UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TESIS

PROPUESTA DE DISEÑO E IMPLEMENTACIÓN DE LA GESTIÓN DE RIESGO OPERACIONAL EN EL SECTOR PRODUCTIVO, FINANCIERO Y DE SERVICIOS

TÍTULO DE : INGENIERO INDUSTRIAL

PRESENTAN

LILIA ORTEGA REPIZO

JUAN ALBERTO PADILLA MONTES DE OCA

Agradecimientos

Para poder realizar esta tesis fue necesario el apoyo y sacrificio de muchas personas a las cuales queremos agradecer:

A nuestros padres y familiares que nos impulsaron a concluir el proyecto que habíamos empezado y que nos dieron palabras de aliento y motivación.

A nuestros amigos y compañeros que nos animaron a terminar este trabajo que sufrió de más de un altibajo.

A nuestros tutores y director de tesis que nos guiaron, ayudaron y corrigieron para poder obtener una tesis de la mejor calidad en forma y contenido.

Gracias a todos y cada uno de ustedes.

ÍNDICE

1. ANTECEDENTES

Antes de entrar en materia financiera, es importante que se establezca la relación que guarda la ingeniería industrial con las finanzas. En primer lugar, la ingeniería es la ciencia dedicada al estudio y aplicación de las diversas ramas de la tecnología, así como de la inventiva y el método científico para desarrollar y concretar ideas que puedan resolver los problemas humanos. Ahora bien, la ingeniería industrial analiza las variables involucradas en la producción de bienes y servicios. Es por ello que el ingeniero industrial se dedica al análisis, diseño, planeación, control y optimización de procesos industriales, sin dejar de considerar el aspecto técnico, económico, financiero y social. Asimismo la ingeniería industrial puede aplicar técnicas, métodos y procedimientos en todos los factores relacionados con la dirección, procesos, distribución y venta de bienes y servicios.

El campo de acción del ingeniero industrial es el siguiente: administración, producción, métodos, procedimientos, ergonomía, diagnóstico de empresas, evaluación de proyectos empresariales e industriales, finanzas, investigación de operaciones, diseño de sistemas productivos, logística, seguridad industrial, impacto ambiental, reingeniería, entre otros. Dado que el campo de acción es amplio, el ingeniero industrial puede desarrollarse en: empresas e instituciones industriales públicas y privadas, instituciones de investigación tecnológica y operativa, proyectos de inversión y de financiamiento para micro, pequeñas, medianas y grandes empresas, empresas de asesoría y consultoría, instituciones financieras y del mercado bursátil, organismos de gestión empresarial, organismos académicos y organización de innovación tecnológica y de la transformación.

Debido al vasto campo de estudio de la ingeniería industrial, se pudo vincular ésta con el riesgo operacional, ya que la gestión de riesgo operacional se puede observar como un proceso de control que tiene como finalidad hacer más eficientes tanto los productos como los servicios que se le ofrecen al cliente, además de mitigar las pérdidas inherentes a la actividad diaria de una institución. Por lo tanto la ingeniería industrial como el riesgo operacional buscan diseñar herramientas que permitan optimar los procesos inherentes a la actividad productiva de una empresa haciéndola más eficiente y por lo tanto rentable.

Una vez establecida la relación que existe entre la ingeniería industrial y el riesgo operacional, se dará inicio al desarrollo de la tesis comenzando con sus antecedentes y definición.

En Diciembre de 1974, los gobernadores del G-10 (de los diez grandes bancos centrales europeos) crearon el Comité de Supervisión Bancaria de Basilea con la finalidad de mejorar la colaboración entre las autoridades de supervisión bancaria de todos los países miembros. A mediados de los años ochenta, los bancos más importantes de Europa Occidental se reunieron para crear en la Ciudad de Basilea, Suiza, las primeras normas que fortalecerían a cualquier institución bancaria contra posibles eventos de pérdida financiera. Hoy en día, el Banco de Pagos Internacionales (Bank for International Settlements, BIS) actúa como una organización internacional que fomenta la cooperación monetaria y financiera internacional además de fungir como banco para los bancos centrales. El BIS cumple este cometido en calidad de:

a) Foro para el debate y la toma de decisiones entre bancos centrales así como en el seno de la comunidad financiera y supervisora internacional.
b) Centro de estudios económicos y monetarios.
c) Entidad de contrapartida principal para las operaciones financieras de los bancos centrales.
d) Agente depositario de garantías en operaciones financieras.

Lo anterior se logró por medio del Acuerdo de Basilea I de 1988 el cual contenía un método para establecer el capital mínimo que debía tener una entidad bancaria en función de sus riesgos; al mismo tiempo proporcionaba incentivos para adoptar los métodos sensibles a los riesgos más avanzados del marco revisado. Las principales limitaciones del acuerdo de Basilea I eran su insensibilidad a las variaciones de riesgo y que ignoraba una dimensión esencial: la de la calidad crediticia y, por lo tanto, la diversa probabilidad de incumplimiento de los distintos prestatarios. Como consecuencia, consideraba que todos los créditos tenían la misma probabilidad de incumplimiento. Ésta fue una de las razones para que los supervisores y los bancos más sofisticados hallaran que las normas estáticas estipuladas en el Acuerdo de 1988 no seguían el ritmo de los avances de las prácticas de gestión de riesgos y, por lo tanto, diversas organizaciones bancarias habían perdido el sentido de usar dicho Acuerdo.

Para conseguir que existiera una normatividad dinámica, el Comité de Basilea propuso en el 2004, un nuevo conjunto de recomendaciones generadas por los gobernadores de bancos centrales y las autoridades de supervisión bancaria del G10, quienes se reunieron y aprobaron la publicación del nuevo marco para la adecuación del capital, conocido como Basilea II. La función de dicho capital es ser la base para el crecimiento futuro de los bancos, además de actuar como un "colchón de seguridad" contra pérdidas inesperadas.

Como se mencionó anteriormente, Basilea II parte de la estructura básica del Acuerdo de 1988 para establecer exigencias de capital y mejorar la sensibilidad del marco de capital a los riesgos que los bancos realmente enfrentan. Esto se logró en parte, al adaptar mejor los requisitos de capital al riesgo de pérdidas por crédito e introducir una nueva exigencia de capital para exposiciones al riesgo de pérdida causada por fallas de operación. El marco de Basilea ofrece un nuevo conjunto de normas para establecer requisitos mínimos de capital para las organizaciones bancarias y adopta un enfoque global de la gestión de riesgos y la supervisión bancaria; además, estipula los detalles para adoptar exigencias mínimas de capital más sensibles al riesgo para las organizaciones bancarias.

Asimismo, el nuevo marco refuerza los requerimientos sensibles al riesgo estableciendo principios para que los bancos se valúen la suficiencia de su capital y para que los supervisores examinen esas evaluaciones y se aseguren de que los bancos posean capital suficiente para solventar sus riesgos. De igual forma, dicho marco pretende incrementar la seguridad y solidez de los bancos para fortalecer la estabilidad del sistema financiero en su conjunto y mejorar la capacidad del sector financiero de servir como fuente de crecimiento sostenible para la economía en general. Los bancos suficientemente capitalizados y bien administrados están mejor preparados para soportar pérdidas y proveer crédito a los consumidores y empresas por igual a lo largo del ciclo económico, incluyendo las fases descendentes. Por lo tanto un nivel adecuado de capital ayuda a promover la confianza del público en el sistema bancario.

El desafío técnico tanto para los bancos como para los supervisores ha sido determinar el capital necesario para proteger al banco contra pérdidas inesperadas. Si el nivel de capital es demasiado bajo, es posible que el banco no pueda absorber pérdidas elevadas. Los niveles excesivamente bajos de capital incrementan el riesgo de quiebras bancarias que, a su vez, podrían poner en peligro los fondos de los depositantes. En cambio, un nivel de capital demasiado alto podría impedir que el banco utilice eficazmente sus recursos y restringir su capacidad de otorgar crédito. La metodología necesaria para el cálculo del requerimiento de capital mínimo por concepto de riesgo operacional está estipulada en el documento de Basilea II.

El Riesgo Operacional está presente en todas las actividades de una entidad financiera, así como en cualquier empresa u organismo, desde el primer instante de su vida y puede presentarse de manera inesperada y afectar las operaciones que ahí se realizan. La administración del riesgo operacional no es nueva en las instituciones financieras, sin embargo en últimas fechas ha crecido la imperiosa necesidad de integrarlo en los procesos de la institución con el fin de mejorar su administración, documentación y mitigación de riesgos operacionales. Es por esto que en el presente documento se propondrán y desarrollarán las herramientas necesarias para la gestión del riesgo

operacional y s e expl icará la manera e n que de ben ser ut ilizadas para obt ener los m ejores resultados. Cabe aclarar que l os ri esgos operac ionales si empre es tarán presentes en cualquier institución y que se traducen en pot enciales pérdidas po r lo que f inalidad de la ges tión d e r iesgo operacional es la mitigación de d ichos riesgos, así como compren der que su v erdadero valor radica en lograr entender que el dinero destinado a su implementación es una inversión que concluirá en la entrega de un mayor valor a los accionistas y un mejor servicio a los clientes.

2. DEFINICIÓN DE RIESGO OPERACIONAL

2.1 Definición de riesgo operacional (Comisión Nacional Bancaria y de Valores)

El Riesgo Operacional se define como la pérdida potencial por fallas o deficiencias en los controles internos, por errores en el procesamiento y almacenamiento de las operaciones o en la transmisión de información, así como por resoluciones administrativas y judiciales adversas, fraudes o robos, eventos externos; y comprende, entre otros, al riesgo tecnológico y al riesgo legal en el entendido de que:

a) El riesgo tecnológico se define como 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.
b) El riesgo legal se define como 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.

2.2 Definición de riesgo operacional (Bank of Internacional Settlements)

El Riesgo Operacional se define como el riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

3. GESTIÓN DE RIESGO OPERACIONAL

La gestión de riesgo operacional se define como la cultura o conjunto de procesos, políticas, procedimientos y acciones que se implementan para identificar, medir, controlar, dar seguimiento y revelar los tipos de riesgo a los que se encuentra expuesta una entidad económica de tal forma que le permita mitigar las pérdidas y maximizar las oportunidades.

Para llevar a cabo la Gestión del Riesgo Operacional, es necesario contar con la mayor cantidad de información disponibles (cualitativa y cuantitativa) y con la participación del personal que ejecuta los procesos y procedimientos, esto con el fin de lograr que las acciones y decisiones que se tomen, consigan alcanzar los niveles de efectividad esperados. La metodología para la gestión de riesgo operacional debe estar acorde con el objeto social, tamaño, naturaleza, complejidad y demás características que tenga cada entidad económica.

La gestión de riesgo operacional puede ser utilizada por instituciones financieras y por las que se dedican a la producción de bienes y/o servicios, ya que la aplicación de la metodología permite un mejor aprovechamiento de los recursos y una disminución de las pérdidas de diferentes naturalezas. Para el caso particular de esta tesis se planteará y desarrollará el Sistema de Gestión de Riesgo Operacional en una institución financiera, sin embargo la metodología es muy parecida a la que se utilizaría en una empresa de bienes y/o servicios.

La gestión de riesgo operacional de una institución financiera tiene como principal objetivo mitigar las pérdidas tanto esperadas como no esperadas que aumentan los requerimientos mínimos de capital necesarios para el funcionamiento de la Institución Bancaria. Los requerimientos mínimos de capital son fondos de seguridad utilizados por el banco, en caso de estar en bancarrota para poder pagar tanto a sus clientes como a sus inversionistas. Estos fondos son considerados desde el punto de vista del banco como capital inactivo, por lo tanto, uno de sus objetivos es minimizar lo más que se pueda dichos requerimientos.

A continuación se da pie al desarrollo de la propuesta de gestión de riesgo operacional para una institución financiera.

3.1 Base de datos.

3.1.1 Objetivo

La base de datos corresponde a la etapa de medición dentro del proceso de gestión de riesgo operacional. La medición permite establecer criterios de calificación y evaluación de riesgos que permitan tomar decisiones pertinentes sobre su mejor tratamiento. Asimismo, el Comité de Basilea busca que las Instituciones comiencen a conformar bases de datos con información suficiente y oportuna, que a futuro les permita estimar las pérdidas esperadas y no esperadas atribuibles al riesgo operacional.

Las bases de datos cuentan con datos internos (datos generados durante la operación de la institución) y datos externos (información proveniente del exterior de la institución). De esta forma la institución puede tener un conocimiento histórico de los factores de riesgo que la impactaron desde adentro, así como de los eventos externos que tuvieron una repercusión negativa sobre ella.

En primer lugar, se explicarán los tipos de datos internos para después dar paso a la explicación de los datos externos. Las instituciones financieras deben realizar un seguimiento de los datos internos relacionados con las pérdidas económicas que se han presentado para lograr el desarrollo y funcionamiento de un sistema efectivo de medición de riesgo operacional. Además, los datos internos de pérdida son necesarios para que la institución pueda realizar estimaciones sobre su historial de pérdidas efectivas tanto esperadas como no esperadas.

Cabe señalar que los datos internos de pérdida son de máxima relevancia cuando guardan una clara relación entre las distintas actividades del negocio, procesos tecnológicos y procedimientos de gestión del riesgo operacional de la institución financiera. Es por ello que se deberá tener documentado los procedimientos pertinentes para evaluar en todo momento los datos históricos de pérdida, considerando situaciones en donde se presenten excepciones discrecionales, ajustes de proporcionalidad o cualquier otro tipo de ajustes, así como el grado en que puedan introducirse tales ajustes y el personal autorizado para tomar esas decisiones. Los eventos de pérdida generados internamente en la institución y utilizados para el cálculo de la capital de requerimiento mínimo deberán basarse en un periodo de mínimo 5 años de observación de datos internos de pérdida, ya sea que se empleen para estimar directamente la pérdida o para validar dicha estimación. Cuando la institución desee utilizar por vez primera los AMA, se aceptará un periodo de observación de datos de tres años.

La recopilación de datos internos de pérdida por parte de la institución financiera deberá satisfacer los siguientes criterios para poder ser utilizados a efectos del requerimiento mínimo de capital:

- Para que la base de datos pueda ser utilizada en la validación supervisora, la institución financiera tiene que ser capaz de asignar a su base histórica de datos de pérdida las categorías de líneas de negocios (Anexos, Tabla 6.1) y tipos de eventos de pérdida (Anexos, Tabla 6. 2), así como proporcionar dichos datos a los supervisores en caso de que así se lo pidieran.
- La institución financiera debe contar con criterios objetivos y documentados sobre la asignación de las pérdidas a las líneas de negocio y a los tipos de eventos de pérdida. No obstante, cuenta con la libertad de decidir en qué medida desea aplicar la clasificación mencionada anteriormente dentro de su sistema de medición interna del riesgo operacional.
- Los datos internos de pérdida de la institución financiera deben ser integrales e incluir la totalidad de las actividades y posiciones relevantes en todos los subsistemas. Además, la institución debe ser capaz de justificar que las actividades o posiciones excluidas, tanto de forma individual como conjunta, no tendrían un efecto significativo sobre las estimaciones generales de riesgo y deberá establecer un umbral mínimo adecuado de pérdidas brutas para la recopilación de datos internos de pérdida. El umbral que se considere adecuado variará dependiendo de cada institución y de cada línea de negocio y/o tipo de evento.
- Además de la información sobre pérdidas brutas, la institución financiera debe recopilar la información sobre la fecha del evento, cualquier recuperación con respecto a las cantidades brutas de las pérdidas, así como información de carácter descriptivo sobre los factores desencadenantes o las causas del evento de pérdida.
- La institución financiera deberá desarrollar criterios específicos para la asignación de datos de pérdidas procedentes de eventos sucedidos en una unidad centralizada o en una actividad que incluya más de una línea de negocio.
- Aquellas pérdidas de riesgo de crédito o de mercado que fueron ocasionadas por algún error operativo deben ser considerados dentro del modelo de gestión y deben ser identificadas en la base de datos internos de riesgo operacional de las instituciones. La importancia de dichas pérdidas puede variar según la institución y según la línea de negocios o el tipo de evento.

Finalmente para la estimación de riesgo operacional de una institución financiera se deben utilizar datos externos relevantes (ya sean datos públicos o datos agregados del sector bancario), especialmente cuando existan motivos para creer que la institución está expuesto a pérdidas de carácter infrecuente, pero potencialmente graves. Estos datos externos deberán incluir información sobre las pérdidas efectivas, la gama de actividades de negocio donde se produjo el evento, las causas y circunstancias de los eventos de pérdida, así como cualquier otra información que permita

evaluar la relevancia del evento de pérdida para otras instituciones. La institución financiera debe contar con un proceso para determinar en qué situaciones deberán utilizarse los datos externos y qué metodologías se emplearán para incorporar tales datos (por ejemplo, introducción de ajustes de proporcionalidad o ajustes cualitativos, o introducción de mejoras en el análisis de escenarios).

3.1.2 Caso Práctico de la Base de Datos

A continuación se describe un ejemplo basado en una institución financiera y de aquí en adelante se le dará continuidad a dicho ejemplo para ilustrar cada elemento que compone a la gestión de riesgo operacional. Para este ejemplo, la base de datos será una tabla conformada por las siguientes columnas:

I. *Número de Referencia*. Es el único número de identificación, por medio del cual se podrá identificar un evento de pérdida determinado.

II. *Fecha.* Se introduce la fecha en la cual aconteció la pérdida. Este campo está dividió en 2 columnas (Trimestre y Año).

III. *Línea de negocio.* Se captura la línea de negocios que fue afectada por el evento de pérdida. Dichas líneas de negocios están definidas dentro de la Tabla 6.1 de los anexos. La nomenclatura usada para cada una de las líneas de negocios es la siguiente:

- **a.** Finanzas Corporativas
- **b.** Negociación y ventas
- **c.** Banca Minorista
- **d.** Banca Comercial
- **e.** Pago y liquidación
- **f.** Servicios de agencia
- **g**. Administración de activos
- **h.** Intermediación minorista

IV. *Monto de pérdida bruta*. Contiene la pérdida ocasionada por el evento de pérdida sin considerar cualquier tipo de recuperación o gasto adicional.

V. *Tipo de evento de pérdida.* Contiene un código que nos permite identificar el Nivel 1 y Nivel 2 del tipo de evento de pérdida que aconteció. Cabe señalar que para el Nivel 1 la referencia va de la letra a-g, mientras que para el Nivel 2 la referencia es del 1 al 22. La tabla 6.2 de los Anexos contiene la información detallada sobre los eventos de pérdida por niveles. A continuación se muestra un resumen de la misma:

- **a.** Fraude interno
  - **1)** Actividades no autorizadas
  - **2)** Hurto y fraudes internos
  - **3)** Seguridad de los sistemas
- **b.** Fraude externo
  - **4)** Hurto y fraudes externos
  - **5)** Seguridad en los sistemas
- **c.** Relaciones laborales y seguridad en el puesto de trabajo

6) Relaciones laborales

7) Higiene y seguridad en el trabajo

8) Diversidad y discriminación

d. Clientes, productos y prácticas empresariales

9) Adecuación, divulgación de información y confianza

10) Prácticas empresariales o de mercado improcedentes

11) Productos defectuosos

12) Selección, patrocinio y riesgos

13) Actividades de asesoramiento

e. Desastres naturales y otros acontecimientos

14) Desastres y otros acontecimientos

f. Incidencias en los negocios y fallos en los sistemas

15) Sistemas

g. Ejecución, entrega y gestión de operaciones

16) Recepción, ejecución y mantenimiento de operaciones

17) Seguimiento y presentación de informes

18) Aceptación de clientes y documentación

19) Gestión de cuentas de clientes

20) Pérdidas derivadas del incumplimiento de la normativa

21) Contrapartes comerciales

22) Distribuidores y proveedores

VI. *Descripción.* Se captura una descripción detallada del evento de pérdida.

VII. *Factor de riesgo.* El factor de riesgo es cualquier característica, condición o circunstancia durante la operación que puede ser generada en el interior y/o exterior de la institución, la cual condiciona una mayor probabilidad de que ocurra un evento de pérdida. Los factores de riesgo que se utilizaron en la base de datos son los siguientes:

- Asaltos
- Cheques
- Errores en la ejecución de operaciones
- Falla en los sistemas
- Falto y falso
- Fraude externo
- Fraude interno
- Fraude tarjetas
- Juicios laborales
- Phising
- Regulatorio

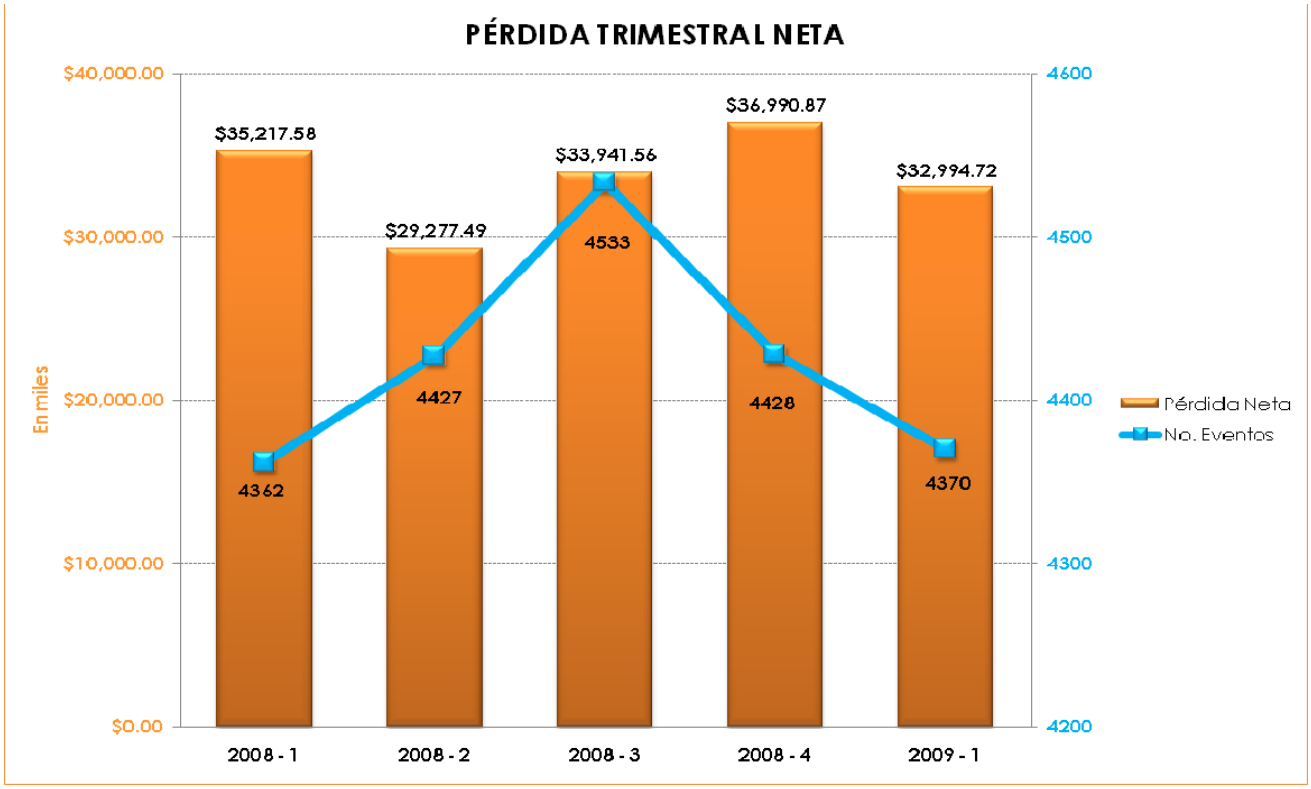
VIII. *Recuperaciones.* Se coloca el monto de cualquier cantidad recuperada, este tipo de recuperaciones se dan principalmente en los factores de riesgo legal y juicios laborales.

IX. *Gastos Adicionales.* Se captura el monto de gastos adicionales generados principalmente por los factores de riesgo legal y juicios laborales.

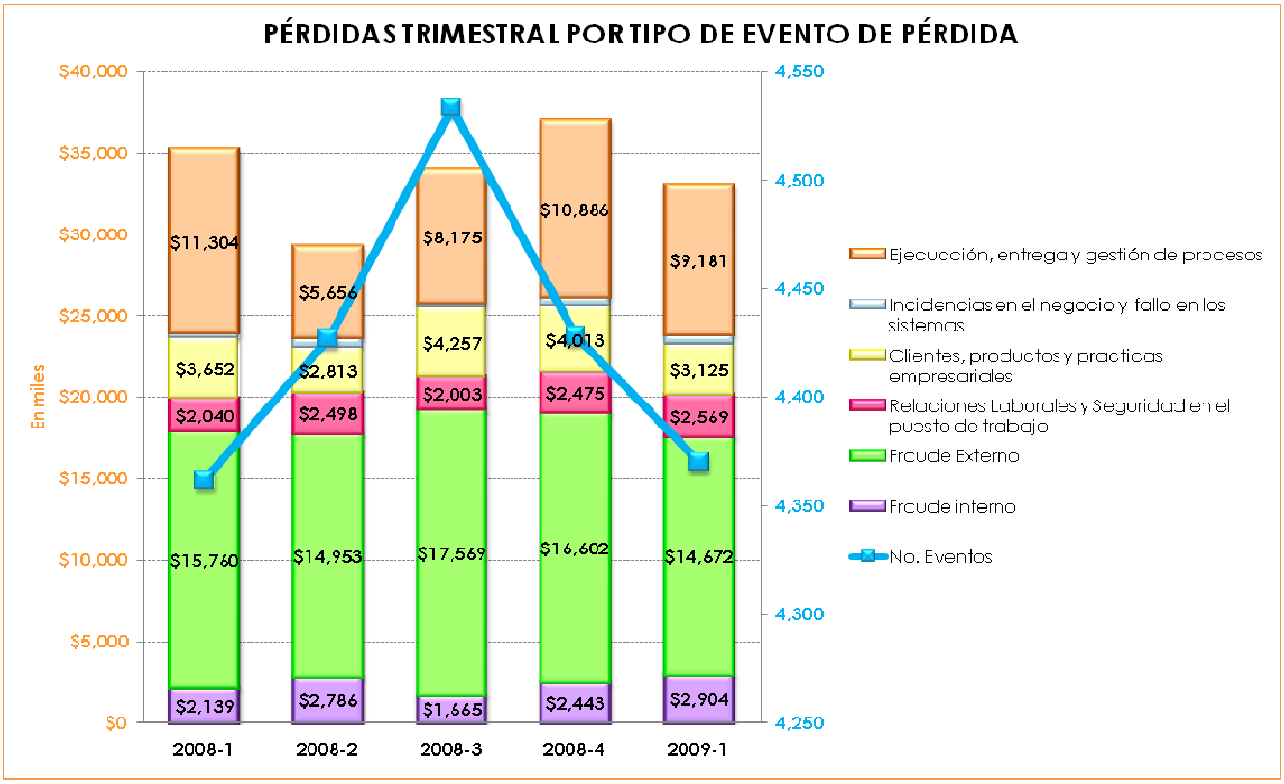
X. *Pérdida neta.* Corresponde a la suma de la pérdida bruta más los gastos adicionales menos las recuperaciones.

Resultados de la Base de Datos

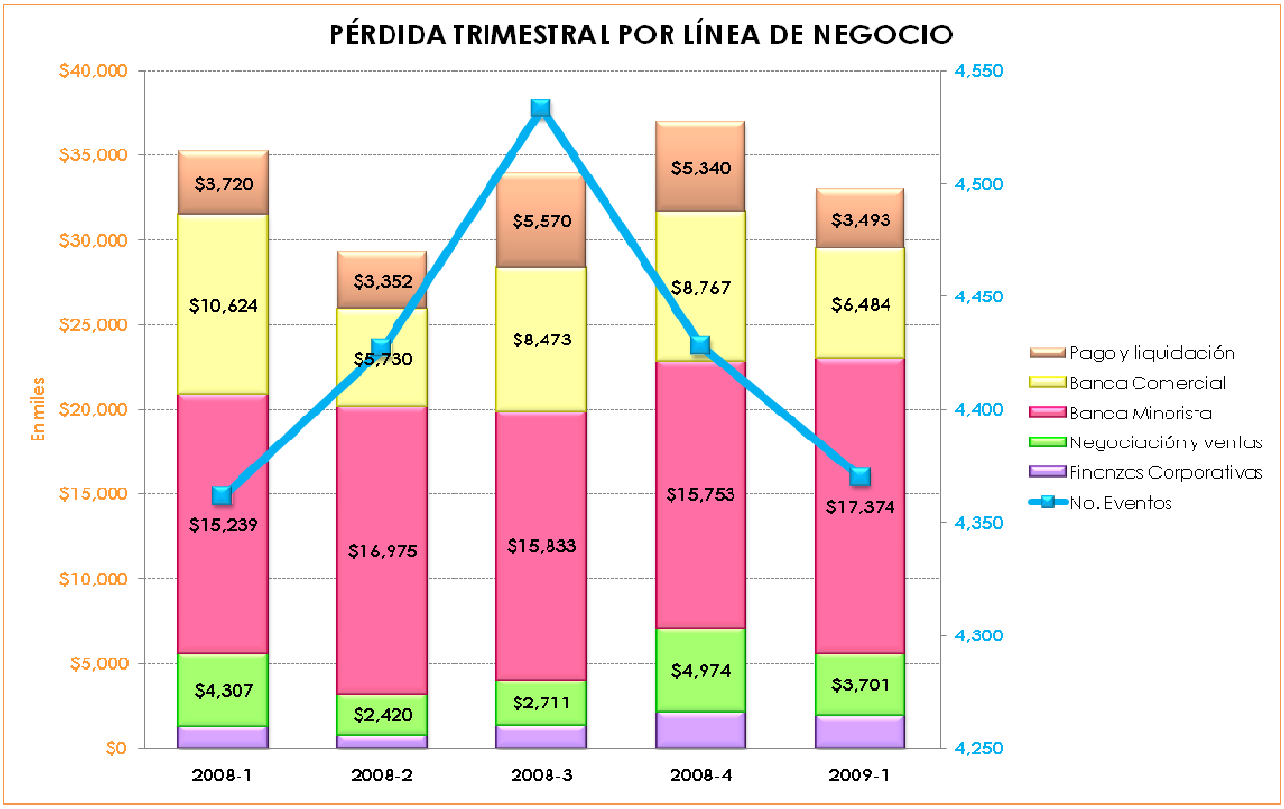
La información contenida en la Base de Datos corresponde a los 4 trimestres del 2008 y del primer trimestre del 2009, dando como resultado un total de 22,120 registros. En las tablas 6.3, 6.4 y 6.5 de los Anexos se muestran tres cuadros resumen de la información contenida en la Base de Datos. La Tabla 6.3 muestra la pérdida neta por nivel 1 y 2 (por evento de pérdida) trimestral, la Tabla 6.4 muestra la pérdida neta por línea de negocios trimestral y la Tabla 6.5 muestra la pérdida neta por factor de riesgo. A continuación se muestran la gráfica 3.1, 3.2, 3.3 y 3.4 las cuales muestran el comportamiento de la pérdida neta por semestre, por evento de pérdida, por línea de negocio y por factor de riesgo de los 5 trimestres analizados en la Base de Datos.



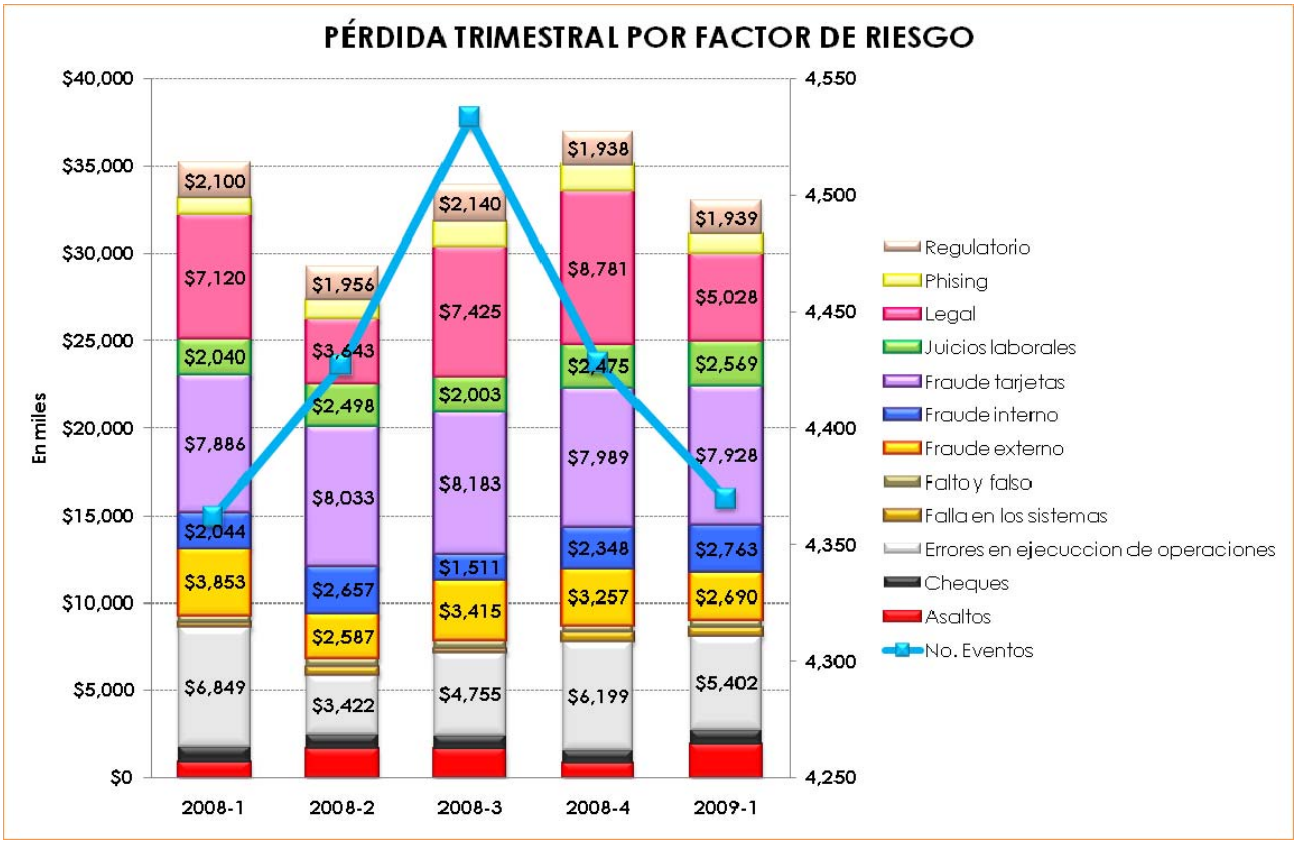
Gráfica 3.1



Gráfica 3.2



Gráfica 3.3



Gráfica 3.4

Conclusión de la Base de Datos

Después de analizar la información contenida tanto en la base como en las gráficas y los cuadros resumen se puede concluir que:

1. El trimestre que obtuvo mayor pérdida neta fue el cuarto trimestre del 2008 con una pérdida neta ***36.9 MM de pesos***. Así mismo se puede observar que el rango de las pérdidas netas por trimestre se mantuvo entre los ***28.5 MM de pesos*** y los ***37 MM de pesos***. Cabe señalar que la pérdida neta del 2008 fue de ***135.43 MM de pesos***.
2. El evento de pérdida que generó la mayor pérdida neta fue el fraude externo, registrando una pérdida de ***17.57 MM de pesos*** durante el tercer trimestre del 2008. La pérdida neta generada por este factor durante los 5 trimestres fue de ***79.56 MM de pesos***. El siguiente factor con mayor pérdida neta registrada es el de ejecución, entrega y gestión de procesos, el cual sufrió su mayor pérdida durante el primer trimestre del 2008 con un monto de ***11.30 MM de pesos*** y la pérdida neta total generada por este factor fue de ***45.20 MM de pesos***.
3. La línea de negocios que mayor pérdida neta obtuvo, fue la banca minorista con un monto de ***81.18 MM de pesos*** durante los 5 trimestres; dicho factor tuvo su mayor pérdida durante el primer trimestre del 2009 al alcanzar un monto de ***17.34 MM de pesos***. Por su parte la banca

comercial, registro su mayor pérdida durante el primer trimestre del 2008 por ***10.63 MM de pesos*** mientras que el acumulado de los 5 trimestres fue de ***40.08 MM de pesos***. El monto obtenido por la banca minorista está muy relacionado con la pérdida generada por el fraude externo, ya que para la banca comercial, el principal evento de pérdida es el fraude externo.

4. El factor de riesgo que generó mayor pérdida neta fue el fraude por tarjetas con un monto de ***40 MM de pesos***, seguido por los factores legal y errores en la ejecución de operaciones con un monto de ***32 MM de pesos*** y ***26.63 MM de pesos*** respectivamente durante los 5 trimestres estudiados. A pesar que el factor de riesgo legal está en tercera posición por el monto total, fue el factor que registro la mayor pérdida durante el cuarto trimestre del 2008 con un monto de ***8.79 MM de pesos***.

Los resultados obtenidos con la base de datos muestran que la pérdida neta promedio trimestral se mantuvo constante durante los cinco trimestres. Inclusive el número de eventos presentados al último trimestre no mostró una disminución considerable. Por ende es necesario analizar la necesidad de la implementación de planes de mitigación.

3.2 *Risk Control Self Assessment (RCSA).*

3.2.1 Objetivo

El Risk Control Self Assessment está relacionado con la etapa cualitativa del proceso de gestión de riesgo operacional, mediante el cual se busca identificar los riesgos operacionales significativos inherentes a los procesos y a la operación diaria de una institución. La identificación de riesgos es una fase fundamental y debe considerar el entorno interno y externo de cada unidad de negocios de la institución para determinar los factores que generan riesgo operacional, el cual puede afectar el logro de los objetivos, rentabilidad, competitividad, productividad y reputación de la Institución y materializarse en pérdidas.

Por otro lado, el proceso de identificación de riesgos permite a la Dirección de la institución tener una visión clara sobre la importancia de los diferentes tipos de exposición al riesgo operacional, con el objeto de alertarla en la toma de decisiones y acciones, como por ejemplo: revisar estrategias y políticas, actualizar o modificar procesos y procedimientos establecidos, implantar o modificar límites de riesgo, construir, incrementar o modificar controles, implantar planes de contingencia y de continuidad del negocio, entre otras.

3.2.2 Beneficios del Risk Control Self Assessment

La aplicación del Risk Control Self Assessment requiere de una inversión tanto en tiempo como en tecnología. A pesar de ello, las organizaciones pueden estar convencidas de que la aplicación del Self Assessment es necesaria para:

- Generar responsabilidades dentro de las áreas de la institución: las áreas administrativas son las responsables cuando se presentan problemas, relacionados con el riesgo operacional y son regularmente las más afectadas. Es por medio del Self Assessment que se logra hacer un análisis explícito por parte de los directores y gerentes generando una mayor responsabilidad ante los resultados obtenidos.
- Reforzar una cultura de transparencia: la ocurrencia de riesgos requiere de una discusión abierta que permita mejorar la conciencia de la institución ante los riesgos así como asignar de manera apropiada los recursos existentes; por medio del Risk Control Self Assesment se crean los espacios donde se puede discutir los riesgos que afectan a la Institución.
- Implementar un proceso proactivo más que un proceso reactivo: los negocios en general funcionan mejor cuando se prevén y corrigen los problemas antes de que estos ocurran. Por lo tanto, la prevención de pérdidas financieras es una meta fundamental e importante para cualquier institución. La aplicación del Self Assessment provee de una metodología para la identificación de las debilidades que se presentan dentro del proceso y desarrolla los planes de acción necesarios para eliminar dichos puntos débiles del proceso.

- Engranar las diferentes partes de la institución: el riesgo operacional tiene contacto con absolutamente toda la institución y por ende afecta cualquier relación existente entre áreas de soporte. El Self Assessment ayuda a derribar las barreras que impiden la comunicación sobre riesgos potenciales a lo largo de la institución.
- Asegurar que todos los riesgos sean considerados: el riesgo operacional no puede ser medido siempre a detalle ya que los indicadores de riesgo que se utilizan sólo miden y analizan la parte cuantitativa del riesgo dejando a un lado la parte cualitativa. El análisis cualitativo derivado de la utilización del Self Assessment asegura un análisis global del riesgo operacional.

3.2.3 Técnicas del Risk Control Self Assessment

No existe una técnica única para realizar el Risk Control Self Assessment. Los procesos tienden a evolucionar con el tiempo y a menudo estos cambios tienen como propósito continuar observando los riesgos que ya se han identificado, así como identificar nuevos riesgos potenciales. Las técnicas alternativas con los que cuenta el RCSA son:

I. *Listas de control (Checklist).* Probablemente es el enfoque más utilizado actualmente. Las listas de control son cuestionarios estructurados de acuerdo con la unidad de negocios a la que se la aplicará, con el fin de identificar el nivel de riesgos y los controles relacionados con ella. Algunos de estos cuestionarios son muy cortos pero con un gran número de categorías de riesgo. Mientras que otras proveen listas más detalladas las cuales incluyen los controles que deberían ser utilizados.

II. *Narraciones.* El punto inicial de las narraciones es diferente que el las listas de control pero el resultado que se obtiene es el mismo. Normalmente las narraciones comienzan definiendo los objetivos y los riesgos que conlleva cada unidad de negocios. En las narraciones en lugar de obtener los controles, que supuestamente debería tener la Institución, las unidades de negocio defienden la forma en que controlan los riegos operativos que se les presentan. Esta alternativa requiere un mayor esfuerzo y raciocinio por parte de las unidades de negocio en el marco de la definición de sus riesgos y controles.

III. *Talleres.* Esta alternativa busca eludir el trabajo en el papel y promover que el personal proponga los controles de los riesgos y cualquier mejora que se requiera. Los talleres son típicamente moderados por una persona líder y los participantes deben tener conocimiento del tema seleccionado a debatir. Los diferentes puntos de vista expuestos generan un mejor consenso y validación de los temas. Los talleres pueden ser utilizados en conjunto con las listas de control y narrativas ya que por medio de éstas se pueden obtener los temas primordiales.

3.2.4 Factores clave para el buen funcionamiento del Risk Control Self Assessment

Existen varios factores que permiten que el proceso del Self Assessment sea satisfactorio, entre los cuales están:

I. *Apoyo de la dirección*. Las Instituciones que intenten iniciar el proceso de RCSA sin el apoyo de la dirección general encontrarán una gran cantidad de dificultades para lograr resultados significativos; ya que los responsables de cada unidad de negocios no se tomarán el tiempo necesario para realizar el proceso y la evaluación no será tan honesta y acertada como se requiere, no se podrá determinar si los controles con los que se cuentan realmente están mitigando los riesgos operativos.

II. *Proceso permanente*. Para que el Self Assessment pueda ser considerado como una herramienta efectiva y funcional, la institución debe diseñarla como un proceso que debe ser ejecutado de manera regular y no como un evento aislado; por lo tanto el Self Assessment debe ser realizado por lo menos de manera anual. La finalidad de esto es obtener las mejoras o deterioros que han tenido los controles así como cualquier cambio que afecte a la Institución y que puede impactar directamente en la productividad y en los resultados del negocio.

III. *Identificación de riesgos de lo general a lo particular*. El primer paso para crear un programa de RCSA funcional es identificar categorías de riesgo generales en toda la institución. Es importante mantener esta selección de categorías lo más ampliamente posible mientras que sea un número de riesgos manejable. Todo esto con el fin de encontrar categorías de riesgo específicas que nos permitan conocer los riesgos operacionales potenciales.

3.2.5 Presentación de Resultados

Exponer los resultados obtenidos de la aplicación del Self Assessment es sumamente importante, ya que estos actúan como un termómetro que expone la condición en la que se encuentra la institución ante el riesgo operacional, es de cir, que tan vulnerable o fortalecida se encuentra la institución para hacer frente ante los riesgos. Por lo tanto el reto es la forma en la que se comunicarán los resultados. Algunas herramientas que permiten comunicar los resultados son:

- *Top-10 risks lists*: como resultado de la aplicación del Self Assessment surgirá una lista con los riesgos más importantes a los cuales la institución está expuesta, la naturaleza de dicho riesgos y la manera en la que se buscara resolverlos.
- *Heat maps*: los heat maps son representaciones gráficas que permiten ver la relación que guarda una variable con respecto de otra. La forma en que se denota el tipo de relación que guardan las variables es a través de colores (usualmente se utilizan los colores rojo, amarillo y verde) que asemejan a un semáforo donde el rojo denota que se tiene un riesgo que es potencialmente alto y requiere que se tomen medidas inmediatas, el amarillo significa que se debe tener precaución

con dichos riesgos para evitar que se conviertan en riesgos y el verde que simboliza que todo está en orden y que se puede continuar operando de la misma manera.

3.2.6 Caso Práctico Risk Control Self Assesment de Riesgo Operacional

Como anteriormente se mencionó, la aplicación del Self Assessment puede llevarse a cabo mediante el uso de diferentes técnicas; para el desarrollo del caso práctico que a continuación se expondrá se usaron tanto las listas de control, la narración y los talleres.

La metodología del Risk Control Self Assessment que esta tesis propone consta de tres partes: la encuesta de auto-evaluación, un taller de análisis y discusión de los resultados de la encuesta y por último la priorización de riesgos y el establecimiento de planes de mitigación.

Encuesta de Auto-evaluación

El proceso de la encuesta de auto-evaluación consiste en enviar a cada uno de los participantes previamente seleccionados por la unidad de negocios que se auto-evaluará, encuestas que deberán contestar y devolver al coordinador del proceso. La encuesta se dividirá en dos partes: la primera está diseñada para obtener información sobre factores del clima organizacional, gerencia y recursos humanos que de no ser identificados y mitigados pueden desencadenar en eventos de pérdida, mientras que la segunda contiene categorías de riesgo específicas que igualmente pueden generar pérdidas económicas a la institución.

Primera parte de la encuesta de RCSA

En la tabla 6.6 de los anexos se muestra el contenido de la primera parte de la encuesta de Risk Control Self Assessment la cual está dividida en 4 segmentos:

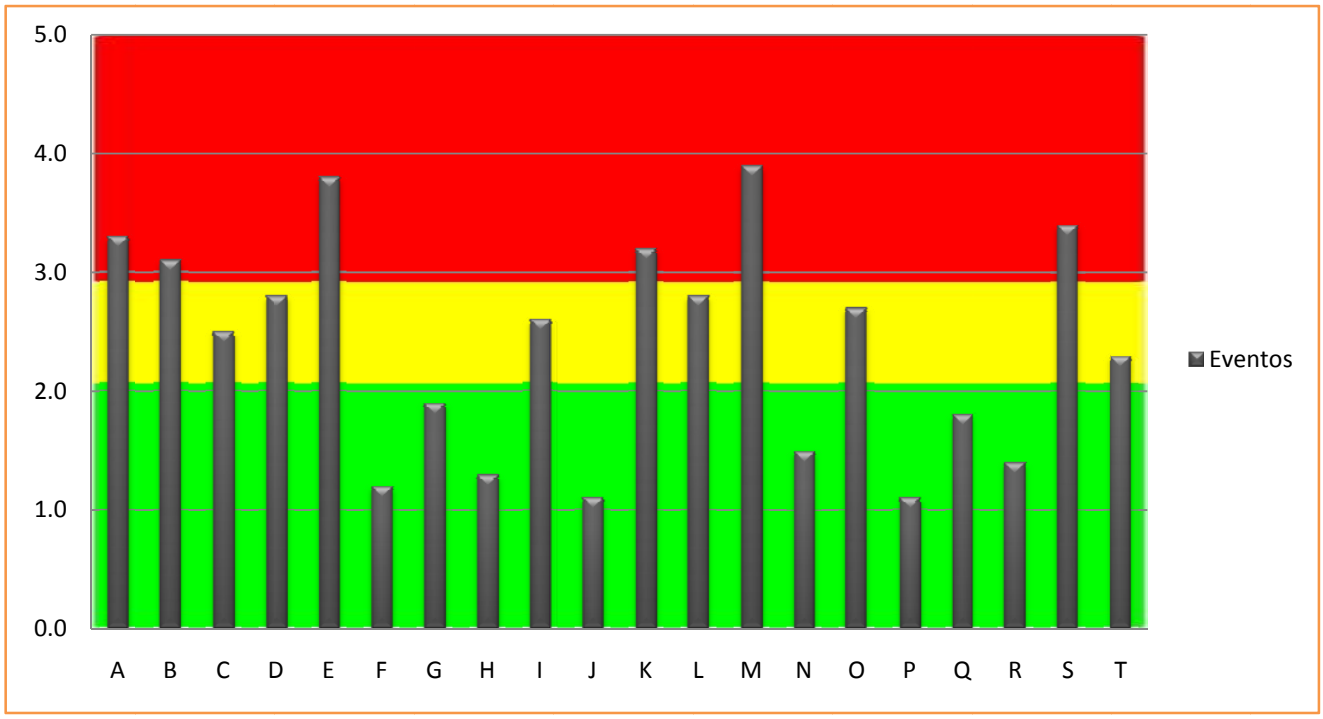
- *Sección*. Muestra las secciones de los aspectos que se están evaluando: Clima organizacional, Gerencia y Recursos humanos.
- *Referencia*. Asigna una letra a cada aspecto lo que permite hacer referencia a cada uno de estos de forma más rápida y sencilla.
- *Descripción.* Especifica los aspectos que se pide evaluar de cada una de las secciones de la columna Sección.
- *Escala.* Establece la escala de valores a considerar para la evaluación; siempre, casi siempre, algunas veces, casi nunca y nunca.

Una vez que se tiene la encuesta contestada la información se graficará sobre una plantilla dividida en tres secciones, para cada sección corresponderá un color de acuerdo a lo siguiente:

Tabla 3.1 Código de colores Primera Sección	
Color	**Descripción**
	Determina que el evento graficado no representa ningún riesgo para la Institución.
	Hace referencia a una señal de advertencia, ya que el evento graficado puede representar un riesgo latente para la Institución.
	Significa que el evento graficado es un riesgo alto para la institución y debe ser corregido de inmediato.

Resultados de la primera parte del Risk Control Self Assessment

En la gráfica 3.5 se observan los resultados obtenidos después de la aplicación de la primera parte de la encuesta de auto-evaluación, cabe señalar que se aplicaron 30 encuestas para realizar el análisis.



Gráfica 3.5

Se puede observar que bajo el código de colores anteriormente establecido, los aspectos que representan un riesgo para la institución son:

Tabla 3.2 Cuadro resumen con los resultados de la primera parte de la encuesta			
Ref.	**Descripción**	**Frecuencia**	**Color**
A	Nuestra unidad trabaja bajo lineamientos y códigos de ética.	3.3	
B	Nuestra unidad fomenta el cumplimiento de los principales valores tales como: integridad, respeto, honestidad, justicia.	3.1	
E	Los miembros de la unidad de negocios se sienten satisfechos con su trabajo.	3.8	
K	Nuestra unidad cuenta con medidas para prevenir la corrupción.	3.2	
M	Nosotros damos seguimiento de los resultados conseguidos de acuerdo con los objetivos y planes establecidos.	3.9	
S	La actual tasa de rotación de personal no afecta significativamente la operación de nuestra unidad.	3.4	
C	Nosotros no comprometemos nuestra integridad personal para alcanzar los objetivos de la unidad.	2.5	
D	Nuestra unidad tiene claramente definidas las funciones de cada puesto y los limites de las responsabilidades.	2.8	
I	Nuestra unidad hace buen uso de los recursos que le son asignados.	2.6	
L	Los objetivos y metas establecidas en la unidad constituyen un incentivo alcanzable.	2.8	
O	Dentro de la unidad no se suelen recibir órdenes contradictorias de diferentes personas.	2.7	
T	Nuestros niveles de personal son adecuados para cumplir con la carga de trabajo requerida y los objetivos trazados.	2.3	

Cabe mencionar que los aspectos en rojo son situaciones que representan un riesgo significativo para la institución; asimismo se observa que 6 aspectos evaluados se encuentran en el área amarilla, muy próxima al área roja de la gráfica 3.5 y que podrán convertirse en un riesgo para la institución.

Conclusiones de la primera parte del Risk Control Self Assessment

La primera parte de la encuesta identificó riesgos que de no ser atendidos pueden desencadenar en eventos de pérdida para la institución. Por lo tanto, es necesario que para cada uno de dichos riesgos se lleve a cabo un análisis y en su caso se diseñen planes de acción que permitan mitigarlos y tener control sobre ellos para poder minimizarlos. A pesar de que por medio del Risk Control Self Assessment se detectaron 12 riesgos que pueden desencadenar en una pérdida, es necesario que se realice una revisión de cada uno de dichos riesgos y se determine cuales son

representativos e importantes y cuáles pueden ser eliminados. Para realizar la revisión es necesario que se reúnan tanto los encargados de aplicar el Risk Control Self Assesment como los dueños del proceso evaluado con el fin de determinar que riesgos son representativos para el proceso. A continuación se muestran los riesgos que, una vez realizada la revisión en el taller de análisis y discusión, se concluyó que, son considerados importantes y por lo tanto se tomaran medidas de necesarias para mitigarlos:

- **A.** Nuestra unidad trabaja bajo lineamientos y códigos de ética.
- **D.** Nuestra unidad tiene claramente definidas las funciones de cada puesto y los limites de las responsabilidades.
- **I.** Nuestra unidad hace buen uso de los recursos que le son asignados.
- **K.** Nuestra unidad cuenta con medidas para prevenir la corrupción.
- **L.** Los objetivos y metas establecidas en la unidad constituyen un incentivo alcanzable.
- **M.** Nosotros damos seguimiento de los resultados conseguidos de acuerdo con los objetivos y planes establecidos.
- **O.** Dentro de la unidad no se suelen recibir órdenes contradictorias de diferentes personas.
- **T.** Nuestros niveles de personal son adecuados para cumplir con la carga de trabajo requerida y los objetivos trazados.

El desarrollo de los planes de mitigación que estarán a cargo de la unidad auto-evaluada se muestra más adelante ya que los planes de acción forman parte de la etapa de seguimiento dentro de la Gestión de Riesgo Operacional.

Segunda parte de la encuesta RCSA

En las tablas 6.7 y 6.8 de los Anexos se muestra la segunda parte de la encuesta de Risk Control Self Assessment la cual está dividida en dos partes; la primera está dirigida a evaluar las funciones de la unidad auto-evaluada y la segunda está dirigida a evaluar las funciones de las unidades de soporte. Es decir, en la primera se evalúan las funciones de la unidad que está se ésta auto-evaluando, mientras que en la segunda la misma unidad evalúa funciones de apoyo que otras unidades le brindan. La segunda partes del Risk Control Self Assessment al igual que la primera parte se encuentra dividida en 4 segmentos:

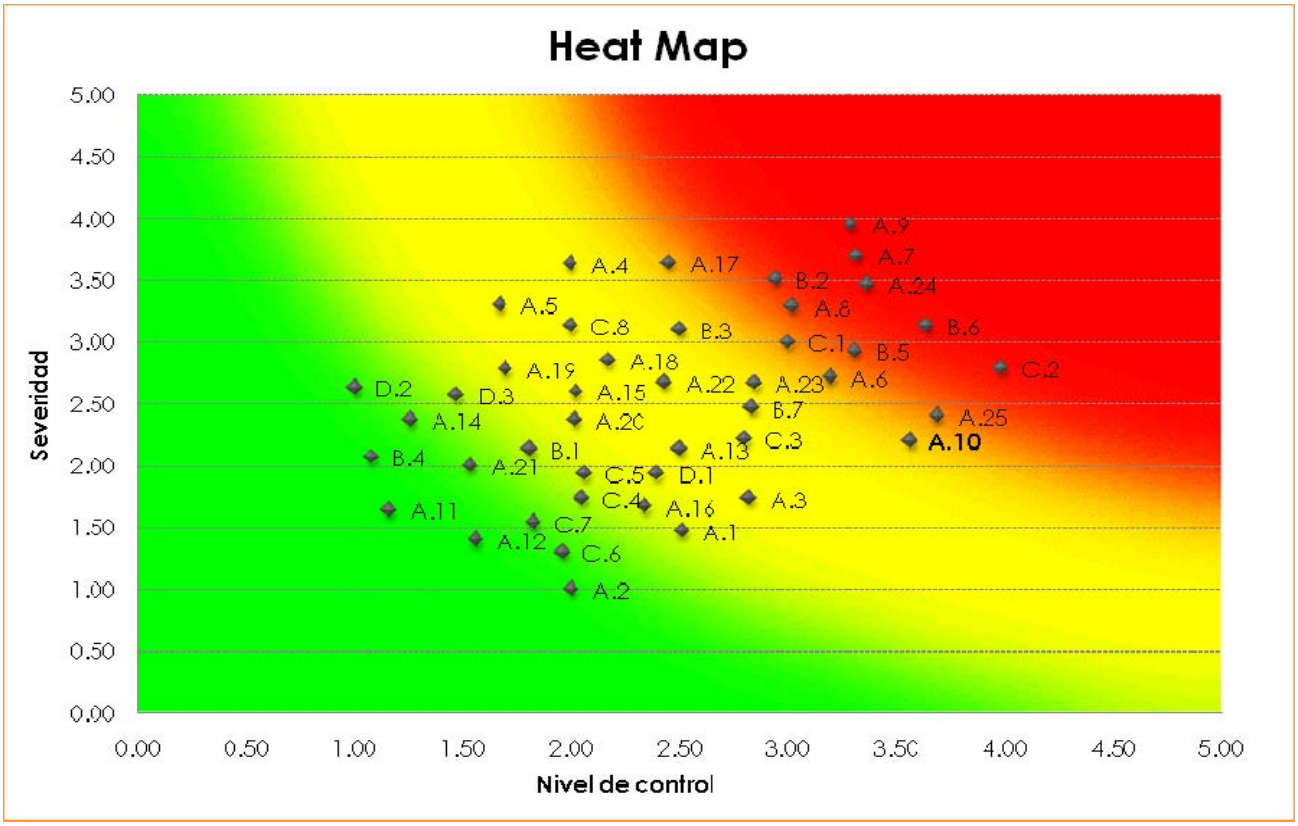
- *Sección.* Especifica el concepto que se está evaluando; procesos, sistemas, personal y eventos externos.
- *Referencia.* Asigna una letra que permite referirse a cada categoría de riesgo de forma más rápida y sencilla.
- *Descripción*. Especifica los aspectos que se quiere evaluar de cado de los conceptos de la columna Sección.

- *Escala.* Establece la escala de valores a considerar para evaluar: severidad (nulo, insignificante, moderado, significante, fuerte y no aplica) y nivel de control (total, alto, medio, bajo, nulo y no aplica)

El código de colores que se utilizó en la primera parte de la encuesta se conserva para la segunda con la diferencia que los factores de riesgo son esquematizados en una gráfica con nivel de control en el eje X y severidad en el eje Y.

Resultados de la segunda parte del Risk Control Self Assessment

En la gráfica 3.6 se observan los resultados obtenidos de la encuesta de auto-evaluación en su segunda parte. Se puede observar que las categorías que representan un riesgo significativo para la institución son aquellos puntos en la gráfica que se encuentran dentro de la zona roja; como se había mencionado anteriormente, estos riesgos son significativos. Además, existen riesgos ubicados en la zona amarilla que fueron tomados en cuenta debido a que una mínima variación de la severidad o del nivel de control puede colocar a dichos puntos dentro de la zona roja.



Gráfica 3.6

A continuación se presenta una lista con los riesgos localizados en la zona roja de la gráfica 3.6 así como los riesgos ubicados en la zona amarilla y que fueron tomados en consideración para su análisis y discusión:

Procesos
- A.6. Los procesos no cumplen con las necesidades del cliente.
- A.7. Las operaciones no se apegan a las políticas, procedimientos y controles existentes.
- A.8. Ineficiente proceso para la detección, corrección y/o reporte de los errores causados durante las operaciones.
- A.9. Es ineficiente el control de desvíos de fondos.
- A.10. Existe uso indebido de facultades y poderes por parte del personal de la unidad de negocios.
- A.17. La planeación de las actividades a desarrollar es deficiente.
- A.23. Falta comunicación y coordinación entre unidades de negocio.
- A.24. El flujo de trabajo entre unidades de negocios es deficiente.
- A.25. La información requerida de otras unidades no es oportuna.

Personal
- B.2. Se realizan despidos injustificados o fuera de las políticas de la compañía.
- B.3.Existen lesiones de clientes y empleados en las instalaciones debido a l incumplimiento de la normativa de seguridad e higiene.
- B.5. La organización y clima laboral no favorecen la realización de actividades.
- B.6. Capacitación deficiente de nuevos productos y/o servicios.
- B.7. Los roles y responsabilidades de las unidades no están definidas claramente.

Sistemas
- C.1. El sistema de seguridad es vulnerable ante ataques e intrusiones informáticas.
- C.2. Existe robo de información privilegiada de los clientes.

Conclusiones de la segunda parte del RCSA

Como se puede observar en la grafica 3.6, se muestran los riesgos tanto de la encuesta de las funciones de la unidad evaluada como la encuesta de la funciones de soporte de otras unidades. Es importante aclarar que para el análisis y discusión los resultados se tomaron en cuenta los riesgos que estaban en la zona roja, así como los riesgos que se hallaron en la frontera entre la zona roja y amarilla. Al igual que para la primera parte del Risk Control Self Assessment es necesario establecer los riesgos que, una vez realizada una segunda evaluación de cada uno de ellos, se consideraron significativos y por lo tanto es necesario establecer planes de acción para ellos. Los riesgos que fueron identificados como significativos corresponden a:

Procesos

- A.6. Los procesos no cumplen con las necesidades del cliente.
- A.7. Las operaciones no se apegan a las políticas, procedimientos y controles existentes.
- A.8. Ineficiente proceso para la detección, corrección y/o reporte de los errores causados durante las operaciones.
- A.9. Es ineficiente el control de desvíos de fondos.
- A.10. Existe uso indebido de facultades y poderes por parte del personal de la unidad de negocios.
- A.17. La planeación de las actividades a desarrollar es deficiente.
- A.23. Falta comunicación y coordinación entre unidades de negocio.

Personal

- B.2. Se realizan despidos injustificados o fuera de las políticas de la compañía.
- B.3. Existen lesiones de clientes y empleados en las instalaciones debido al incumplimiento de la normativa de seguridad e higiene.
- B.5. La organización y clima laboral no favorecen la realización de actividades.

Sistemas

- C.1. El sistema de seguridad es vulnerable ante ataques e intrusiones informáticas.
- C.2. Existe robo de información privilegiada de los clientes.

3.3 *Plan de acción*

3.3.1 Objetivo

El plan de acción está relacionado con la etapa de mitigación y seguimiento dentro del proceso de Gestión de Riesgo Operacional. La mitigación consiste en identificar las herramientas y controles que permitirán a la institución reducir la probabilidad de ocurrencia de pérdidas y el seguimiento consiste en verificar que los planes cumplan con su objetivo en el tiempo previamente establecido.

Es recomendable elaborar un plan de acción cuando se necesita organizar el trabajo y no se tiene muy claro por dónde empezar; asimismo el plan de acción sirve para distribuir las actividades y optimizar el tiempo que se utiliza para realizar una tarea. Elaborar un plan de acción es muy útil para definir las acciones y tareas que se deben realizar, asignar los responsables de cada tarea y las fechas de inicio y término de las actividades.

En una institución, se suele buscar soluciones una vez avanzado el problema, lo que conlleva a estar apagando fuegos, en lugar de atacar el problema de raíz. La forma más sencilla de solucionar de raíz los problemas prioritarios con los que cuenta la institución (considerando como prioritarios aquellos que afecten sus resultados) es dividirlo en partes más pequeñas. Esto permite resolver el problema de lo particular a lo general, garantizando así el pleno conocimiento y solución de la raíz del problema.

Lo primero con lo que debe contar un plan de acción es un objetivo claro, conciso y medible. No es posible comenzar con un plan de acción si no se conoce lo que se quiere lograr con él ni el tiempo que se va a tomar para realizarlo. Una vez que se tiene el objetivo se deben especificar las estrategias que se seguirán para lograrlo. Las estrategias deben mostrar en forma general lo que se está planeando hacer, sin que necesariamente especifiquen exactamente lo que se va a realizar. Dichas estrategias deben mostrar el camino que se seguirá durante el desarrollo y la ejecución del plan de acción. Después de esto, se deben establecer los pasos a seguir para materializar las estrategias propuestas, es decir, se deben plantear de manera detallada y específica las tareas que se llevaran a cabo para lograr el objetivo. Por último, dentro del plan de acción, se deben asignar los responsables de cara tarea, quienes preferentemente deben de estar involucrados directamente con la elaboración del plan de acción.

Una vez que se cuenta con todos los elementos antes mencionados, se procede con la ejecución del plan de acción por lo que cada responsable debe conocer de ante mano las tareas y actividades que debe llevar a cabo para cumplir las estrategias planteadas y por ende lograr el

objetivo final del plan de acción. Es justo en este punto donde el seguimiento del plan de acción toma una vital importancia puesto que ya que se cuenta con los datos específicos tanto de las actividades que se van a realizar como de los tiempos establecidos para cada actividad; se hace necesario tener reuniones de evaluación con el fin de supervisar los avances de cada una de las tareas, realizar anotaciones y definir los que ya se ha cumplido, lo que hace falta y lo que requiere una segunda evaluación con el fin de conseguir el cumplimiento del objetivo. El seguimiento del plan de acción facilita la identificación de necesidades insatisfechas que podrían derivar en el incumplimiento de las tareas y por lo tanto del objetivo.

Es importante que dentro del plan de acción se cuente con una sección enfocada a las fechas de revisión y supervisión donde se indique el avance en porcentaje y comentarios que pueden ser de gran ayuda para el análisis y para la evaluación final. Una vez que se han cumplido los plazos establecidos del plan de acción, es necesario realizar una revisión a conciencia del cumplimiento o incumplimiento del objetivo o plantearse nuevos retos. Esto sirve como reafirmación del compromiso de continuar con el nivel alcanzado hasta el momento.

Finalmente a manera de resumen, los elementos que deben estar incluidos en la elaboración de un plan de acción son:

- Objetivo claro, conciso y medible.
- Estrategias que reflejen el camino a seguir para lograr el objetivo.
- Tareas que describan los pasos exactos para el cumplimiento de las estrategias.
- Tiempos reales de cumplimiento en inicio y fin de cada tarea.
- Responsables directos de cada tarea.
- Seguimiento constante y evaluación de cumplimiento.
- Evaluación final para replanteamiento del plan de acción o elaboración de otro.

3.3.2 Caso Práctico Plan de Acción

Una vez que se han identificado las categorías de riesgo significativas para la institución, se deben desarrollar los planes de acción pertinentes. En el capítulo anterior se obtuvieron los riesgos significativos por medio del Risk Control Self Assessment; a dichos riesgos se les realizó posteriormente una segunda evaluación para determinar los que requieren se les diseñe un plan de acción. Para el ejemplo del presente trabajo se van a desarrollar los planes de acción tanto de la primera como de la segunda parte de la encuesta de auto-evaluación realizada en el capitulo anterior.

En la tabla 6.9 de los anexos se muestran los planes de acción de los riesgos significativos identificados en la primera parte de la encuesta, mientras que en la tabla 6.10 de los anexos se

muestran los planes de acción de los identificados en la segunda parte de la encuesta. Cada una de las tablas esta divida en los siguientes conceptos:

- *Sección*. Especifica el concepto al cual se le va a diseñar el plan de acción.
- *Referencia*. Código de referencia que se utilizó en el capítulo de la encuesta de Risk Control Self Assessment para cada uno de las categorías de riesgo.
- *Descripción*. Detalla la categoría de riesgo.
- *Impacto.* Representa la importancia que tiene la categoría de riesgo además del tiempo de respuesta que éste requiere para ser mitigado. La nomenclatura utilizada en esta columna esta descrita en la siguiente tabla:

Tabla 3.3 Descripción de los niveles de impacto	
Impacto	**Significado**
1 Muy alto	El riesgo es crítico para el proceso por lo que requiere de una acción inmediata
2 Alto	El riesgo es importante en el proceso por lo que se ejecutará la acción a corto plazo (2 meses)
3 Medio	El riesgo es poco importante para el proceso por lo que la acción se realizará a mediano plazo (8 meses)
4 Bajo	El riesgo no es relevante por lo que se atenderán en el proceso del día a día

- Acción. Describe el plan de acción que se tomará para mitigar los riesgos operacionales significativos identificados.

Conclusiones de los planes de acción

Los planes de acción tiene como principal objetivo planear las medidas que se van a llevar a cabo para mitigar los riesgos encontrados. Esto incluye tanto las acciones que se van a tomar como el período de tiempo que se requiere para ejecutarlas. Aquí radica la importancia del impacto, establecido en la Tabla 3.3, que tiene cada una de los riesgos. Para nuestro ejemplo se obtuvieron los siguientes resultados:

Tabla 3.4 Número de riesgos observados por nivel de impacto	
Impacto	**No. de riesgos identificados**
1	7
2	8
3	4
4	1

3.4 Indicadores de riesgo (Key Risk Indicators)

3.4.1 Objetivo

Los indicadores de riesgo están relacionados con la etapa de identificación y seguimiento dentro de la Gestión de Riesgo Operacional. El dar seguimiento a un riesgo permite detectar las exposiciones al riesgo operacional y corregir de manera rápida y oportuna las deficiencias en las políticas, procesos y procedimientos de la institución. La evaluación periódica de los eventos de pérdida por medio de los indicadores de riesgo permite identificar factores de riesgo que se pueden materializar en eventos de pérdida. Los indicadores de riesgo son variables relacionadas con la materialización de riesgos operacionales y pueden actuar como un complemento del proceso del Risk Control Self Assessment generando así un análisis continúo de la efectividad de los controles que tenga la Institución.

Mientras que el proceso del Risk Control Self Assessment se realiza de manera anual, los indicadores de riesgo pueden medirse a diario. Los indicadores son una ayuda que permite que la Gestión de Riesgo Operacional sea un proceso dinámico y genere esbozos actualizados de los riesgos potenciales que pudiera tener la institución.

Cuando se establecen los indicadores de riesgo como parte de la Gestión de Riesgo Operacional existen objetivos primordiales que deben tomarse en cuenta. En primer lugar, los indicadores deben ser sensibles al riesgo, es decir, deben ser capaces de dar a conocer los posibles cambios de la exposición al riesgo. Además los indicadores deben ser consistentes al mostrar los eventos de pérdida sufridos y deberán ser capaces de revelar el riesgo al que se está expuesto por unidad de negocio o proceso.

Paralelamente los indicadores cuentan con limitantes, por ejemplo, muchos indicadores son muy específicos para un riesgo en particular o solo son útiles para una unidad de negocios. Es por esto que resulta difícil diseñar un marco que sea homogéneo para todas las líneas de negocios y todos los eventos de pérdida. Cabe señalar que a pesar de que se haga un esfuerzo por diseñar los indicadores de riesgo, en ocasiones no existirá una correlación entre los indicadores de riesgo y los eventos de pérdida actuales. Es por ello que no siempre se sabe qué indicadores serán predictivos y tampoco se puede conocer el tipo de pérdida que están alertando.

Los indicadores de riesgo son generalmente utilizados por dos tipos de usuarios. Los primeros, son los encargados de la Gestión del Riesgo Operacional quienes administrarán los eventos de pérdida específicos originados por el Riesgo Operacional. Los segundos son los gerentes de cada unidad de negocio quienes serán los que definan y acepten los indicadores de riesgo apropiados

que serán utilizados. Es aquí donde la Gestión de Riesgo Operacional define a los indicadores de riesgo como una herramienta que provee transparencia y genera la comunicación necesaria sobre el comportamiento de los eventos de riesgo.

Mejorar la efectividad en términos de la sensibilidad al riesgo debe ser un objetivo que tengan muy presentes los encargados de la Gestión de Riesgo Operacional. La sensibilidad definirá si los indicadores de riesgo son una medida adecuada para los eventos de pérdida o representan otro tipo de problema. La evaluación de la efectividad de los indicadores de riesgo regularmente inicia cuando de manera intuitiva se eligen los indicadores de riesgo que se cree pueden ser sensibles ante eventos de pérdida futuros. El último paso está encaminado en encontrar los indicadores de riesgo que guarden una correlación entre los factores de riesgo y los eventos de pérdida.

3.4.2. Caso Práctico Indicadores de RIesgo

Los indicadores de riesgo buscan analizar el comportamiento que han tenido los factores de riesgo a lo largo del tiempo para establecer medidas que permitan prevenir futuros eventos de pérdida. Los indicadores que se utilizaron en este trabajo están basados en los factores de riesgo establecidos en la base de datos. Se calcularon 3 indicadores por cada factor de riesgo los cuales se mencionan a continuación: pérdida neta por trimestre, número de eventos que se presentaron por trimestre y el promedio de pérdida trimestral por factor. En las Tablas 6.11, 6.12 y 6.13 de los anexos se encuentra la información de cada uno de los factores de riesgo, por trimestre y por cada uno de los indicadores.

Para elaborar los indicadores de riesgo se eligió una periodicidad trimestral de tal forma que se pudiera evaluar el comportamiento del factor a lo largo del tiempo.

Resultados de los indicadores de riesgo

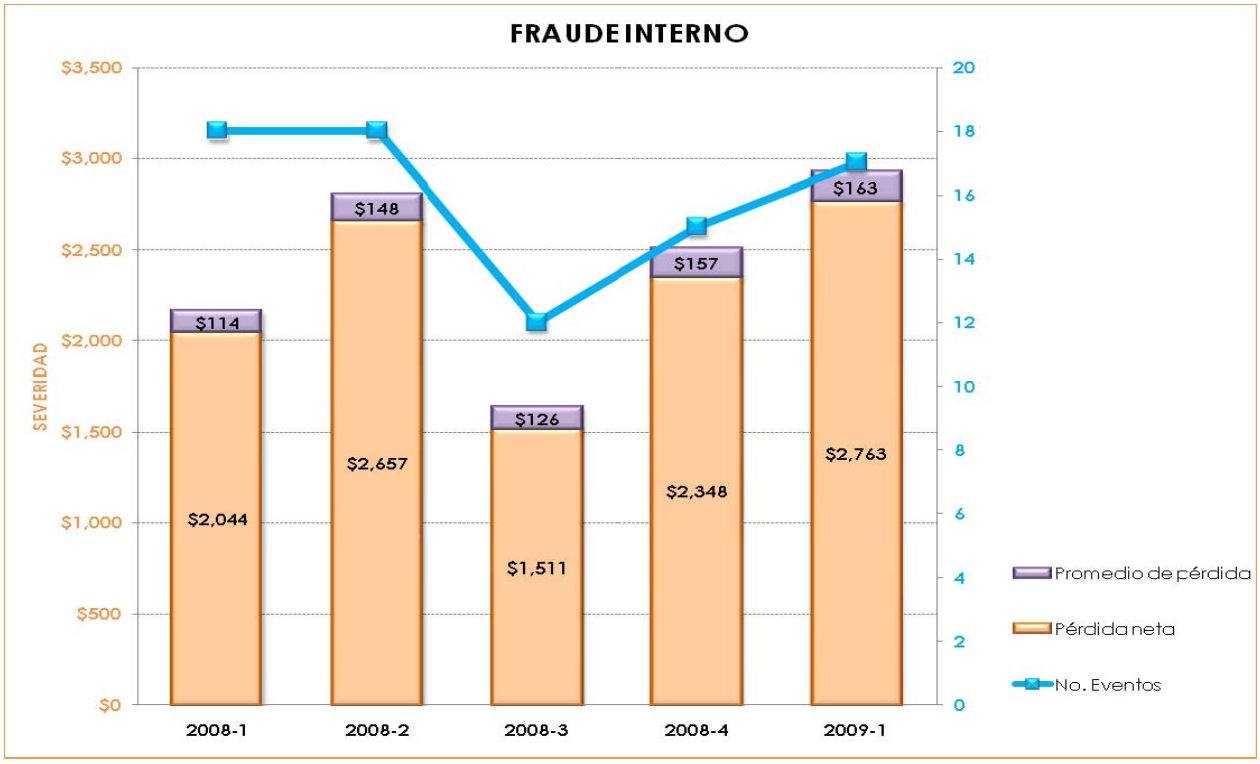
Una vez que se obtuvieron los valores de cada uno de los indicadores por trimestre y por factor, fueron graficados para observar su comportamiento en el tiempo. Para poder clasificar cada uno de los factores de riesgo se utilizó el siguiente código de colores:

Tabla 3.5 Código de colores de los indicadores de riesgo

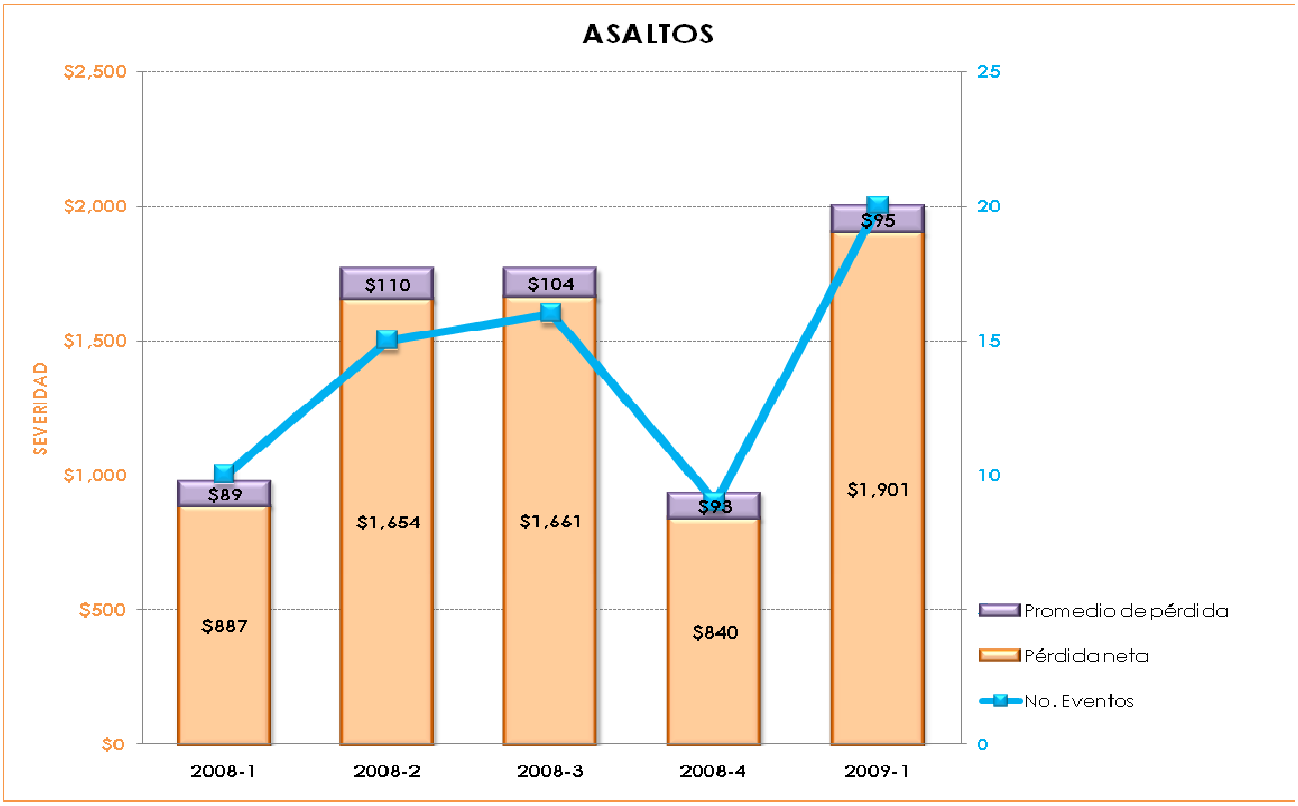
Color	Significado
	Factores de riesgo que representan un riesgo de pérdida bajo, ya que tiene una tendencia estable o a la baja.
	Factores de riesgo que representan un riesgo de pérdida medio ya que muestran una tendencia a incrementarse en el futuro o presentan variaciones con respecto a una tendencia estable.
	Factores de riesgo que representan un riesgo de pérdida alto ya que se ha incrementado sustancialmente la exposición a este riesgo.

A continuación se encuentra una tabla resumen con los factores de riesgo, así como la clasificación que obtuvieron según el código antes descrito. También se pueden observar las gráficas de aquellos factores de riesgo que fueron catalogados dentro del código rojo.

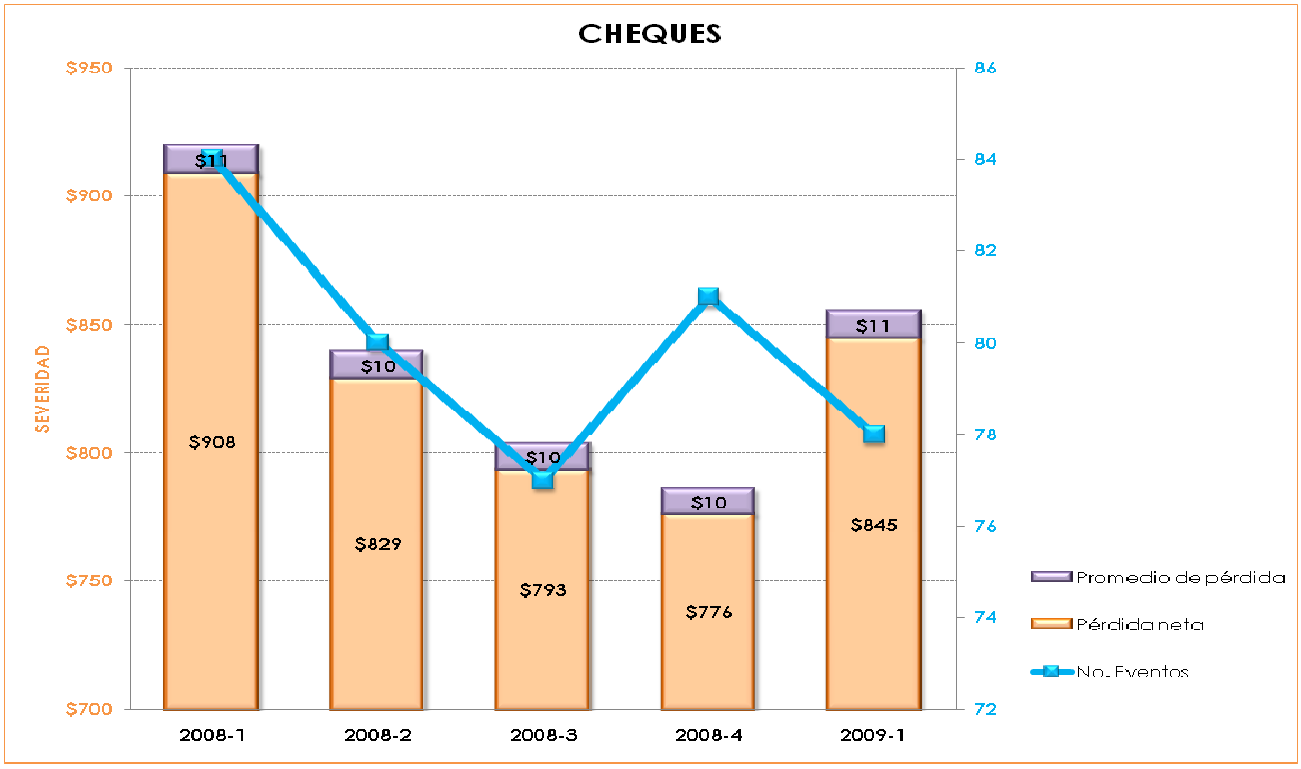
Tabla 3.6 Código de colores para los indicadores de riesgo	
Factor Código	
Legal	
Fraude Externo	
Fraudes Tarjetas	
Regulatorio	
Phishing	
Juicios Laborales	
Falto y Falso	
Fallas de Sistemas	
Errores en Ejecución de Operaciones	
Fraude Interno	
Asaltos	
Cheques	



Gráfica 3.7



Gráfica 3.8



Gráfica 3.9

Conclusiones de los indicadores de riesgo

Como anteriormente se mencionó, los indicadores de riesgo nos permiten evaluar el comportamiento de un factor de riesgo con una periodicidad menor que el RCSA. De esta forma se pueden analizar variaciones que se presenten de manera esporádica y sin periodicidad aparente. En nuestro ejemplo los factores a los que se les tiene que dar seguimiento debido al comportamiento observado fueron:

- *Fraude interno.* Este factor tuvo un decremento en los tres indicadores en el tercer trimestre del 2008, pero comenzó a crecer a partir del 4 trimestre y la tendencia hasta el momento es creciente. Por lo tanto se debe de prestar especial atención en dicho factor.
- *Asalto.* Es importante tomar en cuenta que éste indicador a pesar de tener una caída en el cuatro trimestre del 2008 en cuanto a la pérdida neta y el número de eventos el primer trimestre del 2009 comenzó a incrementarse y la tendencia es que siga subiendo. Además el promedio de pérdida neta se ha mantenido alto y constante a lo largo del año pasado y lo que va del presente.
- *Cheques.* Se debe dar seguimiento a este factor ya que el promedio de pérdida neta que tuvo durante el primer trimestre de este año fue muy elevado lo que significa que han disminuido el número de eventos presentados pero se ha incrementado el monto relacionado a cada uno de los eventos, es decir, cada evento genera una mayor pérdida.

En otras palabras, la institución tiene un eslabón débil en lo que respecta a los controles internos que evitan se cometan operaciones sin autorización, robo de información por parte de los empleados, entre otros eventos de pérdida. Además la seguridad de las sucursales es vulnerable, debido al gran número de asaltos que se presento durante el año así como la pérdida derivada de éstos. Igualmente la institución carece de las herramientas para verificar la autenticidad de cheques falsos ya que se han convertido en una fuente generadora de pérdidas económicas.

3.5 Niveles de tolerancia

3.5.1 Objetivo

Los niveles de tolerancia al igual que los indicadores de riesgo son herramientas incluidas en las etapas de identificación y seguimiento dentro de la Gestión de Riesgo Operacional. La importancia de los niveles de tolerancia radica en el establecimiento de un límite máximo de tolerancia a las pérdidas. De esta manera se evita tomar medidas de acción en pérdidas con bajo monto que representarían una mayor inversión para evitarlas que la pérdida que generan. Por otro lado el nivel superior establece el máximo valor que la institución está dispuesta a perder antes de tomar acciones.

A continuación se presentan algunas definiciones que son establecidos por la Comisión Bancaria y de Valores (CNBV) respecto a los niveles de tolerancia, así como el respectivo procedimiento para generarlos:

- Nivel de tolerancia. Es la magnitud permisible de exposición a un riesgo no discrecional (riesgo operacional), para una Institución en su totalidad.
- Nivel superior de tolerancia. Máxima exposición a riesgos operativos que una Institución puede aceptar sin que esto represente un impacto significativo ni a su operación ni al Gestión de Riesgo Operacional.
- Nivel inferior de tolerancia. Exposición a riesgos operativos que una Institución está dispuesta a asumir para evitar controles excesivos, muy restrictivos o muy cotosos.

El procedimiento para generar los niveles de tolerancia es el siguiente:

a. Recopilación de información.
b. Análisis estadístico.
c. Propuesta de los niveles de tolerancia.
d. Aprobación de los niveles de tolerancia.
e. Identificación de los eventos que traspasaron el límite superior de los niveles de tolerancia establecidos.
f. Seguimiento de los eventos de pérdida que traspasaron el límite superior (se sugiere que el área de Auditoria realice esta función)
g. Instrumentar acciones de mitigación si los eventos sobrepasan los niveles de tolerancia

Los niveles de tolerancia pueden determinarse como un percentil de la distribución de eventos de pérdidas (por ejemplo 95%, 99% o 99.9%).

3.5.2. Caso Práctico Niveles de Tolerancia

La metodología utilizada en esta tesis cumple con los lineamientos establecidos por la CNBV, cabe mencionar que los niveles de tolerancia se obtuvieron de la Base de Datos y se establecieron por factor de riesgo. A continuación se describe el procedimiento utilizado:

I. La información contenida en la Base de Datos se clasifica en dos períodos: periodo muestral y periodo post-muestral. El periodo muestral está constituido por los 4 trimestres del 2008, mientras que el post-muestral está conformado por el primer trimestre del 2009. El objetivo de esta separación es comparar las pérdidas registradas durante el primer trimestre del 2009 contra los niveles de tolerancia calculados con las pérdidas de 2008.

II. Tanto para el periodo muestral como el post-muestral se calcularon el promedio, la varianza y la desviación estándar muestrales de los montos perdidos. Además se especificó cuál fue el valor máximo y el mínimo de cada período. Posteriormente se calcularon los percentiles muestrales 0.05%, 0.50%, 2.50%, 5.00%, 95%, 97.50%, 99.50% y 99.95%.

III. A continuación se graficó el histograma de los datos del periodo muestral que mostraba tanto la frecuencia como el porcentaje acumulado.

IV. Se establecieron los límites superior e inferior, con base en los percentiles antes calculados por lo que los niveles de tolerancia se constituyeron con un 90%, 95%, 99% y 99.9% de confianza.

V. Se etiquetaron con color verde aquellos eventos que se encontraron por debajo del umbral superior y con color rojo aquellos eventos de pérdida que rebasaron el límite superior para su posterior seguimiento.

Resultados de los niveles de tolerancia

Para establecer los niveles de tolerancia por Riesgo Operacional, se determinó que se utilizaría un nivel de confianza del 95%. A continuación se muestra una tabla resumen con los niveles de tolerancia establecidos:

Tabla 3.7 Resultados de los niveles de tolerancia				
Factor	**Limite Superior**	**Eventos bajo el límite superior**	**Total de eventos por arriba del límite superior**	**Monto fuera del intervalo**
Legal $6	61,507	13	0 -	
Regulatorio $86,	678	54	1 $97,	520
Fraudes Tarjetas	$4,399	3,833	118 $	590,742
Fraude Externo	$137,034	50	0 -	
Fraude Interno	$364,584	16	1 $	390,406
Phishing $2	76,652	12	0 -	
Asaltos $2	47,039	20	0 -	
Cheques $33,	975	76	2 $73,	172
Juicios Laborales	$355,760	8	3 $1	,264,653
Falto y Falso	$8,989	115	4 $41,	430
Fallas de Sistemas	$92,277	15	0 -	
Errores en Ejecución de Operaciones	$447,025	29	0 -	

Conclusiones de los niveles de tolerancia

Dados los niveles de tolerancia establecidos, tres factores de riesgo fueron clasificados en color rojo: juicios laborales, fraude interno y fraude por tarjetas, por lo que dichos eventos de pérdida requieren de un seguimiento y análisis para determinar aquellos elementos que están ocasionando estas pérdidas operativas.

3.6 Reportes

3.6.1 Objetivo

Los reportes son informes que permiten recopilar y presentar la información necesaria para los resultados de la gestión de riesgo operacional, de una forma rápida y sencilla. A continuación se exponen los dos tipos de reportes que se pueden realizar: reporte al Consejo de Administración y Alta Dirección y reportes regulatorios. Se comenzará con el reporte al Consejo y a la Alta Dirección:

3.6.2 Reporte de Riesgo Operacional al Consejo de Administración y a la Alta Dirección

Resumen ejecutivo

- **Base de datos.** De las pérdidas contenidas en la base de datos para los eventos registrados durante el primer trimestre del 2009 se obtuvo una pérdida de neta total de **33 MM de pesos** en **4,370** eventos.

- **Indicadores clave de riesgo.** El proceso de indicadores clave de riesgo para el primer trimestre del 2009 identificó 3 indicadores como riesgos potencialmente peligrosos (fraude interno, asaltos y cheques).

Tabla 3.8 Número de indicadores por código de color

Color	No. de indicadores	Factores de riesgo
	2 indicadores	Legal y fraude externo
	7 indicadores	Regulatorio, fraude tarjetas, phishing, juicios laborales, fallas de sistemas, falto y falso y errores en la ejecución de operaciones
	3 indicadores	Fraude interno, asaltos y cheques

- **Niveles de Tolerancia.** Durante el primer trimestre de 2009, 129 de 4,370 eventos de pérdida rebasaron los niveles de tolerancia establecidos en 6 de 12 factores de riesgo y con un monto total fuera de los niveles de MXN 2.5 MM pesos.

- **Risk Control Self Assessment.** El proceso llevado a cabo en la institución identificó los siguientes riesgos:

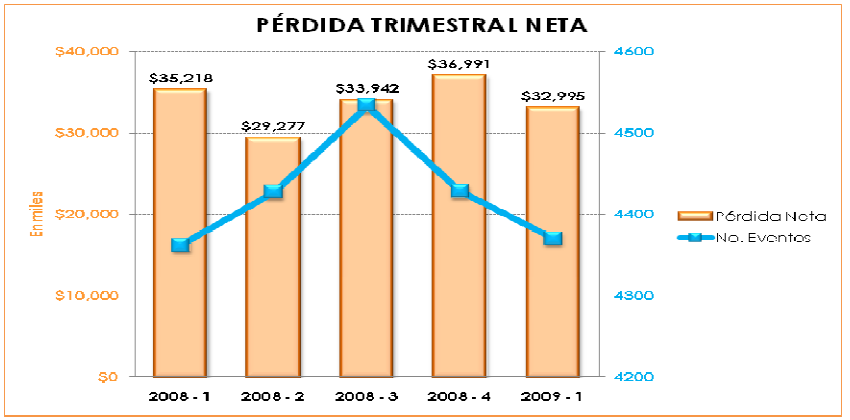
Primera parte		Segunda parte	
Clima organizacional	3 riesgos	Procesos	6 riesgos
Gerencia	4 riesgos	Personal	4 riesgos
Recursos humanos	1 riesgos	Sistemas	2 riesgos

- **Requerimiento de capital por Riesgo Operacional.** Se calculó el requerimiento de capital por los métodos de Indicador Básico, Método Estándar, Método Estándar Alternativo y Método de Medición Avanzada con los siguientes resultados:

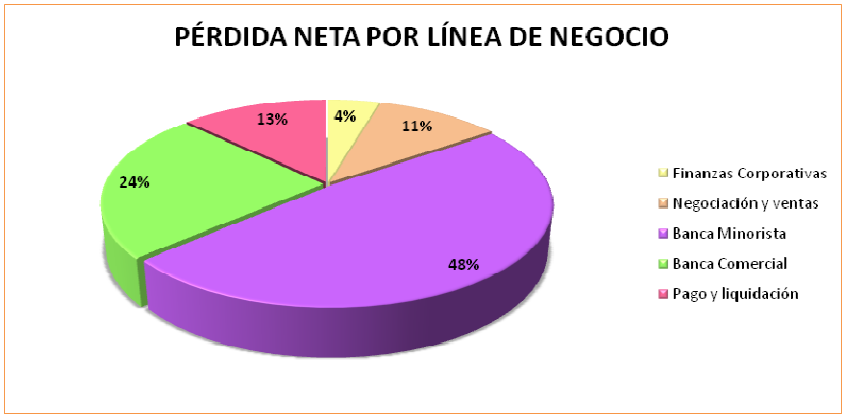
Método	Capital requerido (en miles)
Indicador Básico	49,088
Método estándar	45,750
Método estándar alternativo	27,926
Método de medición avanzada	17,415

Análisis de pérdidas por trimestre

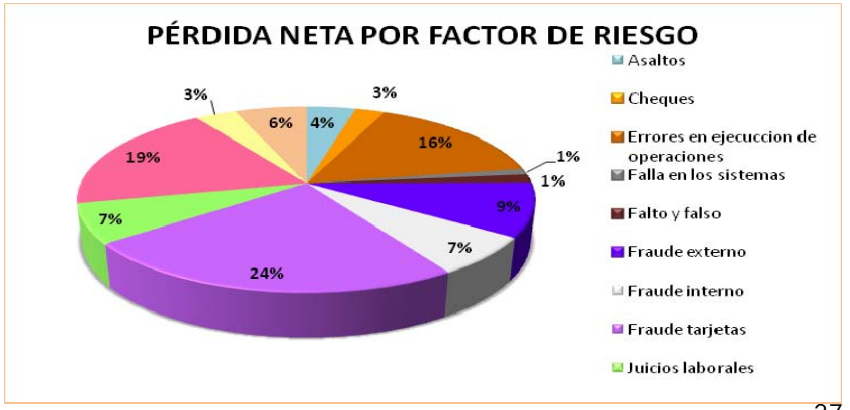
- El cuarto trimestre del 2008 registró la mayor pérdida neta con un total de **40 MM de pesos** *en* 4,428 eventos.
- El trimestre con mayor número de eventos presentados fue el tercer trimestre del 2008 con un total de 4,533 eventos que generaron una pérdida neta de **34 MM de pesos.**



- **Banca Minorista:** acumuló un 48% de las pérdidas netas, con un monto durante los cinco trimestres de **81 MM de pesos**; MXN ***17 MM de pesos*** representa la pérdida generada sólo durante el primer trimestre del 2009 .
- **Banca Comercial:** pérdida neta de **40 MM de pesos** *durante los cinco trimestres y* una pérdida de MXN ***6.5 MM de pesos*** durante el primer trimestre del 2009.



- **Fraude por tarjetas:** pérdida de **40 MM de pesos** durante todo el período y de **8 MM de pesos** durante el primer semestre del 2009.
- **Legal:** pérdida total de ***32 MM de pesos*** y de **5 MM de pesos** en el primer trimestre del 2009.
- **Errores en la ejecución de operaciones:** pérdida total *de MXN* ***26.6 MM de pesos***



Indicadores clave de riesgo

Factor de riesgo
Legal
Fraude Externo
Regulatorio
Fraude tarjetas
Phishing
Juicios laborales
Falto y falso
Falla en sistemas
Errores en la ejecución de operaciones
Fraude Interno
Asaltos
Cheques

Color	**Significado**
	El factor no representa un peligro por su tendencia estable
	El factor representa un peligro moderado debido a su tendencia a incrementarse
	El factor es potencialmente peligroso por su tendencia inestable y creciente

- **Fraude interno:** este factor tuvo un decremento en el tercer trimestre del 2008, pero comenzó a crecer a partir del 4to trimestre y la tendencia hasta el momento es a incrementarse.

- **Asaltos:** a pesar que tuvo una caída en el cuatro trimestre del 2008 en cuanto a la pérdida neta y el número de eventos, el primer trimestre de 2009 comenzó a incrementarse y la tendencia es que siga subiendo. Además el promedio de pérdida neta se ha mantenido alto y constante a lo largo de 2008 y 2009.

- **Cheques:** el promedio de pérdida neta que tuvo durante el primer trimestre de este año fue muy elevado lo que significa que han disminuido el número de eventos presentados pero se ha incrementado el monto relacionado a cada uno de los eventos, es decir, cada evento genera una mayor pérdida.

Niveles de tolerancia

- El período muestral está constituido por los eventos de los cuatro trimestres del 2008, mientras que el período post-muestral está formado por el primer trimestre del 2009.

- El nivel superior de cada factor de riesgo fue establecido con base en las pérdidas del 2008 a un nivel de 95% de confianza. Se muestran aquellos factores que tuvieron rompimientos a los niveles de tolerancia así como el monto total que se encuentra fuera de los niveles establecidos.

Factor	Limite Superior	Eventos bajo el límite superior	Total de eventos por arriba del límite superior	Monto fuera del intervalo
Legal $6	61,507	13	0 -	
Regulatorio $86,	678	54	1 $9	7,520
Fraudes Tarjetas	$4,399	3,833	118 $	590,742
Fraude Externo	$137,034	50	0 -	
Fraude Interno	$364,584	16	1 $	390,406
Phishing $2	76,652	12	0 -	
Asaltos $2	47,039	20	0 -	
Cheques $33,	975	76	2 $7	3,172
Juicios Laborales	$355,760	8	3 $	1,264,653
Falto y Falso	$8,989	115	4 $4	1,430
Fallas de Sistemas	$92,277	15	0 -	
Errores en Ejecución de Operaciones	$447,025	29	0 -	

- **Regulatorio:** recargos generados por incumplimiento de pago de complemento ISR 2007
- **Fraudes Tarjetas:** 43 casos de cloñación de tarjetas, 40 casos de consumos no reconocidos por el cliente y 34 robos o extravíos de tarjetas.
- **Fraude Interno:** cobro de un cheque con firma falsificada del cliente.
- **Cheques:** rembolso de cheques robados y una chequera duplicada.
- **Juicios Laborales:** juicios y gastos por recisión del contrato laboral.
- **Falto y Falso:** faltante de efectivo en cajeros automáticos, sucursales y por billetes falsos.

Risk Control Self Assessment

- El proceso de Risk Control Self Assessment se dividió en dos encuestas: la primera evalúa el clima organizacional, gerencia y recursos humanos, mientras que la segunda evalúa los procesos, al personal y los sistemas.

- Como resultado de la primera parte del Risk Control Self Assessment se obtuvieron 3 eventos para la sección de clima organizacional (dos con impacto 3 y una con impacto 2), por parte de la sección gerencia se obtuvieron 4 eventos (tres con impacto 2 y una con impacto 3) y finalmente para la sección de recursos humanos se obtuvo un evento con impacto 4.

- Para la segunda parte del Risk Control Self Assessment, se obtuvieron 6 eventos para la sección de procesos de los cuales cuatro tuvieron impacto 1 y los dos restantes impacto 2, para la sección de personal se obtuvieron 4 eventos (uno con impacto 1, dos con impacto 2 y el restante con impacto 3) y finalmente la sección de sistemas obtuvo 2 eventos con impacto 1.

Primera parte	
Clima organizacional	3 riesgos
Gerencia	4 riesgos
Recursos humanos	1 riesgos

Segunda parte	
Procesos	6 riesgos
Personal	4 riesgos
Sistemas	2 riesgos

Impacto	**Significado**
1	El factor de riesgo es crítico para el proceso por lo que requiere de una acción inmediata
2	El factor de riesgo es importante en el proceso por lo que se ejecutará la acción a corto plazo (2 meses)
3	El factor de riesgo es poco importante para el proceso por lo que la acción se realizará a mediano plazo (8 meses)
4	El factor de riesgo no es relevante por lo que se atenderán en el proceso del día a día

Cálculo de requerimiento de capital por Riesgo Operacional

Método	Capital requerido (en miles)
Indicador Básico	49,088
Método Estándar	45,750
Método Estándar Alternativo	27,926
Método de Medición Avanzada	17,415

- Conforme se fue aumentando la complejidad de las metodologías se lograba una reducción del capital.
- El método estándar representa una reducción de MXN 3.3 MM comparado con el método del Indicador Básico; por otra parte el requerimiento de capital disminuye en MXN 21 MM al pasar del método de Indicador Básico al Método Estándar Alternativo.
- Al pasar del método de Indicador Básico al método de medición avanzada se observa una reducción en el requerimiento de capital por riesgo operacional de MXN 33 MM.

3.6.3 Reporte regulatorio

Con base en los requerimientos establecidos por la Comisión Nacional Bancaria y de Valores, a continuación se muestran los registros de las pérdidas obtenidas durante los 4 trimestres del 2008 y el primer trimestre del 2009. Se muestran las tablas 3.23 y 3.24 que contienen las pérdidas trimestrales por tipo de evento de pérdida y por línea de negocio.

Distribución trimestral de las pérdidas por tipo de evento de pérdida (en miles de pesos)						
Tipo de evento de pérdida	**2008-1**	**2008-2**	**2008-3**	**2008-4**	**2009-1**	**Total por tipo de evento**
Fraude interno	$2,139	$2,786	$1,665	$2,443	$2,904	**$11,937**
Fraude Externo	$15,760	$14,953	$17,569	$16,602	$14,672	**$79,557**
Relaciones Laborales y Seguridad en el puesto de trabajo	$2,040	$2,498	$2,003	$2,475	$2,569	**$11,586**
Clientes, productos y prácticas empresariales	$3,652	$2,813	$4,257	$4,013	$3,125	**$17,859**
Incidencias en el negocio y fallo en los sistemas	$323	$571	$272	$573	$543	**$2,283**
Ejecución, entrega y gestión de procesos	$11,304	$5,656	$8,175	$10,886	$9,181	**$45,201**
Total trimestral	**$35,218**	**$29,277**	**$33,942**	**$36,991**	**$32,995**	**$168,422**

Distribución trimestral de las pérdida por línea de negocio (en miles de pesos)						
Línea de negocios	**2008-1**	**2008-2**	**2008-3**	**2008-4**	**2009-1**	**Total por tipo de evento**
Finanzas Corporativas	$1,327	$801	$1,355	$2,156	$1,942	**$7,581**
Negociación y ventas	$4,307	$2,420	$2,711	$4,974	$3,701	**$18,113**
Banca Minorista	$15,239	$16,975	$15,833	$15,753	$17,374	**$81,174**
Banca Comercial	$10,624	$5,730	$8,473	$8,767	$6,484	**$40,079**
Pago y liquidación	$3,720	$3,352	$5,570	$5,340	$3,493	**$21,475**
Total trimestral	$35,218	$29,277	$33,942	$36,991	$32,995	**$168,422**

4. CÁLCULO DE PÉRDIDA ESPERADA Y NO ESPERADA

4.1 Objetivo

Cada institución financiera tiene la obligación de calcular sus propios requerimientos de capital mínimo de acuerdo con lo estipulado dentro del Acuerdo de Basilea II; dicho acuerdo establece que existen 4 métodos para el cálculo de requerimientos de capital mínimo por riesgo operacional que se presentarán a continuación en orden creciente de sofisticación y sensibilidad al riesgo. A continuación se muestra la aplicación de cada uno de dichos métodos basándonos en la información de la Tabla 6.14 de los anexos la cuál contiene los ingresos en miles de las líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pago y liquidación, servicios de agencia, administración de activos e intermediación minorista; además contiene los saldos insolutos de la cartera comercial y minorista de los últimos 36 meses.

4.2 Metodologías para el cálculo de requerimiento de capital

a) Método del Indicador Básico.

Los bancos que utilicen este método deberán cubrir el riesgo operacional con un capital equivalente al promedio de los tres últimos años de un porcentaje fijo (denotado como alfa) de sus ingresos brutos anuales positivos. Para el cálculo de este promedio se excluirán los datos de cualquier año en el que el ingreso bruto anual haya sido negativo o igual a cero.

La fórmula para calcular la exigencia de capital puede expresarse del siguiente modo:

$$\mathrm{KBIA} = \frac{[\sum(\mathrm{Gl}_{1\ldots n} * \alpha)]}{n}$$

Donde:

KBIA = la exigencia de capital en el Método del Indicador Básico
GI = ingresos brutos anuales medios, cuando sean positivos, de los tres últimos años
n = número de años (entre los tres últimos) en los que los ingresos brutos fueron positivos
α= 15%, parámetro establecido por el Comité de Basilea.

Los ingresos brutos se definen como los ingresos netos en concepto de intereses más otros ingresos netos ajenos a intereses.

A continuación en la tabla 4.1 se muestra un resumen de los ingresos en miles por línea de negocio para cada uno de los tres años.

Tabla 4.1 Cuadro resumen con los ingresos anuales por línea de negocio				
Descripción	**Año 1**	**Año 2**	**Año 3**	**Promedio de ingresos por línea de negocio**
Finanzas Corporativas	$518	$478	$475	$490
Negociación y Ventas	$44,965	$41,442	$41,221	$42,543
Banca al Menudeo	$183,319	$168,958	$168,058	$173,445
Banca Comercial	96,847	$89,261	$88,785	$91,631
Pago y Liquidación	$20,234	$18,649	$18,549	$19,144
Servicios de Agencia	$0	$0	$0	$0
Administración de activos	$0	$0	$0	$0
Intermediación minorista	$0	$0	$0	$0

Caso Práctico del Método del Indicador Básico

El cálculo del requerimiento de capital por el método del indicador básico es la aplicación del 15% al promedio de los ingresos brutos positivos de los tres últimos años. Como se muestra en la siguiente tabla 4.2 el promedio total de las líneas de negocios fue de **327.25 M M d e pesos**. La aplicación del 15% sobre esta cantidad nos da un monto de ***49 MM de pesos.***

Tabla 4.2 Ingresos promedio por línea de negocio	
Descripción	**Promedio de ingresos (en miles)**
Finanzas Corporativas	$491
Negociación y Ventas	$42,543
Banca al Menudeo	$173,445
Banca Comercial	$91,631
Pago y Liquidación	$19,144
Servicios de agencia	$0
Administración de agencia	$0
Intermediación minorista	$0
Total $32	**7,255**

b) Método Estándar.

En este método las actividades de los bancos se dividen en 8 líneas de negocios: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista. En la tabla 7.1 de los Anexos se definen estas líneas de negocios.

El ingreso bruto de cada línea de negocio es un indicador que permite aproximar el volumen de operaciones de un banco y, con ello, el nivel del riesgo operacional que es probable que asuma dicho banco en estas líneas de negocio. El requerimiento de capital de cada línea se calcula multiplicando el ingreso bruto por un factor (denominado β) que se asigna a cada una de ellas. Beta (β) se utiliza como una aproximación a la relación que existe en el conjunto del sector bancario entre el historial de pérdidas debido al riesgo operacional de cada línea de negocio y el nivel agregado de ingresos brutos generados por esa misma línea. Cabe mencionar que, en el Método Estándar, se calcula el ingreso bruto de cada línea de negocio y no el obtenido por la institución en su conjunto.

La exigencia total de capital se calcula como la media de tres años de la suma simple de las exigencias de capital regulador en cada una de las líneas de negocio cada año. Para un año dado, los requerimientos de capital negativos (resultantes de ingresos brutos negativos) en cualquiera de las líneas de negocio podrán compensar los requerimientos positivos en otras líneas de negocio sin límite alguno. No obstante, cuando el requerimiento de capital agregado para todas las líneas de negocio en un mismo año sea negativo, el argumento del numerador para ese año será cero. El requerimiento total de capital puede expresarse como:

$$K_{TSA} = \frac{\{\sum_{año\ 1-3} max[Gl_{1-8} x \beta_{1-8}, 0]\}}{3}$$

Donde:

K_{TSA} = La exigencia de capital en el Método Estándar.

Gl_{1-8} = Los ingresos brutos anuales de una año dado para cada una de las ocho líneas de negocio.

β_{1-8} = Un porcentaje fijo, establecido por el Comité de Basilea, que relaciona la cantidad de capital requerido con el ingreso bruto de cada una de las 8 líneas de negocio.

Los valores de los factores β se enumeran a continuación:

Tabla 4.3 Valores de Beta	
Línea de negocio	Factor Beta (β)
Finanzas corporativas (β1)	18%
Negociación y ventas (β2)	18%
Banca minorista (β3)	12%
Banca comercial (β4)	15%
Pagos y liquidación (β5)	18%
Servicios de agencia (β6)	15%
Administración de activos (β7)	12%
Intermediación minorista (β8)	12%

Caso Práctico del Método Estándar

Una vez que se tienen separados los ingresos de cada una de las líneas de negocio, éstos permiten aproximar el volumen de operaciones de un banco y, por medio de ello, el nivel de riesgo operacional que probablemente asuma el banco por cada línea de negocio. El cálculo del requerimiento de capital estará conformado por la aplicación de un porcentaje o factor β a los ingresos de cada una de las líneas de negocio. A la información contenida en la tabla 4.2 se le puede añadir la información de los ingresos de las 3 líneas de negocio añadidas en este método (servicios de agencia, administración de activos e intermediación minorista). A continuación en la tabla 4.4 se encuentran los ingresos promedio de cada línea de negocio así como el valor de beta correspondiente para cada una de ellas.

Tabla 4.4 Ingresos promedio y requerimiento de capital por línea de negocio			
Línea de negocio	**Ingresos promedio (en miles)**	**Beta**	**Requerimiento de capital (en miles)**
Finanzas Corporativas	$491	18%	88
Negociación y Ventas	$42,543	18%	$7,658
Banca al Menudeo	$173,445	12%	$20,813
Banca Comercial	$91,631	15%	$13,745
Pago y Liquidación	$19,144	18%	$3,446
Servicios de Agencia	0	15%	0
Administración de Activos	0	12%	0
Intermediación	0	12%	0
Total $32	**7,255**		**$45,750**

El monto del requerimiento de capital para el método estándar es de ***45.75 MM de pesos***. Que representa una reducción del 7% con respecto del método del indicador básico **(3.34 *MM de pesos).***

Método Estándar Alternativo

Este método, como su nombre lo indica, es muy parecido al método estándar. En el método estándar alternativo, el cálculo del requerimiento de capital, es igual que en el método estándar salvo en 2 líneas de negocio: banca minorista y banca comercial. Para estas dos líneas de negocio, los préstamos multiplicados por un factor fijo "m", sustituyen a los ingresos brutos como indicador de riesgo. Los factores beta de la banca minorista y de la banca comercial son los mismos que en el método estándar. La fórmula para el cálculo del requerimiento de capital por método estándar alternativo, tanto para la banca minorista como comercial, puede expresarse como:

$$K_{RB} = (\beta_{RB})(m)(LA_{RB})$$

Donde:

K_{RB} = es el requerimiento de capital de la línea de negocio de banca (minorista/comercial).

B_{RB} = es el factor beta de la línea de negocio de banca (minorista/comercial).

LA_{RB} = es el importe total pendiente de los préstamos (no ponderados por riesgo y brutos de provisiones), promediado durante los tres últimos años.

m = 0.035

Para efectos del método estándar alternativo, los préstamos de la línea de negocio de banca minorista son las cantidades totales utilizadas de las siguientes carteras crediticias: minorista, PYME tratadas como minoristas y derechos de cobro adquiridos frente a minoristas. En el caso de la banca comercial, los préstamos totales incluyen las cantidades utilizadas de las siguientes carteras crediticias: empresas, soberanos, bancos, financiación especializada, PYME tratadas como empresas y derechos de cobro adquiridos frente a empresas. También deberá incluirse el valor contable de los valores mantenidos en la cartera de inversión.

En el método estándar alternativo, los bancos pueden agregar la banca comercial y minorista (si lo desean) utilizando un factor beta del 15%. Asimismo, aquellos bancos que sean incapaces de desagregar sus ingresos brutos en las otras seis líneas de negocio pueden agregar los ingresos brutos totales de esas seis líneas utilizando un factor beta del 18%, aplicándolo a los ingresos brutos negativos.

Al igual que en el método estándar, el requerimiento total de capital en el método estándar alternativo se calcula como la suma simple de los requerimientos de capital regulador para cada una de las ocho líneas de negocio.

Caso Práctico del Método Estándar Alternativo

A continuación en la tabla 4.5 se muestran los ingresos brutos por línea de negocio, los valores de beta y el resultado obtenido tras la aplicación de dicho porcentajes a los ingresos.

Tabla 4.5 Ingresos brutos, valores de beta y requerimiento de capital por línea de negocio

Línea de negocio	Ingresos promedio (en miles)	Saldos insolutos	Beta	Beta adicional	Requerimiento de capital (en miles)
Finanzas Corporativas	$491		18%		$88
Negociación y Ventas	$42,543		18%		$7,658
Banca al Menudeo		$2,040,735	12%	3.5%	$8,571
Banca Comercial		$1,554,846	15%	3.5%	$8,163
Pago y Liquidación	$19,144		18%		$3,446
Servicios de Agencia	0		15%		0
Administración de Activos	0		12%		0
Intermediación	0		12%		0
Total	$62,178	$3,595,581			**$27,926**

El monto del capital requerido tras la aplicación del método estándar alternativo se ve reducido en comparación con el monto calculado con el método estándar en un 61%, ya que de los ***45.75 MM de pesos*** obtenidos anteriormente obtuvo un monto de ***28 MM de pesos***.

c) Métodos de Medición Avanzada.

En los AMA (por sus siglas en inglés, Advance Measurement Approaches), la exigencia de capital mínimo por riesgo operacional es determinada por un sistema interno de estimación de riesgo operacional propio de cada entidad, mediante la aplicación de criterios cuantitativos y cualitativos, y requiere la autorización del supervisor para su implementación.

Los bancos que adopten los AMA, previa aprobación de los supervisores, podrán utilizar un metodología de asignación a efectos de determinar el requerimiento de capital regulador para las filiales de bancos con actividad internacional. El consentimiento del supervisor podrá depender de

que el banco demuestre a los supervisores correspondientes que el mecanismo de distribución entre estas filiales es el adecuado y se apoya en datos empíricos. El Consejo de Administración y la Alta Dirección de cada filial deberán realizar su propia evaluación de los riesgos operativos, así como controlar y asegurar que el capital que mantiene es el adecuado para estos riesgos.

Al determinar si la metodología de asignación resulta adecuada, habrá de tenerse en cuenta el grado de desarrollo de las técnicas de distribución sensibles al riesgo y hasta qué punto reflejan el nivel de riesgo operacional en las entidades legales y en el grupo bancario en su conjunto. Los supervisores entienden que los grupos bancarios que apliquen los AMA se esforzarán constantemente por desarrollar técnicas de distribución del riesgo operacional sensibles al riesgo, sin prejuicio de la aprobación inicial de técnicas basadas en los ingresos brutos o en otras aproximaciones al riesgo operacional.

Los criterios generales que el banco deberá demostrar a su supervisor como mínimo para poder utilizar los AMA son:

- Su Consejo de Administración y su Alta Dirección, participan activamente en la vigilancia del marco de gestión del riesgo operacional.
- Posee un sistema de gestión del riesgo operacional conceptualmente sólido que aplica con integridad.
- Cuenta con recursos suficientes para utilizar la metodología en las principales líneas de negocio, así como en los ámbitos de control y auditoría.

El sistema de medición interna del banco deberá estimar de forma razonable las pérdidas no esperadas, combinando para ello datos relevantes de pérdidas tanto internos como externos, análisis de escenarios, así como el entorno del negocio y los factores de control interno que son específicos al banco. El sistema de medición del banco también deberá poder llevar a cabo la asignación de capital económico por riesgo operacional entre las distintas líneas de negocio de un modo que genere incentivos para la mejora de la gestión del mismo en esas líneas.

Además, los bancos deberán satisfacer los siguientes criterios cualitativos antes de poder ser autorizados a emplear un AMA para calcular su requerimiento de capital por riesgo operacional:

- El banco deberá contar con una unidad de gestión del riesgo operacional que será la encargada realizar y diseñar políticas, metodologías y procedimientos relativos a la gestión del riesgo operacional. Además se encargará de desarrollar estrategias encaminadas a identificar, estimar, observar y controlar/reducir este tipo de riesgo.

- Deberá informarse periódicamente a la dirección de las unidades de negocio, a la Alta Dirección y al Consejo de Administración acerca de las exposiciones al riesgo operacional y del historial de pérdidas debidas a este riesgo.
- El sistema de gestión del riesgo operacional del banco deberá estar bien documentado.
- Los auditores externos y/o internos deberán llevar a cabo exámenes periódicos de los procesos de gestión y los sistemas de medición del riesgo operacional.

Caso Práctico de los Métodos de medición avanzada

Para el caso de la aplicación de los métodos de medición avanzada el requerimiento de capital está determinado por un sistema interno de estimación del riesgo operacional propio de cada entidad, mediante la aplicación de criterios cuantitativos y cualitativos. Aunado a esto se requiere el cálculo de la pérdida esperada y no esperada que será la que determine para los métodos de medición avanzada el requerimiento de capital.

El cálculo de la pérdida esperada y no esperada requiere de un análisis separado de la frecuencia de las pérdidas así como de la severidad que ocasionan. Es por esto que la metodología que se presenta en este trabajo se basa en el ajuste de una distribución de probabilidad para la frecuencia y una distribución para la severidad de las pérdidas causadas por el riesgo operacional. En esta tesis se utilizará la distribución de Poisson para la frecuencia y la distribución Lognormal para la severidad. Cabe señalar que la estimación de los parámetros de las Distribuciones de Poisson y Lognormal se obtendrá por medio del método de Máxima Verosimilitud. El principio de máxima verosimilitud es el siguiente:

Si la distribución que corresponde a una muestra aleatoria de tamaño n, procede de una población con el parámetro desconocido θ, viene dada por $f(x_1, x_2,\ldots, x_n;\theta)$, la estimación de máxima verosimilitud de θ es el número $\hat{\theta}$, si existe, que verifica

$$f(x_1, x_2,\ldots, x_n; \hat{\theta}) > f(x_1, x_2,\ldots, x_n;\theta'); \text{ donde } \theta' \text{ es cualquier otro valor de } \theta$$

En otras palabras lo que el método de Máxima Verosimilitud quiere decir es que se escogerá como valor estimado de un parámetro aquél que tenga mayor probabilidad de ocurrir según lo observado, es decir, aquél valor que es más compatible con los datos observados.

Frecuencia

La distribución de Poisson está dada por:

$$f(n|\lambda) = \frac{\lambda^n}{n!}e^{-\lambda}$$

Donde:

- e es la base del logaritmo natural (e=2.71828…)

- k es el número eventos observados
- λ es el número esperado de ocurrencias durante un intervalo dado

A continuación se describe la estimación del parámetro λ por el principio de máxima verosimilitud.

La función Poisson está determinada por:

$$f(x|\lambda) = \frac{\lambda^x e^{-\lambda}}{x!}$$

La función de verosimilitud es

$$V = \prod_{i=1}^{n} \frac{\lambda^x e^{-\lambda}}{x!}$$

$$V = \frac{\lambda^{\sum x_i} e^{-n\lambda}}{\prod x_i}$$

Se aplica logaritmo natural en los dos lados de la ecuación

$$ln\, V = \left(\sum x_i\right) ln\, \lambda - n\, \lambda - ln\, \left(\prod x_i\right)$$

Se calcula la derivada parcial de lnV con respecto de λ nos da como resultado

$$\frac{\partial lnV}{\partial \lambda} = \frac{\sum x_i}{\hat{\lambda}} - n$$

Se iguala a cero y se despeja el parámetro lambda

$$\frac{\sum x_i}{\hat{\lambda}} - n = 0$$

$$\hat{\boldsymbol{\lambda}} = \frac{\sum \boldsymbol{x_i}}{\boldsymbol{n}}$$

Por lo tanto el parámetro λ de una distribución Poisson es igual a la suma de n observaciones de una población entre el número de eventos

Resultados de la Frecuencia

En la tabla que se encuentra a continuación se muestran el número de eventos observados, es decir, el número de pérdidas encontradas en la Base de Datos por trimestre y por año.

Tabla 4.6 Número de eventos presentados por año		
Año Tr	**imestre**	**Número de eventos**
2008	1	4,362
	2	4,427
	3	4,533
	4	4,428
2009	1	4,370

De ante mano se sabe que E(x) = λ, es decir, que el valor esperado de una distribución Poisson es igual a λ. Para este ejemplo el valor de λ se calculó de la siguiente forma:

$$\bar{\lambda} = \frac{\sum ni}{Número\ de\ trimestres} = \frac{22{,}120}{5} = \mathbf{4{,}424}$$

Severidad

La distribución lognormal está dada por:

$$f(x;\mu,\sigma) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-(\frac{(lnx-\mu)^2}{2\sigma^2})}$$

Donde:

- e es la base del logaritmo natural (e=2.71828…)
- μ es la media
- σ es la desviación estándar

A continuación se describe el procedimiento para la estimación de los parámetros σ y μ por el principio de máxima verosimilitud. Cabe destacar que la demostración está hecha para la distribución normal pero dado que $f_{Normal}(x;\mu,\sigma) = \frac{1}{x} f_{Lognormal}(lnx;\mu,\sigma)$; se puede tomar como cierta la demostración.

Las muestras de tamaño n de una distribución normal tiene por función de densidad:

$$\prod_{i=1}^{n} \frac{1}{\sqrt{2\pi\sigma}} e^{-\left(\frac{1}{2\sigma^2}\right)(x_i-\mu)^2} = \left(\frac{1}{2\pi\sigma^2}\right)^{n/2} e^{-\left(\frac{1}{2\sigma^2}\right)\sum(x_i-\mu)^2}$$

El logaritmo de la función de verosimilitud es

$$L = -\frac{n}{2} log 2\pi - \frac{n}{2} log\sigma^2 - \frac{1}{2\sigma^2}\sum(x_i - \mu)^2$$

Para hallar el máximo, se calcula

$$\frac{\delta L}{\delta \mu} = \frac{1}{\sigma^2}\sum(x_i - \mu)^2$$

$$\frac{\delta L}{\delta \sigma^2} = -\frac{n}{2}\frac{1}{\sigma^2} + \frac{1}{2\sigma^2}\sum(x_i - \mu)^2$$

Y haciendo estas derivadas iguales a cero y resolviendo las ecuaciones que resultan en μ y σ^2, se obtienen los estimadores para la distribución normal:

$$\hat{\mu} = \frac{1}{n}\sum x_i$$

$$\widehat{\sigma^2} = \frac{1}{n}\sum(x_i - \mu)^2$$

Aplicando la igualdad que guarda la distribución normal y lognormal se obtienen los parámetros μ y σ que se van a utilizar:

$$\hat{\mu} = \frac{\sum \ln x_i}{n}$$

$$\widehat{\sigma^2} = \frac{\sum(lnx_i - \hat{\mu})^2}{n}$$

Resultados de la Severidad

Utilizando los estimadores que fueron calculados anteriormente se obtiene que:

$$\hat{\mu} = \frac{\sum \ln x_i}{n} = \frac{170{,}292.9851}{22{,}120} = \mathbf{7.6985}$$

$$\widehat{\sigma^2} = \frac{\sum (lnx_i - \hat{\mu})^2}{n} = \frac{22{,}130.7884}{22{,}120} = \mathbf{1.0004}$$

Una vez que se obtuvieron los parámetros de las dos distribuciones se procede a realizar la Simulación Monte Carlo, que tiene como base la simulación de variables aleatorias Poisson y Lognormal.

Simulación de variable aleatorias

La simulación es una herramienta que se utiliza para experimentar de manera económica y útil sistemas reales que requieren mejorar o controlar su funcionamiento. La simulación de los sistemas requiere la creación de un modelo lógico-matemático que describa mediante un conjunto de ecuaciones las relaciones básicas entre los principales elementos del sistema.

Para realizar la Simulación Monte Carlo primeramente se realizó la simulación de una variable Poisson y con base en este resultado se simularon las variables aleatorias lognormales. A continuación se muestran los algoritmos para simular cada una de las variables aleatorias. Cabe mencionar que en los anexos se pueden encontrar los algoritmos utilizados para simular en Matlab las distribuciones antes enunciadas.

Distribución Poisson-. Si se desean generar los primeros n eventos de una distribución Poisson a una tasa λ, se tiene que hacer uso de los resultados obtenidos de realizar eventos sucesivos bajo un proceso exponencial independiente y con variables aleatorias a una tasa λ. Una manera de simular estos eventos es generar n números aleatorios U_1, U_2, … , U_n y establecer que $X_i = -\frac{1}{\lambda} log U_i$, la variable X_i se considera como el evento ocurrido entre el (i-1) evento y el i-esimo evento en una distribución Poisson. Ya que el j-esimo evento deberá ser la suma de los primeros j eventos, esto nos lleva a que los valores generados por los primeros n eventos esta dado por:

$$\sum_{i=1}^{j} X_i, j = 1, \dots n$$

Si se requiere generar las primeras T unidades de tiempo de una distribución Poisson, se puede seguir el procedimiento antes descrito de manera sucesiva, con el fin de generar los eventos, hasta que la

suma exceda T. El siguiente algoritmo puede ser utilizado para generar un número de eventos cualquiera en un intervalo de (0,T) para una distribución Poisson con una tasa de λ. En el algoritmo t hace referencia al tiempo, I es el número de eventos ocurridos al tiempo t y S(I) es el evento más reciente.

Paso 1. t=0, I=0

Paso 2. Generar valores aleatorios U

Paso 3. $t = t - \frac{1}{\lambda} logU$. Hasta t>T

Paso 4. I = I + 1, S(I) = t

Paso 5. Volver al paso 2

El ultimo valor de I representa el número de eventos que ocurrieron en el tiempo T y los valores S(1), … S(I) son los eventos I en orden creciente.

Distribución Logn ormal-. Para simular una variable aleatoria Lognormal es posible primero simular una variable aleatoria normal y después de esa misma obtener una variable aleatoria exponencial. Para generar una variable aleatoria normal, que tiene una densidad de probabilidad $f(x) = \frac{2}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$; 0 < x < ∞ , la simulación de la variable normal comienza aplicando el método de rechazo a la función de densidad anterior y a una función de densidad exponencial $g(x) = e^{-x}$; 0 < x < ∞.

El método de rechazo es el siguiente, suponiendo que se cuenta con un método para generar una variable aleatoria bajo una función de densidad g(x). Además la función de g(x) se puede utilizar como base para obtener una función continua f(x) generando un valor g(Y) y por último se puede aceptar que el valor generado tiene una probabilidad f(Y)/g(Y) que se puede establecer como una constate c. La expresión del método es la siguiente:

$$\frac{f(y)}{g(y)} \leq c \text{ ; para toda Y}$$

Regresando a la simulación de la distribución normal se tiene que:

$$\frac{f(x)}{g(x)} = \sqrt{\frac{2}{\pi e^{x-\frac{x^2}{2}}}}$$

Cabe destacar que el máximo valor de la razón f(x)/g(x) ocurre cuando se maximiza $x - x^2/2$, es decir cuando x = 1; la expresión que resulta es la siguiente:

$$c = Max \frac{f(x)}{g(x)} = \frac{f(1)}{g(1)} = \sqrt{\frac{2e}{\pi}}$$

Con lo anterior se puede establecer que se puede generar valores de una distribución normal siguiendo los siguientes pasos:

Paso 1. Generar Y que es una variable aleatoria exponencial con una tasa = 1.

Paso 2. Generar números aleatorios U

Paso 3. Si $U \leq \exp\{ -(Y - 1)^2) / 2 \}$, X = Y. Si no se cumple con la condición se regresa al paso 1.

Una vez que se ha simulado la variable aleatoria normal, el siguiente paso es la simulación de la variable aleatoria exponencial. La función de densidad de una variable aleatoria exponencial con una tasa 1 es la siguiente:

$$F(x) = x^n , 0 < x < 1$$

Ahora si $x = F^{-1}(u)$, entonces:

$$u = F(x) = 1 - e^{-x}$$

$$1 - u = e^{-x}$$

Aplicando las leyes de los logaritmos se obtiene:

$$x = -\log (1 - u)$$

Por lo tanto se puede obtener una variable aleatoria exponencial con parámetro 1, generando un número aleatorio U y asumiendo que:

$$X = F^{-1}(U) = -\log(1 - U)$$

Cabe destacar que 1 – U es uniforme para el intervalo (0,1) y por lo tanto –log(1 - U)tiene la misma distribución en la forma –logU.

Con base en la información anterior se puede establecer los siguientes pasos para generar una variable aleatoria exponencial:

Paso 1. Generar números aleatorios U_1 y U_2

Paso 2. Establecer $t = -\log(U_1,U_2)$

Paso 3. Generar un tercer número aleatorio U_3

Paso 4. $X = t\ U_3$, $Y = t - X$

La teoría anteriormente expuesta muestra algunos de los métodos para simular variables aleatorias Poisson y Lognormales, sin embargo, por practicidad y parsimonia en el desarrollo de la simulación Monte Carlo, se utilizarán las funciones de Matlab diseñadas para tal propósito.

Simulación Monte Carlo

La herramienta utilizada para calcular la pérdida esperada y no esperada, una vez que se conocen los parámetros de las distribuciones Poisson y Lognormal, es la simulación Monte Carlo. El método de simulación Monte Carlo incide en la última fase del esquema general de los experimentos de simulación, constituyendo una metodología de estimación bastante potente de parámetros de interés de sistemas reales. Para llevar a cabo esa estimación el método de Monte Carlo explota ampliamente la analogía entre probabilidad y volumen. La Estadística Matemática formaliza la noción intuitiva de probabilidad de un suceso identificándola con su volumen o medida relativa en relación con el del universo de posibles resultados de un experimento aleatorio.

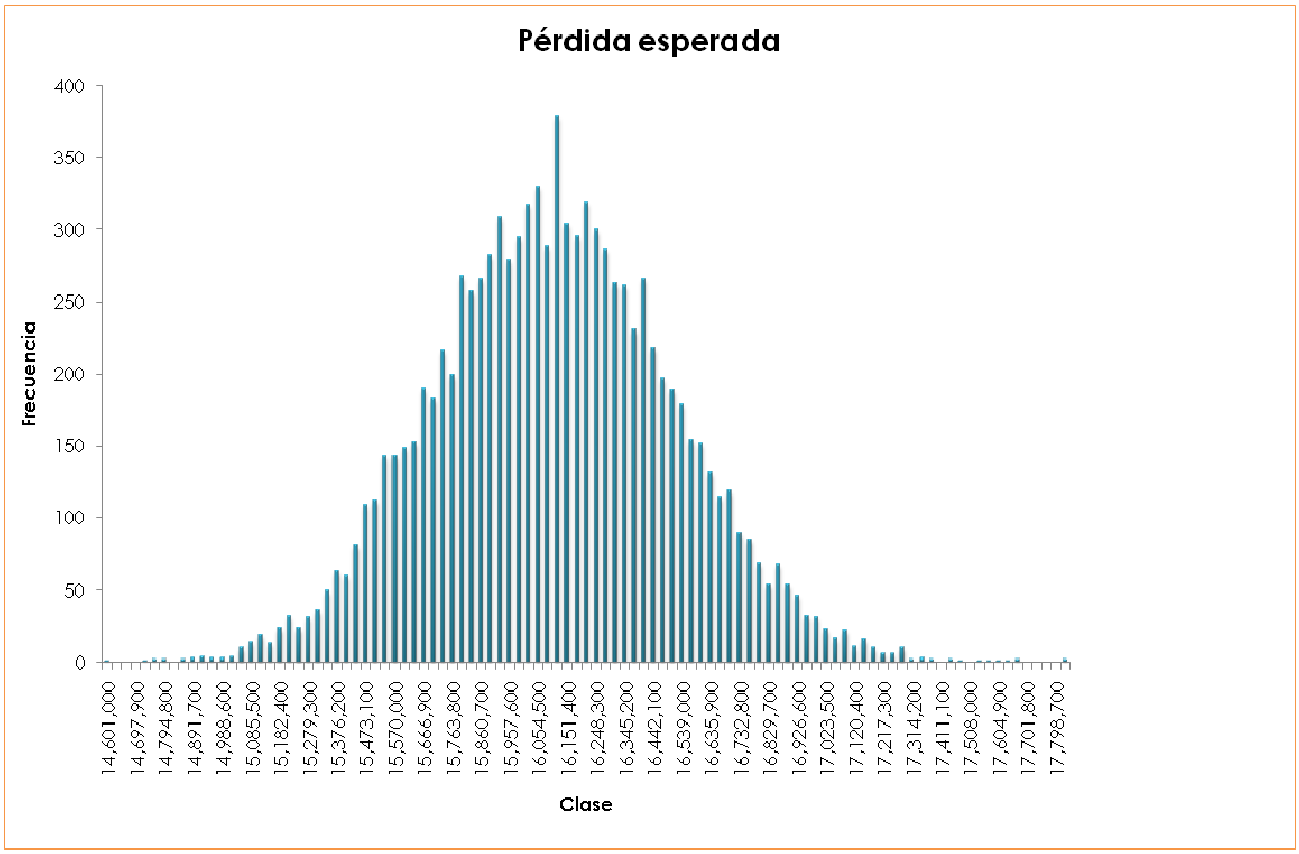
El método de Monte Carlo utiliza esa identificación en la dirección opuesta, es decir calculando el volumen de un conjunto e interpretando dicho volumen como una probabilidad. En el caso más simple eso significa llevar a cabo un muestreo aleatorio del universo de resultados posibles, hacer el recuento de los resultados que pertenecen a un determinado conjunto, calcular la fracción de los resultados pertenecientes a dicho conjunto con respecto al número total de resultados generados, y tomar dicha fracción como una estimación del volumen de dicho conjunto. Dentro de estas hipótesis bastantes generales, la ley de los grandes números asegura que la estimación de parámetros converge al verdadero valor del volumen del conjunto a medida que aumenta el número de resultados generados artificialmente. Además, el teorema central del límite facilita información sobre la magnitud del error de estimación cuanto el tamaño de la muestra generada es finito, como por otra parte siempre va a suceder.

Caso Práctico de la Simulación Monte Carlo

Para el cálculo de la pérdida esperada de nuestro ejemplo se usó la simulación Monte Carlo, la cual conjuntó la distribución Poisson (frecuencia) y Lognormal (severidad) y con ello generó 10,000 simulaciones basadas en los parámetros de las distribuciones calculadas con las pérdidas contenidas en la base de datos. El promedio de todas las pérdidas generadas es igual a la pérdida esperada mientras que la pérdida no esperada está dada por la diferencia entre la pérdida esperada y el percentil 99.9, también conocido como VaR (valor en riesgo). El requerimiento de capital sería equivalente a la suma de las pérdidas esperada y no esperada o lo que es lo mismo al percentil 99.9.

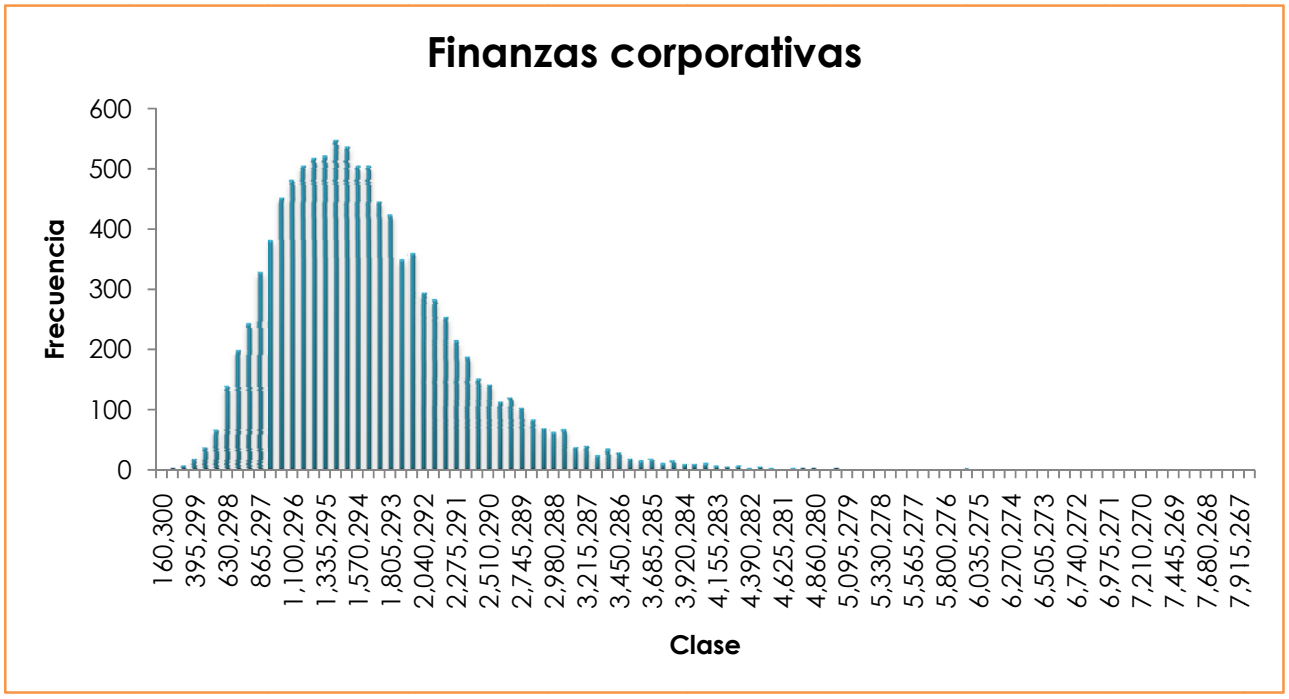
Adicionalmente se realizó la simulación Monte Carlo para las líneas de negocios y los 12 factores de riesgo registrados en la base de datos.

En la tabla 4.7 de los anexos se pueden observar los montos obtenidos de pérdida esperada y no esperada de cada uno de ellos. A continuación en la gráfica 4.1 se muestra un histograma con las pérdidas simuladas mediante la simulación Monte Carlo.

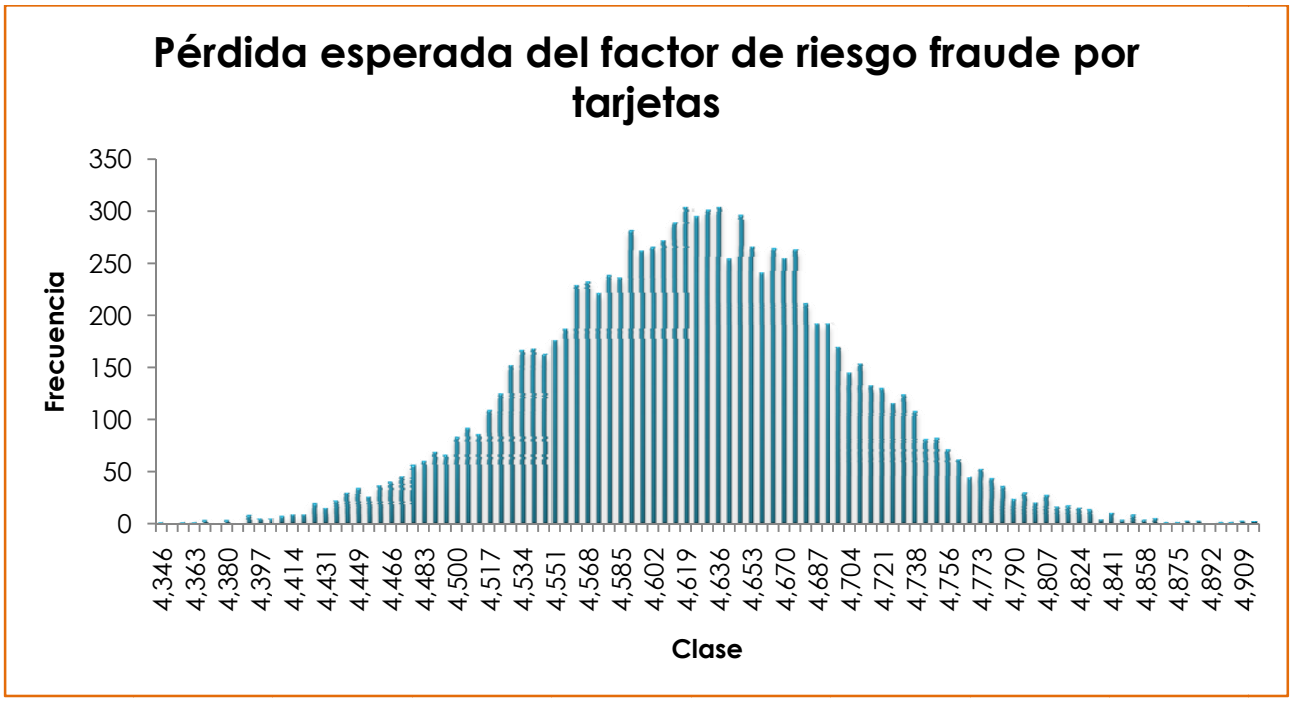


Gráfica 4.1

Como se puede observar en el histograma, la distribución de las perdidas simuladas es simétrica, con una media de **16 MM de pesos** y una desviación de ***403,208 pesos***. No todas las líneas de negocio y los factores de riesgo mostraron el mismo comportamiento, ya que algunos histogramas presentaban algún sesgo. En las gráficas 4.2 y 4.3 se muestran los histogramas de la línea de negocios finanzas corporativas y del factor de riesgo fraude por tarjetas, respectivamente.



Gráfica 4.2

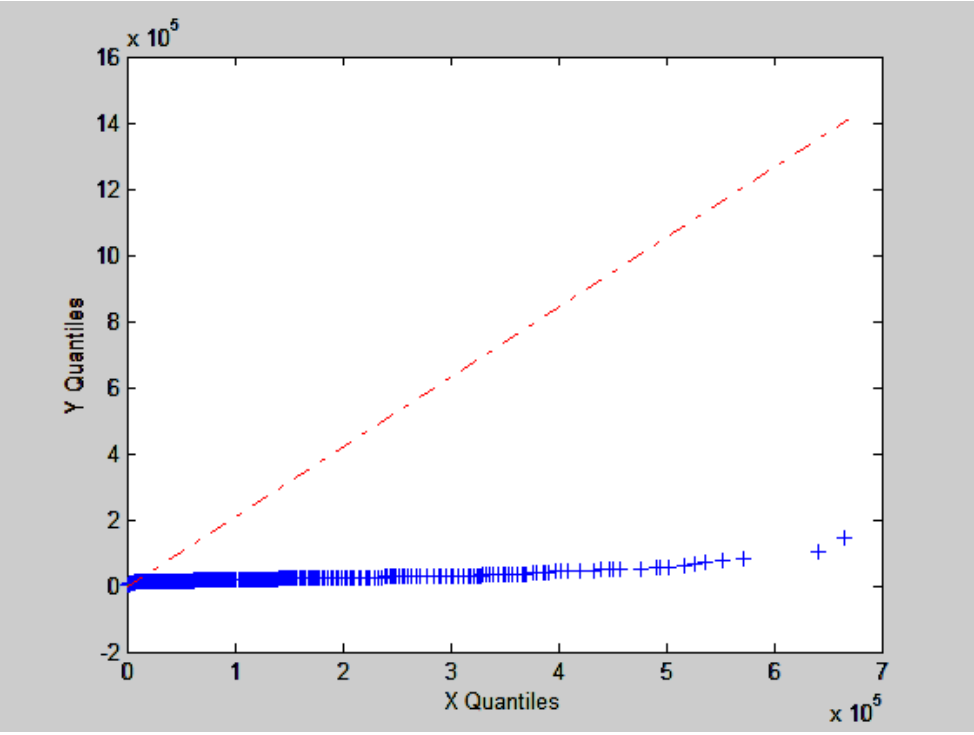


Gráfica 4.3

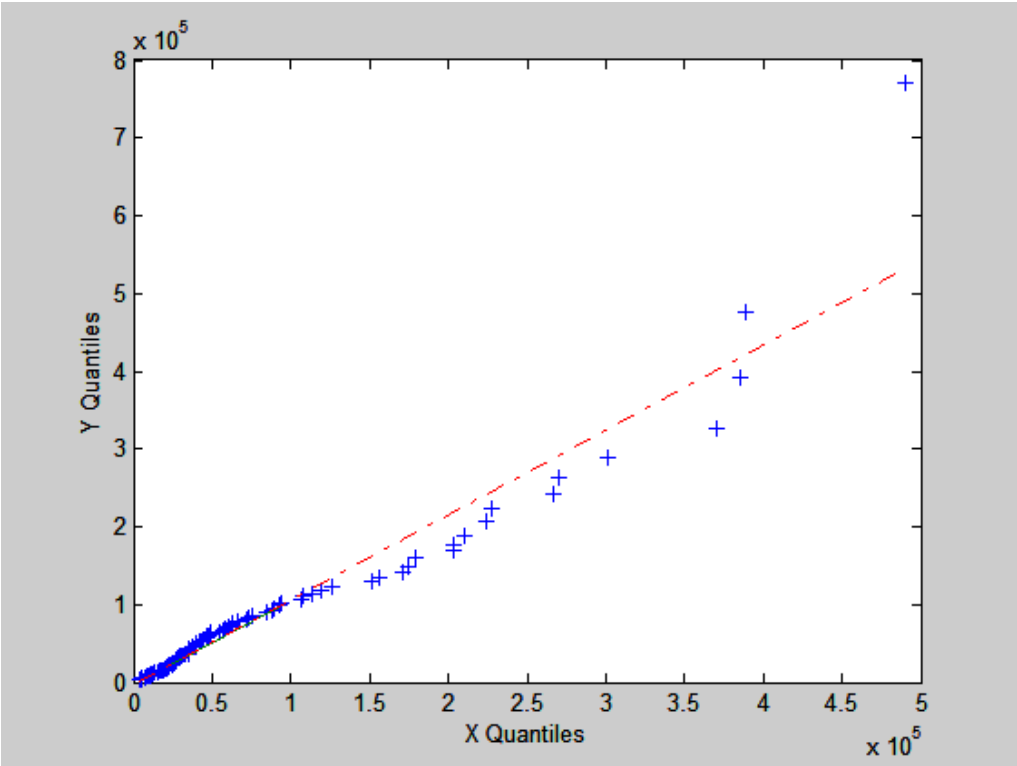
La gráfica 4.2, relativa a finanzas corporativas representa una distribución sesgada a la derecha, mientras que el factor de riesgo fraude por tarjetas, gráfica 4.3, muestra un comportamiento simétrico. Cabe señalar que para las líneas de negocios banca comercial y pago y liquidación, así como los factores de riesgo regulatorio, fraude externo, cheques, falto y falso y errores en la ejecución

de operaciones tuvieron un comportamiento por demás irregular, en sus histogramas, ya que la mayor parte de las pérdidas simuladas se encuentran concentradas en cero y además los valores obtenidos de la simulación representan cifras estratosféricas.

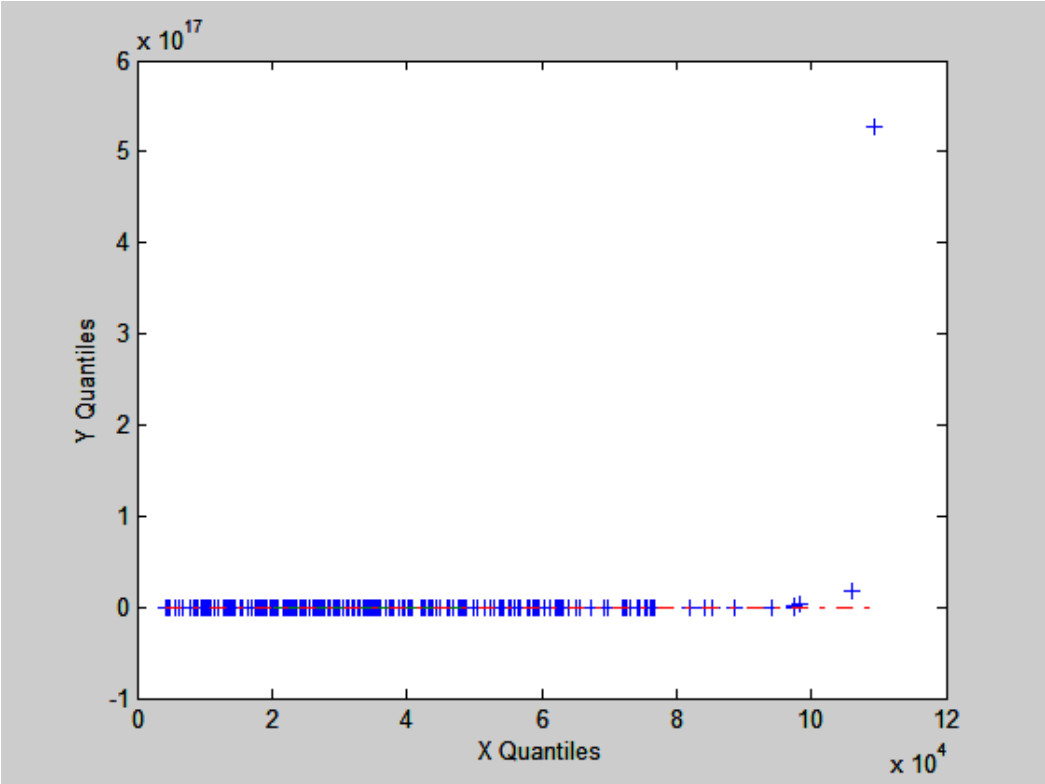
La razón por la cual se obtuvieron diferentes comportamientos es el grado en el que las distribuciones Poisson y Lognormal se aproximan al comportamiento de las pérdidas reales de cada una de las líneas de negocio o factores de riesgo. Una herramienta que permite conocer que tan bien se ajusta una distribución de probabilidad a las pérdidas reales es la gráfica Q-Q. En estadística, un gráfico Q-Q es un método gráfico para identificar la diferencias entre una distribución de probabilidad de una población de la que se ha extraído una muestra aleatoria y una distribución usada para su comparación. Si en el gráfico Q-Q se obtiene una línea recta a 45°, quiere decir que la distribución de probabilidad seleccionada para modelar el comportamiento de las pérdidas se ajusta a las mismas. A continuación se muestran en las graficas 4.4, 4.5 y 4.6 los gráficos obtenidos para las pérdidas totales, para la línea finanzas corporativas y para el factor de riesgo regulatorio.



Gráfica 4.4 Pérdida Total



Gráfica 4.5 Finanzas Corporativas



Gráfica 4.6 Factor regulatorio

Se puede observar que para algunas líneas de negocio y factores de riesgos las distribuciones propuestas inicialmente para modelar su frecuencia y severidad no representan un buen ajuste, por lo que resta para un futuro trabajo proponer distribuciones más sofisticadas que capturen el comportamiento de la distribución empírica (por ejemplo las colas pesadas).

Una de las razones que determinó que la distribución lognormal no representara un buen ajuste para algunos factores de riesgo y líneas de negocios, fue a una desviación estándar estimada grande. Con aquellas variables de varianza o desviación estándar muy grandes, los números aleatorios normales pueden ser negativos "grandes" de tal forma que al generar la exponencial de dichos valores tienden a cero.

Conclusión del cálculo de la Pérdida Esperada y No Esperada

Una vez que se ha calculado el requerimiento de capital con cada uno de los métodos establecidos en el Acuerdo de Basilea II, se puede concluir que conforme se fueron aplicando los métodos del básico al avanzado se obtuvo una reducción en el capital mínimo requerido. A continuación en la tabla 4.7 se muestra un resumen de los valores obtenidos con cada uno de los métodos.

Tabla 4.7 Cuadro resumen con los monto obtenidos para el requerimiento de capital

Método Capital	**requerido (en miles)**
Indicador Básico	49,088
Método estándar	45,750
Método estándar alternativo	27,926
Método de medición avanzada	17,415

La disminución del capital requerido representa un aumento en la capacidad financiera de la Institución. En otras palabras, debido a que el capital requerido se redujo de ***49 MM de pesos*** a ***17.5 MM de pesos***; lo que representa una disminución del 67%. Esta cantidad que la institución se ha ahorrado constituye para la compañía un mayor flujo de efectivo; el cual puede ser utilizado en inversiones o en préstamos comerciales o minoristas.

CONCLUSIONES

Con el paso de los años los sectores: empresarial, industrial y de negocios han visto recrudecer los enfrentamientos que existen entre instituciones, las cuales, buscan la supervivencia y por en de el derrocamiento de sus competidoras. Hoy en día , hacer más con m enos, hacer las cosas bi en a la primera y cada vez mejor y por supuesto innovar en los procedimientos con el fin de obtener ventajas competitivas son herramientas que deben de i r de la m ano y trabajar d e manera conjun ta, para poder cumpl ir e l obje tivo que ti ene cual quier empresa de product os, servicios e incluso de l sect or bancario o financiero que es la supervivencia y ge nerar ingresos. No obstante que las herramientas anteriormente mencionadas perm iten mejorar l os re sultados de cualquier sect or de negocios, es importante, no dejar a un lado la gestión de eventos internos o externos a la compañía que al pasar desapercibidos en el día a día dan l ugar a fa ctores generador es d e i mportantes pérdidas económicas para las compañías. La gestión de di chos eventos es lo que se con oce como gestión de riesgo operacional.

La importancia de crear un model o de gesti ón de ri ego operaci onal radi ca en pre venir la materialización de pérdidas económicas para las instituciones tanto del sector productivo, financiero, como de servicios. El modelo de gestión de riesgo operacional está conformado por el conjunto de procesos, procedimientos, pol íticas y acciones que permiten la mi tigación de l as pérd idas ocasionadas por errores o perativos y p or e nde maximizar su utilidad. E sto lo l ogra al id entificar, cuantificar, dar seguimiento y monitorear los di ferentes tipos de ri esgo a los que s e encu entra expuesta una institución d e tal f orma q ue esto p ermita la mitigación de las p érdidas. Es importante señalar que dada la naturaleza de las diferentes operaciones existentes en cada uno de los sectores, resulta d ifícil plasmar en un sol o document o las di ferentes herramientas i nherentes a l a gest ión del riesgo operacional en cada uno de ellos. Es por ello que la idea trascendental que se desea resaltar es el beneficio económico que resulta de la aplicación de las diferentes herramientas que conforman a la gestión de riesgo operacional.

El beneficio gen erado p or l a a plicación de l a gestión de ri esgo oper acional es q ue las instituciones cuen ten con un may or margen de utilidad debi do a la d isminución de pé rdidas esperadas y no esperadas que reducen sus ingresos. No debe perderse de vista que la aplicación del modelo de gest ión se deberá hacer bajo la premi sa de que cada sector requeri rá de diferentes metodologías e instrumentos que les perm itan la m itigación de s us respec tivos riesgos . No s e debe olvidar que l as pérdidas oc urren a d iario y paradójicamente siempre est arán ahí con o si n l a aplicación de herramientas qu e permita su erradicación pero l a f recuencia y severidad de l as pérdidas estarán acordes al grado de control que tenga sobre ellas la institución. Es por es o que las entidades financieras d eben desarrollar me todologías avanzadas y ef icientes de admin istración d e

%5

sus riesgos operacionales, con la finalidad de obtener modelos que permitan la cuantificación de las pérdidas derivadas de dichos riesgos, y por ende lograr una mejor administración de los mismos. Esto se traduce en ahorros concretos de capital, y en una mejor posición de solvencia frente a posibles debilidades.

Como se mencionó anteriormente la relación que existe entre la ingeniería industrial y el riesgo operacional es muy estrecha debido a que el ingeniero industrial es capaz de mejorar la forma de hacer empresa derivado de su versatilidad y capacidad de adaptarse a cualquier medio empresarial y concentrándose en obtener el máximo rendimiento de los recursos humanos, materiales, tecnológicos y financieros. Para mejorar el rendimiento de una institución se requiere de herramientas de control aplicables a las operaciones realizadas en el mundo empresarial, él cual, ha tenido un crecimiento en los últimos años; no solo en volumen sino también en complejidad y cantidad de servicios y productos que se ofrecen.

Por lo tanto, la ingeniería industrial es el medio por el cual las empresas de servicios, productos y financieras pueden generar procesos de gestión de riesgo operacional que les permitan poder mitigar sus respectivos riesgos. Cabe señalar que cada una de las instituciones tendrá una meta diferente de disminución del requerimiento de capital que sería el objetivo más importante de la gestión de riesgo operacional en una institución financiera; por ejemplo tanto la industria de servicios como la de productos buscarán incrementar la utilidad de la institución al mitigar todos aquellos posibles riesgo que reduzcan los ingresos de la compañía.

1. ANEXOS

Tabla 6.1 Definición de las Líneas de Negocio		
Nivel 1	**Nivel 2**	**Grupos de Actividades**
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, bursatilizaciones, servicio de estudios, deuda, acciones, sindicaciones, ofertas públicas iniciales, colocaciones privadas en mercados secundarios.
	Finanzas de Administraciones locales / públicas	
	Banca de inversión	
	Servicios de consultoría	
Negociación y ventas	Compras y ventas	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.
	Formación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Créditos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarias.
	Banca privada o patrimonial	Créditos y depósitos de clientes de banca privada o patrimonial, servicios bancarios, fideicomisos y testamentarías, y asesoría de inversión.
	Servicios de tarjetas	Tarjetas de empresa / comerciales, de marca privada y minoristas
Banca comercial	Banca comercial	Financiamiento de proyectos, bienes raíces, financiamiento de exportaciones, financiamiento comercial, factoraje, arrendamiento financiero, préstamo, garantías, letras de cambio.
Pago y liquidación	Clientes externos	Pagos y cobranzas, transferencia de fondos, compensación y liquidación.
Servicios de agencia	Custodia	Depósitos en custodia, certificados de depósito, operaciones de sociedades (clientes) para préstamo de valores.
	Agencia para empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos, participaciones accionarias.
	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable

Tabla 6.1 Definición de las Líneas de Negocio		
Nivel 1	**Nivel 2**	**Grupos de Actividades**
Intermediación minorista / operaciones de corretaje al menudeo	Intermediación minorista / operaciones de corretaje al menudeo	Recepción, registro, ejecución y asignación.

Tabla 6.2 Clasificación de tipos de eventos de pérdida			
Tipo de evento de pérdida (Nivel 1)	**Definición**	**Nivel 2**	**Ejemplos de actividades (Nivel 3)**
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	Operaciones no reveladas (intencionalmente) Operaciones no autorizadas (con pérdidas pecuniarias) Valoración errónea de posiciones (intencional)
		Hurto y fraude	Fraude / fraude crediticio/ depósitos sin valor Hurto / extorsión / malversación / robo Apropiación indebida de activos, Destrucción dolosa de activos , Falsificación Utilización de cheques sin fondos, Contrabando Apropiación de cuentas, de identidad, etc. Incumplimiento / evasión de impuestos (intencional) Soborno / cohecho Abuso de información privilegiada (no a favor de la empresa)
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	Hurto/ robo, Falsificación Utilización de cheques sin fondos.
		Seguridad de los sistemas	Daños por ataques informáticos Robo de información (con pérdidas pecuniarias)

Tipo de evento de pérdida (Nivel 1)	Definición	Nivel 2	Ejemplos de actividades
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad / discriminación	Relaciones laborales	Cuestiones relativas a remuneración, Prestaciones sociales, extinción de contratos. Organización laboral
		Higiene y seguridad en el trabajo	Responsabilidad en general (resbalones, etc.) Casos relacionados con las normas de higiene y seguridad en el trabajo Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas Aspectos de adecuación / divulgación de Información (know your customer KYC, etc.) Quebrantamiento de la privacidad de información sobre clientes minoristas Quebrantamiento de privacidad Ventas agresivas Confusión de cuentas Abuso de información confidencial Responsabilidad del prestamista

Tipo de evento de pérdida (Nivel 1)	Definición	Nivel 2	Ejemplos de actividades
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencia Prácticas comerciales / de mercado improcedentes Manipulación del mercado Abuso de información privilegiada (en favor de la empresa) Actividades no autorizadas Blanqueo de dinero
		Productos defectuosos	Defectos del producto (no autorizado, etc.) Error de los modelos
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices Superación de los límites de riesgo frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y otros acontecimientos	Pérdidas por desastres naturales Pérdidas humanas por causas externas (terrorismo, vandalismo)
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas	Sistemas	Hardware Software Telecomunicaciones Interrupción / incidencias en el suministro

Tipo de evento de pérdida (Nivel 1)	Definición	Nivel 2	Ejemplos de actividades
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Comunicación defectuosa Errores de introducción de datos, mantenimiento o descarga, Incumplimiento de plazos o de responsabilidades Ejecución errónea de modelos / sistemas Error contable / atribución a entidades erróneas Errores en otras tareas Fallo en la entrega Fallo en la gestión del colateral Mantenimiento de datos de referencia
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar Inexactitud de informes externos (con generación de pérdidas)
		Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas, Registros incorrectos de clientes (con generación de pérdidas) Pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	Subcontratación Litigios con distribuidores

Tabla 6.3 Cuadro resumen de la pérdida neta por nivel 1 y 2 trimestral						
Tipo de evento de pérdida nivel 1 y 2	**2008 -1**	**2008-2**	**2008-3 200**	**8-4 200**	**9-1**	**Total por evento de pérdida**
a1	$812,206.52	$578,476.83	$493,863.59	$1,6	04,716.25 $28	8,354.73	$3,777,617.92
a2	$707,135.82 $	982,049.55	$522,580.92	$416,252.38	$1,824,227.32	$4,452,245.99
a3	$619,858.23	$1,225,321.79	$648,880.96	$4	21,744.50 $79	1,039.85	$3,706,845.34
b4	$6,951,437.57	$7,129,393.69	$9,577,938.58	$8,3	34,799.47 $7,4	12,762.17	$39,406,331.48
b5	$8,808,753.00	$7,824,083.49	$7,990,948.13	$8,2	67,574.01 $7,2	59,343.17	$40,150,701.81
c6	$704,419.05	$797,021.31	$863,103.74	$4	98,609.89 $56	5,722.18	$3,428,876.17
c7	$1,096,147.11	$290,012.58	$715,996.58	$7	39,144.74 $78	0,399.85	$3,621,700.86
c8	$239,168.65 $	1,411,369.50	$424,257.30	$1,236,945.03	$1,223,206.04	$4,534,946.53
d10	$816,820.16	$66,749.65	$467,406.30	$7	95,044.24 $53	9,068.09	$2,685,088.44
d11	$749,382.67	$558,447.92	$359,521.50	$3	60,035.72 $55	4,579.03	$2,581,966.83
d12	$1,086,016.89 $	1,061,503.80	$2,385,930.72	$494,684.41	$717,153.38	$5,745,289.19
d13	$797,753.26	$895,111.75	$300,977.91	$5	80,846.38 $50	6,898.07	$3,081,587.36
d9	$201,528.32	$231,172.34	$742,749.76	$1,7	82,360.64 $80	7,396.85	$3,765,207.90
f15	$323,418.64	$571,051.77	$272,134.93	$5	72,515.47 $54	3,429.33	$2,282,550.14
g16	$1,120,838.31	$361,827.18	$1,383,988.85	$1,6	51,316.28 $1,4	10,114.92	$5,928,085.53
g17	$1,147,993.41	$753,358.10	$297,933.08	$1,1	33,911.87 $49	2,033.34	$3,825,229.79
g18	$1,790,577.37	$848,230.56	$1,030,823.48	$1,7	98,215.39 $1,4	43,358.05	$6,911,204.85

g19	$1,128,739.99	$818,800.13	$1,619,592.95 $1,7	12,851.02 $2,9	46,379.68	$8,226,363.77
g20	$2,592,856.83 $	636,580.96	$898,114.24	$2,663,071.71	$1,441,823.82	$8,232,447.55
g21	$1,342,502.90 $	939,751.79	$1,291,570.76	$752,429.99	$271,182.23	$4,597,437.67
g22	$2,180,027.56	$1,297,177.35	$1,653,246.86 $	1,173,796.27 $	1,176,250.25	$7,480,498.29
Total por trimestre	$35,217,582.25	$29,277,492.04	$33,941,561.15 $	36,990,865.65 $	32,994,722.33	**$168,422,223.41**

Tabla 6.4 Cuadro resumen con la pérdida neta por línea de negocio trimestral

Tipo de evento de pérdida Línea de negocio	2008-1 200	8-2	2008-3	2008-4	2009-1	Total por Línea de Negocio
Finanzas Corporativas	$1,327,028.24	$801,172.35	$1,354,939.73 $	2,156,086.18 $	1,941,945.98	$7,581,172.47
Negociación y ventas	$4,307,237.71	$2,420,180.38	$2,710,798.41 $	4,973,722.51 $	3,700,772.21	$18,112,711.23
Banca Minorista	$15,238,822.20	$16,974,610.84	$15,832,859.07 $	15,753,452.54 $	17,374,387.93	$81,174,132.58
Banca Comercial	$10,624,131.30	$5,730,010.28	$8,473,211.22 $	8,767,345.77 $	6,484,140.43	$40,078,839.00
Pago y liquidación	$3,720,362.80	$3,351,518.19	$5,569,752.72 $	5,340,258.65 $	3,493,475.78	$21,475,368.13
Total por trimestre	$35,217,582.25	$29,277,492.04	$33,941,561.15 $	36,990,865.65 $	32,994,722.33	**$168,422,223.41**

Tabla 6.5 Cuadro resumen con la pérdida neta por factor de riesgo trimestral						
Factor de riesgo	**2008-1**	**2008-2**	**2008-3**	**2008-4**	**2009-1**	**Total por factor de riesgo**
Asaltos	$886,979.69 $	1,654,042.18	$1,661,151.29	$839,909.58	$1,901,076.45	$6,943,159.20
Cheques	$908,409.39 $	829,034.88	$793,136.08	$776,087.13	$844,536.79	$4,151,204.27
Errores en la Ejecución de operaciones	$6,848,783.52 $	3,422,340.80	$4,755,283.63	$6,199,419.64	$5,402,007.63	$26,627,835.22
Falla en los sistemas	$228,353.98 $	413,099.89	$154,228.71	$489,464.92	$443,638.08	$1,728,785.57
Falto y falso	$432,938.44 $	527,504.79	$520,547.84	$444,074.78	$475,735.16	$2,400,801.01
Fraude externo	$3,853,210.52 $	2,586,956.14	$3,414,730.59	$3,257,475.84	$2,689,688.92	$15,802,062.02
Fraude interno	$2,043,899.83 $	2,656,603.05	$1,511,044.15	$2,347,818.60	$2,763,199.56	$11,322,565.18
Fraude tarjetas	$7,886,278.47 $	8,032,557.64	$8,183,338.35	$7,989,003.35	$7,928,284.32	$40,019,462.14
Juicios laborales	$2,039,734.81 $	2,498,403.39	$2,003,357.63	$2,474,699.67	$2,569,328.07	$11,585,523.56
Legal	$7,120,414.90 $	3,643,192.51	$7,424,631.47	$8,780,565.10	$5,027,976.04	$31,996,780.03
Phising	$868,949.31 $	1,058,005.48	$1,379,907.42	$1,454,820.05	$1,010,281.83	$5,771,964.09
Regulatorio	$2,099,629.40 $	1,955,751.28	$2,140,203.99	$1,937,526.98	$1,938,969.47	$10,072,081.12
Total por trimestre	$35,217,582.25 $	29,277,492.04	$33,941,561.15	$36,990,865.65	$32,994,722.33	**$168,422,223.41**

Tabla 6.6 Ejemplo del formato de la encuesta para la primera parte del Risk Control Self Assessment

Risk Control Self Assessment (1ª parte)			Siempre	Casi siempre	Algunas veces	Casi nunca	Nunca
Sección	**Ref.**	**Descripción**	**1**	**2 3**	**4**		**5**
Clima Organizacional	A	Nuestra unidad trabaja bajo lineamientos y códigos de ética.					
	B	Nuestra unidad fomenta el cumplimiento de los principales valores tales como: integridad, respeto, honestidad, justicia.					
	C	Nosotros no comprometemos nuestra integridad personal para alcanzar los objetivos de la unidad.					
	D	Nuestra unidad tiene claramente definidas las funciones de cada puesto y los limites de las responsabilidades.					
	E	Los miembros de la unidad de negocios se sienten satisfechos con su trabajo.					
	F	La responsabilidad de los trabajos en equipo es compartida.					
	G	Las opiniones, ideas y sugerencias de los trabajadores son aceptadas y consideradas en la toma de decisiones.					
	H	Nuestra unidad interactúa y coopera con las demás unidades de negocios.					
	I	Nuestra unidad hace buen uso de los recursos que le son asignados.					
Gerencia	J	Nuestra unidad define y proporciona claramente los objetivos y metas a alcanzar.					
	K	Nuestra unidad cuenta con medidas para prevenir la corrupción.					
	L	Los objetivos y metas establecidas en la unidad constituyen un incentivo alcanzable.					
	M	Nosotros damos seguimiento de los resultados conseguidos de acuerdo con los objetivos y planes establecidos.					
	N	Nuestra unidad está alineada a los procedimientos establecidos.					
	O	Dentro de la unidad no se suelen recibir órdenes contradictorias de diferentes personas.					
Recursos Humanos	P	Nuestra unidad cuenta con perfiles elaborados para la identificación y contratación de personal calificado y competente.					
	Q	Nuestra unidad cuenta con un programa equitativo y justo para la evaluación de funciones y desempeño.					
	R	Nuestra unidad brinda capacitación, entrenamiento y asesoría a sus empelados.					
	S	La actual tasa de rotación de personal no afecta significativamente la operación de nuestra unidad.					
	T	Nuestros niveles de personal son adecuados para cumplir con la carga de trabajo requerida y los objetivos trazados.					

Tabla 6.7 Ejemplo del formato de la encuesta para la segunda parte del Risk Control Self Assessment

Risk Control Self Assessment (2 ª parte) Funciones de la Unidad Evaluada			Severidad						Nivel de control					
			Nulo	Insignificante	Moderado	Significante	Fuerte	No aplica	Total	Alto	Medio	Bajo	Nulo	No aplica
Sección	**Ref.**	**Descripción**	**1 2**		**3 4**		**5 0**	**1**		**2 3**	**4**		**5 0**	
Procesos	A.1	El servicio que proporciona la unidad a los clientes internos y/o externos no es oportuno y eficiente.												
	A.2	La calidad en el servicio al cliente es deficiente.												
	A.3	El seguimiento y resolución de quejas es poco efectivo.												
	A.4	Es ineficiente la verificación de la información y datos de nuevos clientes.												
	A.5	Los clientes no cumplen las condiciones estipuladas en los contratos.												
	A.6	Los procesos no cumplen con las necesidades del cliente.												
	A.7	Las operaciones no se apegan a las políticas, procedimientos y controles existentes.												
	A.8	Ineficiente proceso para la detección, corrección y/o reporte de los errores causados durante las operaciones.												
	A.9	Es ineficiente el control de desvíos de fondos.												
	A.10	Existe uso indebido de facultades y poderes por parte del personal de la unidad de negocios.												
	A.11	El personal de la unidad de negocios realiza operaciones no reveladas y no autorizadas por la dirección.												
	A.12	Ineficiente proceso para la prevención de fraudes, hurtos, extorsiones, robos, falsificaciones, contrabando, sobornos tanto externos como internos.												

Procesos	A.13	Existe mal uso de la información confidencial de clientes e inversionistas.														
	A.14	No se cumple en tiempo y forma con las tareas y responsabilidades asignadas.														
	A.15	No se conoce o no se cumple con la Normativa fiscal y bancaria.														
	A.16	No se cuenta con la información requerida para que la unidad pueda llevar a cabo sus funciones.														
	A.17	La planeación de las actividades a desarrollar es deficiente.														
	A.18	Eventos significativos no están bajo supervisión para garantizar la implementación de los cambios o acciones necesarios.														
	A.19	No se conocen las necesidades de los clientes y usuarios de la unidad														
Personal	B.1	Existe discriminación, acoso y violación de la privacidad en el trabajo.														
	B.2	Se realizan despidos injustificados o fuera de las políticas de la compañía.														
	B.3	Existen lesiones de clientes y empleados en las instalaciones debido al incumplimiento de la normativa de seguridad e higiene.														
	B.4	Las actividades y responsabilidades del personal no son definidas ni comunicadas claramente.														
	B.5	La organización y clima laboral no favorecen la realización de actividades.														
Sistemas	C.1	El sistema de seguridad es vulnerable ante ataques e intrusiones informáticas.														
	C.2	Existe robo de información privilegiada de los clientes.														
	C.3	El personal utiliza inadecuadamente las claves de acceso y/o niveles de autorización.														
	C.4	A menudo se tienen problemas con el Hardware y Software utilizados.														

Eventos externos	D.1	Ausencia de planes de acción ante desastres naturales.													
	D.2	Las instalaciones no están aseguradas ante eventos externos.													
	D.3	Ausencia de planes de acción ante eventos tales como: vandalismo o terrorismo.													

Tabla 6.8 Ejemplo del formato de la encuesta para la segunda parte del Risk Control Self Assessment

Risk Control Self Assessment (2 ª parte) Funciones de soporte de otras unidades.			Severidad						Nivel de control					
			Nulo	Insignificante	Moderado	Significante	Fuerte	No aplica	Total	Alto	Medio	Bajo	Nulo	No aplica
Sección	**Ref.**	**Descripción**	**1**	**2 3**	**4**		**5 0**	**5**		**4 3**	**2**		**1**	**0**
Procesos	A.20	Inadecuada planeación y calendarización de proyectos e iniciativas planteadas.												
	A.21	Los productos y/o servicios no cumplen con los requerimientos del mercado.												
	A.22	Ineficiente servicio y soporte proporcionado por otras unidades de negocio.												
	A.23	Falta comunicación y coordinación entre unidades de negocio.												
	A.24	El flujo de trabajo entre unidades de negocios es deficiente.												
	A.25	La información requerida de otras unidades no es oportuna.												
Personal	B.6	Capacitación deficiente de nuevos productos y/o servicios.												
	B.7	Los roles y responsabilidades de las unidades no están definidas claramente.												
Sistemas	C.5	Ineficiente diseño de sistemas y continuos modificaciones.												
	C.6	Las unidades de negocio no participan en el diseño de los sistemas.												
	C.7	Fallos y caídas continúas de los sistemas.												
	C.8	Falta de seguridad en la custodia de passwords, claves, combinaciones e identificadores de usuario.												

Tabla 6.9 Planes de acción de la primera parte del RCSA				
Sección Ref.		**Descripción**	**Impacto**	**Acción**
Clima Organizacional	A	Nuestra unidad trabaja bajo lineamientos y códigos de ética.	3	Diseñar y elaborar un manual de políticas para la institución. Este manual incluirá los códigos de ética a los cuales se apegarán los trabajadores, además se dará a conocer a todo el personal los efectos positivos y negativos que acarrean el cumplimiento e incumplimiento de las normas respectivamente.
	D	Nuestra unidad tiene claramente definidas las funciones de cada puesto y los limites de las responsabilidades.	3	Reestructuración del organigrama estableciendo los alcances de cada nivel y puesto, así como la definición de los roles y responsabilidades de cada uno de ellos. Una vez completada esta tarea se debe dar a conocer a todo el personal.
	I	Nuestra unidad hace buen uso de los recursos que le son asignados.	2	Diseñar y elaborar un reglamento interno de trabajo donde se establezcan las pautas que se deben cumplir en la utilización de recursos financieros, materiales y humanos.
Gerencia	K	Nuestra unidad cuenta con medidas para prevenir la corrupción.	2	Diseñar y elaborar un manual de políticas para la institución.
	L	Los objetivos y metas establecidas en la unidad constituyen un incentivo alcanzable.	3	Involucrar al personal de todos los niveles de la institución para establecer las estrategias a corto, mediano y largo plazo de tal forma que se asegure la viabilidad para todas las unidades de negocio.
	M	Nosotros damos seguimiento de los resultados conseguidos de acuerdo con los objetivos y planes establecidos.	2	Constituir un cronograma por medio del cual un responsable de cada unidad realizará el seguimiento en el cumplimiento de los objetivos y planes establecidos. Por lo tanto, es necesario que previamente se determine la periodicidad con la que se llevará a cabo el seguimiento acorde a la importancia que el personal involucrado haya estipulado.

O		Dentro de la unidad no se suelen recibir órdenes contradictorias de diferentes personas.	2	Reestructuración del organigrama estableciendo los alcances de cada nivel y puesto, así como la definición de los roles y responsabilidades de cada uno de ellos. Una vez completada esta tarea se debe dar a conocer a todo el personal.
Recursos Humanos	T	Nuestros niveles de personal son adecuados para cumplir con la carga de trabajo requerida y los objetivos trazados.	4	No es necesario establecer acciones de mitigación en virtud de que se entiende que ya se están atendiendo en el proceso del día a día.

Tabla 6.10 Planes de acción de la segunda parte del RCSA

Sección R	ef.	Descripción Impac	to	Acción
Procesos	A.6	Los procesos no cumplen con las necesidades del cliente.	1	Se realizarán investigaciones de mercado con el fin de conocer las tendencias, necesidades y preferencias de los clientes. Así como las expectativas que tiene de los productos o servicios. Principalmente se buscará indagar más directamente con el cliente y poder enfocarse a sus verdaderas necesidades.
	A.7	Las operaciones no se apegan a las políticas, procedimientos y controles existentes.	1	Llevar a cabo una campaña sobre la concientización del cumplimiento de las políticas, procedimientos y controles con el fin de evitar operaciones no esperadas.
	A.8	Ineficiente proceso para la detección, corrección y/o reporte de los errores causados durante las operaciones.	1	Realizar capacitación sobre la metodología de la gestión y control de errores durante la operación.
	A.9	Es ineficiente el control de desvíos de fondos.	2	Rediseñar los controles con el fin de restringir los accesos que permitan hacer uso de fondos de clientes o inversionistas.

	A.10	Existe uso indebido de facultades y poderes por parte del personal de la unidad de negocios.	1	Diseñar y elaborar un manual de políticas para la institución. Este manual incluirá los códigos de ética a los cuales se apegarán los trabajadores, además se dará a conocer a todo el personal los efectos positivos y negativos que acarrean el cumplimiento e incumplimiento de las normas respectivamente. Así mismo, se sancionará el incumplimiento del mismo.
	A.23	Falta comunicación y coordinación entre unidades de negocio.	2	Motivar la integración del personal mediante talleres donde se destaque la integración multi-disciplinaria, trabajo en equipo y de comunicación efectiva.
Personal	B.2	Se realizan despidos injustificados o fuera de las políticas de la compañía.	2	Examinar las condiciones y razones bajo las cuales se realizaron los despidos.
	B.3	Existen lesiones de clientes y empleados en las instalaciones debido al incumplimiento de la normativa de seguridad e higiene.	1	Evaluar las instalaciones bajo la normativa pertinente; lo que dará pie remodelaciones, adecuaciones o rediseño que las instalaciones necesiten.
	B.5	Las actividades y responsabilidades del personal no son definidas ni comunicadas claramente.	2	Reestructuración del organigrama estableciendo los alcances de cada nivel y puesto, así como la definición de los roles y responsabilidades de cada uno de ellos. Una vez completada esta tarea se debe dar a conocer a todo el personal.
	B.6	La organización y clima laboral no favorecen la realización de actividades.	3	Promover actividades fuera del horario de trabajo que permitan la integración del personal así como el desarrollo del sentido de pertenencia de los trabajadores con la empresa.
Sistemas	C.1	El sistema de seguridad es vulnerable ante ataques e intrusiones informáticas.	1	Diseñar un sistema de seguridad mas robusto y confiable que reduzca la vulnerabilidad del banco ante posibles ataques.
	C.2	Existe robo de información privilegiada de los clientes.	1	Crear candados y accesos de seguridad que restrinjan el saqueo o robo de información.

Tabla 6.11 Tabla con la pérdida neta obtenida por factor de riesgo trimestral					
Factor de riesgo	**Pérdida neta trimestral**				
	2008-1 2	**008-2**	***2008-3***	***2008-4***	***2009-1***
Legal	*$7,126,599*	$3,643,193 $7	,431,020	$8,785,259	$5,033,039
Regulatorio	*$1,955,751*	$2,099,629 $2	,140,204	$1,937,527	$1,938,969
Fraudes Tarjetas	*$7,886,278*	$8,032,558 $8	,183,338	$7,989,003	$7,928,284
Fraude Externo	*$3,853,210*	$2,586,956 $3	,414,731	$3,257,476	$2,689,689
Fraude Interno	*$2,043,899*	$2,656,603 $1	,511,044	$2,347,819	$2,763,200
Phishing	*$868,949*	$1,058,005 $1	,379,907	$1,454,820	$1,010,282
Asaltos	*$886,979*	$1,654,042 $1	,661,151	$839,910	$1,901,076
Cheques	*$908,409*	$829,035 $79	3,136	$776,087	$844,537
Juicios Laborales	*$2,039,734*	$2,498,403 $2	,003,358	$2,474,700	$2,569,328
Falto y Falso	*$432,938*	$527,505 $52	0,548	$444,075	$475,735
Fallas de Sistemas	*$228,353*	$413,100 $15	4,229	$489,465	$443,638
Errores en Ejecución de Operaciones	*$6,848,783*	$3,422,341 $4	,755,284	$6,199,420	$5,402,008

Tabla 6.12 Tabla con el número de eventos presentados por factor de riesgo trimestral					
Factor de riesgo	**Número de eventos por trimestre**				
	2008-1 200	**8-2**	***2008-3***	***2008-4***	***2009-1***
Legal	$17	$9	$19 $	22 $13	
Regulatorio	$52	$56	$59 $	58 $55	
Fraudes Tarjetas	$3,942 $4	,016	$4,097	$3,994	$3,951
Fraude Externo	$57	$51	$64 $	58 $50	
Fraude Interno	$18	$18	$12 $	15 $17	
Phishing	$9	$7	$16 $	16 $12	
Asaltos	$10 $	15	$16	$9	$20
Cheques	$84	$80	$77 $	81 $78	
Juicios Laborales	$10	$13	$11 $	15 $11	
Falto y Falso	$113 $12	7	$126	$115	$119
Fallas de Sistemas	$8 $	15	$8	$14	$15
Errores en Ejecución de Operaciones	$38	$24	$28 $	31 $29	

Tabla 6.13 Tabla con el promedio de pérdida neta por factor de riesgo trimestral					
Factor de riesgo	**Promedio de pérdida neta**				
	2008-1 20	**08-2**	***2008-3***	***2008-4***	***2009-1***
Legal	$419,212 $40	4,799	$391,106	$399,330	$387,157
Regulatorio	$37,611 $	37,493	$36,275	$33,406	$35,254
Fraudes Tarjetas	$2,001 $2	,000	$1,997	$2,000	$2,007
Fraude Externo	$67,600 $	50,725	$53,355	$56,163	$53,794
Fraude Interno	$113,550 $14	7,589	$125,920	$156,521	$162,541
Phishing	$96,550 $15	1,144	$86,244	$90,926	$84,190
Asaltos	$88,698 $11	0,269	$103,822	$93,323	$95,054
Cheques	$10,814 $	10,363	$10,300	$9,581	$10,827
Juicios Laborales	$203,973 $19	2,185	$182,123	$164,980	$233,575
Falto y Falso	$3,831 $4	,154	$4,131	$3,862	$3,998
Fallas de Sistemas	$28,544 $	27,540	$19,279	$34,962	$29,576
Errores en Ejecución de Operaciones	$180,231 $14	2,598	$169,832	$199,981	$186,276

Tabla 6.14 Ingresos por línea de negocio y saldos insolutos de cartera								
Mes	**Finanzas Corporativas**	**Negociación y Ventas**	**Banca al Menudeo**	**Banca Comercial**	**Pago y Liquidación**	**Total**	**Saldo insoluto Cartera Comercial**	**Saldo insoluto Cartera de Menudeo**
t-1 $37		$3,243	$13,220	$6,984	$1,459	**$24,943**	$142,036 $1	86,422
t-2 $39		$3,412	$13,909	$7,348	$1,535	**$26,242**	$150,630 $1	97,702
t-3 $44		$3,811	$15,536	$8,208	$1,715	**$29,313**	$132,855 $1	74,372
t-4 $48		$4,121	$16,801	$8,876	$1,854	**$31,699**	$140,692 $1	84,658
t-5 $45		$3,861	$15,742	$8,317	$1,738	**$29,703**	$115,314 $1	51,349
t-6 $35		$3,043	$12,406	$6,554	$1,369	**$23,407**	$137,857 $1	80,937
t-7 $46		$4,007	$16,337	$8,631	$1,803	**$30,825**	$112,270 $1	47,354
t-8 $43		$3,752	$15,296	$8,081	$1,688	**$28,861**	$146,483 $1	92,259
t-9 $47		$4,081	$16,637	$8,789	$1,836	**$31,390**	$111,115 $1	45,839
t-10 $47		$4,113	$16,768	$8,859	$1,851	**$31,638**	$135,391 $1	77,701
t-11 $40		$3,470	$14,145	$7,473	$1,561	**$26,689**	$131,899 $1	73,118
t-12 $47		$4,053	$16,523	$8,729	$1,824	**$31,176**	$112,069 $1	47,091
t-13 $46		$3,949	$16,099	$8,505	$1,777	**$30,375**	$148,004 $1	94,255
t-14 $42		$3,680	$15,004	$7,926	$1,656	**$28,309**	$113,924 $1	49,526
t-15 $35		$3,006	$12,254	$6,474	$1,353	**$23,121**	$125,144 $1	64,251
t-16 $39		$3,364	$13,713	$7,244	$1,514	**$25,873**	$150,678 $1	97,765
t-17 $47		$4,103	$16,729	$8,838	$1,847	**$31,565**	$122,550 $1	60,847

t-18 $42		$3,642	$14,847	$7,843	$1,639	**$28,012**	$115,548 $1	51,657
t-19 $34		$2,903	$11,835	$6,253	$1,306	**$22,331**	$135,284 $1	77,560
t-20 $35		$3,025	$12,332	$6,515	$1,361	**$23,269**	$138,252 $1	81,456
t-21 $34		$2,921	$11,907	$6,290	$1,314	**$22,466**	$150,812 $1	97,941
t-22 $46		$3,991	$16,272	$8,597	$1,796	**$30,703**	$140,946 $1	84,992
t-23 $36		$3,151	$12,847	$6,787	$1,418	**$24,241**	$113,919 $1	49,518
t-24 $43		$3,708	$15,118	$7,987	$1,669	**$28,525**	$118,751 $1	55,861
t-25 $44		$3,848	$15,687	$8,288	$1,732	**$29,599**	$150,899 $1	98,055
t-26 $34		$2,941	$11,992	$6,335	$1,324	**$22,626**	$132,070 $1	73,342
t-27 $40		$3,446	$14,050	$7,423	$1,551	**$26,510**	$111,655 $1	46,547
t-28 $33		$2,861	$11,664	$6,162	$1,287	**$22,008**	$111,862 $1	46,819
t-29 $40		$3,432	$13,991	$7,392	$1,544	**$26,398**	$127,052 $1	66,755
t-30 $47		$4,066	$16,575	$8,757	$1,830	**$31,274**	$119,366 $1	56,668
t-31 $46		$4,004	$16,324	$8,624	$1,802	**$30,800**	$141,850 $1	86,178
t-32 $34		$2,973	$12,121	$6,404	$1,338	**$22,871**	$111,416 $1	46,233
t-33 $36		$3,112	$12,687	$6,702	$1,400	**$23,937**	$111,396 $1	46,207
t-34 $41		$3,592	$14,644	$7,737	$1,616	**$27,631**	$110,921 $1	45,583
t-35 $38		$3,302	$13,463	$7,112	$1,486	**$25,401**	$145,622 $1	91,129
t-36 $42		$3,645	$14,859	$7,850	$1,640	**$28,035**	$148,007 $1	94,259

Algoritmo utilizado para la simulación Monte Carlo

```
%%%% Este programa realiza la Simulacion Monte Carlo%%%%%

%%%% El resultado será la distribución de las pérdidas totales trimestrales %%%%

%%%% Primero se simula una v.a. N~Poisson(lambda estimada) y despues se simulan N v.a.'s
LogNormal(mu estimada, sigma estimada)%%%%

function y=simulacion_MC(simulaciones,lambda,mu,sigma)

%%%% Se inician en cero las variables %%%%

N=zeros(simulaciones,1);

X=zeros(simulaciones,1);

%%%% Simulacion v.a.'s Poisson y LogNormal %%%%

N=poissrnd(lambda,simulaciones,1);

for k=1:simulaciones

   X(k)=sum(lognrnd(mu,sigma,N(k),1));

end

%%%% Defino vector de resultados %%%%

y=X;
```

Tabla 6.15 Cuadro resumen del cálculo de la pérdida esperada y no esperada								
	Pérdida esperada	**Pérdida no esperada**	**Desviación estándar**	**Variancia**	**Valor mínimo**	**Valor máximo**	**Monto por encima del VaR**	**Promedio del monto**
Total $16,0	**91**	**$1,324**	**403**	**162560329**	**$14,601**	**$17,8 31**	**$176,118**	**$17,612**
Finanzas corporativas	$1,599 $	3,360	668	446792084	$160	$7,994	$57,257	$5,726
Negociación y ventas	$4,859 $14,	624	2342	5486535186	$601	$48, 119	$272,525	$27,253
Banca minorista	$5.47 $	0.32	0.1	10.85	$5.05	$5.85	$58.12	$5.81
Banca comercial	1.49E+15 5.	71E+16	7.71E+16	5.94E+36	0	6.39E+18	1.44E+19 1	.44E+18
Pago y liquidación	3.00E+12 1.	00E+14	2.19E+14	4.81E+31	0	2.15E+16	2.85E+16 2	.85E+15
Legal	$6,200 $	5,454	1567	2455269221	$751	$12, 766	$121,611	$12,161
Regulatorio	2.99E+20 7.	01E+20	2.71E+22	7.37E+47	0	2.71E+24	2.97E+24 3	.30E+23
Fraude tarjetas	$5 $	0	0.08	6	$4	$5	$49	$5
Fraude externo	5.28E+22 3.	72E+22	4.91E+24	2.41E+52	0	4.90E+26	5.27E+26 5	.86E+25
Fraude interno	$2,036 $	1,988	557	310189383	$199	$4,370	$41,567	$4,157
Phising	$1,036 $	1,197	332	110343902	$72	$2,430	$23,046	$2,305
Asaltos	$1,257 $	1,234	356	126538487	$143	$2,745	$26,231	$2,623
Cheques	8.32E+23 -7	.32E+23	6.81E+25	4.63E+54	0	6.60E+27	8.32E+27 8	.32E+26
Juicios laborales	$2,099 $	2,318	636	403893697	$159	$4,878	$45,671	$4,567
Falto y falso	2.05E+13 1.	42E+15	8.91E+14	7.94E+32	0	6.85E+16	1.88E+17 1	.88E+16
Falla de los sistemas	$314 $	398	108	11596096	$20	$745	$7,288	$729
Errores en ejecución de operaciones	4.84E+31 -3	.84E+31	4.72E+33	2.22E+70	0	4.72E+35	4.84E+35 5	.38E+34

BIBLIOGRAFÍA

- LÓPEZ AGÜI Juan Carlos, "*Guía básica para la simulación de Monte Carlo*", AENOR, Madrid, 2008.

- MOOD Alexander McFarlane, "*Introducción a la teoría de la estadística*", *Aguilar, Madrid, 1972*, cuarta edición.

- ROSS Sheldon, *"Simulation"*, Academic, Amsterdam, 2006, cuarta edición.

Fuentes electrónicas

- BANK FOR INTERNATIONAL SETTLEMENTS, "*Convergencia internacional de medidas y normas de capital*", en http://www.bis.org/about/index.htm

- COMISION NACIONAL BANCARIA Y DE VALORES, "*Disposiciones de carácter general aplicable a las instituciones de crédito*", 2 de diciembre del 2005, en http://www.cnbv.gob.mx/seccion.asp?sec_id=10&com_id=0

- COMISION NACIONAL BANCARIA Y DE VALORES, "*Requisitos para la elaboración y actualización de la base de datos histórica que contenga el registro sistémico de los diferentes tipos de pérdida asociada al riesgo operacional de las instituciones de crédito*", en http://www.cnbv.gob.mx/seccion.asp?sec_id=10&com_id=0

- Paradigma Pro Business, "*¿Para qué sirve un plan de acción?*", en http://ppbconsultores.com.mx/2007/12/11/para-que-sirve-un-plan-de-accion/

- ESCANDON VILCHIS Angel Antonio, "*Elabora un plan de acción y ejecutelo*", 31 de Julio del 2009, en http://www.gestiopolis.com/canales7/eco/Capital/70-plan-de-accion-y-su-ejecucion.htm

- JUANICO Xavier, "*Como medir y gestionar el clima laboral*", en http://www.arearh.com/rrhh/clima_laboral.htm

- CHAKRAVARTY Ranjita y TOPPER Frank, "Risk and Control Self-Assessment(RCSA): A useful complement to information systems audits at Standford university", Information System Control Journal, Volume 1, 2001, en

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17149&TEMPLATE=/ContentManagement/ContentDisplay.cfm

- BALFAN Mark, GLEDHILL Phil y HAUBENSTOCK Michael, "*Self-assessment of operational risk*", The RMA Journal, Febrero 2002, en http://findarticles.com/p/articles/mi_m0ITW/is_5_84/ai_n14897063/?tag=content;col1

- DURON ESQUIVEL Gabriel, "Plan de acción. Hacia una ejecución de las tareas y metas programadas", Junio 2004, en http://www.gestiopolis.com/canales2/gerencia/1/planaccion.htm

- ROMERO Francisco, "*Banco Internacional de Pagos de BAsilea*", en Revista Iberoamericana de Sostentabilidad, Sección de Organismos Internacionales, Año 3, No 28, Octubre 2007, en http://www.otromundoesposible.net/default.php?mod=magazine_detail&id=377

- GONZALEZ CERVANTES Fernando, "*Formación en riesgo operacional*", en http://www.fermacrisk.com/RiesgoOperacional.htm

- Federal Reserve Bank of Kansas City and Federal Reserve Bank of St. Louis, "*Key Risk Indicators(KRIs)*", en http://www.stlouisfed.org/col/director/Materials/rumor_keyriskindicators.html

- DAVIS Jonathan y HAUBENSTOCK Michael, "*Building effective indicators to monitor operational risk*", The RMA Journal, Mayo 2002, en http://findarticles.com/p/articles/mi_m0ITW/is_8_84/ai_n14897107/

- Federación Latinoamericana de Bancos, "*Definición y análisis de factores de riesgo*", en http://www.felaban.com/lavado/cap4_definicion.php

- FERNANDEZ Pita y MONTERO Carpente, "*Determinación de factores de riesgo*", en http://www.fisterra.com/mbe/investiga/3f_de_riesgo/3f_de_riesgo.asp

- MOCHAL Tom, "*Determine your tolerance when managing risk*", Tech Republic, Febrero 2006, en http://articles.techrepublic.com.com/5100-10878_11-6035405.html

- WALLS Michael, "*Measuring and utilizing corporate risk tolerance to improve investment decision making*", Engineering Economist, Diciembre 2005, en http://www.allbusiness.com/management/857831-1.html

- PEREZ GALINDO Héctor, "Administración de riesgos operativos: paradigmas y realidades en el nuevo milenio", Octubre 2008.

- Comité de Basilea de Supervisión Bancaria, "*Prácticas sanas para la administración y supervisión del riesgo operativo*", Febrero 2003.

- DAVIES Jonathan, FINLAY Mike, MCLENAGHEN Tara y WILSON Duncan, "*Key Risk Indicators: Their role in operational risk management and measurement*", Risk Business International Limited, Febrero 2006.

- LLAGUNOS MUSONS José Ignacio, "*Gestión del riesgo operativo en las entidades de crédito: un camino sin retorno*", Departamento de Economía Financiera II, Universidad del país Vasco, Noviembre 2005.

- MARASCA Ruben, "*Basilea II: Hacia un nuevo esquema de medición de riesgo"*, Superintendencia de entidades financieras y cambiarias, diciembre 2003.