regular el cumplimiento de dichas obligaciones, la CNBV emitió las *Disposiciones de carácter general aplicables a las instituciones de crédito (Las Disposiciones)* en donde solicita a las instituciones financieras administrar (identificar, medir, vigilar, limitar, controlar, informar y revelar) los riesgos a los que se encuentran expuestas.

I.2.1. Clasificación de riesgos de acuerdo a la CNBV

En *Las Disposiciones* se establece que los riesgos a los que se encuentran expuestas las instituciones financieras se clasifican en riesgos cuantificables y riesgos no cuantificables.

1) Riesgos Cuantificables: Son aquéllos para los cuales es posible conformar bases estadísticas que permitan medir sus pérdidas potenciales, y dentro de éstos se encuentran:

   a) Riesgos Discrecionales: Son los riesgos resultantes de la toma de una posición de riesgo, tales como el riesgo de crédito o crediticio, el riesgo de liquidez y el riesgo de mercado.

      - Riesgo de Crédito o Crediticio.- Es la pérdida potencial por la falta de pago de un acreditado o contraparte en las operaciones que efectúan las instituciones, incluyendo las garantías reales o personales que les otorguen, así como cualquier otro mecanismo de mitigación utilizado por las instituciones.

      - Riesgo de Liquidez.- Es la pérdida potencial por la imposibilidad o dificultad de renovar pasivos o de contratar otros en condiciones normales para la institución, por la venta anticipada o forzosa de activos a descuentos inusuales para hacer frente a sus obligaciones, o bien, por el hecho de que una posición no pueda ser oportunamente enajenada, adquirida o cubierta mediante el establecimiento de una posición contraria equivalente.

- Riesgo de Mercado.- Es la pérdida potencial por cambios en los factores de riesgo que inciden sobre la valuación o sobre los resultados esperados de las operaciones activas, pasivas o causantes de pasivo contingente, tales como tasas de interés, tipos de cambio e índices de precios, entre otros.

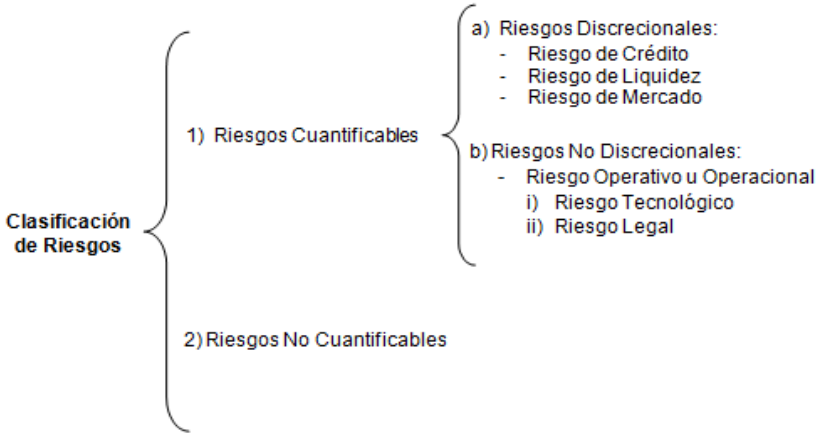
b) Riesgos No Discrecionales: Son los riesgos resultantes de la operación del negocio, pero que no son producto de la toma de una posición de riesgo, tales como el riesgo operacional, el cual comprende al riesgo tecnológico y al riesgo legal.

- Riesgo operativo u operacional.- Es la pérdida potencial por fallas o deficiencias en los controles internos, por errores en el procesamiento y almacenamiento de las operaciones o en la transmisión de información, así como por resoluciones administrativas y judiciales adversas, fraudes o robos, y comprende, entre otros, al riesgo tecnológico y al riesgo legal.

  i) Riesgo Tecnológico: Es la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios con los clientes de la institución.

  ii) Riesgo Legal: Es la pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las instituciones llevan a cabo.

2) Riesgos No Cuantificables: Son aquéllos derivados de eventos imprevistos para los cuales no se puede conformar una base estadística que permita medir las pérdidas potenciales. Aunque en la literatura la taxonomía de estos riesgos no es homogénea, dentro de los riesgos no cuantificables a los que puede verse expuesta una institución se consideran el reputacional, el estratégico, el de negocio, el regulatorio y el político.



Para contrastar las definiciones anteriores, a continuación se citan algunas definiciones particulares de instituciones de crédito:

BBVA define riesgo operativo como *"aquél no tipificable como riesgo de crédito, de mercado o de seguro"*. Credit Suisse lo define como el *"riesgo de impacto adverso al negocio como consecuencia de conducirlo de una forma inadecuada y puede ser resultante de factores externos. El riesgo operativo puede manifestarse tangiblemente como interrupciones en la operación, fallas de control, errores, conductas inadecuadas o eventos externos".*

BNP Paribas define el riesgo operativo como el *"riesgo de pérdida resultante de fallas o procesos inadecuados o de eventos externos"*. Esta definición es diferente a la de incidente de riesgo operacional, ya que este es *un suceso real, resultante de procesos internos inadecuados o de fallas en ellos o de eventos externos que han, podrían o habrían podido conducir a una pérdida, una ganancia o un costo de oportunidad*.

El Nuevo Acuerdo de Basilea o Basilea II establece en su definición una taxonomía de riesgos operacionales integrada por cuatro categorías básicas (no establece subcategorías), que son: procesos internos, personal, sistemas y factores externos.

La Comisión Nacional Bancaria y de Valores complementa su definición con una clasificación más detallada de los principales eventos de pérdida por riesgo operacional, los cuales están relacionados con:

- Fraude interno: Errores intencionados en la información sobre posiciones, robos por parte de empleados, utilización de información confidencial en beneficio de la cuenta del empleado, etc.
- Fraude externo: Atraco, falsificación, circulación de cheques en descubierto, daños por intrusión en los sistemas informáticos, etc.
- Relaciones laborales y seguridad en el puesto de trabajo: Solicitud de indemnizaciones por parte de empleados, infracción de las normas laborales de seguridad e higiene, organización de actividades laborales, acusaciones de discriminación, responsabilidades generales, etc.
- Prácticas con clientes, productos y negocios: Abusos de confianza, abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas del banco, blanqueo de capitales, venta de productos no autorizados, etc.
- Daños a activos materiales: Terrorismo, vandalismo, terremotos, incendios, inundaciones, etc.
- Incidencias en el negocio y fallas en los sistemas: Fallas del hardware o del software, problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etc.
- Ejecución, entrega y gestión de procesos: Errores en la introducción de datos, fallas en la administración del colateral, documentación jurídica incompleta, concesión de

acceso no autorizado a las cuentas de los clientes, prácticas inadecuadas de contrapartes distintas de clientes, litigios con distribuidores, etc.

El interés de las instituciones en la identificación de los eventos de riesgo operacional es evitar los fraudes, mantener la integridad de los controles internos, reducir los errores en las operaciones, etc. Lo anterior, se debe a que cada vez más instituciones se convencen de que los programas de gestión integral del riesgo operacional les proporcionan seguridad y solidez.

I.3. Nuevo Acuerdo de Capital o Basilea II

Su objetivo principal es mejorar la seguridad y solvencia del sistema financiero. Representa una norma de adecuación de capital más sensible al riesgo de las operaciones bancarias y estimula a las entidades en la mejora de sus capacidades de gestión y control de riesgos. Además, introduce unos requerimientos de capital propios por riesgo operacional.

El Acuerdo de Basilea II se basa en dos plataformas:

a) El ámbito de aplicación, que determina en qué entidades se debe cumplir el coeficiente de solvencia; y

b) Los denominados tres pilares:

- Pilar 1: Requerimientos mínimos de capital
- Pilar 2: Proceso de supervisión, y
- Pilar 3: La disciplina de mercado.

El Pilar 1 establece la medición del cargo de capital por riesgo operacional, donde permite que los reguladores opten por cualquiera de los métodos de medición para calcular el capital de los bancos en función de sus riesgos. Este pilar se basa en las *Buenas prácticas y principios* emitidos por el Comité de Basilea como condición previa para la aplicación de los métodos de medición del capital por riesgo operacional, los cuales son: el Método del Indicador Básico, el Método Estándar y el Método Avanzado; debido a su importancia, se explicarán en detalle más adelante.

El Pilar 2 enfatiza la independencia del supervisor y su papel en el seguimiento de las operaciones bancarias, su intervención en el sector y los requerimientos de capital de las instituciones de crédito. Además, no solo tiene como objetivo que las entidades posean un capital adecuado para cubrir todos los riesgos de su negocio, sino que impulsa a los bancos a que desarrollen y utilicen mejores técnicas de gestión de riesgos para su seguimiento y control. El rol del supervisor es el de evaluar si las entidades cuantifican sus necesidades de capital en función de sus riesgos, interviniendo cuando sea necesario.

Por último, el Pilar 3 se refiere al requerimiento de revelación de información a los mercados. Su propósito es complementar los requerimientos de capital mínimo y el proceso de revisión del supervisor, estableciendo las mejores prácticas aplicables respecto a la divulgación de información.

La adopción de estos tres pilares logrará un mayor nivel de solidez y estabilidad del sistema financiero, por lo cual se enfatiza la conveniencia de ponerlos en práctica.

El riesgo operacional no es un riesgo nuevo, ya que es inherente a cualquier negocio y no es exclusivo de la actividad financiera. Debido a la desregulación y globalización de los servicios financieros, junto con la creciente sofisticación de la tecnología financiera, las actividades de los bancos son cada vez más diversas y complejas y, por lo tanto, sus perfiles de riesgo. El desarrollo de las prácticas bancarias sugiere que además de los riesgos de crédito, mercado, de tipo de interés, entre otros, para efectos de supervisión se pueden considerar otros riesgos como el operacional.

El Comité reconoce que en la práctica, el enfoque exacto elegido por cada entidad para la administración del riesgo operacional depende de una variedad de factores, incluyendo su tamaño, sofisticación, y la naturaleza y complejidad de sus actividades. Sin embargo, además de esas diferencias, existen varios elementos que resultan clave para conseguir un esquema efectivo de administración del riesgo operacional para bancos de cualquier tamaño y alcance. Esos elementos son:

- *Estrategias* claramente definidas y su seguimiento por parte del consejo de administración y de la alta dirección;
- una sólida *cultura* de *gestión* del riesgo operacional y de *control* interno (incluyendo entre otras cosas, líneas claras de responsabilidad y segregación de funciones) y;
- herramientas eficaces para la transmisión interna de *información* y *planes de contingencia.*

I.4. Basilea II: "Sanas prácticas para la administración y supervisión del riesgo operacional"

Cuando el Comité de Supervisión Bancaria de Basilea habla de *gestión del riesgo operacional*, se refiere a la "identificación, evaluación, seguimiento y control/cobertura" de este riesgo. En febrero de 2003, el Comité publicó el documento *"Sanas prácticas para la administración y supervisión del riesgo operacional"* en donde se establecen una serie de principios para su gestión y supervisión eficaz, de modo que los bancos y autoridades supervisoras puedan utilizarlos al evaluar políticas destinadas a gestionar este tipo de riesgo. Dichos *Principios* están agrupados en cuatro áreas:

- *Desarrollo de un marco adecuado para la gestión del riesgo*

Principio 1: El consejo de administración deberá conocer cuáles son los principales aspectos de los riesgos operacionales del banco, en tanto que categoría de riesgo diferenciada y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo. Este marco deberá ofrecer una definición de riesgo operacional válida para toda la empresa y establecer los principios para definir, evaluar, monitorear y controlar o mitigar este tipo de riesgo.

Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operacional en el banco esté sujeto a un proceso de auditoría eficaz e integral

por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operacional.

Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operacional aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades con respecto a la administración del riesgo operacional. 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 operacional 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 operacional inherente.

Principio 5: Los bancos deberán vigilar periódicamente los perfiles de riesgo operacional y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operacional.

Principio 6: Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operacionales más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operacional según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por riesgo y a su perfil de riesgo.

Principio 7: Los bancos deberán contar con planes de contingencia y de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

- *El papel de los supervisores*

Principio 8: Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operacionales más relevantes, como parte de su aproximación general a la gestión de riesgos.

Principio 9: Los supervisores deberán realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos con los que cuentan los bancos para gestionar sus riesgos operacionales. Además, deberán cerciorarse de que se han puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en un banco.

- *El papel de la divulgación de información*

Principio 10: Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estrategias de gestión del riesgo operacional.

I.5. Tipos de estructura para gestionar los riesgos operacionales

Las instituciones pueden instrumentar dos esquemas básicos de estructura para la gestión de sus riesgos operacionales:

- Estructura Centralizada: La administración de riesgos operacionales está a cargo de una determinada área que puede ser:
  - La Unidad de Administración Integral de Riesgos;
  - un Comité o Subcomité de Administración de Riesgos Operacionales; o,
  - un área de auditoría interna, independiente del área u órgano interno de control de la institución.

  Una ventaja que tiene este tipo de estructura, es que el área encargada de la administración de los riesgos operacionales es la encargada de recopilar y concentrar toda la información de los eventos de pérdida para conformar la base de datos que servirá para calcular los requerimientos de capital por riesgo operacional.

  Una desventaja importante es que, al no contar con personal de apoyo designado en cada área de negocios y por no conocer con detalle cada uno de los procesos sustantivos de la institución, se pueden pasar por alto riesgos operacionales relevantes que pueden causar grandes pérdidas.

- Estructura Descentralizada: La administración de riesgos operacionales está a cargo de una persona o sub-área dentro de cada área de negocios, por ejemplo, un coordinador o monitor de riesgos operacionales.

  Sus ventajas son:

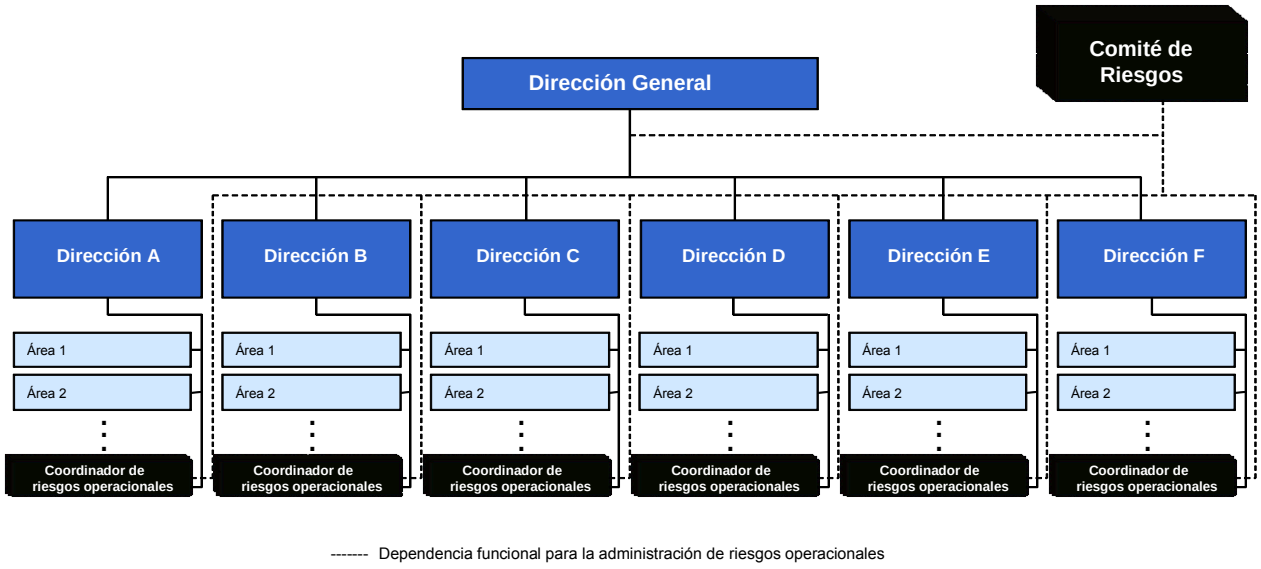
  - La Alta Dirección se debe involucrar totalmente en la administración de los riesgos operacionales de la institución.
  - Los dueños del negocio serán los responsables de la gestión del riesgo operacional en sus áreas, pudiendo existir coordinadores y monitores del riesgo operacional que les apoyen en esta tarea, lo que es benéfico para la institución porque son los que mejor conocen los procesos y las posibles debilidades de los sistemas que utilizan.
  - La Unidad de Riesgos se encarga de recopilar y concentrar toda la información de los eventos de pérdida para conformar la base de datos que servirá para calcular los requerimientos de capital por riesgo operacional.
  - Existe un área de la institución encargada de desarrollar la infraestructura para la gestión de los riesgos operacionales.

Desventaja:

- El temor de los responsables de los procesos a informar posibles eventos de pérdida porque significa aceptar sus errores.

En instituciones bancarias, es recomendable optar por una estructura descentralizada en donde el Consejo Directivo de la institución debe supervisar a través del Comité de Riesgos (o la Unidad de Administración de Riesgos), la implantación de la función de administración de riesgos operacionales, apoyándose en uno o más monitores o coordinadores de riesgos operacionales dentro de cada unidad de negocios o de apoyo.

El siguiente esquema muestra un ejemplo de estructura descentralizada para la gestión de riesgos operacionales en una institución bancaria:



Responsabilidades:

La Unidad de Administración de Riesgos es la responsable de desarrollar la infraestructura para la gestión de los riesgos operacionales, como son:

- Las Políticas para la administración de los riesgos operacionales,
- la adquisición o desarrollo de la tecnología necesaria,
- la elaboración de los informes que deberá presentar periódicamente al Consejo Directivo y al Comité de Riesgos.

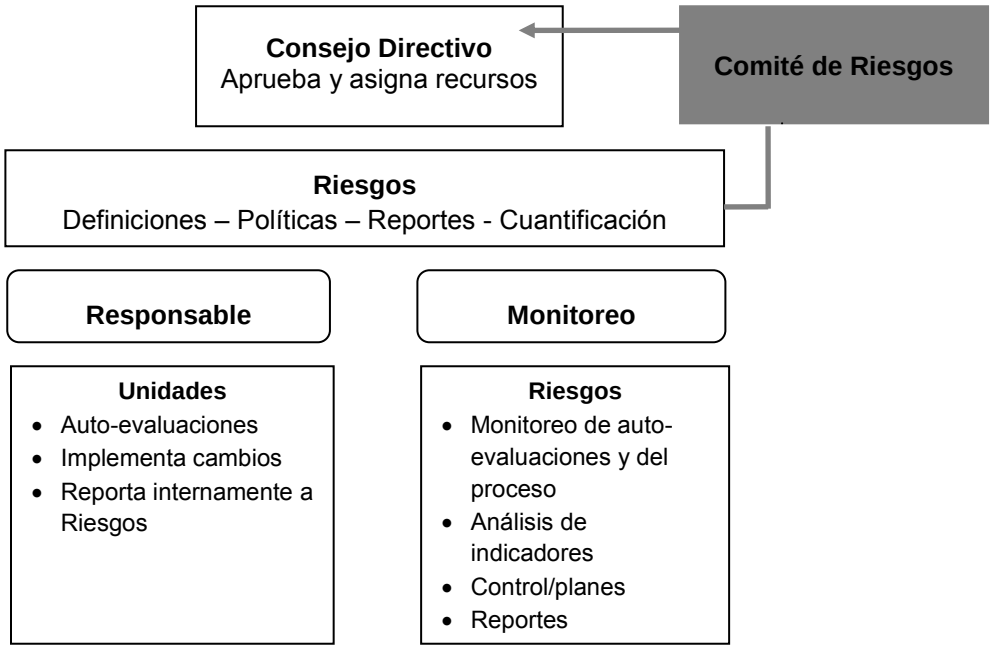
La Unidad o Dirección de Administración de Riesgos, debe designar a un encargado o responsable de la administración de los riesgos operacionales que tendrá entre sus funciones:

- Implementar políticas y procedimientos para llevar a cabo la administración de los riesgos operacionales,

- proveer información a la Unidad de Administración de Riesgos,
- supervisar las funciones que delegue en los monitores o coordinadores de riesgos operacionales que serán designados en cada una de las áreas de negocios de la institución.

Por otro lado, es necesario que todas las áreas de la institución se involucren y tengan muy claras y definidas sus responsabilidades dentro del proceso:

- El área encargada de la gestión de los riesgos operacionales debe definir las políticas, la selección y manejo de las herramientas más adecuadas, el diseño de tableros de información, así como sugerir planes de acción y realizar actividades de seguimiento de los riesgos identificados;
- Las unidades de negocio son las responsables últimas de los riesgos operacionales.



Responsabilidades de las diferentes áreas involucradas en la gestión del riesgo operacional

I.6. Principales objetivos de la gestión del riesgo operacional

Los principales objetivos de la gestión del riesgo operacional son:

- Mejorar la eficiencia operacional de la institución.
- Evitar pérdidas inesperadas.
- Distribuir el capital eficientemente a las líneas de negocio.
- Medir los resultados utilizando beneficios de capital ajustados al riesgo.
- Determinar el cálculo del capital económico.
- Cumplimiento de la legislación.

Lo anterior, sin perder de vista la protección del capital y la creación de valor. Para lograrlo se deben implementar medidas de mitigación de los riesgos operacionales relevantes de la institución, para así lograr un equilibrio entre el nivel de riesgo asumido y el costo del control.

Por otro lado, la gestión del riesgo operacional en las instituciones, contempla una gran variedad de tareas a realizar:

- Establecimiento de normas internas y políticas de riesgo operacional.
- Control de los procesos de autoevaluación en cada unidad de negocio.
- Descripción y modelización de todos los procesos internos. Análisis de los mismos para detectar sus puntos débiles.
- Desarrollo de la tecnología para riesgo operacional (incluidas las bases de datos pertinentes).
- Desarrollo de los Key Risk Indicators (KRI's).
- Definición de los planes de contingencia para las interrupciones importantes del negocio.
- Mantenimiento de la base de datos de riesgo operacional.
- Desarrollo de métricas para las exposiciones a riesgo operacional.
- Desarrollo de métricas para la eficiencia de los controles.
- Modelación de las pérdidas a partir de la severidad y la frecuencia.
- Modelación de las pérdidas potenciales a partir de modelos estadísticos.
- Cálculo del capital económico/regulatorio por riesgo operacional.

II. Herramientas cualitativas para la gestión de riesgos operacionales

En el pasado, las instituciones utilizaban únicamente controles internos y la función de auditoría para gestionar sus riesgos operacionales. Actualmente, las instituciones se inclinan por los programas de administración del riesgo operacional ya que les proporcionan seguridad y solidez, por lo que el avance en el trato a dicho riesgo es similar al de los riesgos de crédito y de mercado.

El análisis del riesgo operacional no sólo se trata de mediciones estadísticas de distintas distribuciones de pérdidas (análisis con datos históricos), sino del estudio de escenarios posibles. Por otro lado, la gestión del riesgo operacional debe incluir el juicio del experto, ya que este organiza las actividades para la mejora de acuerdo a su importancia y considerando las diversas fuentes y situaciones en las que se encuentra este riesgo.

Algunas técnicas para la gestión del riesgo operacional más difundidas son: la autoevaluación, los indicadores clave de riesgo (KRIs), los procesos de asignación del riesgo, las tarjetas de puntaje (scorecards) y el análisis de escenarios, pero su aplicación depende en gran medida de las características de cada entidad. Sin embargo, son el principal complemento en la creación y uso de la base de datos interna, así como de aquellos datos provenientes de fuentes externas.

II.1. Técnicas cualitativas para la gestión del riesgo operacional

Las técnicas cualitativas de gestión del riesgo operacional contribuyen, entre otras cosas, a:

- Tener una visión “forward looking”.- Las decisiones empresariales pueden afectar el perfil de riesgo operacional de la institución de diversas maneras (por ejemplo, a través de cambios en los procedimientos de control, sistemas, recursos humanos, entre otros), ninguna de las cuales puede ser capturada total y directamente a través de un modelo de medición. Las metodologías que se basan en fundamentos estadísticos contendrían un sesgo, dado que la información histórica reflejará un riesgo y un ambiente de control que no necesariamente existe en el presente. Es por ello que el uso de algunas de las técnicas cualitativas (autoevaluación, KRIs, etc.) brindan la posibilidad de anticiparse a eventos aún en el caso que no hayan sido observados en el pasado.
- Mitigar el riesgo operacional.- Mediante la implementación de sistemas de control y seguimiento de procesos y productos.
- Incrementar la transparencia.- Hacer más evidentes los riesgos existentes.
- Asignar la responsabilidad de los riesgos identificados a determinadas personas o niveles.

En el documento “Sanas prácticas para la administración y supervisión del riesgo operacional” publicado por el Comité de Basilea, se establece que la identificación del riesgo operacional es fundamental para el posterior desarrollo de un sistema viable de control y seguimiento del mismo. Asimismo, señala que además de la recolección de

datos históricos de pérdidas operativas (datos internos de las entidades), del mismo modo deben identificar y evaluar sus riesgos operacionales a través del uso de herramientas tales como:

- ✓ Autoevaluación o evaluación del riesgo operacional, incluyendo el uso de "scorecards" que proveen un medio para trasladar las evaluaciones cualitativas obtenidas de las unidades de negocio, a una métrica cuantitativa;
- ✓ indicadores de riesgo o KRI's;
- ✓ asignación o "mapeo" de riesgos (risk mapping).

Por otra parte, el Comité de Basilea (Basilea II) resalta en el documento "Nuevo Marco de Capitales" que las técnicas cualitativas para gestionar el riesgo operacional permiten identificar los factores básicos del entorno de negocio y del control interno que pueden modificar el perfil de riesgo operacional de las instituciones financieras. El utilizar dichos factores permite que las evaluaciones del riesgo que lleven a cabo las instituciones se orienten más hacia el futuro; reflejen de manera directa la calidad de los entornos operativos y de control de la institución; contribuyan a alinear las evaluaciones de capital con los objetivos de la gestión de riesgos y reconozcan de una manera más inmediata tanto la mejora como el deterioro de los perfiles de riesgo operacional.

Los factores básicos del entorno de negocio y del control interno se conocen en la industria financiera como *"Business Environment & Internal Control Factors"* (o BIECFs), definidos como los indicadores del perfil de riesgo operacional de una entidad financiera y reflejan una evaluación presente y "forward looking" de los factores de riesgo de negocios subyacentes y del ambiente de controles internos. Las herramientas utilizadas en este análisis son las auto-evaluaciones de riesgo y control ("Requirement Risk and Control Self Assessments" o RCSA), el uso de Scorecards, KRIs, "Key Performance Indicator" (o KPIs), y la asignación o mapeo de procesos.

II.1.1. Autoevaluación

La autoevaluación de riesgos se refiere al proceso de identificación y evaluación de los riesgos existentes en la entidad, sumado a una evaluación de los controles establecidos para su administración y mitigación. Este proceso puede aplicarse a todos los riesgos (crédito, mercado, liquidez, operacional, etc.). Es un componente crítico del marco de gestión del riesgo operacional, ya que con base en dicho proceso la entidad financiera puede comprobar la vulnerabilidad de sus operaciones y actividades ante el riesgo operacional. En general, este proceso debe adecuarse al tamaño e importancia del riesgo para la entidad, ya que, por ejemplo, un riesgo específico puede ser crítico para una organización pequeña, pero de muy bajo impacto para una entidad más grande o de diferente complejidad.

El proceso de autoevaluación es interno e incorpora información provista por la alta gerencia así como por el personal de línea de la entidad financiera. Dicha información se refiere a procesos, actividades, funciones y proyectos, tanto a nivel de unidades de negocio como de toda la organización. La información se puede mantener actualizada a través de "workshops (o talleres)", reuniones y/o cuestionarios realizados con

determinada frecuencia. Su efectividad radica en el establecimiento de un lenguaje común y una categorización del riesgo que permita analizar y consolidar los resultados de la autoevaluación.

Para facilitar la implementación de esta técnica, se debe establecer una función específica encargada de coordinar el proceso de autoevaluación y de proveer de entrenamiento apropiado para la identificación de los riesgos y los controles correspondientes.

La autoevaluación del riesgo operacional generalmente se compone de las siguientes etapas: identificación, evaluación, control y seguimiento, las que se describirán más adelante.

Los principales beneficios de la autoevaluación de riesgos son:

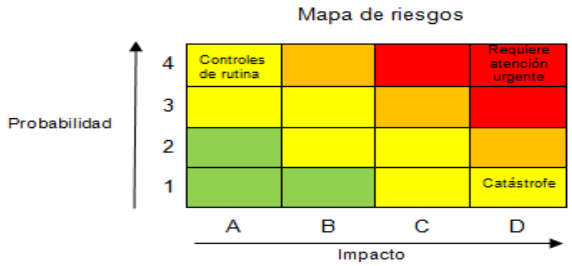
- Permite entender los riesgos inherentes en los procesos del negocio.
- Evalúa la efectividad de los controles internos.
- Revela áreas prioritarias de trabajo.
- Acuerda planes de acción para tratar riesgos que excedan el nivel de riesgo tolerable (por ejemplo, a través del tratamiento de debilidades identificadas en los controles internos).
- Permite adjudicar la propiedad de los riesgos y controles al personal mejor preparado para administrarlos.

II.1.2. Asignación de riesgos o mapeo de riesgos (risk mapping)

El mapeo de riesgos o “risk mapping” es el proceso a través del cual se agrupan por tipo de riesgo las diferentes unidades de negocio, funciones organizativas o procesos. Ello puede dejar al descubierto ámbitos que presenten deficiencias así como ayudar a determinar las prioridades para su gestión. Se puede realizar en forma indistinta a un nivel alto o bajo con el objetivo de identificar “qué puede fallar” en un proceso determinado y sus resultados pueden ser representados visualmente a través de un diagrama de flujo de proceso o de un mapa de riesgos.

Existen varias maneras de realizar una asignación de riesgos, siendo una técnica habitual su representación a través de una figura bidimensional cuyas dimensiones son la probabilidad (o frecuencia) y el impacto (o severidad de la pérdida). Este mapa permite desagregar los riesgos de acuerdo a estas dos dimensiones, pero no da indicaciones sobre las medidas a tomar para modificar el perfil existente de riesgos.

La siguiente figura es un ejemplo de un mapa de riesgos en donde los colores representan la tolerancia al riesgo de la entidad y el resultado es una herramienta gráfica muy simple que permite resaltar aquellos riesgos que requerirían ser rápidamente mitigados.



Hay otras metodologías alternativas para la realización de mapas de riesgos: la asignación de riesgos a áreas, la asignación de riesgos a procesos y la asignación simultánea de riesgos a áreas, procesos y productos. En el presente trabajo, estas no se analizarán, ya que la más sencilla y representativa es la descrita anteriormente.

II.1.3. Indicadores clave de riesgo (KRI o Key Risk Indicator)

El documento "Buenas prácticas para la gestión y supervisión del riesgo operacional" (febrero de 2003), del Comité de Supervisión Bancaria de Basilea, define los indicadores clave de riesgo o KRI's como "*estadísticas o parámetros, a menudo financieros, que pueden revelar qué riesgos asume cada banco*. *Estos indicadores suelen ser revisados periódicamente (mensual o trimestralmente) para alertar a los bancos sobre cambios que puedan ser reveladores de problemas con el riesgo. Se suelen utilizar parámetros como el número de operaciones fallidas, las tasas de rotación de asalariados y la frecuencia y/o gravedad de los errores u omisiones".*

Los KRI pueden ser de carácter cualitativo o cuantitativo, aunque estos últimos suelen ser más objetivos a efectos de ser incorporados a las técnicas de estimación del riesgo operacional. Se pueden expresar en porcentajes, cantidades o montos de dinero, pero principalmente deben tener un vínculo con la causa de origen que genera los eventos de pérdida por este tipo de riesgo. Los KRI pueden ser, según su naturaleza, de carácter anticipado, histórico, actual, o bien una combinación de los tres.

Algunas de las cualidades deseables de los KRI son:

- que permitan establecer niveles de riesgo actuales, a través de medidas precisas del estado de un riesgo identificado y la efectividad para su control;
- sean útiles para el control del riesgo operacional, permitiendo acciones preventivas o que minimicen pérdidas materiales al posibilitar una acción temprana;
- posibiliten la detección de tendencias y cambios en el nivel de riesgo, y;
- ofrezcan señales de alerta temprana al hacer resaltar los cambios en el entorno, eficiencia de los controles y exposición a riesgos potenciales antes que se materialicen.

Los KRI pueden coadyuvar en la toma de decisiones mediante el establecimiento de umbrales mínimos y rangos de tolerancia para los diversos riesgos, y deben ser definidos por las máximas autoridades de la entidad. Dichos umbrales pueden ajustarse

posteriormente para alinearse con la dinámica del entorno de negocios. Usualmente se establecen rangos de valores para cada indicador que permiten asociar un riesgo identificado con las diferentes zonas de un mapa de riesgos. De manera particular, se pueden diseñar planes de mitigación específicos cuando los valores de los KRI vayan ingresando en zonas de mayor riesgo.

Los indicadores se pueden clasificar en tres grandes clases: como medidas de riesgo (KRI), medidas de desempeño (*Key Performance Indicator* o KPI) y medidas de control (*Key Control Indicator* o KCI). Los KCI se definen como indicadores que miden la efectividad (p. ej. diseño y performance) de un control específico, de tal manera que un deterioro en un KCI puede indicar un incremento en la probabilidad o impacto de un riesgo residual. Por otro lado, los KPI son medidas que permiten cuantificar objetivos vinculados al desempeño estratégico de una organización. Sin embargo, hay cierta dificultad para clasificar cada indicador de manera unívoca, ya que un mismo indicador puede adjudicarse a distintas clases según el usuario que lo utilice[2]. Aunque todos son importantes, los más relevantes para efectos de la administración del riesgo operacional, son los KRI.

Como ya se mencionó, se debe realizar un seguimiento del nivel de riesgo, razón por la que los KRI deben revisarse en forma periódica y sistemática para alertar cambios que puedan indicar problemas. Asimismo, los umbrales y rangos establecidos deben ser revisados periódicamente para asegurar que permanezcan alineados con el cambiante entorno de los negocios y los riesgos significativos asumidos por la entidad en cualquier momento del tiempo.

Las fuentes de información que permiten identificar riesgos significativos y contribuyen en el diseño de KRI son las bases de datos de pérdida por riesgo operacional, los resultados de los procesos de autoevaluación del riesgo operacional, los informes de auditoría interna y externa y de los órganos de supervisión, así como la información obtenida a través de entrevistas con el personal de las diversas líneas de negocio.

Entre algunas de las funciones de los KRI se pueden mencionar:

- ✓ Potencial para identificar zonas de alto riesgo, lo cual permite anticiparse y minimizar pérdidas.
- ✓ Capacidad para identificar procesos y/o debilidades en los controles, lo que permite fortalecer los mismos y resolver problemas.
- ✓ Establecer objetivos en términos de los KRI, a través de los cuales puede condicionarse la conducta del personal para lograr los resultados deseados.

[2] Por *ejemplo*: Una operación de "Trading and Sales" ejecutada por un operador la cual es reconfirmada con la contraparte a través de un tercero, y que además involucra una tercera función que liquida las correspondientes obligaciones. Un indicador que registra el número de transacciones aun no confirmadas podría ser interpretada como un KPI para el operador (pues mide la frecuencia de errores), un KCI para el tercero independiente (pues representa el número de transacciones no confirmadas lo que implicaría la necesidad de mejoras), y un KRI para la función que cierra la operación (pues este tipo de operaciones puede resultar en errores o en impagos).

- ✓ Alcanzar los niveles de apetito por riesgo de la entidad, estableciendo niveles de tolerancia para los diversos KRI.
- ✓ Cumplimiento regulatorio: la identificación y administración de los KRI puede ser objeto del control del ente regulador.
- ✓ Asignación de capital económico a las diversas líneas.

Para definir un indicador, es necesario responder a una serie de preguntas: ¿Qué queremos medir?, ¿Para qué?, ¿Cuándo vamos a medirlo?, ¿Qué tipo de información nos va a dar la medición?, ¿Cuándo y cómo reaccionar (planes de contingencia)?, ¿A quién se debe informar?, etc.

Para encontrar los KRI más adecuados, la forma más práctica radica en concentrarse en los riesgos operacionales significativos y sus causas y considerar indicadores históricos y/o *"forward-looking"* cuya evolución pueda estar vinculada a ellos. A veces las instituciones aplican técnicas estadísticas como análisis de componentes principales, análisis discriminatorio y control estadístico de los procesos, para explorar la relación entre los KRI y las pérdidas operativas, así como para encontrar la importancia relativa de un indicador dentro de un gran conjunto de KRI's. Ejemplos de indicadores relativos a la evolución pueden ser: daños a activos físicos de una entidad, el fraude con tarjeta o cheque bancario, el número de retrocesiones en una sucursal (cuando se tiene que regresar dinero a un banco por un error), el número de "caídas" de los sistemas, etc.

Por otro lado, los indicadores preventivos son los que permiten evitar alcanzar un nivel crítico, por ejemplo: número de llamadas no atendidas, rotación del personal o periodos sin vacaciones, etc.

Otros ejemplos de indicadores son:

- Número de caídas del servicio de Internet.
- Número de clientes clasificados como morosos y cuyas tarjetas no han sido bloqueadas.
- Número de reclamaciones de organismos oficiales por pagos de pensiones indebidos.
- Porcentaje del número de oficinas con dos empleados o menos sobre el total de oficina.
- Porcentaje de tarjetas de débito bloqueadas.
- Número de clientes con residencia en paraísos fiscales.
- Número de demandas judiciales realizadas por empleados contra la entidad.
- Porcentaje de procesos "críticos" de batch que se ejecuten fuera de su ventana temporal asignada.
- Porcentaje de sistemas para los que no existe copia de seguridad externa.
- Número de horas de formación por empleado.

Los indicadores de riesgo deben tener las siguientes propiedades[3]:

- ✓ Relevantes.- La información que proporcionan debe ser oportuna y significativa.
- ✓ No redundantes.- Si dos indicadores presentan una alta correlación, sólo uno debe ser seleccionado.
- ✓ Objetivos.- Su valor no puede depender de interpretaciones subjetivas.
- ✓ Simples.- Deben ser fáciles de entender, pero sobre todo su gestión debe ser fácil (actualizaciones, etc.).
- ✓ Verificables.- Sus valores deben ser comprobados.

Puede suceder que algunos de estos aspectos no se puedan implementar de manera fácil, pero seguir estas recomendaciones ayudará a constituir una base de buenas prácticas, útiles para la gestión del riesgo operacional.

II.1.4. Scorecards/RDCA

Las tarjetas de puntaje o scorecards son un conjunto de sistemas expertos para la medición del riesgo operacional que tienen en común la evaluación de los generadores de riesgo ("risk drivers"), así como la amplitud y calidad del ambiente interno de controles de riesgos, todo ello a través del uso de cuestionarios. La metodología de tarjetas de puntaje también suele ser reconocida como *"Risk Drivers and Control Approaches"* (RDCA).

Los cuestionarios se basan en una serie de preguntas ponderadas y basadas en el nivel de riesgo de la línea de negocio consultada, que permiten trasladar evaluaciones cualitativas a una métrica cuantitativa. El cuestionario se debe diseñar de tal manera que refleje el perfil de riesgos único de la entidad, lo que se logrará con la implementación de preguntas específicas para la entidad, la calibración de las respuestas y la aplicación de ponderadores y puntajes alineados con la importancia relativa del riesgo para la entidad.

El scorecard transforma evaluaciones de carácter cualitativo en medidas cuantitativas que permiten clasificar de forma relativa los diferentes tipos de exposiciones al riesgo operacional. Al involucrar a las líneas de negocio en el desarrollo y diseño del marco del RDCA, las responsabiliza por los resultados informados. Asimismo, su participación fortalece el desarrollo colectivo del conocimiento del riesgo operacional al involucrar también a los especialistas de los riesgos clave. Por otro lado, es útil ya que motiva a cada unidad de negocios a pensar en los riesgos operacionales a los que se encuentran expuestas.

La importancia del scorecard radica en que evalúa el riesgo operacional al momento de detectarse las debilidades y vulnerabilidades, es decir, cuando la probabilidad de ocurrencia es alta, por lo que se considera como una herramienta de carácter "forward looking". Lo anterior contrasta con la estimación del riesgo operacional cuando se obtiene

[3] Scandizzo (2005).

únicamente de datos de pérdida históricas, por lo que, como las acciones correctivas son posteriores, la probabilidad de pérdidas se ve afectada.

Las ventajas de utilizar este tipo de evaluaciones radican en que son explícitas y transparentes, principalmente para los gerentes de líneas de negocio y suelen estar sujetas a revisiones regulares por parte de la gerencia, la auditoría y los supervisores. Además, el scorecard responde rápidamente a cambios en el entorno de negocios, o a la aparición de nuevos riesgos operacionales, permitiendo acomodar los nuevos riesgos a medida que van surgiendo, agregando preguntas o cambiando otras, sin necesidad de esperar a que se materialicen las pérdidas. Por su diseño, los scorecards están totalmente alineados con el marco de gestión del riesgo operacional de la entidad, vinculando en consecuencia la medición con el seguimiento de dicho riesgo.

Del mismo modo, esta técnica la pueden utilizar las entidades para asignar el nivel de capital económico que corresponde a cada línea de negocio dependiendo de los resultados de la gestión y control de diversos aspectos del riesgo operacional. La vinculación directa entre el capital económico y el desempeño de las gerencias tiene como incentivo la realización de mejoras en la gestión del riesgo operacional, al centrar los esfuerzos de las unidades de negocio en mitigar el riesgo y mejorar los controles internos.

II.1.5. Análisis de escenarios (SBA)

El análisis de escenarios (“Scenario Based Approach” o SBA) se basa en la modificación conjunta de un rango de parámetros que afectan la posición de la entidad financiera en forma coherente y simultánea. Constituyen eventos hipotéticos que podrían ocurrir y deben ser representativos para cada entidad, teniendo en cuenta todos los factores de riesgo relevantes. Los escenarios pueden involucrar la ocurrencia de eventos catastróficos de carácter financiero u operacional, pero también pueden involucrar cambios en los planes de negocio, cambios en los ciclos económicos y daños a la reputación de la entidad debidos a fraudes o escándalos financieros.

Por otro lado, los escenarios se pueden generar de diversas maneras, por ejemplo, a partir de modelos estadísticos basados en las distribuciones de frecuencia y la severidad de los eventos de riesgo operacional, el análisis o repetición de eventos históricos, o eventos hipotéticos.

Para implementar el análisis de escenarios, en primer lugar, se categorizan los factores de riesgo. Al mismo tiempo, se puede desagregar la entidad en áreas organizacionales en las cuales pueda evaluarse el riesgo operacional en forma independiente. Enseguida se identifica un conjunto razonable de eventos realistas que reflejen la dinámica del negocio, basados en el marco de la administración de riesgos, el registro de riesgos, las opiniones de la línea gerencial y las opiniones de expertos en el tema. Los eventos que generan pérdidas esperadas (las que deben ser previstas), pérdidas inesperadas (se les asigna capital económico) y pérdidas extremas, son los que deben ser considerados y cuantificados con esta técnica.

Con la información anterior, se generan clases de escenarios que deben tener:

- Consistencia: Cada área de la entidad considera al menos un conjunto común de clases de escenarios, para lo cual una serie de *workshops* facilitados por una función centralizada de gestión del riesgo operacional puede ser efectiva. A efectos de una mayor consistencia también puede contribuir una revisión por parte de control interno.
- Relevancia: Cada área de la entidad determina si los escenarios son relevantes para su actividad.
- Los escenarios determinados deben maximizar la cobertura de los riesgos previstos. Esto se puede lograr a través de una discusión con todas las áreas para garantizar que se cubran cada uno de sus riesgos específicos.

Cada área de la entidad debe evaluar el impacto de los escenarios, para lo cual se pueden usar: cuestionarios, "workshops" guiados, matrices de recursos críticos vs. estado de los riesgos y la propia experiencia de la alta gerencia.

La importancia de implementar las técnicas antes mencionadas radica en que:

- ✓ Son *forward-looking*, se vinculan directamente con el proceso de gestión y promueven una sana administración del riesgo.
- ✓ El proceso de evaluación y análisis de los factores de riesgo permite una mayor comprensión de los riesgos operacionales y proveen información importante para mejorar la gestión.
- ✓ Capturan de manera rápida, cambios en el perfil de riesgos de la entidad y/o en la estructura organizacional.
- ✓ Establecen lazos entre los riesgos y sus controles.
- ✓ Ayudan a evaluar el impacto financiero y no-financiero de eventos extremos con grandes pérdidas inesperadas.
- ✓ Ayudan a determinar el perfil global de riesgos de la entidad y a establecer el apetito por riesgo dada su capacidad de asumirlo.
- ✓ A partir de la razonabilidad de los resultados, permiten validar modelos y los análisis estocásticos realizados, así como la calibración de las hipótesis del modelo.
- ✓ Proveen información para la determinación del capital económico y son por ello un elemento integral del marco de administración de riesgos de la entidad.

II.2. Marco para el manejo del riesgo operacional

El Nuevo Acuerdo de Capital de Basilea establece una serie de requisitos para el tratamiento del riesgo operacional:

Requisitos cualitativos:

- ✓ Función independiente de gestión del riesgo operacional.

- ✓ Implicación de la alta dirección.
- ✓ Sistema integrado en la gestión del día a día.
- ✓ Sistema de *reporting* de la exposición y de las pérdidas.
- ✓ Análisis de posibles escenarios para eventos extremos.
- ✓ Políticas y procedimientos de gestión del riesgo.
- ✓ Revisión por parte de auditores internos y externos.

Requisitos cuantitativos:

- ✓ Que el cálculo refleje en un periodo de un año un nivel de confianza del 99.9%.
- ✓ Capturar las colas de la distribución.
- ✓ Coherente con la definición de riesgo operacional.
- ✓ Usar una base de datos interna de pérdidas.
- ✓ Procedimientos para la asignación de pérdidas a las líneas de negocio y para la utilización de datos de pérdidas externas.
- ✓ Utilización de series de datos que cubran un mínimo de tres años.
- ✓ Posibilidad de utilizar correlaciones.
- ✓ Reconocimiento de la utilización de seguros para mitigación del riesgo.
- ✓ Ajustes cualitativos o scorecards (tarjetas de puntaje).

II.3. Criterios generales para utilizar modelos avanzados AMA

Para el cálculo del requerimiento de capital, Basilea II establece estrictos criterios generales, cualitativos y cuantitativos, que todas las instituciones deben cumplir si siguen modelos AMA para obtener la aprobación del supervisor:

- *Criterios cualitativos*: Desarrollo de indicadores y autoevaluaciones, identificación de riesgos, mapas de riesgos y la definición de la estructura organizativa y políticas.
- *Criterios cuantitativos*: Integración de gestiones cualitativas y cuantitativas, cálculo del capital con modelos avanzados, desarrollo del modelo de cuantificación, captura de datos y mantenimiento de la base de eventos de pérdida.

Y no menos importante, la *cultura*, que se refiere a criterios generales de concientización sobre la importancia del riesgo operacional.

Criterios cualitativos

El desarrollo de la gestión cualitativa adecuada contiene tres aspectos: la identificación de riesgos, el modelo organizativo y las herramientas de gestión utilizadas. El primer paso es la elaboración de un mapa de procesos de la entidad, el cual sirve para detectar los riesgos y controles existentes, así como para la evaluación de los eventos de pérdida por frecuencia y severidad.

En el segundo paso, es necesaria la creación de una unidad independiente, responsable de la gestión del riesgo operacional y que será la encargada de crear los mecanismos adecuados para la administración del riesgo.

Por último, contar con un sistema de medición del riesgo operacional que permita estimar de manera razonable las pérdidas esperadas combinando datos relevantes de pérdidas, tanto internos como externos, análisis de escenarios, así como el entorno del negocio y los factores de control interno específicos de la institución.

Es necesario que la entidad asigne capital económico por riesgo operacional entre las distintas líneas de negocio de manera que genere incentivos que mejoren la gestión del riesgo operacional en esas líneas.

Criterios cuantitativos

Un elemento fundamental para que las entidades puedan pasar de un enfoque cualitativo hacia un marco de gestión integral del riesgo operacional es la creación de una base de datos de pérdidas operacionales. Este es el mayor desafío al que se enfrentan las instituciones en México y América Latina debido a la escasez de datos internos por el temor o desconfianza del personal para revelar sus errores y debilidades, ya que sería como aceptar falta de capacidad o negligencia en el desempeño de sus tareas.

Cabe aclarar, que los eventos de pérdida pasados puede que no se repitan en el futuro, pero hasta el día de hoy es la fuente más confiable de información objetiva y verificable.

Una opción para completar la información interna es la recopilación de datos externos, pero existen dificultades para obtenerla ya que por un lado hay cierto recelo de parte de las entidades en compartir información de estas características (el tema de la cultura y la concientización vuelve a hacerse presente), así como por la baja cantidad de entidades que se encuentran recolectando información histórica.

Además de la recopilación, los datos externos presentan otro problema: su integración en el modelo, ya que su uso no debe dar lugar a que se modifique el perfil de riesgo de la propia entidad. El banco debe poner en marcha un proceso sistemático de determinación de las situaciones en las que se utilicen los datos externos y de las metodologías de empleo de tales datos (por ejemplo, introducción de ajustes de proporcionalidad y de ajustes cualitativos, o la introducción de mejoras en el análisis de escenarios). Las prácticas y condiciones para el uso de datos externos deben ser revisadas regularmente, documentadas y sometidas a exámenes periódicos independientes.

La labor de creación de bases de datos de pérdidas emprendida por las instituciones financieras representa un camino difícil, pero a su vez, tiene la gran ventaja de centralizar en una unidad toda la información valiosa para la gestión que anteriormente estaba dispersa en la organización. Dicha información permite llevar a cabo un estudio estadístico de las pérdidas y analizar los errores cometidos en el pasado así como sus causas, lo que facilita la implantación de acciones correctivas. Conviene recordar que la creación de bases de datos de pérdidas solamente es el punto de partida para la construcción del modelo de riesgo operacional, y una herramienta más para la gestión de

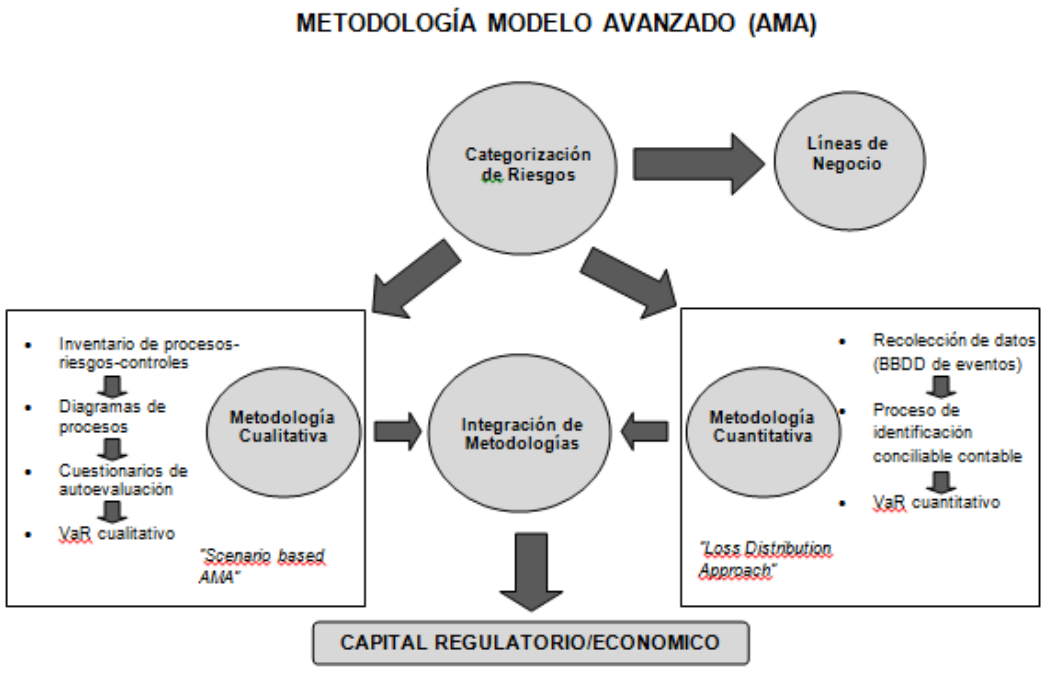
dicho riesgo, pero no es el objetivo primordial de la gestión del mismo (en la sección II.5. se detalla la información sobre las bases de datos por riesgo operacional).

Una vez finalizada la construcción de la base de datos, es conveniente que la institución proceda al desarrollo de un modelo de medición del riesgo operacional. La correcta cuantificación del riesgo operacional permitirá, entre otras cosas, facilitar la racionalización de las pólizas de seguros, y por lo tanto, una reducción de capital regulatorio para los enfoques más avanzados. Además, la medición del riesgo operacional permite incluirlo en el cálculo de la rentabilidad ajustada al riesgo y, por lo tanto, acercar más a la realidad el modelo de creación de valor de la compañía.

Las instituciones pueden seguir las siguientes pautas:

- Registrar los eventos operativos si su impacto es cuantificable.
- El método de medición que empleen debe ser capaz de identificar eventos situados en las “colas” de la distribución de probabilidad, por ser generadores de pérdidas graves en los supuestos sobre distribuciones de probabilidad que se utilicen para estimar el riesgo operacional en la determinación del capital regulatorio.
- Diferenciar entre la pérdida esperada (EL) y de la pérdida no esperada (UL) por eventos operacionales.
- El sistema de medición del riesgo operacional debe ser capaz de identificar los principales factores de riesgo operacional que influyen en la forma de las colas de la distribución de las estimaciones de pérdida.
- Los elementos básicos que el sistema de cálculo del riesgo debe tener son: utilización de datos internos, datos externos relevantes, análisis de escenarios y factores que reflejen el entorno del negocio y los sistemas de control interno.
- El método que utilice el banco debe ser coherente de manera interna y evitar la doble contabilización de las evaluaciones cuantitativas o las coberturas del riesgo que ya se hayan identificado en otros elementos del proceso.

Un ejemplo para alcanzar el modelo avanzado (AMA) supone la categorización de riesgos en niveles y la asignación de las líneas de negocio según las directrices de Basilea II; la metodología cuantitativa (registro de eventos de pérdida); la metodología cualitativa (opinión de expertos vista a un año); y, la integración de la metodología cualitativa/cuantitativa/cálculo de capital.



Cultura

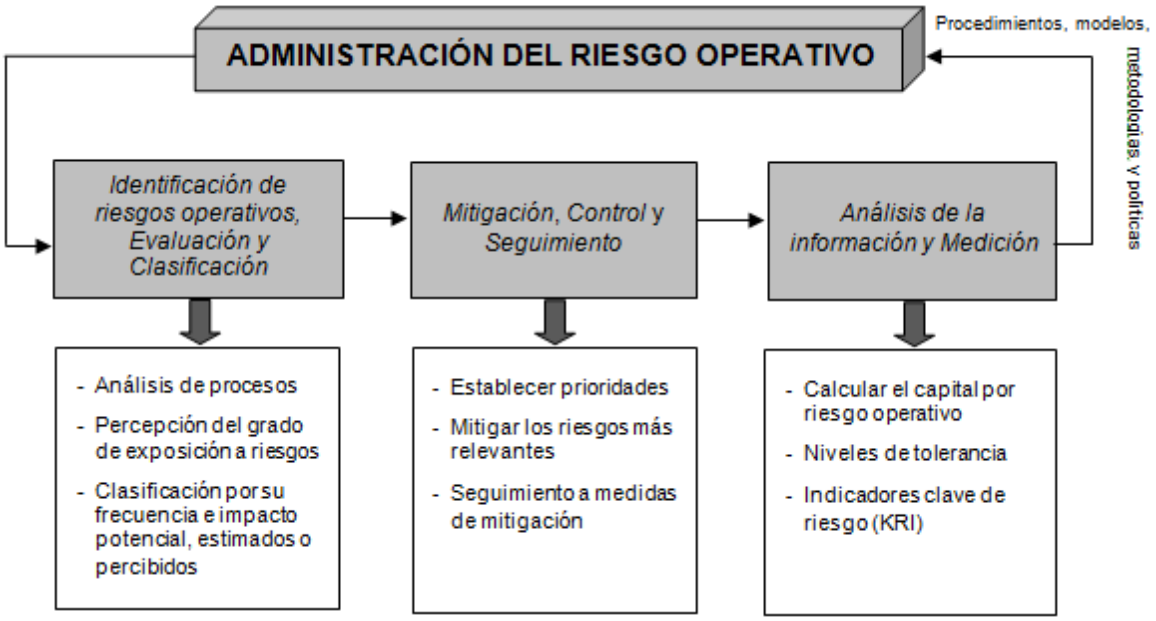
Este criterio tiene una relevancia significativa, ya que implica el convencimiento de la alta dirección de los beneficios y de la necesidad de implantar un marco de administración del riesgo operacional. Las razones para llevarla a cabo, son:

- Las presiones regulatorias.
- La comprensión del impacto del riesgo operacional.
- La necesidad de obtener información de gestión sobre las causas y consecuencias del riesgo operacional.
- El poder asignar el capital según el riesgo asumido.
- El poder remunerar teniendo en cuenta la rentabilidad y el riesgo operacional asumido.
- La necesidad de obtener más información que permita mejorar las decisiones sobre la mitigación del riesgo operacional.

El convencimiento de la alta dirección es sólo el primer paso en la generación de conciencia para la adecuada gestión del riesgo operacional, ya que otra parte importante es el trabajo de capacitación y la generación de cultura en las unidades de negocio y en las áreas de soporte de las entidades, ya que es ahí donde se realiza la efectiva gestión del riesgo operacional. Dichas áreas deben entender la utilidad de realizar determinadas tareas y de buscar una efectiva aplicación de las soluciones de mejora, así como el monitoreo y el control de los riesgos inherentes a su operación habitual.

II.4. Ciclo de gestión de riesgos operacionales

El proceso de gestión de los riesgos operacionales comprende la identificación, evaluación, categorización, seguimiento, mitigación, medición y control de los principales riesgos operacionales de la institución. Dicho ciclo debe repetirse periódicamente (en la práctica, por lo menos una vez al año) ya que los riesgos operacionales a los que está expuesta cualquier institución cambian o surgen nuevos riesgos.



II.4.1. Identificación, Evaluación y Clasificación de riesgos operacionales

El propósito principal de la identificación de los riesgos operacionales, es el conocimiento por parte de la institución de su perfil de riesgos, la cual se logra registrando las causas de las exposiciones tanto internas como externas para evaluar las estrategias que más le convengan y así mitigar sus riesgos.

Para identificar los riesgos operacionales asociados a los procesos, primero hay que determinar los elementos que los conforman, tales como:

- Documentación del proceso.
- Personal que interviene.
- Áreas que intervienen.
- Tecnología de apoyo.
- Medidas de control y supervisión.
- Interacciones con otros procesos.
- Segregación de funciones.
- Factores externos que pueden afectar el proceso.

La identificación de riesgos operacionales en las instituciones bancarias se realiza a través del análisis de los procesos para conocer la exposición a dichos riesgos y sus estadísticas de pérdidas, la autoevaluación del entorno y control interno, y el análisis de escenarios. Para lograrlo, es necesario reconocer sus componentes, así como las fortalezas y debilidades mediante la aplicación de ciertas herramientas o combinaciones de ellas, como son los procesos grupales, las entrevistas personales y los cuestionarios de autoevaluación.

Es necesario que el personal que participe en los ejercicios conozca perfectamente la operación del negocio, los espacios de mejora y las deficiencias; por otro lado, debe tener una visión integral del proceso, sus interacciones con otros procesos y su importancia dentro de los objetivos de la institución.

Los cuestionarios para la identificación de riesgos operacionales pueden permitir evaluar la frecuencia y la severidad de las pérdidas que pueden ocasionar los riesgos percibidos. Su aplicación puede crear conciencia y entendimiento de estos riesgos siempre y cuando se abarquen las múltiples fuentes de riesgo que pueden afectar los procesos de la institución (más allá de los que el entrevistado perciba). La escala de medición puede ser distinta para cada área, dependiendo de su volumen de operación y actividad.

El siguiente cuadro es un ejemplo de escalas de medición de un cuestionario:

¿Recibe quejas de clientes relacionadas con la atención que reciben?	➢ Nunca ➢ De 1 a 50 al mes ➢ De 51 a 200 al mes ➢ Más de 201 al mes
Estas quejas, ¿ocasionan pérdidas económicas?	➢ Mínimas (0 – 10,000) ➢ Bajas (10,001 – 300,000) ➢ Medias (300,001 – 700,000) ➢ Altas (más de 700,000)

El análisis de escenarios es el ejercicio de identificar eventos de pérdida por riesgos operacionales, hipotéticos pero factibles, que puede sufrir una institución basado en las opiniones de expertos en el negocio, opiniones de especialistas en riesgos e información externa (eventos sufridos por otras instituciones de características similares). Plantear diversos escenarios ayuda a estimar las pérdidas no esperadas potenciales aun cuando no se haya presentado o identificado un incidente de esa naturaleza en la institución, así como debilidades, vulnerabilidades o amenazas.

Con esta herramienta se pueden estimar la frecuencia y severidad de los eventos de pérdida para el diseño de “trajes” a la medida según la actividad del área, la línea de negocio de que se trate o del tamaño de la institución.

Por ejemplo, si se cuenta con un sistema de cómputo obsoleto, los posibles factores que podrían ocasionar riesgos operacionales serían errores en la captura de la información,

incumplimiento en tiempo y forma de las obligaciones establecidas por los reguladores, etc.

SISTEMA OBSOLETO	Mínimo 0-50,000	Bajo 50,000-300,000	Moderado 300,000-1,000,000	Medio 1,000,000-5,000,000	Alto Mayor a 5,000,000
Errores en la captura	5 al año	2 al año	1 al año	1 cada dos años	1 cada cinco años
Incumplimiento de obligaciones	3 al año	2 al año	1 cada dos años		

Los eventos de pérdida que ocasionan los riesgos operacionales, están relacionados con cualquiera de los siguientes factores:

- El ***personal****:* Perfiles laborales, capacitación y experiencia del personal para desempeñar sus funciones, índices de rotación del personal, elevadas cargas de trabajo.
- La ***tecnología****:* Grado de automatización de los procesos, obsolescencia tecnológica, suficiencia y actualización de hardware, interrupciones en comunicaciones, caídas de redes y sistemas
- Los ***procesos operativos****: D*ocumentación del proceso, asignación de funciones que no generen conflictos de intereses, auditorías al proceso, controles o revisiones redundantes en operaciones sensibles, inadecuada asesoría a clientes.
- ***Factores externos***: Posibilidad de incumplimiento de proveedores, afectación al proceso por fenómenos naturales, posibilidad de afectación por motines o bloqueos, exposición a vandalismo y robo.

Los factores de riesgo se definen como cualquier suceso que en sí mismo constituye una fuente elemental y homogénea (causal) de riesgo operacional.

Asimismo, las causas que pueden provocar riesgos operacionales pueden ser externas e internas.

Causas externas.- Demanda del mercado de nuevos productos, incremento de la competencia, rápida obsolescencia de la experiencia, incremento del uso de medios electrónicos para la realización de operaciones, rápida evolución tecnológica, cambios en la regulación, entorno propenso a la corrupción, entorno político agitado, entorno económico recesivo, cambios climáticos, etc.

Causas internas.- Lentitud de la institución para responder al cambio, rotación excesiva del personal, crecimiento acelerado de los volúmenes del negocio, clima laboral deteriorado, falta de capacitación, etc.

La estimación preliminar del riesgo debe considerar la identificación y registro de los riesgos, su calificación y verificación, así como la cuantificación de sus frecuencias de ocurrencia e impacto económico.

Toda entidad debe tener recursos suficientes para absorber las pérdidas de su actividad sin llegar a la insolvencia o la quiebra. Estos recursos se materializan en:

- Pérdidas esperadas.- Son un coste del negocio, reflejan lo que realmente se espera perder en promedio (valor medio de las pérdidas).
- Pérdidas inesperadas.- Son una medida de riesgo (volatilidad de pérdidas) que surge como consecuencia de que las pérdidas reales pueden ser superiores a las esperadas.

Los riesgos operacionales se pueden categorizar en relación a sus pros y contras, según se trate de los eventos de pérdida, sus causas y sus consecuencias. Los eventos de pérdida son los únicos contemplados en el Nuevo Acuerdo de Capital y se refiere al hecho que ocasionó el quebranto; las causas a los factores de riesgo y las consecuencias a los tipos de pérdida.

En el Nuevo Acuerdo de Basilea se establece una clasificación detallada de los tipos de eventos de pérdida. Dicha clasificación consta de tres niveles: el primer nivel contiene siete tipos de eventos de pérdida por riesgo operacional y sus definiciones. Cada entidad debe asignar sus datos de pérdidas a cada una de las siguientes categorías:

i. Fraude interno

ii. Fraude externo

iii. Relaciones laborales y seguridad en el puesto de trabajo

iv. Prácticas con clientes, productos y negocios

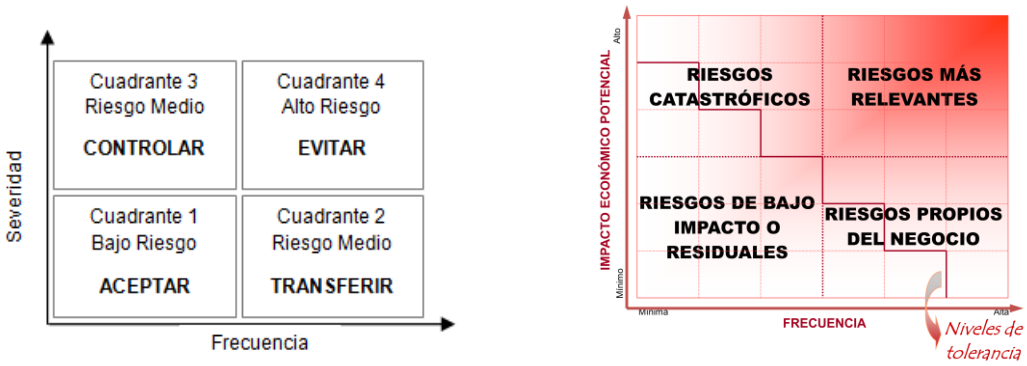
v. Daños a activos materiales

vi. Incidencias en el negocio y fallos en los sistemas

vii. Ejecución, entrega y gestión de procesos

En cualquier institución financiera, se pueden identificar gran cantidad de riesgos operacionales en todas sus áreas. Como no es posible atenderlos todos simultáneamente porque se requeriría de tiempo y recursos cuantiosos, es necesario el establecimiento de prioridades de acuerdo con la frecuencia (probabilidad de ocurrencia) y la severidad de las pérdidas que generan (impacto económico) que señalan la vulnerabilidad de la institución a dichos riesgos. Con estas dos variables se construye un espacio de dos dimensiones con cuatro zonas o cuadrantes que permite clasificar los riesgos a fin de establecer prioridades en la gestión y mitigación de los mismos. Dicho espacio se conoce como mapa de riesgos.

Mapas de riesgos



El objetivo de los mapas de riesgos es hacer una revisión y diagnóstico del sistema de control interno existente en la institución mediante la identificación de los principales riesgos a los que están expuestas las actividades realizadas, los controles existentes para mitigarlos y las oportunidades de mejora en el proceso de gestión del riesgo.

Los eventos que se sitúan en el cuadrante 1, son los riesgos de bajo impacto o residuales y suponen un bajo riesgo, por lo que no se destinan recursos adicionales de control. Estos riesgos es mejor asumirlos e implementar programas de seguimiento, para que en caso de que cambien su perfil de riesgo, se actúe inmediatamente para su control.

Los riesgos más relevantes se sitúan en el cuadrante 4 y su riesgo es elevado, ya que se trata de hechos de pérdida económica potencial elevada y gran probabilidad de ocurrencia. Las instituciones deben centrar sus esfuerzos de gestión en estos riesgos, estableciendo planes de mitigación[4].

Los eventos del cuadrante 2, son los riesgos propios del negocio, donde la institución debe contar con datos suficientes por ser incidentes de alta frecuencia y baja severidad. Además, debe utilizar herramientas estadísticas o redes causales y darles seguimiento a través de indicadores de riesgo. Se pueden mitigar a través del desarrollo de controles automáticos, de tal forma que su costo no resulte más elevado que las pérdidas que generan. Tal es el caso de errores en liquidaciones, fraudes con tarjeta, fallos de la contraparte, etc.

En el cuadrante 3, se encuentran los riesgos catastróficos, que son los eventos de baja frecuencia y alta severidad, donde la institución probablemente enfrente la falta de datos disponibles. Es común modelarlos con una pérdida esperada (media) relativamente pequeña, pero una gran cola de pérdidas, siendo necesario un plan de contingencias o la contratación de una póliza de seguros para afrontarlos. Para este tipo de eventos, la

[4] Es conveniente gestionar las *near-misses* o eventos próximos a la pérdida pero que se solventaron a tiempo, ya que pueden ser una señal de futuros riesgos operacionales. El principal inconveniente es incorporarlas en las bases de datos, ya que no se reflejan en la contabilidad.

entidad debe destinar capital para su cobertura. Aquí se pueden incluir los litigios, caídas del sistema tecnológico o los desastres naturales.

Para facilitar la identificación de los posibles eventos de pérdida debidos al riesgo operacional, es conveniente categorizar dichos eventos, para lo cual es posible utilizar la clasificación definida por el Comité de Basilea (Anexo 12 A), la cual puede ser modificada de acuerdo a los juicios de los expertos en cada una de las instituciones financieras.

Para que un sistema de control interno sea efectivo, el proceso de identificación y análisis del riesgo así como los controles, deben ser continuos. Para lograrlo, es necesario que todos los niveles directivos de la institución se involucren en la gestión de los riesgos y controles de las áreas de negocio de la entidad y se fomente una cultura de control interno que ayude a la entidad a conseguir sus objetivos de rentabilidad y rendimiento y a prevenir la pérdida de recursos.

II.4.2. Mitigación, Control y Seguimiento

Día con día, las instituciones financieras están propensas a múltiples riesgos operacionales en todas las áreas de negocio, sean conocidos o no. Vigilarlos simultáneamente requeriría de tiempo y recursos considerables, por lo que es necesario establecer prioridades por la frecuencia de los eventos de pérdida que generan y la severidad de tales pérdidas para implementar medidas de mitigación, de control, eliminación de los incidentes de pérdida o rediseño del sistema que los contiene según sea el caso.

El desarrollo de procedimientos de control y gestión del riesgo operacional comprende:

- Estrategias para la gestión del riesgo operacional: criterios para evitar, reducir, transferir o asumir el riesgo operacional.
- Análisis de escenarios potenciales de riesgo operacional (stress-testing).
- Análisis de correlaciones intrarriesgos e intrerriesgos (con riesgo de crédito, con riesgo de mercado, con riesgo de seguros, etc.).

La clasificación de los riesgos operacionales permite desarrollar e instrumentar las acciones pertinentes de mitigación y control de acuerdo con un análisis de costo/ beneficio.

El objetivo de mitigar, controlar y dar seguimiento a los riesgos operacionales, es llevarlos a niveles aceptables para la institución y así reducir los costos, las reservas y el capital necesarios para hacerle frente a las pérdidas causadas por dichos riesgos.

El hecho de evaluar y cuantificar los riesgos, permite a los responsables de su gestión:

- Identificar las exposiciones de riesgo que son inaceptables para la institución o que se encuentran fuera de su apetito de riesgo;
- Seleccionar y priorizar los mecanismos adecuados para su mitigación; y
- Comparar los riesgos con sus estrategias y políticas de riesgo operacional (ROp).

La administración de riesgos operacionales debe evaluar la suficiencia de las medidas preventivas, tanto en términos de su efectividad en la reducción de la probabilidad de ocurrencia de ciertos riesgos como de su efectividad en disminuir el impacto en caso de ocurrir. Las Disposiciones emitidas por la CNBV, establecen entre otras cosas, que la unidad de riesgos es la responsable de proponer acciones correctivas cuando se observen desviaciones de los niveles de tolerancia establecidos por las unidades de negocios.

Para llevar a cabo acciones de mitigación, es necesario analizar el costo/beneficio, ya que en el caso de los riesgos de bajo impacto, el costo de su mitigación puede rebasar el monto de las pérdidas que ocasionan, por lo que es mejor asumirlos. Por otro lado, los riesgos catastróficos se pueden evitar mediante la confección de planes de contingencia.

II.4.3. Análisis de la información y Medición

Para calcular el capital por riesgo operacional, se utiliza la información de la base de datos de eventos de pérdida, la cual se conforma por diversas fuentes derivadas de la identificación de riesgos operacionales y de la estimación de la frecuencia y severidad de las pérdidas. Las fuentes a utilizar son: la información histórica interna, la autoevaluación del entorno y del control interno, el análisis de escenarios y la información histórica externa. Además, las fuentes de información deben ponderarse según su nivel de *credibilidad*.

En las etapas iniciales de la administración de riesgos operacionales, para el cálculo del capital, el análisis de escenarios lleva el mayor peso y la información histórica externa el menor, derivado de la poca información interna que las instituciones han podido recoger ya que no existe una cultura para la gestión del riesgo operacional. Cuando las bases de datos sean gruesas, la tendencia será que la información histórica interna tenga mayor ponderación, ya que se "puede" tener confianza en la validez de los datos por ser un reflejo de los eventos de pérdida que se han presentado en la institución.

La medición de riesgos operacionales pretende acercarse al cálculo del VaR operacional, para lo cual es necesario modelar la frecuencia aplicando, por ejemplo, una distribución Poisson y para la severidad se puede optar por cualquiera de las siguientes distribuciones: Exponencial, Lognormal, Pareto, Weibull, Burr, etc. Finalmente, la idea es obtener una distribución agregada que permita trabajar en términos similares a la metodología VaR.

La distribución de pérdidas permite distinguir entre *pérdida esperada*, asociada a eventos localizados en el cuadrante 2 que representan un coste habitual, la *pérdida inesperada* o riesgos de control debidos a las debilidades de los sistemas de control interno (eventos del cuadrante 4) que se cubren a través de planes de mitigación, y *pérdida excepcional* (eventos del cuadrante 3), tales como fraudes o desastres cuya magnitud puede afectar potencialmente la supervivencia de la institución, que son cubiertos con planes de contingencia o seguros.

Cualquiera que sea el caso, por presentar características distintas a los riesgos de crédito y de mercado, las dificultades para la gestión del riesgo operacional se originan porque:

- ✓ Se relaciona más con los procesos que con el producto.
- ✓ No siempre se basa en transacciones, ni aparece en las cuentas anuales, ni se audita.
- ✓ Las pérdidas históricas no son una referencia para pérdidas futuras, lo que dificulta el diseño de escenarios.
- ✓ Se dificulta especificar un horizonte temporal, ya que depende de la frecuencia de la pérdida.
- ✓ El efecto de la diversificación es incierto: ante la confluencia de varios riesgos operacionales, las pérdidas pueden multiplicarse.
- ✓ Los riesgos de crédito o mercado deben ser asumidos para lograr beneficios, no así el operacional.
- ✓ Su componente subjetivo es mucho más destacado que en otros riesgos, especialmente por la ausencia de datos en aquellos eventos que tienen lugar de forma esporádica.

II.5. Base de datos de pérdidas ocasionadas por riesgos operacionales

Para el diseño de un sistema integral de gestión de riesgos operacionales, es conveniente seguir un proceso que inicie con entrevistas al personal implicado en los procesos y sistemas de control de la institución, con la finalidad de determinar los factores más relevantes a considerar y concretar los objetivos de la gestión de riesgos.

El siguiente paso es la conformación de una base de datos que contenga toda la información necesaria para el posterior desarrollo de la metodología para el cálculo de capital de riesgo operacional. Lo ideal, sería poder trabajar con datos internos (difíciles de recopilar en caso de pérdidas poco frecuentes), por lo que de ser necesario, se podrá acudir a datos externos, tanto de carácter público como obtenidos de consorcios de datos (por ejemplo, ORX[5]). La base de datos permitirá evaluar los eventos de riesgo operacional más significativos, y será el punto de partida para otros análisis: distribuciones estadísticas, relaciones causales, seguimiento de indicadores de riesgo, etc.

En un esquema de administración del riesgo operacional, la constitución de una base interna de eventos operacionales es una práctica estandarizada. Para cualquier institución, la recopilación de esos eventos debe contribuir al objetivo de reducción de incidentes y montos de pérdidas. El proceso de recolección de datos internos de riesgo operacional debe tener una serie de incentivos y controles para asegurar un alto nivel de cobertura y calidad de los datos.

La información de pérdidas experimentada por cada entidad es el mejor reflejo del perfil de riesgo operacional de cada institución. De hecho, en la gestión de este riesgo, la mayoría de las instituciones ya está trabajando en la elaboración de bases de datos internas de pérdidas por ser información útil para la gestión, independientemente de que vayan a abordar o no la construcción de un modelo interno de medición del riesgo.

La recopilación de información de pérdidas por este tipo de riesgo en las entidades financieras, tanto interna (propia de la institución) como externa (de otras entidades similares), tiene como finalidad la estimación de las pérdidas esperadas y las no esperadas.

Una base de datos interna debe incluir información acerca del monto de la pérdida, dónde se ha detectado, descripción del evento, tipo de evento, unidad de negocio a que corresponde, fecha de la pérdida y momento en que se tuvo constancia de ella, fecha final del evento, acciones de gestión emprendidas, recuperación (si hay seguros y otros mecanismos) y ajuste de estimación de pérdidas. Diariamente se deben capturar en la base de datos, los eventos operacionales que se presenten, clasificados según su causa y con un nivel de desglose suficiente pero no excesivo, en términos de frecuencia y

[5] ORX: Operational Riskdata EXchange Association. Es una asociación formada por 66 bancos líderes de 20 países sin fines de lucro dedicada al avance de la medición y gestión del riesgo operacional en la industria de servicios financieros. Fue fundada en 2002 con el objetivo principal de crear una plataforma para el intercambio seguro y anónimo de datos de pérdidas por riesgo operacional de alta calidad.

severidad (costo de la pérdida). Esta información es útil para realizar comparaciones temporales (dentro de una unidad de negocio) y entre unidades distintas (oficinas, líneas de negocio, etc.).

Basilea II establece unos requisitos mínimos que deben reunir los datos internos para asegurar que dicha base sea suficiente tanto en términos cuantitativos como en la calidad de los mismos:

- Los datos de pérdida deben ser completos y recoger la totalidad de las actividades y exposiciones de relevancia en todas las ubicaciones geográficas. En el caso de que algunas actividades o exposiciones queden excluidas, se deberá motivar su eliminación. Es importante no olvidar que muchos de los eventos de riesgo operacional se han producido en sucursales o filiales alejadas de la casa matriz en las que, precisamente, se habían relajado los sistemas de control (por ejemplo, los casos de Barings o Allied Irish Banks).
- En lo que se refiere al umbral de pérdida bruta adecuado o importe a partir del cual se deben recopilar los eventos, la cifra que se maneja en Europa es de 10,000 euros. Esta cifra no es prescriptiva, pero aporta cierta homologación a los umbrales utilizados en el sector financiero internacional. Cabe aclarar, que algunas instituciones están actuando con umbrales inferiores o, incluso, recopilando todo tipo de pérdidas.

  En Estados Unidos, el umbral que se maneja en la mayoría de las entidades es de 10,000 dólares. En el caso de México, no hay un umbral establecido.
- La delimitación del riesgo operacional con respecto a otros riesgos es una de las dificultades en la creación de las bases de datos internas. Es muy frecuente encontrar pérdidas por riesgo de crédito que inicialmente se originaron por algún evento de tipo operacional (por ejemplo, un defecto legal o de control, el cual se manifiesta posteriormente con un impago). Usualmente, estas pérdidas se han tratado como riesgo de crédito; y en entidades que siguen modelos de medición interna, las pérdidas forman parte de las bases de datos para el cálculo de los requerimientos de capital por riesgo de crédito.

  En el caso de riesgo de mercado, todas las pérdidas por riesgo operacional relacionadas con este riesgo se deben tratar como pérdidas por riesgo operacional a efectos de capital. En este caso, el problema reside principalmente en su identificación, dado que muchas de las pérdidas por riesgo operacional en esta área quedan enmascaradas en la cuenta de pérdidas y ganancias como resultados por operaciones financieras, por lo que difícilmente se pueden identificar (por ejemplo, un error en la compra de una referencia que se soluciona mediante su venta y posterior compra correcta).
- En la recopilación de datos de eventos de pérdida, un caso especial es el tratamiento de eventos múltiples (aquellos que, siendo un único evento, afectan a varias líneas de negocio; por ejemplo, el incendio de la sede principal) y eventos prolongados en el tiempo (por ejemplo, un fraude concebido bajo un plan de acción

y materializado en varias operaciones secuenciales). A efectos de cálculo de capital es importante que no se fraccionen, sino que se traten como un único evento, reflejando así la realidad del mismo. Basilea II determina que las entidades deben establecer sistemas para la recopilación de este tipo de eventos.

- Se exige un periodo mínimo de observación de cinco años para asegurar una base suficiente de eventos. Como la creación de estas bases de datos es relativamente reciente, la primera vez que el banco presente el modelo interno a efectos regulatorios se aceptará un mínimo de tres años de base histórica.
- Por último, la institución debe ser capaz de asignar los datos recopilados a las categorías supervisoras de eventos de pérdidas y líneas de negocio. Además de la pérdida bruta, se debe reunir información adicional sobre el evento, detallando como mínimo la fecha, sus causas y las recuperaciones realizadas.

Como la mayoría de los riesgos operacionales corresponden a eventos sin reflejo contable y en pocos casos el registro de pérdidas es sencillo por tratarse de datos contables, se debe realizar un mayor esfuerzo informático para el diseño de un soporte que logre homogeneizar la recolección de datos en una entidad financiera, desde sus oficinas centrales hasta las sucursales.

A partir de la información recolectada en la base de datos, es conveniente diseñar indicadores de riesgo con el objeto de reflejar la exposición a riesgos de la entidad. La combinación de ellos definirá el perfil de riesgos de la institución al nivel de desglose deseado y así centrar la atención sobre aquellas actividades que requieran mayor control.

Algunos ejemplos de indicadores de riesgos operacionales asociados a las causas que considera Basilea II son:

INDICADORES DE PROCESOS	**INDICADORES DE RECURSOS HUMANOS**
✓ Volúmenes procesados*: Volumen actual medio/ Capacidad máxima; (si < 1 no riesgo, si > 1 riesgo creciente) ✓ Número de incidencias/Errores ✓ Partidas en investigación ✓ Frecuencia de los cuadres de partidas (conciliación de cuentas) ✓ Cuadres entre aplicativos (en qué medida las aplicaciones se adecúan a las tareas que deberían realizar) ✓ Frecuencia de arqueos y cuadres ✓ Operaciones pendientes de liquidar (%) ✓ Segregación funcional ✓ Manualidad de los procesos ✓ Cruce de confirmaciones ✓ Contratos: calidad jurídica de los contratos, antigüedad del modelo, poderes de los firmantes, custodia del contrato ✓ Cumplimiento normativa bancaria ✓ Segregación funcional ✓ Número de reclamaciones de clientes ✓ Número de sanciones del supervisor bancario	✓ Calificación/Evaluación de la plantilla ✓ Antigüedad de la plantilla ✓ Temporalidad: personas con contrato temporal/total plantilla (%) ✓ Grado de formación ✓ Rotación ✓ Pérdida de talento: número bajas voluntarias último año/ total plantilla ✓ Cumplimiento normativa laboral: número de sanciones laborales ✓ Número empleados ✓ Personal inadecuado para actividades a desempeñar ✓ Falta de capacitación ✓ Mal proceso de selección del personal ✓ Tiempo medio de ausentismo por trabajador ✓ Personal contratado/Permanente ✓ Vacantes sin completar – Volúmenes en “posiciones clave” ✓ Recompensa vs normas generales de mercado

INDICADORES DE SISTEMAS	INDICADORES DE RIESGOS EXTERNOS
✓ Seguridad lógica (seguridad en Internet, virus informáticos, intentos de rupturas,…) ✓ Número de solicitudes de renovación de claves de acceso ✓ Número de intentos de acceso malintencionados ✓ Disponibilidad de las aplicaciones: Tiempo sistema disponible/tiempo total período ✓ Número de usuarios por aplicación ✓ Estado de las comunicaciones ✓ Fallos en aplicativos ✓ Tiempos de respuesta (copia de seguridad) ✓ Ataques a la web ✓ Ataques de virus ✓ Capacidad CPU utilizada (%) ✓ Éxito de proyectos según medidas de tiempo/coste/ calidad ✓ Eventos de gestión de cambio ✓ Rating de satisfacción de los clientes con la tecnología ✓ Desarrollo del proceso del ciclo de vida	*Desastres:* ✓ Calidad planes de contingencia ✓ Calidad planes continuidad del negocio ✓ Operaciones en off (%) ✓ Seguridad edificios: escaleras de incendio, extintores/ mangueras, detectores de humo, control de acceso,.. ✓ Nivel de cobertura de pólizas de seguro ✓ Tipo de custodia documentos ✓ Planes de evacuación (test anual) *Proveedores:* ✓ Calidad proveedores ✓ Diversificación proveedores ✓ Rating proveedores

(*) Número de transacciones que procesa una unidad, sin incluir horas extras y cumpliendo todos los pasos que marcan los procedimientos (controles incluidos)

En términos de seguimiento y control, es fundamental el papel que juegan los indicadores de riesgo operacional, ya que si se combinan con diagramas de control ayudan a la identificación de variables específicas de importancia para los gestores de operaciones, como pueden ser: número de eventos de pérdida, número de transacciones, exceso sobre los límites, número de apuntes no conciliados o factores de riesgo significativos.

Por otro lado, permiten describir la variación temporal intrínseca en una variable muestral, verificando si su distribución ha cambiado de nivel, recorrido o forma. Si el cambio en la variable es significativo, indicará que el proceso ya no está “bajo control estadístico”, por lo que al situarse fuera de los límites superior de control (LSC) e inferior de control (LIC), se notará la necesidad de vigilar esa variable.

Dependiendo del tipo de eventos operacionales a tratar, en la etapa final del proceso se pueden combinar las herramientas que se pueden utilizar como apoyo, tales como:

1. Redes causales.- Son representaciones gráficas de relaciones causa-efecto entre variables establecidas en un dominio y representa eventos que pueden tener un determinado número de estados. En la estructuración más sencilla (2 variables), una es causa de la otra y cada una de ellas sólo representa dos estados.

   La teoría de decisión bayesiana es una herramienta de apoyo para la toma de decisiones en incertidumbre. Los modelos causales se sustentan en dicha teoría y son aplicables en la medición del riesgo operacional.

2. Plan de contingencias.- Es un procedimiento alternativo previsto para afrontar situaciones extremas, de modo que ante sucesos que pondrían en peligro la continuidad de la actividad, pueda disponerse de un espacio físico alternativo, otros equipos informáticos, etc. Se prevé para interrupciones temporales pero

prolongadas de las funciones de la empresa, motivadas por riesgos externos y poco frecuentes.

Es necesario evaluar la seguridad física de la entidad, por lo que deben considerarse aspectos como el acceso a personas y a materiales, acceso a zonas restringidas, mantenimiento de instalaciones, protección de las comunicaciones, procedimientos seguros de evacuación, detectores de humo, sistemas antirrobo, etc.

3. Seguros.- Como no todos los riesgos pueden ser eliminados, si la entidad decide continuar con aquellas actividades que los generen, puede optar por asumirlos (mediante la reserva de fondos) o transferirlos a través de seguros. El seguro trasfiere las consecuencias del riesgo al asegurador, y permite reducir las pérdidas financieras (sustituye al capital).

   Para que un riesgo sea asegurable, debe ser definible y calculable. No se contrata para contingencias que no suponen pérdidas ni ante eventos previsibles, sino para hechos específicos que podrían generar una pérdida inesperada. Las compañías aseguradoras añaden los riesgos transferidos por varias entidades y se benefician de economías de escala y de los efectos de la diversificación.

   Tradicionalmente, los seguros contratados para riesgo operacional han sido de carácter específico, asociados a una categoría de riesgo.

Ejemplos de seguros específicos

Fianza a todo riesgo	Robo y fraude (malversación y robo, apropiación de activos, destrucción maliciosa de activos, falsificación, evasión deliberada de impuestos, etc.), delito computacional (robo de información, manipulación de datos, contraseñas inadecuadas, etc.), fraude externo (robo, falsificación, soborno, etc.)
Delito contra computador electrónico	Robo de información, manipulación de datos, etc.
Propiedad no financiera	Sistemas (caída de hardware, fallas en telecomunicaciones, fallas de seguridad, errores humanos, virus, falla técnica, etc.), daño a activos físicos (tormenta, huracán, inundación, granizo, terrorismo, fuego, etc.)
Responsabilidad de los directivos	Idoneidad, información y fiduciario, negocio inapropiado y prácticas de mercado, supervisión e información (falla en información obligatoria, informes externos inapropiados, etc.)
Responsabilidad de prácticas de los empleados	Relaciones de trabajadores (entorno hostil, despido improcedente, acosos, difamación y calumnia), diversidad y discriminación (por sexo, raza, edad, religión, nacionalidad, etc.)

Debido a que la financiación de los seguros específicos es cuestionada actualmente al aparecer brechas o superposiciones en la cobertura de riesgos, se plantean diversas alternativas:

- Seguro multiproducto.- incluye algunas/todas las políticas de riesgo específico, eliminando tanto gaps como superposiciones derivadas de seguros específicos, además de conllevar una gestión integral de riesgos. Sin embargo, excesivo coste y la inexistencia de un mercado real para su contratación lo platean como una opción de futuro.
- Titulización o compra de derivados contra riesgos asegurados.- el banco emite un bono (cat bond catastrophe bond) cuyo valor depende de unas pérdidas operacionales predefinidas.
- Recurrir al auto-seguro o mantenimiento de capital, como retención de riesgos.
- Reasegurar las pérdidas, acentuando la diversificación y reduciendo la volatilidad.
- Externalización de actividades (outsourcing) para que las realicen expertos, que puedan lograr una ventaja comparativa con esa gestión, buscando mejorar la calidad de los procesos.

III. Herramientas cuantitativas para estimar la exposición a riesgo operacional

El objetivo final de las instituciones, es buscar la integración de todos los aspectos tanto cualitativos como cuantitativos, lo que implica diseñar y establecer la relación entre los datos recopilados, los indicadores, los mapas de riesgos y controles y las mediciones de capital. El enfoque debe ser dinámico y contribuir al establecimiento de un plan de acciones correctivas para afrontar las debilidades detectadas.

La construcción completa de la base de datos, permite a la institución continuar con el desarrollo de un modelo de medición del riesgo operacional.

En los modelos avanzados, el Comité de Basilea no especifica un método o los supuestos de las distribuciones de probabilidad que se usan para medir el riesgo operacional en lo que se refiere al capital regulador, debido a la evolución continua de los métodos analíticos en el tratamiento y medición de dicho riesgo. No obstante, cualquiera que sea el método que utilice la institución, debe demostrar que identifica los eventos situados en las colas de la distribución de probabilidad y que generan pérdidas grandes, demostrando que su medida del riesgo operacional está calculado en un horizonte temporal de un año y con un nivel de confianza del 99.9%.

El Comité propone tres enfoques para calcular los requerimientos de capital por riesgo operacional, que de menor a mayor sofisticación y sensibilidad al riesgo son: el método del indicador básico (Basic Indicador Approach o BIA); el método estándar (Standardized Approach o SA); y las metodologías de medición avanzada (Advanced Measurement Approach o AMA). Cabe destacar que el método del indicador básico está orientado a los ingresos y el avanzado a las pérdidas.

El siguiente cuadro resume los métodos para el cálculo de capital por riesgo operacional:

	METODOLOGÍA	**REQUERIMIENTOS**
INDICADOR BÁSICO	15% de los ingresos brutos anuales (promedio de los últimos 3 años).	Sólo se aconseja a los bancos seguir las *"Sanas Prácticas para la Administración del Riesgo operacional".*
ESTÁNDAR	Un porcentaje que puede ser 12, 15 o 18% de los ingresos brutos de cada una de las líneas de negocio del banco.	• Participación activa del consejo y la alta dirección en la vigilancia de la gestión del riesgo operacional. • Sistema de gestión del riesgo. • Control y auditoría del sistema. • Creación de una unidad de gestión del riesgo operacional para los bancos con actividad internacional.
MEDICIÓN AVANZADA	Capital calculado con base en las estadísticas propias de pérdidas por riesgo operacional.	• Adicionalmente a los requerimientos del método estándar, cinco años de información histórica para ser usado para estimar pérdidas. • Tres años cuando se use por primera vez un método de medición avanzada.

Estos métodos no son excluyentes, pueden usarse simultáneamente para líneas de negocio distintas.

III.1. Método del Indicador Básico (BIA)

Es el método más simple de todos, en el que el capital se determina aplicando el 15% sobre los ingresos brutos de los tres ejercicios anteriores. Los ingresos brutos se conocen como los ingresos financieros netos más los ingresos no financieros.

Consiste en aplicar un factor, denominado α y fijado actualmente en 15%, sobre el promedio de los ingresos brutos anuales positivos de los tres últimos años. Es decir, se excluyen tanto del numerador como del denominador los ingresos brutos que presentan valores menores o iguales a ceros, lo que no permite la compensación entre ingresos brutos positivos y negativos en distintos años. En términos matemáticos, se puede expresar como sigue:

$$K_{BIA} = \frac{(G1 + G2 + G3)}{3} * \alpha$$

Donde:

- K_{BIA} es el requerimiento de capital
- G_i con $i \in \{1, 2, 3\}$ son los ingresos brutos anuales positivos
- α es el factor establecido por el Comité, actualmente es del 15%
- Ingreso bruto:
  - Ingresos netos por intereses (margen financiero)
  - Otros ingresos netos ajenos a intereses (ingresos no financieros)
  - Bruto de provisiones
  - Bruto de gastos de explotación

El Método BIA no permite el cálculo de mitigadores de riesgo operacional mediante seguros externos, por lo que no existen incentivos explícitos para contratarlos. El Comité reconoce que el BIA es sólo un punto de partida para la estimación del riesgo operacional e insta a los bancos a seguir en conjunto recomendaciones publicadas en el documento "Sanas prácticas para la gestión y supervisión del riesgo operacional"[6]. Asimismo, invita a los bancos internacionalmente activos y/o con una importante exposición a riesgo operacional, a utilizar métodos más avanzados.

La utilización de los ingresos brutos como variable representativa de la exposición por riesgo operacional y la estimación del factor fijo α se basan, principalmente, en información de pérdidas y de capital económico por riesgo operacional de bancos de distintas naciones, así como de estudios empíricos sobre aquella información, realizados por el Comité entre los años 2001 y 2002[7].

---

[6] BCBS, 2003.

[7] Principalmente sobre la información recolectada de los ejercicios QIS 2 y QIS 2.5, sobre los cuales el Comité determinó que, en promedio, la relación entre el capital económico por riesgo operacional sobre el capital mínimo regulatorio esa de aproximadamente un 12%.

El enfoque BIA es una primera aproximación para medir el riesgo operacional, por lo que se espera que sea utilizado en los inicios del tránsito hacia Basilea II o, durante algún tiempo, por los bancos de pequeña escala, con pocas líneas de negocio y con baja disponibilidad de información desagregada.

III.2. Método Estándar (SA)

Este método desagrega las actividades de los bancos en número de unidades de negocio estandarizadas y líneas de negocio para reflejar los distintos perfiles de riesgo entre bancos por sus actividades de negocio. El ingreso bruto de cada línea de negocio se utiliza como indicador (G_{ij}) para reflejar el tamaño y volumen de las operaciones del banco en dicha área. El capital requerido en cada línea de negocio se calcula multiplicando el ingreso bruto por un factor (β), que se asigna a cada una de las líneas.

El requerimiento de capital se calcula como la suma de un porcentaje de los ingresos brutos de las diferentes líneas de negocio:

$$K_{SA} = \sum_{j=1}^{3} \left[\sum_{i=1}^{8} \frac{(G_{ij} * \beta_i)}{3} \right]$$

Donde:

- K_{SA} es el requerimiento de capital
- G_{ij} con $i \in \{1, 2,\ldots 8\}$ son los ingresos brutos anuales (positivos o negativos) en cada una de las líneas de negocio del banco en el año j con $j \in \{1, 2,3\}$
- β_j con $j \in \{1, 2,\ldots 8\}$ son los factores por línea de negocio establecidos en el Acuerdo de Basilea.

Se identifican ocho líneas de negocio sin asociarlas a unidades de negocio, se homogeneiza G_{ij} (el importe medio anual de los ingresos brutos obtenidos en los tres últimos años en cada línea) y se fijan los beta (pérdidas causadas por el riesgo operacional en esa línea respecto a los ingresos brutos de esa línea). Si el requerimiento de capital en un año resulta negativo, se considera igual a cero.

Bajo el Método Estándar, existe la posibilidad de compensación entre ingresos brutos positivos y negativos para distintas líneas de negocio en un mismo año. Sin embargo, esto no resulta posible entre ingresos brutos de distintos años. El Comité otorga explícitamente discrecionalidad nacional a los supervisores para adoptar:

- un métodos más conservador para el tratamiento de los ingresos brutos negativos de las líneas de negocio; y
- acciones supervisoras (incluidas en el Pilar II de Basilea II) o la utilización de consideraciones especiales al Método Estándar, ante cómputos nulos de capital por riesgo operacional.

Este método tampoco considera la posibilidad de calcular descuentos en los requerimientos de capital por el uso de seguros externos como mitigador de riesgo operacional.

Las exigencias del Método Estándar para estimar ingresos brutos por línea de negocio pueden resultar complejas para algunas instituciones; no obstante, según la opinión del Comité resulta en una metodología más sensible del verdadero perfil de riesgo de la institución, así como en una oportunidad para identificar sus actividades y/o productos más riesgosos.

Los porcentajes a aplicar a cada línea de negocios definidos por Basilea y adoptados por la CNBV, en el Anexo 12-A de la Circular Única son:

LÍNEA DE NEGOCIO Nivel 1	**SUB-LÍNEA DE NEGOCIO (ACTIVIDADES) Nivel 2**	**Grupo de Actividades Nivel 3**
Finanzas Corporativas β_j= 18%	Finanzas corporativas Finanzas de Administraciones locales/públicas Banca de inversión Servicios de consultoría	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, bursatilizaciones, servicio de estudios, deuda, acciones, sindicaciones, ofertas públicas iniciales, colocaciones privadas en mercados secundarios.
Negociación y ventas β_j= 18%	Compras y ventas Formación de mercado Posiciones propias Tesorería	Renta fija, renta variable, divisas, crédito, posiciones propias en valores, préstamo de valores, reportos y operaciones similares, operaciones financieras derivadas, intermediación y servicios adicionales, y deuda.
Banca minorista β_j= 12%	Banca minorista Banca privada o patrimonial Servicios de tarjetas	Créditos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarias. Créditos y depósitos de clientes de banca privada o patrimonial, servicios bancarios, fideicomisos y testamentarias, y asesoría de inversión. Tarjetas de empresa/comerciales, de marca privada y minoristas.
Banca comercial β_j= 15%	Banca comercial	Financiamiento de proyectos, bienes raíces, exportaciones, comercial, factoraje, arrendamiento financiero, préstamo, garantías, letras de cambio.
Pagos y liquidación β_j= 18%	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación.
Servicios de agencia β_j= 15%	Custodia Agencia para empresas Fideicomisos de empresas	Depósitos en custodia, certificados de depósito, operaciones de sociedades (clientes) para préstamo de valores. Agentes de emisiones y pagos.
Administración de activos β_j= 12%	Administración discrecional de fondos Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos, participaciones accionarias. Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable.
Intermediación minorista β_j= 12%	Intermediación minorista	Ejecución y servicio completo

III.3. Parámetros para la identificación de pérdidas

Los parámetros necesarios para identificar las pérdidas son:

- Severidad: Monto de las pérdidas.
- Frecuencia: Cantidad de veces que se repite el evento o la probabilidad de que ocurra.

Los datos internos son cruciales para la medición interna, los cuales muchas veces no son fáciles de obtener por lo que se dificulta la tarea.

Los beneficios que le aportan las bases de datos a las instituciones son, desde el punto de vista de la cultura, la conciencia de los costos del riesgo operacional; y en la gestión integral de riesgos, promueve un mayor análisis del origen de los riesgos.

Como los datos internos no contienen el rango completo de pérdidas, principalmente de los sucesos de las colas, son necesarios los datos externos.

A fin de generar la base de datos internos se requiere de políticas y procesos que garanticen la consistencia y veracidad de todos los datos. Dichas políticas deben ser claras y se deben aplicar consistentemente a través de sus productos, ubicación y categoría de riesgos. Los datos que superen determinado umbral, incluyendo pérdidas indirectas, *near miss* (casi-pérdidas) y costos de oportunidad, deben ser verificados e ingresados a las bases de pérdidas. Los cambios posteriores en los montos de pérdida, pagos posteriores de pólizas de seguro y reclamos de compensación adicionales, deben ser agregados en una forma auditable.

La inferencia estadística sobre las pérdidas esperadas y no esperadas, sólo es posible si se tiene un registro histórico riguroso de todos los eventos, sus causas y sus consecuencias. Es decir, requiere la creación e implantación de una base de datos que acopie las incidencias de naturaleza operacional y establezca el vínculo entre los factores de riesgo y los tipos de pérdida, además de que permita asignar los costos operativos a las unidades, a las líneas de negocio y a las de apoyo que contribuyan a ello.

La base de datos de pérdidas interna, es fundamental para la administración de riesgos operacionales de las instituciones bancarias, en especial para calibrar los modelos cuantitativos para el cálculo del capital económico.

Integrar la base de datos no es fácil debido a la renuencia a reconocer pérdidas por riesgos operacionales. Al interior de las instituciones, los problemas para identificar costos o pérdidas por riesgo operacional cuestionan la validez de la base de datos de incidentes de este tipo de riesgo para la estimación de las pérdidas.

La información que debe contener la base de datos de riesgos operacionales incluye:

- Aspectos cuantitativos como: el importe o costo de la pérdida (con un umbral eventual de corte), la fecha (aspecto importante donde pueden aparecer varias fechas: inicio, fin, identificación, etc.), entre otras.
- Descripción del evento: actividad, unidad de negocio, causa (distinguiendo entre los eventos de pérdida y los factores de riesgo), consecuencias (tipos de afectaciones que

pueden ser mayores que la pérdida directa, tales como la reputación, el rating, las reservas, etc.).

- Códigos identificadores: Del evento, de la unidad de negocio, de la actividad y/o de la causa.

Cuanto más completa sea la descripción de los eventos de pérdida de la base de datos, más fácil será adaptarla a cambios futuros, tanto del negocio como del regulador, por lo que, al registrarlos, es necesario describirlo, identificar las causas que lo provocaron, su impacto económico y, si es posible, las medidas para su mitigación.

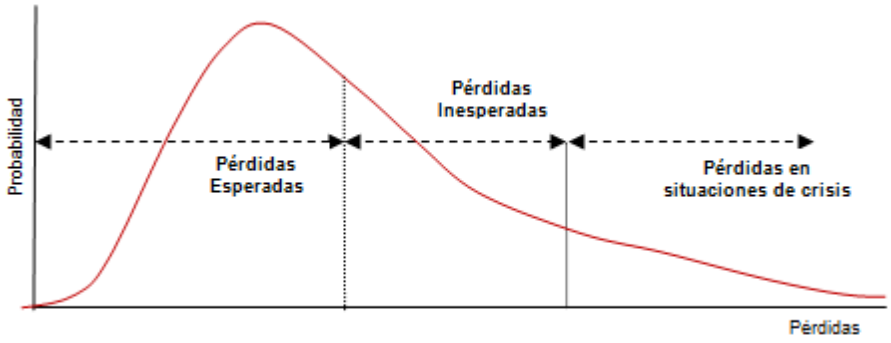
Un evento de pérdida es un incidente ocasionado por la materialización de un riesgo operacional que ocasiona una pérdida o ganancia, incurrida o por incurrir, directa (se identifica fácilmente en la contabilidad) o indirecta (está inmersa en los movimientos de las cuentas de la operación habitual u ocasiona un costo de oportunidad), o a un cambio en el valor de cualquier activo de la institución.

La información que se puede asociar claramente a incidentes de riesgo operacional puede estar en algunas cuentas contables como son: multas y recargos, quitas y castigos (cuando sea posible identificar que la causa de la pérdida se deriva de deficiencias en el proceso de crédito). Desafortunadamente, la mayoría de los costos causados por riesgos operacionales, están inmersos en los costos e ingresos normales de operación, por lo cual no es fácil identificarlos. Algunos ejemplos son: los errores humanos en las operaciones bursátiles, la reimpresión de documentos, el daño al equipo de transporte, etc.

Entre los beneficios de construir una base de datos interna destacan que:

- permite tomar conciencia de que las exposiciones al riesgo operacional pueden ser potencialmente negativas para la institución;
- el cuantificar la exposición ayuda a focalizar los recursos para su mitigación;
- al analizar las causas básicas de los eventos, los eventos aquellos que se repiten pueden indicar áreas de mejora.

Una vez que se cuente con bases de datos consistentes, el siguiente paso será determinar las funciones de densidad de mayor representatividad y precisión para estimar las pérdidas inesperadas (desviación estándar de las pérdidas) y de las pérdidas en caso de crisis (bajo supuestos de estrés, y de grandes pérdidas).



DISTRIBUCIÓN DE PÉRDIDAS POR RIESGO OPERACIONAL

Debido a que los estudios cuantitativos, basados en datos y experiencias, no tienen suficiente base estadística y no cubren las mejoras operativas, de procesos, de nuevas tecnologías, etc. que utilizan las instituciones de crédito en su supervivencia competitiva, es necesario que se apoyen en estudios cualitativos, de prevención de eventos de riesgo y de estimación subjetiva de los mismos.

Conforme se vaya incrementando la base de datos de la institución y se afinen en el diseño y control de los indicadores clave del riesgo operacional, las instituciones de crédito deben afinar sus sistemas de gestión del riesgo operacional, con el objeto de aproximarse al método AMA (Advanced Measurement Approach) para reducir los requisitos de capital regulatorio y obtener eficiencia en términos financieros y de gestión en general.

III.4. Método de Medición Avanzada (AMA)

La mayor novedad de Basilea II ha sido la aprobación de los modelos internos de medición del riesgo operacional de las instituciones para calcular los requerimientos de capital, previa aprobación del supervisor.

Es un enfoque más avanzado que el que se utiliza en riesgo de crédito. Las instituciones, al utilizar modelos internos de riesgo operacional, tienen la flexibilidad de usar el resultado de su propio modelo (diseñado según sus necesidades de gestión y experiencia propia) y no están obligadas a aplicar un modelo específico para la medición.

Para que las entidades puedan adoptar modelos avanzados (AMA) y obtener la aprobación del supervisor, Basilea II establece unos criterios generales cualitativos y cuantitativos muy rigurosos que deberán cumplir:

- Requiere la participación activa de la alta dirección y del consejo de administración en la gestión del riesgo operacional.
- El modelo interno debe ser sólido y estar plenamente integrado en los sistemas de medición y gestión de riesgos de la institución.
- La entidad debe contar con recursos suficientes tanto en las líneas de negocio como en las áreas de control y auditoría.

- Desde el punto de vista del supervisor, un requisito primordial en la validación de los modelos internos a efectos de capital, es la comprobación de que el modelo de medición sirve para la gestión activa del riesgo y que es utilizado diariamente por la organización. Es decir, en ningún caso será admisible un modelo cuya única finalidad sea el cálculo de los requerimientos regulatorios de capital.

Como el tratamiento del riesgo operacional es flexible, es imprescindible que las instituciones implanten y mantengan rigurosos procedimientos para la elaboración de sus modelos internos y que se efectúe una validación independiente a dichos modelos. Los requisitos cualitativos que debe cumplir la institución son:

- Contar con una unidad independiente de gestión del riesgo operacional responsable del desarrollo e implantación de la metodología de cálculo.
- El modelo interno de medición de riesgo operacional debe estar totalmente integrado en los procesos de gestión de riesgos de la entidad.
- Debe existir un sistema de información periódica a las direcciones de las líneas de negocio, a la alta dirección y al consejo de administración.
- El sistema debe estar suficientemente documentado.
- Debe ser validado interna y externamente.

En lo que se refiere a los requisitos cuantitativos, el Comité de Basilea no especifica el método o los supuestos sobre las distribuciones de probabilidad utilizados para medir el riesgo operacional a efectos de capital regulador, debido a la continua evolución de los métodos analíticos en su tratamiento y medición.

Sin embargo, la institución debe demostrar que el método utilizado identifica los eventos situados en las colas de la distribución de probabilidad y que le generan grandes pérdidas. Además, debe demostrar que su medida del riesgo operacional satisface criterios de solidez comparables, como son un horizonte temporal de un año y un nivel de confianza del 99.9%.

Los supervisores exigirán a las instituciones que el cálculo de su requerimiento de capital regulatorio sea la suma de la pérdida esperada y la inesperada, a menos que puedan demostrar que efectuaron la medición de la pérdida esperada y que la están cubriendo de alguna forma.

Requerimientos del método AMA:

- Establecer un **umbral mínimo** para la recopilación de datos de los eventos de pérdida (actualmente se ha adoptado como umbral €10,000 en Europa y USD $10,000 en los Estados Unidos).
- Documentar información sobre las **causas** de los eventos de pérdida.
- Tener criterios para la **asignación de pérdidas** entre las distintas áreas involucradas.

- Las **pérdidas operativas relacionadas con riesgo de crédito**, deberán considerarse en un solo tipo de riesgo (ya sea crédito u operacional).

Para estimar el capital por riesgo operacional, el segundo acuerdo de Basilea requiere que los métodos de medición avanzada incluyan al menos cuatro componentes (además de información interna):

- *Información externa*: Se deberá utilizar datos externos relevantes (públicos o agregados del sector bancario), especialmente si la institución pudiera estar expuesta a pérdidas poco frecuentes, pero graves.
- *Análisis de escenarios*: El banco deberá utilizar análisis de escenarios basados en opiniones periciales (de expertos) para evaluar su exposición a eventos que puedan ocasionar pérdidas muy graves.
- *Entorno del negocio y control interno*: Es necesario identificar aquellos que puedan modificar su perfil de riesgo operacional.
- *Cobertura del riesgo*: Los bancos pueden utilizar coberturas como seguros las cuales deben ser consideradas en el cálculo del capital.

La cuantificación permite integrar las etapas del proceso, otorgando mayor objetividad a la gestión del riesgo operacional y permitiendo una mayor eficacia en la asignación de recursos para minimizar el impacto de las pérdidas operativas.

Los dos primeros métodos de cálculo de capital establecidos en el segundo Acuerdo de Basilea (Métodos Básico y Estándar) no son sensibles al riesgo, ya que determinan los requerimientos de capital en forma simplificada a través del producto entre los ingresos brutos anuales medios y el coeficiente de exigencia de capital. Ambos métodos son cuestionados, ya que las entidades son penalizadas por el solo hecho de tener elevados ingresos brutos y porque el requerimiento de capital podría depender de las prácticas contables de cada país, posibilitando así el llamado arbitraje regulatorio. Cabe recordar que el ánimo de Basilea II es que estos métodos sean de transición mientras las entidades desarrollan métodos más avanzados.

En los AMA, el requerimiento de capital está determinado con la estimación real del riesgo operacional al que está expuesta la institución, por lo que se desarrollan modelos estadísticos de medición interna. Basilea II menciona la posibilidad de utilizar modelos internos siempre y cuando estén sujetos a la aprobación del supervisor así como con el cumplimiento de requerimientos cualitativos adicionales.

El utilizar los métodos AMA para calcular el requerimiento de capital por riesgo operacional, es similar al concepto de VaR (Valor en Riesgo o Value at Risk) aplicado a riesgo de mercado. Una vez estimada la distribución de pérdidas agregadas, Basilea requiere que el requerimiento de capital sea el que acumula el 99.9% de las pérdidas en un año. Es decir, la institución tiene que comprobar que cuenta con el capital suficiente para absorber las pérdidas que surjan en un periodo de un año en el 99.9% de los casos, arriesgándose a no cubrir en el 0.1% de los casos restantes, su capital.

Uno de los métodos internos de medición avanzada es el Loss Distribution Approach (LDA) o Enfoque de Distribución de Pérdidas, el cual es un modelo muy difundido para cuantificar el riesgo operacional. El modelo LDA es una herramienta estadística utilizada en el ámbito actuarial en la industria aseguradora, el cual se está convirtiendo en uno de los instrumentos más utilizados en el ámbito bancario.

El objetivo del método LDA es obtener la función de distribución agregada de pérdidas operacionales, la cual se obtiene de la acumulación de distribuciones de pérdidas para cada línea de negocio, tipo de riesgo o una combinación de ambas.

Para que los resultados que arroje el LDA tengan niveles de precisión aceptables, es necesario contar con:

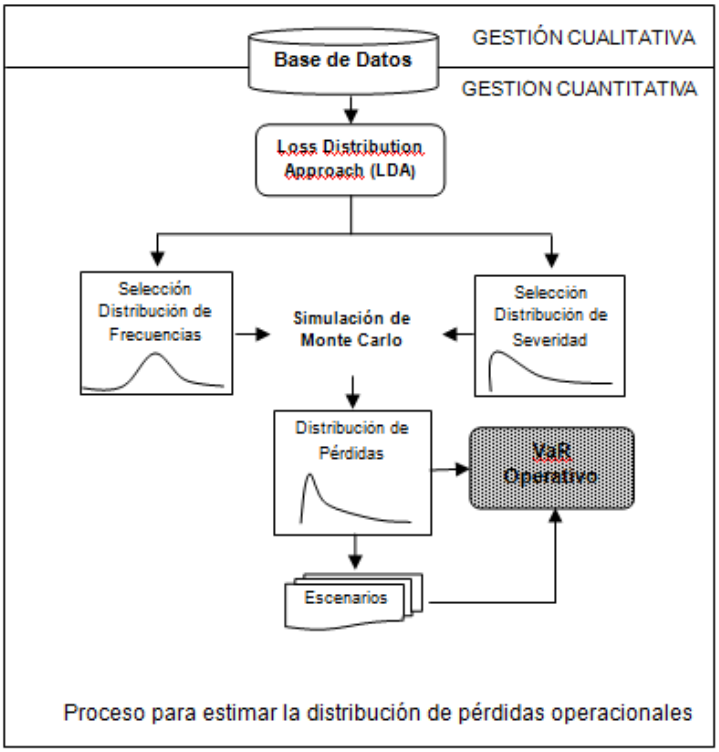
- Una adecuada selección de las distribuciones de frecuencia y severidad.
- Una apropiada parametrización de las distribuciones seleccionadas.

Cabe destacar que mientras más robusta sea la distribución de pérdidas (basada en agrupaciones con eventos de pérdida homogéneos), más precisas serán las distribuciones de pérdida que describen el perfil de riesgo, debido a la mayor homogeneidad de los eventos de pérdida dentro de cada grupo.

Los eventos de pérdidas operativas se pueden desagregar en dos componentes: la frecuencia, la cual representa todas las cantidades posibles de eventos con su respectiva probabilidad y la severidad o intensidad, que son todos los posibles valores de pérdida por evento y su probabilidad una vez ocurridos los eventos. Como ambos componentes tienen comportamientos específicos, en la distribución de probabilidades de pérdidas se pueden desagregar dichos componentes y basarse en la estimación separada de la frecuencia y severidad. Para juntar nuevamente ambos componentes y explicar el suceso de las pérdidas operativas, es necesario utilizar métodos de simulación Montecarlo.

Para calcular tanto la distribución de frecuencia como la distribución de severidad, es necesario estimarlas con base en las pérdidas operativas observadas en la institución y registradas en su base de datos de pérdidas.

El proceso para estimar la distribución de pérdidas operacionales se sintetiza en la siguiente figura:



Proceso para estimar la distribución de pérdidas operacionales

El modelo LDA se establece sobre la información de pérdidas históricas, registradas en base a la matriz que conforman las ocho líneas de negocio y los siete tipos de riesgos estandarizados por el Comité. A la relación entre procesos operativos y factores de riesgo se le conoce como mapa o matriz de riesgos operacionales. El siguiente diagrama es un ejemplo de esta matriz:

							Procesos operativos
							Tecnología
							Personal
							Factores externos
Función 1	Función 2	Función 3	Función 4	Función 5	.....	Función N	

Proceso α
Proceso β
.....
Proceso £
Área 1
Área 2
Área N

Para cada una de las 56 casillas, se deben estimar la distribución de frecuencia y la de severidad; el siguiente paso es obtener la distribución de pérdidas agregadas por riesgo operacional adscrita a cada celda. Para calcular el capital regulatorio vinculado a cada casilla, se utiliza la idea de Valor en Riesgo de riesgo operacional (OpVaR).

III.5. Value at Risk (VaR)

El uso de las metodologías tipo VaR es el común denominador de los modelos avanzados, que define el capital regulatorio como un determinado percentil de la distribución de pérdidas.

El Value at Risk o Valor en Riesgo (VaR) es una medida de riesgo de tipo estadístico que tiene como objetivo calcular la pérdida máxima en un horizonte temporal determinado con una cierta probabilidad; proporciona una medida homogénea del riesgo asumido; y, considera todos los factores de riesgo dando como resultado un único dato que sirve para la comparación. Los dos factores que considera son:

1) Nivel de confianza: Es una elección arbitraria, aunque la mayoría de las instituciones financieras opta por elegir un nivel entre el 95% y 99.9%. Cuanto mayor el nivel de confianza, menor el margen de error.

2) Intervalo de tiempo: Puede variar entre un día hasta un año. Para elegir el intervalo se debe tener en cuenta la frecuencia con la que varía el portafolio o en el caso de riesgo operacional, el tiempo necesario para mitigarlo. Para su elección se debe tener en cuenta el menor de los siguientes:

   - El período de tiempo necesario para liquidar una cartera (Riesgo de Mercado).
   - El período de tiempo necesario para cubrir una cartera (Riesgo de Crédito).
   - El período de tiempo necesario para cambiar los sistemas o procesos de control (Riesgo Operacional).

Para el riesgo de mercado, el Comité de Basilea recomienda un 99% (1% de probabilidad, lo que equivale a –2.33 desviaciones estándares) a 10 días. Sin embargo, RiskMetrics recomienda un 95% (5% de probabilidad, lo que equivale a -1.65 desviaciones estándares) a un día.

En el caso de los riesgos de mercado y de crédito, la metodología proporciona una medida del riesgo en condiciones normales de mercado, es decir, cuando no existen en el mercado “escenarios turbulentos” económicos y financieros. De manera gráfica, en un histograma se puede observar la distribución de densidad de la serie de retornos del portafolio, los cuales fluctúan en torno a la media que es distinta de cero y la distribución se realiza aproximadamente en forma normal, ya que se asume simetría en la misma.

Además, se determina el punto de la función de densidad que deja un 1% o un 5% del área en su rango inferior. La distancia entre ese punto y la media es el VaR.

En respuesta a los grandes desastres financieros ocurridos en los años 90, se desarrolló el VaR y su popularidad se debió a tres factores básicamente: la presión de los organismos reguladores, la globalización de los mercados financieros y los avances

tecnológicos. A partir de 1995, el Comité de Basilea recomienda a los bancos el uso del VaR con el fin de calcular sus requerimientos de capital por riesgos de mercado.

La importancia del VaR radica en que permite medir el riesgo de diferentes instrumentos financieros (divisas, instrumentos de renta fija y de renta variable, opciones, etc.) que conforman un portafolio; y constituye un gran avance con respecto a las medidas tradicionales como la duración para instrumentos de renta fija.

Existen tres formas de calcular el VaR, cada una con sus ventajas y desventajas; cada una presenta un trade-off entre exactitud y rapidez. Dichas formas de cálculo son: el método histórico (metodología de simulación), la metodología paramétrica y el método de simulación de Montecarlo.

En el Nuevo Acuerdo de Basilea se exige a las instituciones medir, controlar y gestionar el riesgo operacional, de tal forma que el VaR es la piedra angular para calcular el Capital Económico en Riesgo (CaR). De tal manera, que la fórmula para calcular el CaR incluye el requerimiento de capital por riesgo operacional, que sumado a los requerimientos por riesgo de crédito y de mercado es la siguiente:

$$\frac{\textit{Capital Regulatorio}}{\textit{Activos ponderados Riesgo de Crédito} + 12.5\ (\textit{Riesgo Mercado} + \textit{Riesgo Operacional})} \geq 8$$

Anteriormente, el riesgo operacional se definía como todo aquello que no era ni riesgo de crédito ni riesgo de mercado. Dicho riesgo abarca diferentes situaciones desde fraudes hasta riesgos como el tecnológico, por lo cual, dada su heterogeneidad, es muy difícil su control y gestión.

IV. Distribuciones de probabilidad para la frecuencia y la severidad de los eventos de pérdida por riesgo operacional

Una vez conformada la base de datos interna y considerando todas las fuentes de información, se procede a seleccionar las distribuciones de frecuencia y severidad que mejor se ajusten a los datos.

El objetivo es modelar la función de distribución de las pérdidas operativas para cada tipo de evento y línea de negocio durante un periodo de tiempo determinado, para lo cual se llevan a cabo las siguientes etapas:

- Modelación de la función de distribución de la frecuencia de ocurrencia de los eventos operacionales.
- Modelación de la función de distribución de los impactos o pérdidas económicos por evento (severidad de las pérdidas).
- Obtención de la distribución agregada de pérdidas operacionales para dicho evento/línea de negocio. El cálculo del VaR es una de las tareas más difíciles en la administración del riesgo operacional y consiste en estimar el nivel apropiado de capital para cubrir las pérdidas no esperadas.

IV.1 Principales distribuciones para modelar la frecuencia

Para modelar la frecuencia de eventos en un horizonte determinado, se utiliza una distribución de conteo que explica la probabilidad de ocurrencia de una determinada cantidad de eventos para dicho horizonte a partir de las pérdidas registradas por la entidad. Por lo general, se utiliza la distribución Poisson, ya que por sus características permite establecer apropiadamente el número de eventos a partir de la media de la frecuencia de eventos observados en el pasado.

La función de densidad Poisson es:

$$f(x) = \frac{e^{-\lambda}\lambda^{x}}{x!}, \qquad x = 0, 1, 2, \ldots. \quad \lambda > 0$$

Donde,

λ es la esperanza de la distribución y representa el número esperado de eventos de pérdida (observados o estimados) en un día, mes o año.

Para ajustar la distribución del número de pérdidas por periodo, se utiliza la información de las pérdidas observadas y registradas en la institución.

La distribución Binomial Negativa se utiliza mucho en el modelado de eventos de pérdida por periodo, ya que debido a que depende de dos parámetros (p y r), tiene más flexibilidad que la distribución Poisson.

Su función de densidad es:

$$f(x) = p^r \binom{x+r-1}{r-1} q^x$$

Donde,

$$q = 1 - p$$

La distribución Binomial tiene la función:

$$f(x) = \binom{n}{x} p^x q^{n-x}$$

Donde,

n es el número de riesgos sujetos a un cierto evento de pérdida

p es la probabilidad de ocurrencia del evento de pérdida que se calcula

$$p = \frac{\text{Núm. eventos observados}}{\text{Máximo número de eventos posibles}}$$

Después de estimar la distribución de frecuencia, se procede a estimar la distribución del monto de las pérdidas (severidad) de los eventos, para lo cual es necesario analizar la base de pérdidas operacionales para "ajustar" la distribución paramétrica que mejor se adapte a los datos observados de montos de pérdidas.

IV.2 Principales distribuciones para modelar la severidad

La distribución que se ajuste para modelar el impacto económico o severidad de las pérdidas por riesgo operacional, debe reflejar la probabilidad de que ocurra un evento de pérdida de una magnitud específica.

Para estimar la severidad de las pérdidas, generalmente se ajusta una distribución continua que es independiente de la distribución de la frecuencia de los eventos de pérdida.

La distribución más utilizada para estimar la severidad de las pérdidas, es la Lognormal cuya función de densidad es:

$$f(x) = \frac{1}{x\beta\sqrt{2\pi}}\, e^{-\left(\frac{1}{2\beta^2}\right)(\log x - \log\alpha)^2}$$

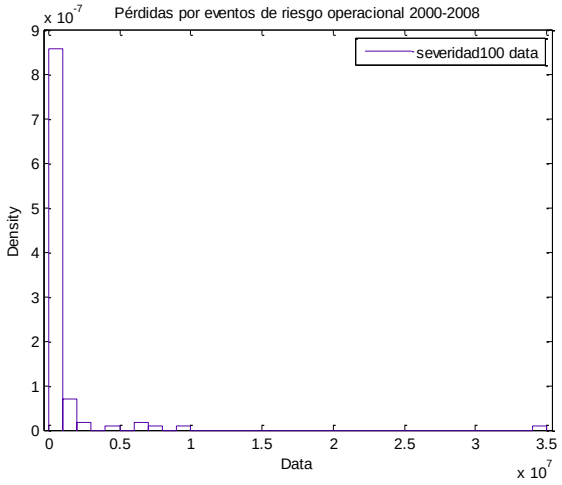
Además de utilizar la distribución Lognormal, también es frecuente el uso de la distribución Exponencial, que está dada por la función:

$$f(x) = \frac{e^{-x/\lambda}}{\lambda}, \qquad 0 < x < \infty, \quad \lambda > 0$$

Otras distribuciones utilizadas para modelar la severidad de las pérdidas son la Normal, Normal Inversa, Pareto, de Valores Extremos, entre otras.

IV.3 Teoría de Valores Extremos

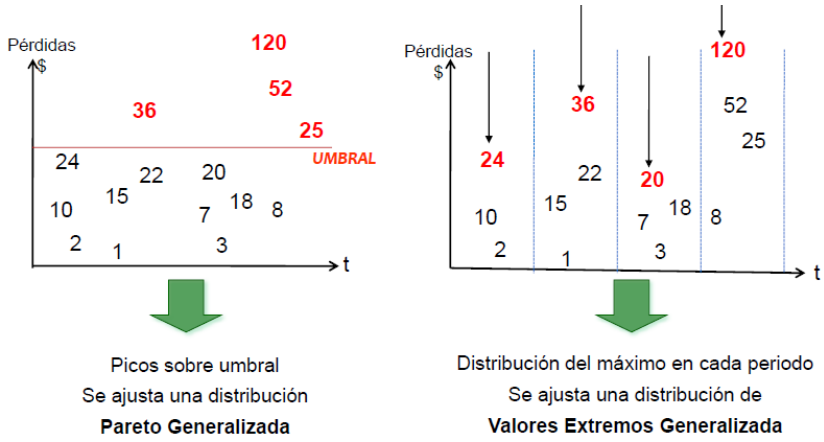
La información de pérdidas en eventos por riesgo operacional, frecuentemente tiene observaciones extremas.



Para la modelación de la severidad de las pérdidas por riesgo operacional, se ha aplicado la Teoría de Valores Extremos (TVE), debido a que:

- Da herramientas para realizar estimaciones confiables de la posibilidad de ocurrencia de eventos que nunca se han observado en el pasado.
- Se usa en la teoría de la credibilidad, seguros y monitoreo ambiental, entre otras aplicaciones.
- Basilea II establece que el VaR operacional (anual) debe calcularse al 99.9% de confianza, por lo que sólo se dejan fuera los eventos que pueden ocurrir una vez cada 1,000 años (0.1% = 1/1,000).
- En este cálculo las pérdidas muy altas pero de frecuencia muy baja son relevantes.

Hay dos formas básicas de aplicar la TVE a la modelación de la severidad de los eventos de pérdida:



Las dos técnicas para modelar valores extremos son: la primera denominada *excesos sobre un umbral*, en la cual se modelan todas las observaciones grandes que exceden un umbral dado (generalmente alto); el método discrimina menos datos (de por sí escasos) y se considera muy útil en aplicaciones prácticas. Están relacionados con las DGP, cuya forma estándar está dada por:

$$W\gamma\,(x) = 1 - (1 + \gamma x)^{-1/\gamma}$$

Donde,

Si $x > 0$ y $\gamma = 0$, la distribución es exponencial;

Si $x > 0$ y $\gamma > 0$, la distribución es Pareto; y

Si $0 < x < (1/|\gamma|)$ y $\gamma < 0$, la distribución es Beta.

La segunda técnica denominada *máximo por bloques*, que implica recoger sólo las observaciones mayores para un periodo dado y supone grandes muestras idénticamente distribuidas. Este método discrimina una gran cantidad de datos y está relacionada con las Distribuciones Generalizadas de Valores Extremos (DVE), cuya forma estándar está dada por:

$$G\gamma\,(X) = e^{-(1+\gamma x)^{-1/\gamma}} \quad ; \qquad 1+\gamma x > 0,\ \gamma \neq 0$$

Donde,

Si $\gamma = 0$, la distribución es Gumbel estándar;

Si $\gamma > 0$, la distribución es Fréchet; y

Si $\gamma < 0$, la distribución es Weibull.

El objetivo es modelar las máximas observaciones en una muestra de variables aleatorias, que se estandarizan por:

- Ubicación con el parámetro μ
- Escala con el parámetro ψ
- Forma con el parámetro ξ

Los parámetros se ajustan para obtener una distribución apropiada para los extremos.

Algunos autores hablan del uso de distribuciones "mixtas" para también considerar los potenciales eventos de pérdidas ubicados en la "cola" de la distribución. Es decir, se puede utilizar una distribución para modelar el cuerpo y otra para la cola, pero debido a que aún no se estima un modelo sencillo en México, este tipo de mezclas no se presentan en este trabajo. Es preferible comenzar a calcular las pérdidas totales anuales y el VaR de riesgo operacional con métodos más sencillos, sin dejar de ser un método avanzado.

IV.4 Modelo de distribución de probabilidad de pérdidas totales por riesgos operacionales

Para obtener la distribución agregada o de pérdidas totales, se tienen que modelar tanto la frecuencia como la severidad de las pérdidas registradas en la base de datos.

Modelar la frecuencia es más fácil y se basa principalmente en los datos internos, pero hay que vigilar los datos recientes ya que el perfil de riesgo pudo haber cambiado. El modelado de la severidad es el tema clave, en particular, por las colas de las distribuciones.

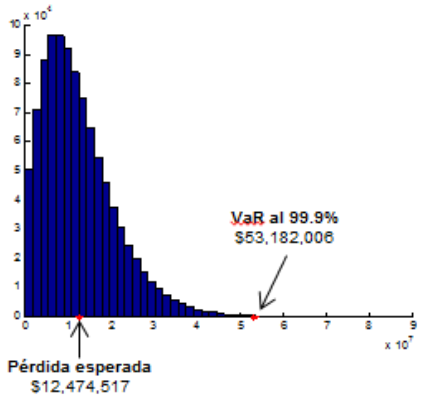
IV.4.1. Procedimiento para modelar la distribución de probabilidad de pérdidas totales

Se realizan pruebas de bondad de ajuste a las distribuciones de frecuencia y severidad que se ajustan a la base de datos de pérdidas por riesgos operacionales y se seleccionan las mejores en cada caso para generar la distribución de pérdidas totales por riesgos operacionales mediante el método de simulación Montecarlo, técnica que consiste en la repetición del siguiente algoritmo:

1. Extracción de un número *n* de eventos por año de la distribución de frecuencia (por ejemplo, Poisson).
2. Extracción de *m* números $\{m_1, m_2, \ldots, m_n\}$ aleatorios de la distribución de monto de pérdidas por evento (por ejemplo, Lognormal).
3. Se calcula la sumatoria de los *m* números y se sitúa el resultado en el histograma (distribución empírica de probabilidad) de las pérdidas anuales por riesgo operacional.
4. Se repiten los pasos 1. a 3. un número grande de veces (algún múltiplo de 1,000).

5. El histograma que resulta de estas repeticiones es la distribución de probabilidad de las pérdidas anuales por riesgo operacional.

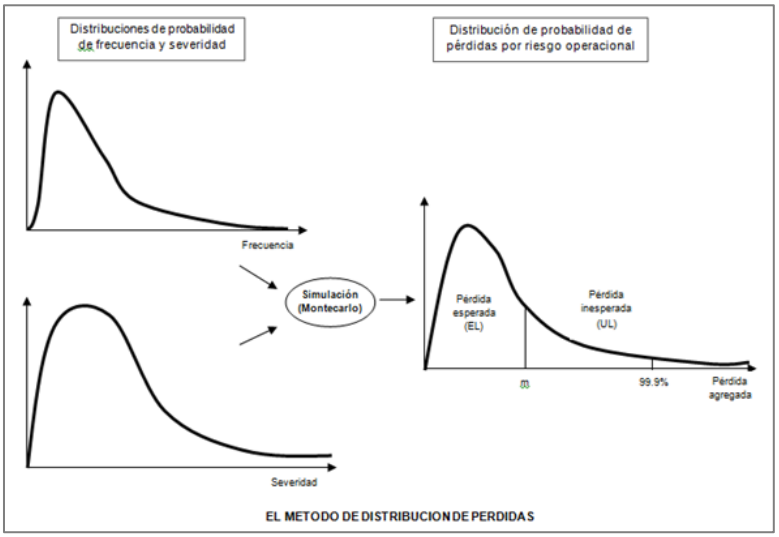
   El cuantil 99.9% de esa distribución es el VaR por riesgo operacional estimado con ese nivel de confianza.



El VaR por riesgo operacional debe calcularse según el período establecido (generalmente anual) y cada vez que se exceda el límite superior de tolerancia global, ya que indicaría que la institución se está exponiendo con mayor frecuencia a riesgos que le pueden causar grandes pérdidas.

El proceso anterior estima la distribución de pérdidas utilizando un número suficiente de escenarios hipotéticos, generados aleatoriamente, a partir de las estimaciones de las distribuciones de frecuencia y severidad.

Cada una de las repeticiones, simulaciones o escenarios hipotéticos, representa las pérdidas operativas para el periodo fijado como horizonte de tiempo. La cantidad de repeticiones o iteraciones debe ser elevada con la finalidad de lograr estabilidad en los resultados de las simulaciones y así construir la distribución de pérdidas anuales por riesgo operacional.



El uso de la distribución de pérdidas de riesgo operacional da como resultado la estimación de la pérdida esperada y los requerimientos de capital necesarios para hacer frente a este tipo de riesgos.

La pérdida esperada representa, básicamente, los eventos de alta frecuencia y baja severidad (se considera como un costo continuo y debe reflejarse en la contabilidad). La pérdida no esperada es la diferencia entre un determinado cuantil y la pérdida esperada, y tiene que ver con los eventos de baja frecuencia y alta severidad (estas pérdidas se compensan con las reservas de capital o seguros).

Las pérdidas catastróficas o stress loss son las pérdidas mayores a la pérdida inesperada. Son raras pero de altísimo impacto para la entidad. Por ejemplo, los casos de Barings o el incendio del Credit Lyonnais; por su naturaleza se hacen públicos y no se pueden cubrir con capital de la entidad (pérdida excesivamente grande), por lo que de ser posible se recurre a seguros (otro problema del riesgo operacional: tiempo que pasará hasta cobrar).

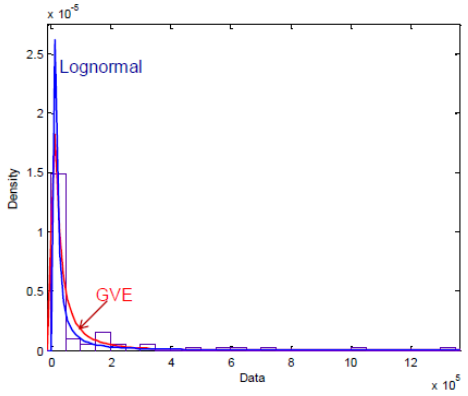
Como se puede inferir, la cuantificación del riesgo operacional es una fuente inagotable de problemas estadísticos interesantes. Además de los ya mencionados, se pueden mencionar la dificultad de contar con datos relevantes para la estimación (datos que provienen de diversas fuentes, con diferentes umbrales, …), la problemática del cálculo de correlaciones y la incorporación de las técnicas de mitigación del riesgo en el modelo.

No se debe olvidar que el campo de los modelos internos de medición del riesgo no es una ciencia exacta y que la metodología de medición no es una finalidad en sí misma, sino una herramienta más que debe servir al sistema de gestión de la institución y, en este sentido, debe ayudar al control y a la mitigación del mismo.

IV.4.2. Pruebas de bondad de ajuste de las distribuciones

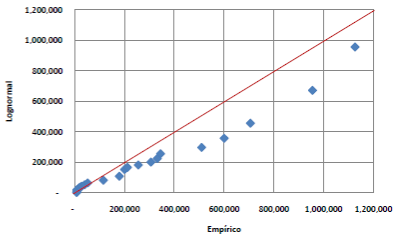
Las pruebas que se utilizan para validar los ajustes de las distribuciones pueden ser gráficas y analíticas. La prueba gráfica que tiene gran credibilidad es la gráfica cuantil-cuantil ó q-q y la prueba formal es la X^2 de Pearson.

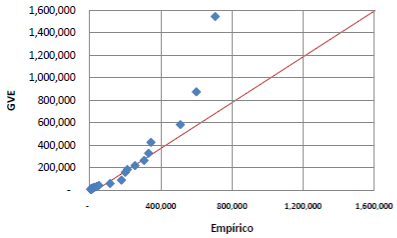
La gráfica q-q consiste en graficar los cuantiles empíricos vs los cuantiles de la distribución ajustada a los datos; si la distribución se ajusta bien a los datos se acercará a una línea de 45°. Un ejemplo de bondad de ajuste se presenta con las distribuciones Lognormal y GVE:



Gráficamente,

El ajuste de la distribución lognormal tiende a dar menos probabilidad en la cola de la distribución, es decir, decae a cero más rápidamente que los datos empíricos.





La distribución GEV tiende a dar mucha mayor densidad en la cola de la distribución que la observada en la información empírica.

En el caso de la prueba X^2 de Pearson, es particularmente útil para distribuciones discretas. Se contrastan las hipótesis:

H_0: La frecuencia de los eventos sigue la distribución adoptada.

H_1: La frecuencia de los eventos no sigue la distribución.

La estadística de prueba es:

$$\chi^2 = \sum_{k=1}^{K} \frac{(n_k - n_k^*)^2}{n_k^*}$$

Donde:

η_k es la frecuencia observada

η^*_k es la frecuencia estimada (el valor esperado)

El valor que se obtiene se compara contra el cuantil correspondiente al nivel de significancia deseado de una distribución X^2 con k-1 grados de libertad. Si es mayor, se debe rechazar el modelo.

V. Caso práctico

Como ya se vio a lo largo de este trabajo, la base de datos interna es el punto clave para la medición y gestión del riesgo operacional, por lo que es necesario recolectar la información útil para ambos casos:

- Las líneas y sub-líneas del negocio y los tipos y subtipos de riesgos (Anexo 12-A de la Circular Única de Bancos); y
- Causas, consecuencias, factores, etc.

Otra información necesaria para ajustar las distribuciones son las fechas y los montos de las pérdidas. También se deben tener en cuenta las frecuencias y severidades "reales", la opinión de los expertos y el análisis de escenarios incluyendo los extremos.

Uno de los principales requerimientos de Basilea II, es el uso de datos externos para completar la falta de eventos de alta severidad y baja frecuencia en la base de datos interna, pero debido a que en México no existen organizaciones o consorcios que se dediquen a la recolección de datos de alta calidad para su intercambio con todas las entidades bancarias del país (como la ORX en Europa), para la realización del presente trabajo solo se utilizaron los datos recolectados en la institución. Cabe aclarar que este es un ejercicio inicial para el análisis y conformación de la base de datos, pero que sirvió para desarrollar un primer modelo para la distribución agregada de pérdidas y el cálculo del VaR por riesgo operacional.

Por otro lado, Basilea II señala que se debe establecer un umbral mínimo adecuado de pérdidas brutas para la recopilación de datos internos de pérdida, por ejemplo se adopta con frecuencia, 10,000 euros para el caso de Europa y de 10,000 dólares para Estados Unidos. Probablemente este umbral ya no es adecuado y es demasiado alto para muchas instituciones de otras partes del mundo, por lo que la recolección de datos la están haciendo a partir de umbrales muy inferiores. En México, los reguladores no han establecido un umbral mínimo para la recolección de la información.

V.1 Depuración de la Base de Datos Interna

Para conformar la base de datos interna de eventos de pérdida por riesgos operacionales, se analizaron los incidentes que se presentaron durante el periodo comprendido del 1° de enero de 2000 al 31 de diciembre de 2008 de una institución bancaria. Para proteger la confidencialidad de la información de la institución, los datos se transformaron aplicándoles un factor aleatorio; asimismo, para poder comparar la información desde su inicio a la fecha de cálculo, se actualizó cada monto a valor presente utilizando la inflación anual acumulada por año.

Antes de trabajar con la base de datos, se hizo un análisis profundo para separar los eventos cuyo origen se debía a un riesgo operacional y se eliminaron los que se demostró o consideró que eran derivados de riesgos de mercado, crédito o cualquier otro diferente a riesgo operacional. No es una tarea fácil discriminar el origen de los eventos; sin embargo, la experiencia de los dueños de los negocios es la clave para lograr una buena identificación y clasificación.

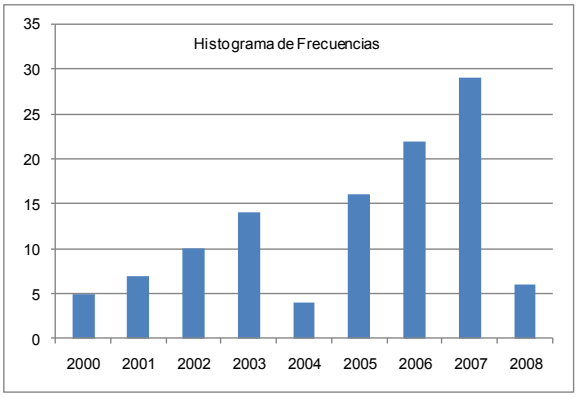
La base de datos original tenía 549 eventos de pérdida. El umbral mínimo que se fijó para la recopilación de datos fue de $100,000.00, razón por la que la base de datos quedó con 113 eventos que se utilizaron para desarrollar el modelo (Anexo1).

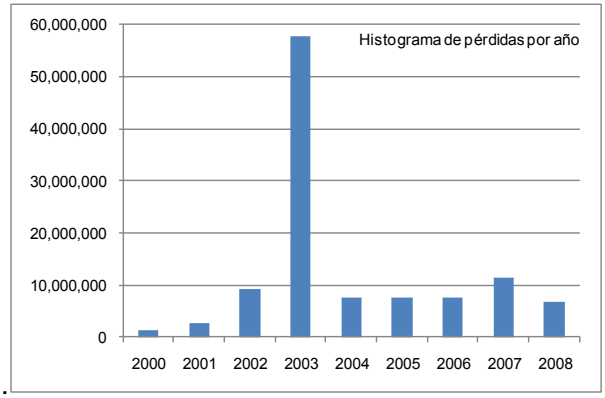
Por no contar con bases de datos externas y no tener acceso al personal para realizar cuestionarios de autoevaluación, únicamente se utilizaron los datos internos registrados por la institución.

Las pérdidas por año fueron las siguientes:

Año	Eventos por año	Pérdidas anuales
2000	5	$1,336,821
2001	7	$2,658,074
2002	10	$9,349,355
2003	14	$57,593,398
2004	4	$7,559,167
2005	16	$7,667,201
2006	22	$7,644,790
2007	29	$11,439,877
2008	6	$6,909,184
TOTAL	**113**	**$112,157,867**

A continuación se muestran la frecuencia y la severidad de los datos de pérdida de la base de datos del estudio, antes de ajustarle cualquier distribución:





Para hacer los ajustes de las distintas funciones de distribución de la frecuencia y la severidad de las pérdidas, se utilizó el software Matlab.

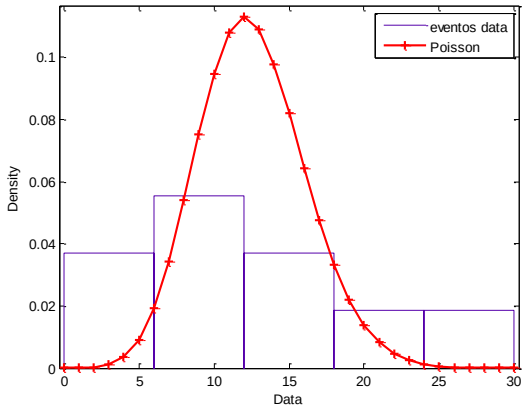
V.2 Modelo *plain vanilla*

La probabilidad de que en un periodo de tiempo se presenten cierto número de eventos se puede estimar con la distribución empírica del número de incidentes por periodo (frecuencia). Por otro lado, la probabilidad de que ocurra un evento de pérdida de una magnitud específica está dada por la distribución del impacto económico (severidad).

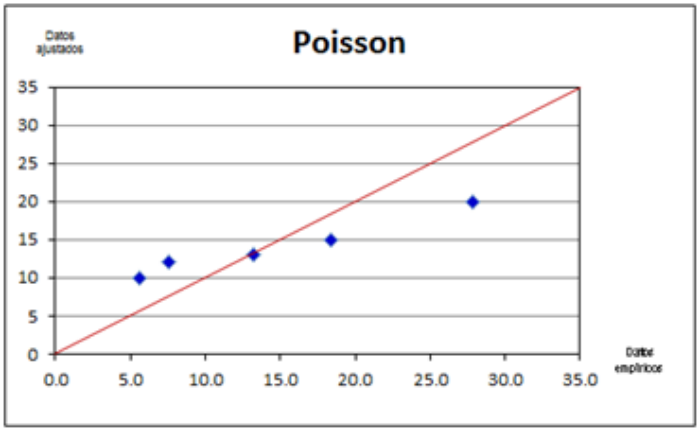
Antes de utilizar un modelo complejo, se ajustó el modelo más sencillo conocido como *plain vanilla*, que consiste en ajustar una función Poisson al número de incidentes de riesgo operacional por periodo, ya que su función de densidad depende de un solo parámetro λ que es el número promedio de eventos de pérdida (observados o estimados) en un día, mes o año; y la Lognormal para calcular la probabilidad de que ocurra un evento de pérdida de una magnitud específica, es decir, para la severidad de los eventos de pérdida.

Generalmente, se ajusta una distribución continua para la severidad y se asume que es independiente de la distribución de la frecuencia de los eventos de pérdida.

Al ajustar la distribución Poisson a los 113 datos, se obtuvo que la media, la desviación estándar y lambda (λ) tienen un valor de 12.5556. La gráfica es la siguiente:

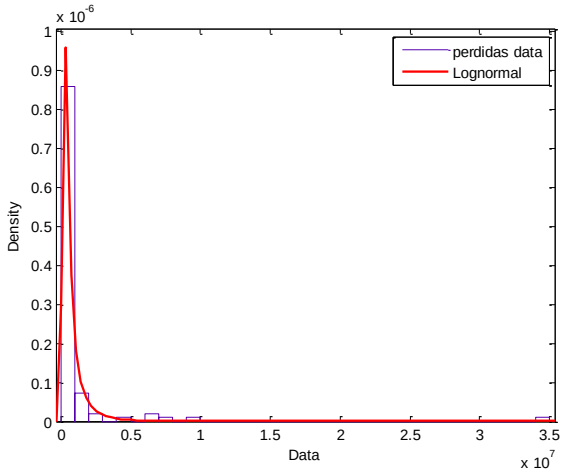


Se observa que la Poisson le da peso bajo a los datos representados en las columnas 4 y 5 ya que decrece rápidamente hacia el eje horizontal, lo que significa que no le da peso a la “cola” de la distribución. Para corroborar qué tan bueno es el ajuste de la distribución, se hizo la prueba de la gráfica cuantil-cuantil o q-q, que consiste en graficar los cuantiles de los datos empíricos contra los cuantiles de los datos de la distribución ajustada; en este caso, la Poisson. Cuando los datos se ajustan bien a la distribución, se acercan a una línea de 45°.



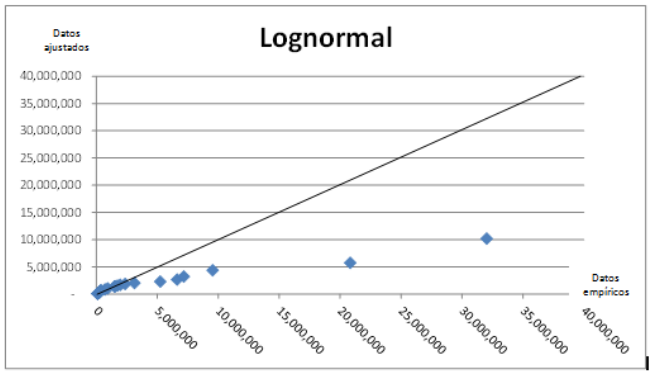
En la gráfica q-q se observa que no hay un buen ajuste, ya que el modelo Poisson no le da peso a los datos grandes que están en la "cola" de la distribución porque están por debajo de la recta. Cuando los datos grandes están por encima de la recta, se puede decir que la función de distribución si le da peso a la "cola".

Continuando con el *plain vanilla*, se ajustó la distribución Lognormal a los 113 montos de las pérdidas y los parámetros que se obtuvieron fueron μ = 12.6967 y sigma = 1.11298, mientras que la media = 606,883 y la varianza = 9.02796 x $10^{11.}$



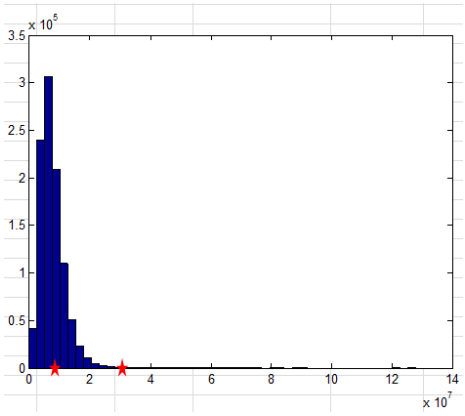
Se observa que la distribución Lognormal no le da peso a la "cola" ya que se pega rápidamente al 0, aunque si le da mucho peso a las pérdidas pequeñas.

La gráfica q-q de la Lognormal se presenta a continuación:



Se puede apreciar que, como en el caso de la Poisson, el modelo Lognormal no le da peso a la "cola" de la distribución porque los datos se ubican por debajo de la recta de 45°.

A continuación, mediante un proceso de simulación MonteCarlo, se generó la distribución de probabilidad de las pérdidas totales anuales y el VaR por riesgo operacional con el software Matlab utilizando los parámetros obtenidos de las distribuciones Poisson y Lognormal.



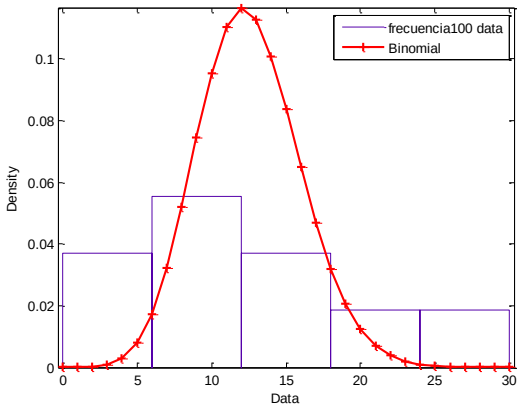
Histograma de pérdidas totales anuales

La pérdida esperada anual que se obtuvo fue de $7,615,286.39 y el VaR (Valor en Riesgo) por riesgo operacional de $31,625,333.77, generados con 1,000,000 de simulaciones y un nivel de confianza del 99.9% como lo establece Basilea II en su documento. Lo anterior quiere decir que un evento con estas pérdidas se puede presentar una vez cada 1,000 años.

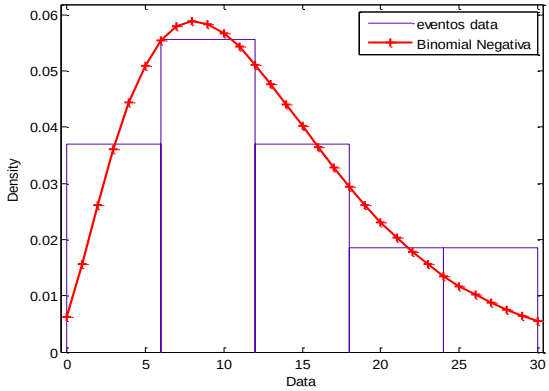
Al analizar las gráficas de las distribuciones y las gráficas q-q, se puede ver que el *plain vanilla* no es una buena opción como modelo para el cálculo de las pérdidas totales anuales y del VaR por riesgo operacional, ya que no hay un buen ajuste de los datos en las "colas" de las distribuciones para la frecuencia y la severidad de los eventos de pérdidas ni se ajustan a la recta de 45° en las gráficas q-q, por lo que se buscaron otros modelos que se ajustaran mejor a la información de la base de datos del caso de estudio.

V.3 Ajuste de la distribución de la frecuencia de los eventos de pérdida

En el capítulo III, se mencionaron las distribuciones más utilizadas para modelar la frecuencia, además de la Poisson, por lo que se hicieron ajustes para la frecuencia con las distribuciones Binomial y Binomial Negativa. Las gráficas y los parámetros obtenidos son los siguientes:



Binomial
Umbral = 100,000
N = 200 p = 0.0627778
Log. de verosim. = -422.178



Binomial Negativa
Umbral = 100,000
r = 3.18237 p = 0.20221
Log. de verosim. = -30.2039

A simple vista se observa que la distribución Binomial Negativa se ajusta mejor a los datos, ya que le da peso a la mayoría de los datos del histograma, lo que da posibilidad de que ocurran muchos eventos en un periodo de tiempo y no converge tan rápido al 0 como en el caso de la Poisson y de la Binomial que son muy parecidas. Además, como la Binomial Negativa depende de dos parámetros (p y r), tiene más flexibilidad que una distribución Poisson.

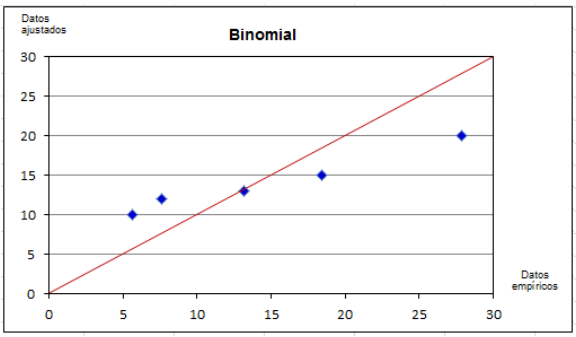
Para corroborar la apreciación anterior, se elaboraron las gráficas q-q donde también se observa que en la función Binomial Negativa hay un mejor ajuste, ya que los puntos se pegan más a la recta de 45°, lo que significa que le está dando peso adecuado a la "cola" de la distribución.

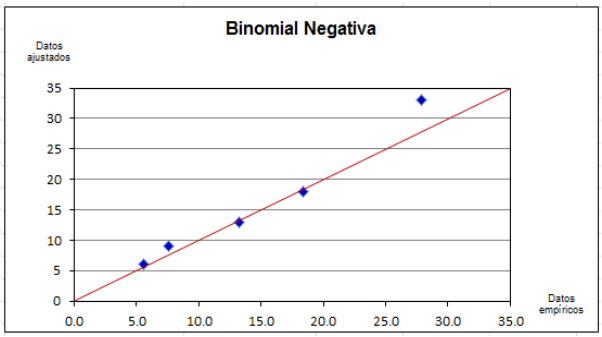
Cabe aclarar que los datos empíricos de los cuantiles se obtuvieron con Excel y los datos ajustados con Matlab, calculando la función acumulada de cada distribución.

Cuantiles de la frecuencia

		Ajustados		
Probabilidades	Empírico	Poisson	Binomial	Bin. Neg
0.2	5.6	10	10	6
0.4	7.6	12	12	9
0.6	13.2	13	13	13
0.8	18.4	15	15	18
0.98	27.88	20	20	33

Las pruebas q-q se hicieron graficando los datos empíricos contra los datos ajustados de cada distribución que se probó.



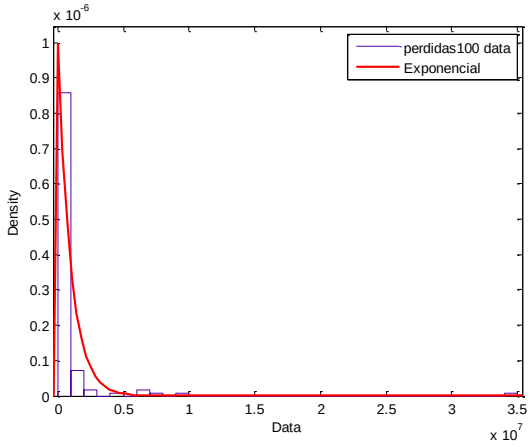


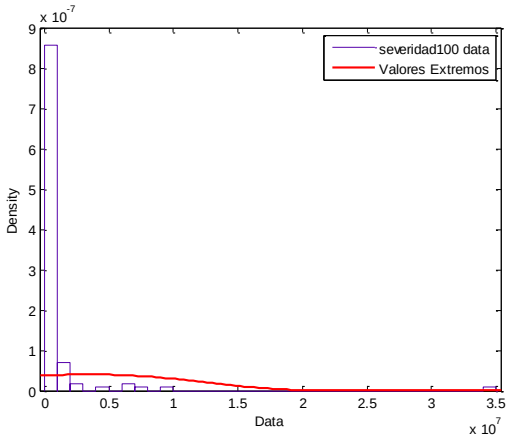
Al analizar las dos pruebas anteriores, la distribución y la gráfica q-q, se decidió que el modelo estará formado por la distribución Binomial Negativa para los datos de la frecuencia de las pérdidas.

V.4 Ajuste de la distribución de la severidad de los eventos de pérdida

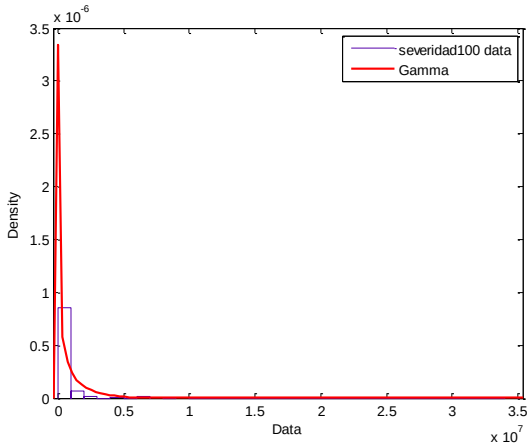
Para modelar la severidad de las pérdidas, además de la distribución Lognormal se ajustaron otras distribuciones como la Exponencial, la Gamma, la de Valores Extremos y la Pareto Generalizada, entre otras. A continuación se muestran las gráficas de algunas de estas distribuciones para tener una idea visual de cuál o cuáles son las que mejor modelan la base de datos de las pérdidas.

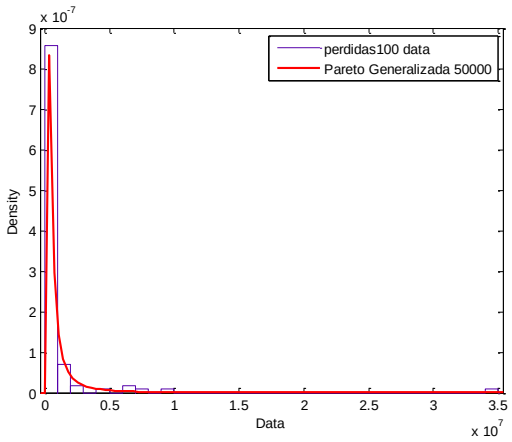
Al ajustarse la distribución Exponencial (gráfica izquierda) a las pérdidas, se observa que ésta converge rápidamente a 0, sin darle peso a las pérdidas extremas que se encuentran en la parte derecha de la gráfica o de la “cola”.



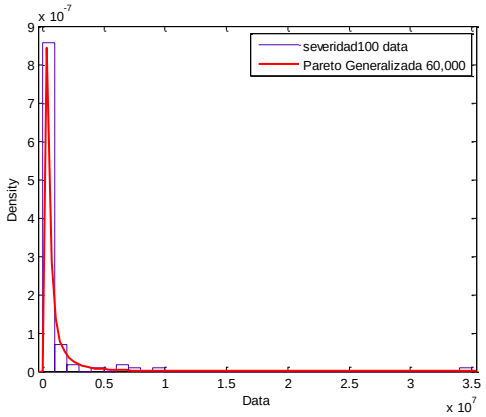


En la gráfica de la distribución de Valores Extremos (gráfica derecha), se percibe que casi no ajusta en el cuerpo de la distribución (donde están las pérdidas pequeñas) aunque si le da peso a los valores de la “cola” o pérdidas grandes.

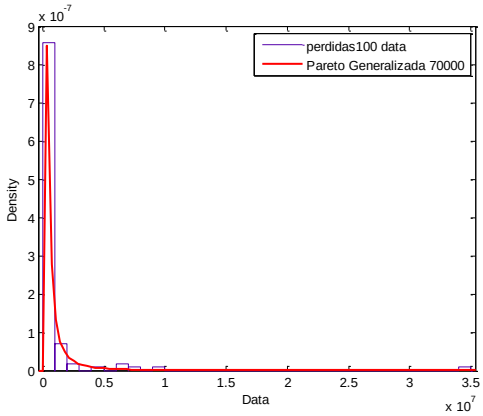




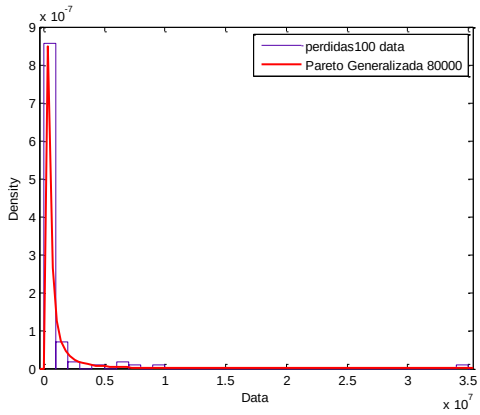
La distribución Gamma sobrevalua las pérdidas pequeñas y no le da peso a las pérdidas extremas, ya que converge rápidamente al eje horizontal. Como aparentemente la Pareto Generalizada tiene un mejor ajuste que las anteriores, se le realizaron varias pruebas con diferentes umbrales o parámetros de ubicación a partir de los cuales se hicieron los ajustes, tales como 50,000, 60,000, 70,000, 80,000 y 100,000.



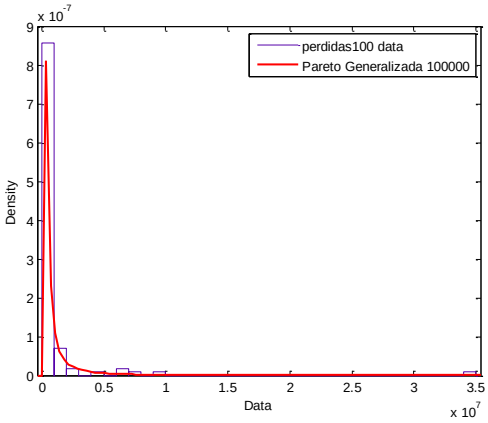
Media = 984,781
Varianza = Infinita
Logaritmo de la verosimilitud = - 1,591.57



Media = 1.10798e+006
Varianza = Infinita
Logaritmo de la verosimilitud = -1,586.34



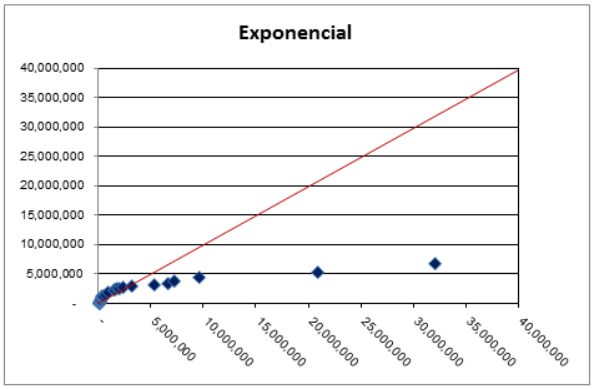
Media = 1.38576e+006
Varianza = Infinita
Logaritmo de la verosimilitud = - 1,580.57

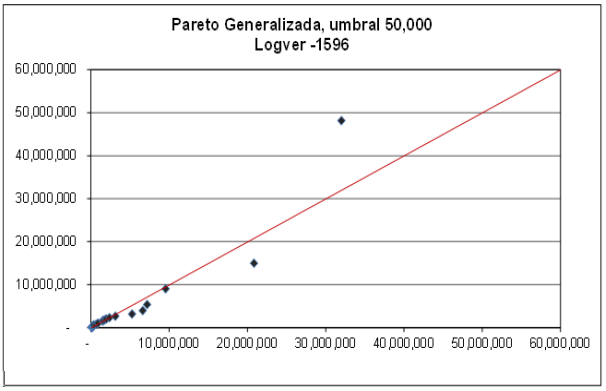


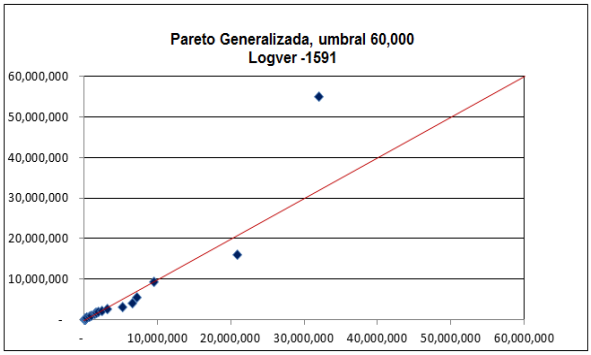
Media = Infinita
Varianza = Infinita
Logaritmo de la verosimilitud = -1,566.47

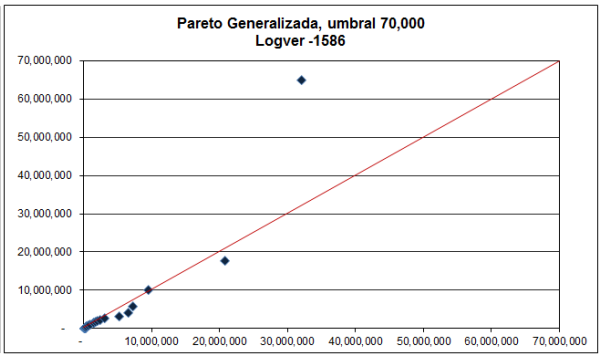
Las gráficas son muy parecidas, pero al observar el logaritmo de la verosimilitud, se pensaría que el umbral de 100,000 es el mejor por estar más cercano al cero. Sin embargo, no es conveniente usarlo en el modelo, ya que por tener media y varianza infinitas, nos arroja un VaR muy grande.

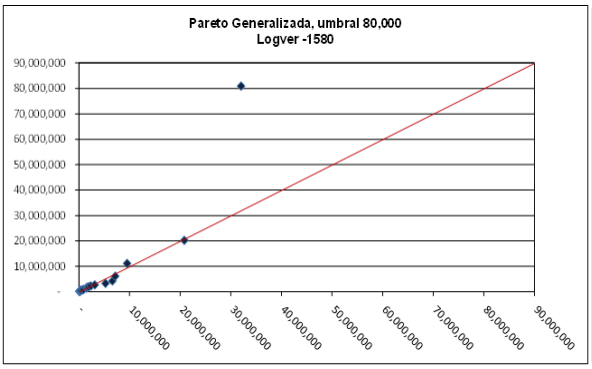
Para elegir la mejor distribución para el modelo, se elaboraron y analizaron las gráficas q-q comparando los datos empíricos contra los ajustados de cada distribución (ver cuadro en el Anexo 2).

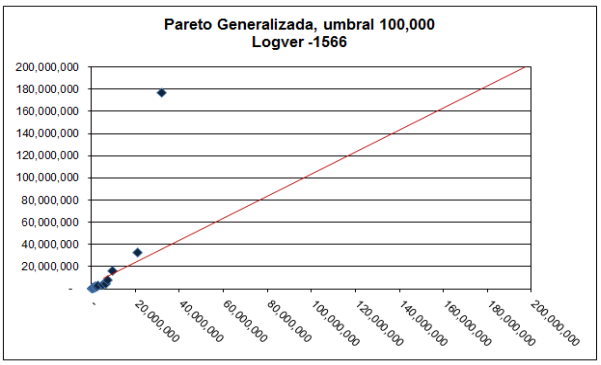












La distribución Exponencial tiene como parámetro μ = 992,547 y el logaritmo de la verosimilitud = -1,673.31. La gráfica q-q muestra que esta distribución no le da peso a la cola, ya que los puntos extremos están por debajo de la recta de 45° y están muy alejados de ella. Por lo tanto, no se considera buena para el ajuste.

En el caso de la Pareto Generalizada, se puede ver que el ajuste en las cinco gráficas es muy similar, pero al comparar el logaritmo de verosimilitud, se observa que el máximo es el del umbral 100,000 (-1,566.47) seguido por el umbral de 80,000 (-1,580.57).

Un inconveniente de utilizar como umbral de ajuste 100,000 es que la media y la varianza son infinitas[8], por lo que al hacer la simulación Montecarlo dio como resultado un VaR muy grande ($2,519,926,572.67), ya que la distribución tiene una cola muy pesada.

En el caso de la distribución con parámetro de ubicación 50,000, el ajuste es mejor porque los puntos que están en la parte superior de la recta de 45° no están muy alejados, lo que nos hace pensar que las pérdidas más grandes no son tan extremas. Sin embargo, las distribuciones con parámetros de ubicación de 70,000 y 80,000 le dan peso elevado a las colas y los datos inferiores a estas, se pegan bastante a la recta de 45°; por otro lado, las pérdidas totales anuales y el VaR por riesgo operacional que se obtuvieron se consideran razonables comparándolos con los montos obtenidos por la institución mediante el método básico.

El siguiente cuadro muestra los valores obtenidos con las distribuciones ajustadas para la severidad:

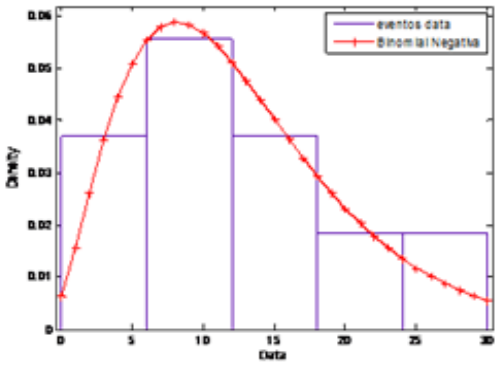
	Lognormal	Exponencial	Gamma	Teoría de Valores Extremos	Pareto Generalizada
Logaritmo de la verosimilitud	-1606.67	-1673.31	-1657.33	-1956.67	-1586.34
Media	606883	992547	992547	-1.64807e+006	1.10798e+006
Varianza	9.02796e+011	9.85151e+011	1.75445e+012	1.37239e+014	Inf

[8] Rootzén, Holger; Klüppelberg, Claudia: "A single number can´t hedge against economic catastrophes", 1999.

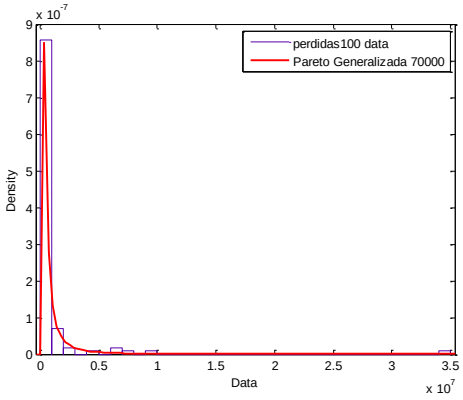
V.5 Distribución de las pérdidas anuales por riesgo operacional y VaR operacional

Las distribuciones que se seleccionaron para integrarse en el modelo fueron la Binomial Negativa y la Pareto Generalizada con umbral o parámetro de ubicación de 70,000, aunque con umbral 80,000 también era buena opción. La elección de la distribución con parámetro de ubicación 70,000 se debió a que los datos se pegan bien a la recta, mientras más bajo el umbral se pierde menos información y tiene más sentido el capital calculado.

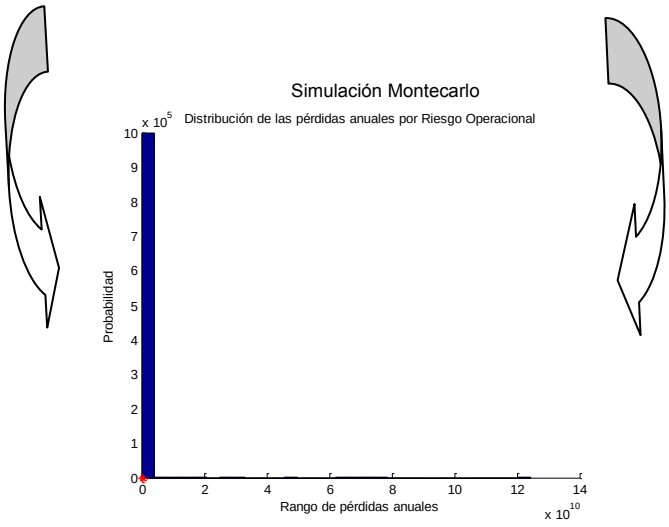
Por simulación Montecarlo se generó la distribución de probabilidad de las pérdidas anuales de la institución y se obtuvo de pérdida esperada $13,640,660 y de VaR $510,577,170 (código de Matlab en el Anexo 3).



Distribución de la frecuencia



Distribución de la severidad



Al interpretar los resultados podemos ver que la pérdida promedio por los eventos de riesgo operacional en un año es de $13,640,660 y, si se llegaran a presentar muchos eventos de riesgo operacional en dicho periodo o eventos con severidad elevada, la pérdida máxima podría alcanzar $510,577,170 (con un 99.9% de confianza).

Asimismo, los valores obtenidos pueden ayudar a la institución a calcular sus reservas para hacer frente a eventos catastróficos futuros sin afectar el patrimonio de la entidad, analizar la contratación de seguros e implementar mejores controles para su prevención.

Los resultados se pueden considerar “válidos” en este momento considerando el monto obtenido por la institución con el método básico establecido por Basilea II y adoptado por la Comisión Nacional Bancaria y de Valores. Pero no hay que olvidar que la información de la base de datos que se utilizó abarca hasta 2008 y que aunque se actualizó con base en el índice de la inflación anual, es necesario repetir el ejercicio año con año hasta el momento actual y hacer un análisis y comparación de las variaciones que sufra el modelo.

Conclusiones

A pesar de que los riesgos operacionales han causado pérdidas de capital mayores que las producidas por la falta de control de los riesgos de crédito y de mercado, el desarrollo de modelos que permitan medirlo y controlarlo está en sus primeras etapas. Lo anterior, debido a que en la industria financiera no existe información suficiente –o incluso en algunos casos la información disponible es nula- que permita estimar con un nivel de confianza definido a cuánto podrían ascender las pérdidas en el caso de presentarse eventos operativos adversos como: fraudes, abusos por información privilegiada, fallas en los sistemas de cómputo, falta de control entre las mesas de negocios y las de operación, e inversión en instrumentos no autorizados, entre otros.

La administración del riesgo operacional no es nueva en las instituciones financieras, sin embargo, ha crecido la necesidad de integrarlo dentro de todos los procesos de la institución con el objetivo de mejorar su administración, documentar y corregir debilidades en los procesos y generar reportes más eficientes a lo largo de toda la entidad para poder reducir los requerimientos mínimos de capital y estar mejor informado para una mejor toma de decisiones.

El incremento de los casos relacionados con el riesgo operacional no deja duda de la importancia que ha adquirido dentro de las instituciones financieras así como para los reguladores, por lo que es importante que todas las áreas de la institución y su alta dirección, participen. Además, es necesario incorporar buenas prácticas operativas, definir políticas y procedimientos y aplicar metodologías de medición adecuadas.

Debido a que las entidades financieras tienen particularidades que las diferencian entre sí, no existe una técnica única o metodología universalmente aplicada con idénticas características, sino que la implementación práctica depende en gran medida de las características específicas, negocios, procesos y controles internos de cada entidad.

Para una adecuada metodología de administración de riesgos operacionales, se deberán tener modelos fiables y validarlos, principalmente en relación con el carácter aleatorio de los mismos. Además, se deberá recurrir a opiniones de expertos en el análisis de escenarios junto con datos externos para valorar su exposición a sucesos de alta severidad, que se podrán traducir en los parámetros de una distribución de pérdidas y en la estimación de desviaciones respecto de las correlaciones estimadas.

Algunas reflexiones derivadas del presente trabajo son, que el cálculo del VaR permite hacer comparaciones por ser una medida en términos monetarios. Basilea contempla obtener el VaR por riesgo operacional en cada celda de la matriz de líneas de negocios y tipos de riesgo (8 x 7). En el caso de la institución bajo estudio, por ser Banca de Desarrollo, no es posible hacerlo ya que sólo se identifican dos líneas de negocio: Fideicomisos y Banca de Gobierno; por lo que la escasez de datos hace más complicado el cálculo.

Más del 90% del requerimiento de capital generalmente se debe a un pequeño número de eventos. La pérdida más grande puede estar a 30 o más desviaciones estándar de la

distancia de la media. Por ello, se sugiere el uso de la Teoría de Valores Extremos para su modelación.

En lo que se refiere al uso de umbrales o parámetros de ubicación en el caso bajo estudio, después de ajustar la distribución Pareto Generalizada con diferentes parámetros, se visualiza que cuanto más bajo sea el umbral, menos información se pierde y más sentido económico tiene el capital calculado. La elección del umbral puede tener un gran impacto tanto en la pérdida no esperada como en la esperada.

La repetición continua del proceso de administración de riesgos operacionales (por lo menos una vez al año) es necesaria, ya que los riesgos a los que está expuesta cualquier institución cambian su perfil o surgen nuevos riesgos. Por lo anterior, sería conveniente obtener la información de la base de datos de la institución del estudio, actualizada hasta el momento, para analizar los cambios que ha sufrido desde 2008 a la fecha y poder hacer las comparaciones pertinentes en todos los aspectos de la administración de riesgos operacionales con los ajustes adecuados.

Para continuar con este tema de investigación podría profundizarse en las mezclas de distribuciones: una que modele el cuerpo y otra la cola de la distribución. El resultado obtenido será una combinación de distribuciones ajustadas que pueden mejorar el pronóstico de las pérdidas por riesgo operacional.

Para finalizar, el principal problema para controlar el riesgo operacional es cómo cuantificarlo. En la mayoría de los casos no se cuenta con información suficiente para construir distribuciones de frecuencia y severidad de los eventos operativos que nos permitan estimar un valor en riesgo. Las principales causas son:

- No hay un patrón en los parámetros para estimar los riesgos operacionales. Las probabilidades de su ocurrencia son diferentes en cada institución financiera y en las entidades.
- No existe un procedimiento generalizado que permita identificar los riesgos operacionales y sus causas, así como ordenar los resultados en una base de datos (derivado de la administración de los riesgos operacionales y/o de los análisis de las auditorías).
- Como muchos de estos riesgos son subjetivos, no se les da la misma atención que a los demás riesgos.
- En muchas instituciones financieras se confunde el costo operativo con el riesgo operacional. Por ejemplo, la adquisición de un sistema de cómputo de baja calidad implicará que los costos operativos disminuyan, pero los riesgos seguramente aumentarán.

Para controlar de manera eficiente el riesgo operacional es necesario enfatizar en los siguientes aspectos: participación de la alta dirección, código de ética sólido, separación de funciones, riesgo del modelo, procedimientos de negociación, operación y registro de las transacciones, políticas de control y de riesgo y, definición de la plataforma de sistemas, entre otros.

Anexo 1. Cuadro. Base de Datos de estudio (113 eventos)

No. de evento	Fecha	Monto del evento	No. de evento	Fecha	Monto del evento	No. de evento	Fecha	Monto del evento
1	31/08/2000	204,114	40	18/11/2004	219,634	79	18/01/2007	1,727,491
2	31/10/2000	226,403	41	28/01/2005	118,077	80	02/02/2007	1,897,452
3	31/10/2000	275,046	42	28/01/2005	156,425	81	14/02/2007	218,127
4	31/10/2000	350,526	43	28/01/2005	194,220	82	28/03/2007	270,333
5	29/11/2000	280,732	44	28/01/2005	196,958	83	22/06/2007	142,500
6	23/05/2001	107,120	45	28/01/2005	353,465	84	22/06/2007	178,549
7	28/05/2001	123,213	46	28/01/2005	1,419,206	85	22/06/2007	212,347
8	17/10/2001	100,457	47	14/02/2005	204,675	86	22/06/2007	251,360
9	23/10/2001	348,996	48	26/05/2005	106,467	87	22/06/2007	262,293
10	13/11/2001	1,214,116	49	20/06/2005	771,592	88	22/06/2007	327,246
11	26/12/2001	114,635	50	15/08/2005	2,344,600	89	28/06/2007	111,796
12	26/12/2001	649,538	51	11/10/2005	112,247	90	28/06/2007	114,058
13	15/02/2002	117,957	52	11/10/2005	195,506	91	28/06/2007	126,019
14	15/03/2002	238,339	53	11/10/2005	311,248	92	28/06/2007	127,261
15	22/03/2002	1,532,398	54	31/10/2005	251,684	93	28/06/2007	137,338
16	14/05/2002	107,987	55	23/11/2005	829,598	94	28/06/2007	139,476
17	17/07/2002	115,332	56	21/12/2005	101,232	95	28/06/2007	199,015
18	22/08/2002	160,092	57	24/01/2006	261,508	96	28/06/2007	227,502
19	09/10/2002	6,268,260	58	30/06/2006	331,994	97	28/06/2007	269,791
20	08/12/2002	165,126	59	17/08/2006	216,634	98	28/06/2007	272,436
21	19/12/2002	315,905	60	26/09/2006	100,815	99	28/06/2007	290,131
22	19/12/2002	327,959	61	26/09/2006	119,238	100	28/06/2007	323,446
23	27/01/2003	7,286,669	62	26/09/2006	119,919	101	28/06/2007	360,453
24	14/02/2003	422,822	63	26/09/2006	120,226	102	28/06/2007	434,753
25	10/03/2003	9,853,505	64	26/09/2006	122,787	103	28/06/2007	940,876
26	10/03/2003	34,819,263	65	26/09/2006	152,050	104	28/06/2007	1,039,843
27	02/04/2003	1,534,464	66	26/09/2006	177,935	105	26/09/2007	112,539
28	14/05/2003	248,430	67	26/09/2006	212,580	106	22/11/2007	356,557
29	25/08/2003	252,497	68	26/09/2006	244,946	107	26/11/2007	368,885
30	25/08/2003	283,590	69	26/09/2006	291,497	108	18/02/2008	472,051
31	25/08/2003	735,319	70	30/09/2006	108,174	109	05/05/2008	198,939
32	25/08/2003	892,625	71	30/09/2006	170,054	110	01/07/2008	1,370,460
33	02/09/2003	104,350	72	09/10/2006	143,634	111	24/07/2008	351,839
34	23/09/2003	163,846	73	09/10/2006	234,618	112	24/07/2008	351,839
35	23/09/2003	885,057	74	09/10/2006	430,594	113	26/08/2008	4,164,056
36	15/12/2003	110,961	75	09/10/2006	2,444,563			
37	15/04/2004	156,921	76	30/10/2006	950,980			
38	04/05/2004	345,819	77	06/11/2006	391,565			
39	07/05/2004	6,836,792	78	14/12/2006	298,478			
							Total	**$112,157,867**

Anexo 2. Cuadro. Distribuciones acumuladas empíricas contra ajustadas

Cuantiles de la severidad

				Pareto generalizada				
Probs.	Empírico	Lognormal	Exponencial	Umbral 50,000 Logver -1596	Umbral 60,000 Logver -1566	Umbral 70,000 Logver -1586	Umbral 80,000 Logver -	Umbral 100,000 Logver -1566
0.0500	107,640	52,366	50,911	62,815	71,832	80,803	89,711	107,145
0.1000	112,843	78,461	104,575	76,842	84,809	92,682	100,421	115,102
0.1500	119,006	103,071	161,308	92,275	99,118	105,812	112,296	124,018
0.2000	126,516	128,026	221,480	109,350	114,985	120,411	125,545	134,075
0.2500	152,050	154,200	285,538	128,362	132,693	136,752	140,428	145,506
0.3000	168,083	182,235	354,017	149,683	152,604	155,181	157,276	158,609
0.3500	197,354	212,744	427,572	173,790	175,179	176,145	176,520	173,776
0.4000	212,534	246,404	507,018	201,308	201,024	200,231	198,727	191,534
0.4500	230,348	284,032	593,381	233,069	230,950	228,226	224,662	212,599
0.5000	251,684	326,668	687,981	270,210	266,068	261,217	255,384	237,982
0.5500	271,595	375,705	792,556	314,332	307,948	300,742	292,402	269,146
0.6000	292,893	433,077	909,462	367,768	358,886	349,062	337,946	308,298
0.6500	327,817	501,598	1,041,998	434,065	422,390	409,653	395,466	358,925
0.7000	351,839	585,574	1,195,000	518,925	504,127	488,155	470,606	426,867
0.7500	391,565	692,036	1,375,962	632,184	613,926	594,430	573,311	522,716
0.8000	701,006	833,516	1,597,443	792,545	770,609	747,508	722,975	667,819
0.8500	942,897	1,035,329	1,882,981	1,041,012	1,015,786	989,889	963,454	912,494
0.9000	1,509,760	1,360,063	2,285,424	1,490,778	1,465,625	1,441,834	1,420,935	1,409,715
0.9100	1,534,299	1,452,699	2,389,999	1,630,678	1,606,876	1,585,352	1,568,250	1,577,278
0.9200	1,734,289	1,560,500	2,506,904	1,800,109	1,778,677	1,760,807	1,749,498	1,787,792
0.9300	1,968,996	1,688,289	2,639,441	2,010,322	1,992,862	1,980,815	1,978,405	2,059,997
0.9400	2,372,590	1,843,418	2,792,442	2,279,392	2,268,539	2,265,865	2,277,432	2,425,310
0.9500	3,132,360	2,037,816	2,973,405	2,638,507	2,638,862	2,651,757	2,686,157	2,940,665
0.9600	5,258,242	2,292,558	3,194,886	3,146,974	3,167,315	3,207,596	3,281,759	3,720,854
0.9700	6,632,120	2,649,776	3,480,424	3,934,801	3,994,237	4,087,705	4,238,768	5,036,413
0.9800	7,178,698	3,212,248	3,882,867	5,360,901	5,511,435	5,728,753	6,059,356	7,709,854
0.9900	9,545,485	4,350,836	4,570,848	9,000,071	9,468,473	10,122,088	11,094,433	15,941,423
0.9950	20,838,439	5,743,311	5,258,829	14,982,003	16,148,233	17,777,859	20,221,743	32,927,813
0.9990	32,023,098	10,181,336	6,856,272	48,138,289	55,032,234	65,046,253	80,879,028	177,175,438

Anexo 3. Código de Simulación Montecarlo. Matlab

```
function VaR=bineg_pg(r,p,N,K,sigma,theta,q)
donde:
r y p son los parámetros de la binomial negativa,
N es el número de años que se van a simular,
K, sigma y theta son los parámetros de la pareto generalizada, y
q es el cuantil al que se quiere calcular el VaR por riesgo operacional

 BinNeg = nbinrnd(r,p,N,1);
Suma=zeros(N,1);
for i=1:N

ParetoGeneralizada=gprnd(K,sigma,theta,BinNeg(i),1,1);
Suma(i)=sum(ParetoGeneralizada);
end

format long g
VaR = quantile(Suma,q);
disp('Pérdida esperada')
mean(Suma)
disp('Valor en Riesgo')

hold on
hist(Suma,30)
plot(quantile(Suma,q),0,'r*')
plot(mean(Suma),0,'r*')

end
```

GLOSARIO

- **Administración de Riesgos:** Cultura, procesos y estructura que se dirigen a las oportunidades potenciales manejando los efectos adversos.
- **Amenaza:** Una fuente de daño potencial.
- **Análisis de riesgo:** Proceso sistemático para entender la naturaleza del riesgo y reducir su nivel.
- **Consecuencia:** Resultado o impacto de un evento.
- **Control:** Un proceso existente, política, dispositivo, práctica u otra acción que actúa para minimizar riesgos negativos o mejorar oportunidades positivas.
- **Evaluación de riesgo:** Proceso de comparación del nivel de riesgo contra el criterio de riesgo.
- **Evento:** Ocurrencia de un conjunto particular de circunstancias.
- **Evento de pérdida:** Incidente ocasionado por la materialización de un riesgo operacional que ocasiona una pérdida o ganancia, incurrida o por incurrir, directa (se encuentra claramente identificable en la contabilidad) o indirecta (se encuentra inmersa en los movimientos de las cuentas de la operación habitual u ocasiona un costo de oportunidad), o a un cambio en el valor de cualquier activo de la institución.
- **Frecuencia:** Medida del número de ocurrencias o una serie de ocurrencias.
- **Identificación de riesgos:** Proceso para determinar qué, dónde, cuándo, por qué y cómo podría ocurrir algo.
- **Marco de administración de riesgos:** Conjunto de elementos del sistema de administración de una organización referentes a la administración de riesgos.
- **Monitoreo:** Verificar, supervisar, observar críticamente o medir el progreso de una actividad, acción o sistema sobre una base regular para identificar cambios del nivel de desempeño requerido o esperado.
- **Near miss:** Situaciones de riesgo que no hayan causado pérdidas o que hayan originado una ganancia.
- **Pérdida:** Una consecuencia negativa o efecto adverso, financiero u otro.
- **Pérdida esperada:** Es la pérdida promedio de una organización generada por el curso natural de su operación cotidiana.
- **Pérdida no esperada:** Es una desviación de ese promedio que en un momento dado puede poner en riesgo la organización.
- **Probabilidad:** Mide las oportunidades de ocurrencia expresado como un número entre 0 y 1.
- **Riesgo:** La oportunidad de que algo que ocurra pueda tener un impacto sobre los objetivos del negocio.
- **Riesgo residual:** Riesgo remanente después de implementar un tratamiento para el riesgo.

Bibliografía

- Basel Committee on Banking Supervision: “International Convergence of Capital Measurement and Capital Standards: a Revised Framework”, (junio 2006).
- Basel Committee on Banking Supervision: “Sanas prácticas para la gestión y supervisión del riesgo operativo”, 2003.
- Cruz, Marcelo: “Modeling, Measuring and Hedging Operational Risk”. Wiley 2001.
- Carrillo Menéndez, Santiago. Artículo: “Basilea II: Una mirada crítica”. Colección Mediterráneo Económico: Los restos de la industria bancaria en España, 2005.
- RiskMathics, curso: “Riesgo Operativo. Julio de 2012.
- Scandizzo, S.: “The Operational Risk Manger’s Guide: How to understand methodologies, policies and procedures, Risk Books. London 2007.
- Llaguno Musons, José Ignacio: “Gestión del riesgo operativo en las entidades de crédito: un camino sin retorno”. España, 2005.
- Boletín Asesoría Gerencial, artículo: “Gestión de Riesgo Operacional: una oportunidad para la creación de valor en las instituciones financieras”. No . 2, 2008.
- “Estudio de los sistemas de información requeridos para la medición del Riesgo Operativo”. Gerencia de Investigación y Planificación Normativa y Gerencia de Régimen Informativo del Banco Central de la República Argentina, octubre 2006.
- Fontnouvelle, Patrick de; Jordan, Jhon; Rosengren, Eric: “Implication of Alternative Operational Risk Modeling Techniques. Nber Workng Paper Series, February 2005.
- Cruz, Marcelo: “Extreme Value Theory: A useful framework for modeling extreme OR events”.
- Jiménez Rodríguez, Enrique José; Martín Marín, José Luis: “El Nuevo Acuerdo de Basilea y la gestión del Riesgo Operacional”. Universia Business Review, número 007; Grupo Recoletos Comunicación. Madrid, España, 2005.
- Power, Michael: “La invención del Riesgo Operativo”. Universidad de Oxford, junio 2003.
- Carrillo Menéndez, Santiago: “How to Use Consistently Internal Data, External Data and Scenarios”. Conferencia en México, Julio de 2012.
- Sánchez Cerón, Carlos: “Valor en Riesgo y otras aproximaciones”. Valuación, Análisis y Riesgo, S.C. Febrero de 2001.
- Rootzén, Holger; Klüppelberg, Claudia: “A single number can´t hedge against economic catastrophes”, October 3, 1999.