UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

SECCIÓN DE POSGRADO

METODOLOGÍA PARA LA GESTIÓN DEL RIESGO OPERATIVO DE UN ORGANISMO FINANCIERO PERUANO SEGÚN EL NUEVO ACUERDO DE CAPITALES "BASILEA II"

TESIS

PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN CIENCIAS CON MENCIÓN EN

INGENIERÍA DE SISTEMAS

Ricardo Roland Berrospi Taquire

Lima-Perú

2011

Este trabajo está dedicado a mi familia por su apoyo incondicional y a mi hija Sofía para que la motive a ser mejor que yo.

A los Integrantes de la Sección de Postgrado de la Facultad de Ingeniería Industrial y de Sistemas – Universidad Nacional de Ingeniería, por su valiosa colaboración.

ÍNDICE

ANEXOS

TABLAS

FIGURAS

DESCRIPTORES TEMÁTICOS

- Riesgo Operacional
- Basilea
- Organismo Financiero
- Riesgo
- Nuevo Acuerdo de Capitales (NAC)
- Eventos de Pérdida de Riesgo Operacional
- Procesos Internos
- Personas
- Eventos Externos
- Tecnología
- Método de Indicador Básico
- Método Estándar
- Método Avanzado

RESUMEN

El presente documento expone el estudio materia del título, el cual está enmarcado dentro de las líneas de investigación maestras de "Gestión de Riesgos Informáticos" propuesta por la sección de Postgrado FIIS – UNI.

Dicha investigación surge de la que existe una carencia de componentes metodológicos cualitativos y cuantitativos, o metodologías no totalmente maduras que tienen las empresas del sistema financiero para gestionar sus riesgos. Efectivamente, debido a que el mercado de riesgo operativo aún está en etapa de desarrollo y madurez, lo cierto es que existen dificultades e inconvenientes en su implementación, entre los cuales se encuentra, después de la cultura de la empresa, la falta de un marco metodológico acorde.

Este trabajo propone la creación de un marco metodológico que permita la gestión cualitativa y cuantitativa del riesgo operativo. Para ello, sugiere el establecimiento de un Marco de Gestión Integral de Riesgo Operativo, el cual, debe considerar la composición de los elementos estratégicos y de organización entre los cuales destacan la estructura organizativa, la definición de un modelo general, así como las políticas y la metodología propiamente dicha.

Respecto a la gestión cualitativa, se plantea un marco con enfoque mixto en el que se conjuguen diversas herramientas como las autoevaluación de riesgos, los mapas de riesgo e indicadores. Del mismo modo, para la cuantificación del riesgo operativo, se plantea un enfoque basado en la gestión de riesgo operativo propuesto por el Nuevo Acuerdo de Capital Basilea II. (NAC), el cual es analizado y comparado de modo que

El trabajo finaliza con la ejemplarización de las diferentes herramientas y casos de uso en lo que respecta la gestión del riesgo propiamente dicha.

INTRODUCCIÓN

En la actualidad, existe una carencia de componentes metodológicos cualitativos y cuantitativos en las empresas del sistema financiero peruano, que no les permite realizar eficientemente la gestión del riesgo operacional.

Si bien, en el 2009, la Superintendencia de Banca, Seguros y Administradora de Fondos de Pensiones (SBS) en su rol de supervisor y regulador del sistema financiero peruano, ha dictado una serie de normas relacionadas con la gestión del riesgo operacional, las mismas que están basadas en el Nuevo Acuerdo de Capitales (NAC) Basilea II, en la últimos años, los procesos y aplicación de dicho riesgo aún se encuentran en etapa de maduración y justamente en ese sentido una de las debilidades es la carencia de una metodología de gestión de riesgo operacional.

En este sentido, este trabajo de investigación, propone una metodología para la gestión de riesgo operacional, para ello el documento se ha estructurado en siete (07) capítulos que siguen las recomendaciones de la Sección de Postgrado, de los jurados especialistas así como del propio autor.

El capítulo I describe el procedimiento metodológico realizado para desarrollar la tesis, se incluyen el enunciado del problema, la pregunta de

investigación, los objetivos e hipótesis de la tesis, la justificación, alcances, limitaciones, así como el tipo de investigación, diseño de la investigación, unidades de estudio, técnicas e instrumentos de recolección de datos y las técnicas de medición cuantitativa de riesgos.

El capítulo II, contiene las principales definiciones para situar al lector en el ámbito y campo de estudio que es el sector financiero, bajo el cual recae este estudios, se explica el Principio del Nuevo Acuerdo de Capitales Basilea II y se describen las principales definiciones de Riesgo haciendo énfasis en el Riesgo Operativo.

El capítulo III, desarrollar un análisis de la situación actual de la gestión de riesgo operativo del país, de mismo modo explorar cual es el marco regulatorio que rige bajo este riesgo.

El capítulo IV, describe la metodología propuesta para la gestión de riesgo operativo en una entidad financiera la misma que contempla tanto el enfoque cualitativo así como el cuantitativo.

El capítulo V, con el objetivo de este capítulo es facilitar la comprensión y entendimiento de la metodología propuesta en el capítulo anterior, explica mediante ejemplos cómo una entidad financiera mide el riesgo.

El capítulo VI, dar a conocer los beneficios que tendría la entidad financiera en el caso adopte una metodología de riesgos operativos, se plantean beneficios cualitativos y beneficios cuantitativos para lo cual se realiza un análisis financiero.

Finalmente, se concluye el documento con unas conclusiones y recomendaciones las cuales resumen las principales consideraciones a tener en cuenta en la gestión el riesgo operacional.

CAPÍTULO I

MARCO METODOLÓGICO EMPLEADO EN LA ELABORACIÓN DE LA TESIS

Este capítulo tiene como objetivo presentar todo el procedimiento metodológico realizado para desarrollar la tesis, se parte del enunciado del problema, la pregunta de investigación, los objetivos e hipótesis de la tesis, la justificación, alcances, limitaciones, así como el tipo de investigación, diseño de la investigación, unidades de estudio, técnicas e instrumentos de recolección de datos y las técnicas de medición cuantitativa de riesgos.

1.1. El Problema que se afronta

En la toma de decisiones de las empresas se distingue, que gran parte de las grandes decisiones están soportadas, principalmente, en decisiones de índole financiero, esto se traduce, simplemente, bajo ciertos niveles de rentabilidad y riesgo, en resultados que significarán para la empresa pérdidas o ganancias. Por otro lado, sabemos que en estos últimos años, los principales índices macroeconómicos de nuestro país han mejorado y que en la actualidad le han servido para obtener el grado de inversión.

En ambos escenarios, las empresas del sistema financiero, han venido tomando decisiones que tienen que ver con los niveles de capitalización, administración de carteras, valuación de desempeño, asignación de créditos, inversiones en activos financieros. En adición a los tipos de decisiones mencionados, hoy en día se ha sumado las decisiones por asegurar los procesos y controles internos ya que si estos fallan pueden representar un serio problema que se podría traducir en pérdidas inesperadas.

En ese contexto, las experiencias en pérdidas sufridas por fallas operativo es en organismos financieros de todo el mundo son muchas, por citar algunas podemos mencionar los casos siguientes: *(i)* el caso del Banco Barings, con pérdidas operativas cercanas a los 850 millones de USD; *(ii)* el caso del Daiwa Bank, con pérdidas operativas de alrededor de 1.000 millones de USD. *(iii)* El caso del Sumitomo Bank, con pérdidas por riesgo operativo de 2.600 millones de USD. *(iv)* El caso de Allied Irish Bank, cuyos problemas por riesgo operativo ocasionaron pérdidas por aproximadamente 700 millones de USD. *(v)* El caso de la caída del mayor banco de la República Dominicana (Baninter), que además de producir una crisis financiera, también tuvo un fuerte impacto en la economía del país y como no mencionar el último caso sonado en setiembre del 2011 que ocupó las páginas del Wall Stree Journal (ver Figura I.1) y del diario El Comercio: El caso de fraude en el Banco Suizo UBS en el que un corredor causó una pérdida de US$2.000 millones.

En el Perú, la Superintendencia de Bancos, Seguros y AFP (SBS), en su rol de Supervisor y Regulador, teniendo como base el Nuevo Acuerdo de

Capital - Basilea II (NAC) [1], tiene el deber de implementar un marco adecuado y dar las directrices para la correcta identificación, evaluación, seguimiento y control/mitigación del riesgo de sus supervisados, por ello tanto SBS como sus supervisados se están preparando en este nuevo tema ante la necesidad de brindar mayor seguridad y niveles de confianza para la toma de decisiones.

Figura I.1 Noticia de Fraude

b16 | EL COMERCIO viernes 16 de setiembre del 2011

THE WALL STREET JOURNAL AMERICAS

© 2011 Reservados todos los derechos.

VIERNES, 10 DE SETIEMBRE DEL 2011

What's News

UBS, golpeado por un fraude

Un corredor causó una pérdida de US$2.000 millones en el banco suizo

También plantea dudas sobre los sistemas de gestión y control de riesgo del banco,

[1] Basilea II es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, publicado inicialmente en Junio de 2004, es la creación de un standard internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos..

Fuente y Elaboración: Diario el Comercio

Si bien en el NAC existen directrices, estas no han sido implementadas. Es decir, actualmente, se presenta un escenario en el cual la SBS tiene la necesidad de incorporar una metodología de gestión de riesgos (crédito, de mercado, liquidez, operativo).

En el caso peruano, para el caso de cuantificación del riesgo operativo, es necesario que se incorpore los diversos métodos para cuantificar cada uno de los riesgos. Para ello, en primer lugar se deberá validar cada uno de los métodos para el caso peruano, valga la aclaración los mercados financieros no son iguales a las de Estados Unidos o Suiza,

Por otro lado esta validación y selección de los métodos adecuados dependerá de los resultados coherentes.

En el caso de cualitativo, la existencia de la Norma Técnica Peruana NTP-ISO/IEC 17799 así como las diversas metodologías de gestión de riesgos como la de COSO ERM ofrecen una literatura que debería permitir la identificación los riesgos, la generación de un modelo organizativo y definir herramientas de gestión de riesgos.

En suma, el enunciado del problema es el siguiente:

Se desconocen los métodos de evaluación cualitativa y cuantitativa que contemplará la metodología que permitan gestionar los riesgos operativos de las entidades supervisadas por la SBS.

1.2. Pregunta de Investigación

1.2.1. Pregunta general

¿Cómo se puede gestionar y medir el riesgo operativo en las entidades supervisadas por la SBS, basada para la parte cuantitativa en los métodos propuestos por el NAC y para la parte cualitativa en las principales directrices y buenas prácticas del mercado así como de estándares internacionales?

1.2.2. Pregunta específicas

- ¿Cuál es la estructura y funcionamiento del sistema financiero?
- ¿Cuáles son los principales riesgos a los que están expuestos las empresas del sistema financiero?
- ¿Cómo se puede medir el riesgo operativo?

1.3. Objetivos

1.3.1. Objetivo general

Elaborar una metodología de gestión de riesgo operativo, para su aplicación en las entidades supervisadas por la SBS, teniendo como base, para la parte cualitativa las principales directrices y buenas prácticas del mercado y para la parte cuantitativa los métodos propuestos por el NAC.

1.3.2. Objetivos específicos

- Identificar la estructura y funcionamiento del sistema financiero.
- Identificar los principales riesgos a los que están expuestos las empresas del sistema financiero.
- Analizar los diferentes métodos de gestión y medición del riesgo operativo.

1.4. Hipótesis

1.4.1. Hipótesis General

Para alcanzar dicho objetivo, se formula la hipótesis siguiente:

H1: La metodología para Gestionar el Riesgo Operativo no presenta el nivel de madurez deseado para gestionar integralmente el riesgo operativo pudiendo ser una dificultad cuando se trate de gestionar dicho riesgo.

1.4.2. Hipótesis Específicas

Hla. Todavía son muchas las entidades que no incluyen en su metodología los componentes necesarios para gestionar sus riesgos operativos.

Hlb. Implementar la metodología en las entidades puede ser dificultoso.

1.5. Justificación

Hoy en día, la importancia de evaluar los riesgos en toda actividad económica no tiene cuestionamiento, más aún, en las empresas

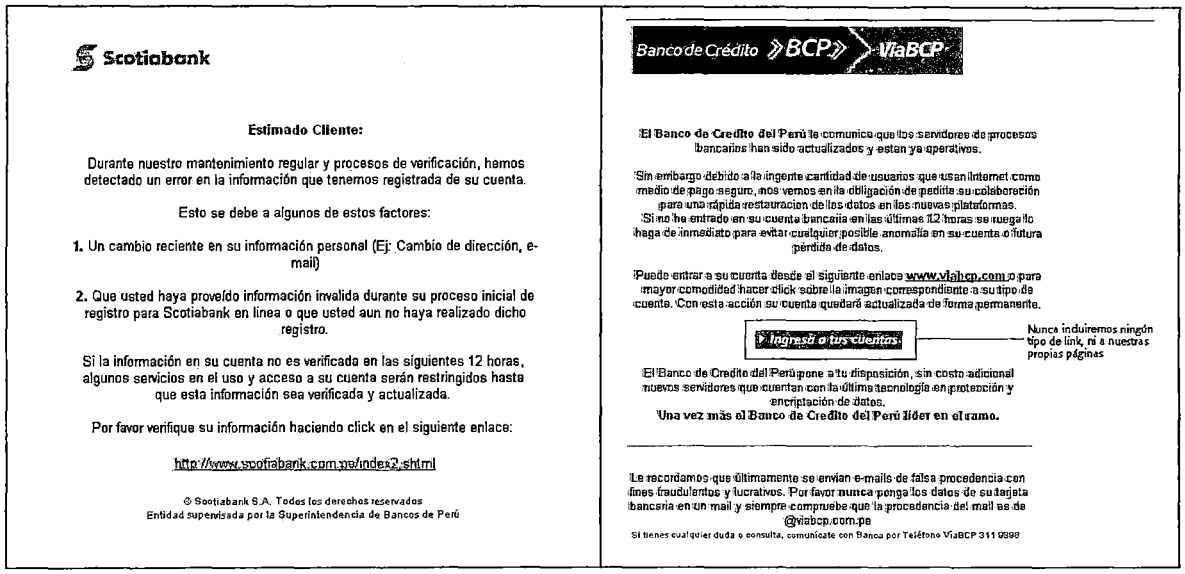
financieras, cuya preocupación por lo general ha estado centrada en los riesgos de crédito (incertidumbre en la recuperación de los préstamos concedidos) y mercado (alteraciones en los precios que afectan el portafolio de la empresa), se ha desplazado hacia otro tipo de problemas bancarios de múltiples causas englobados bajo el término riesgo operativo.

En los noventa, estas incertidumbres pasan de referirse a eventos pequeños, predecibles y frecuentes (errores de procesos, fallos técnicos, entre otros) a protagonizar las quiebras bancarias más significativas y copar las páginas de los periódicos, motivando una creciente preocupación en el sector y suscitando la atención de los reguladores. Estas grandes pérdidas se deben a problemas legales, deficiencias de control interno, débil supervisión de los empleados, fraudes, falsificación de cuentas o contabilidad creativa, factores en muchos casos motivados por el desarrollo tecnológico, la creciente complejidad de las operaciones, la diversificación de productos, los nuevos canales de distribución e inclusive en el *outsourcing*.

Por ejemplo, en el caso peruano haciendo uso de la técnica de "Phishing", que hace referencia a las actividades criminales que imitan los correos electrónicos, sitios web de compañías legítimas (como en el mostrado en a Figura I.2) para invitar a sus usuarios a proporcionar información confidencial como contraseñas, nombres de usuario y números de cuenta y que en definitiva pueden llegar a arruinar al usuario, solo al año pasado la DIVINDAT ha recibido 276 denuncias asociadas a

ese tema lo que significa que han sido perjudicados tanto usuarios como los mismos bancos.

Figura I.2 Mensajes electrónicos falsos para estafar a incautos con la técnica del Phishing



Scotiabank

Estimado Cliente:

Durante nuestro mantenimiento regular y procesos de verificación, hemos detectado un error en la información que tenemos registrada de su cuenta.

Esto se debe a algunos de estos factores:

1. Un cambio reciente en su información personal (Ej: Cambio de dirección, e-mail)

2. Que usted haya proveído información invalida durante su proceso inicial de registro para Scotiabank en linea o que usted aun no haya realizado dicho registro.

Si la información en su cuenta no es verificada en las siguientes 12 horas, algunos servicios en el uso y acceso a su cuenta serán restringidos hasta que esta información sea verificada y actualizada.

Por favor verifique su información haciendo click en el siguiente enlace:

http://www.scotiabank.com.pe/index2.shtml

© Scotiabank S.A. Todos los derechos reservados
Entidad supervisada por la Superintendencia de Bancos de Perú

Banco de Crédito BCP ViaBCP

El Banco de Credito del Perú le comunica que los servidores de procesos bancarios han sido actualizados y estan ya operativos.

Sin embargo debido a la ingente cantidad de usuarios que usan Internet como medio de pago seguro, nos vemos en la obligación de pedirle su colaboración para una rápida restauracion de los datos en los nuevas plataformas.
Si no ha entrado en su cuenta bancaria en las últimas 12 horas se ruega lo haga de inmediato para evitar cualquier posible anomalia en su cuenta o futura pérdida de datos.

Puede entrar a su cuenta desde el siguiente enlace www.viabcp.com o para mayor comodidad hacer click sobre la imagen correspondiente a su tipo de cuenta. Con esta acción su cuenta quedará actualizada de forma permanente.

Ingresa a tus clientes

Nunca induiremos ningún tipo de link, ni a nuestras propias páginas

El Banco de Credito del Perú pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptación de datos.
Una vez más el Banco de Credito del Perú líder en el ramo.

Le recordamos que últimamente se envían e-mails de falsa procedencia con fines fraudulentos y lucrativos. Por favor nunca ponga los datos de su tarjeta bancaria en un mail y siempre compruebe que la procedencia del mail es de @viabcp.com.pe
Si tienes cualquier duda o consulta, comunícate con Banca por Teléfono ViaBCP 311 9999

Fuente y Elaboración: Mensajes de correos electrónicos (tipo SPAM) de Hackers anónimos.

Es así que, a medida que tanto la industria bancaria como académicos y supervisores han sido conscientes de la importancia del riesgo operativo, no han cesado los intentos por definirlo y proponer herramientas para su gestión. En el caso Peruano es importante y necesario adecuarnos por un lado a las directrices internacionales y por otro lado, es necesario establecer el marco regulatorio para crear la debida estabilidad de cada uno de los sistemas supervisados.

1.6. Alcance y limitaciones

1.6.1. Alcance

La presente tesis efectúa el tratamiento del riesgo operativo aplicado a una empresa del sistema financiero peruano, como la información que se obtenga de la entidad puede resultar confidencial, se omite el nombre de la entidad y se ejemplariza como si fuera un banco Tipo.

Por otro lado, se revisa el enfoque regulatorio, tratando de identificar los problemas de las entidades y algunos cambios normativos que harían más efectiva y más fácil la gestión de este tipo de riesgo.

Por último, se efectúa el tratamiento del riesgo operativo desde un enfoque metodológico, que contenga tanto la parte cuantitativa como cualitativa la misma que partirá de la exploración y análisis de metodologías, guías, directrices actuales, haciendo un análisis de sus aspectos positivos y sus deficiencias y extrayendo lo que se adecue y permita generar un documento de valor que sirva a las empresas supervisadas como una guía de gestión de riesgos.

1.6.2. Limitaciones:

Una de las limitantes de la presente investigación está dada por el carácter temporal de la información utilizada como insumo de la investigación, la cual considera las cifras de los años 2008 y 2010. Otra de las limitantes es la zona geográfica, la misma que se circunscribe al Perú. Por otro lado, si bien existe una serie de métodos para calcular los

diferentes tipos de riesgo en esta investigación se delimitará al análisis al riesgo operativo.

1.7. Descripción del Marco Metodológico para realizar el Desarrollo de la Tesis

Para explicar el procedimiento utilizado se describe el marco metodológico utilizado, este se basa principalmente en una investigación de la forma analítica sintética del tipo documental en donde la unidad de estudio es la conjunción de un supervisor y una empresa financiera supervisada por dicho supervisor. La presente tesis se desarrolló recopilando información de fuentes secundarias, adicionalmente se emplearon como instrumentos de recolección de información a) un cuestionario a 25 entidades del sistema financiero y b) una entrevista de preguntas abiertas a un experto mundial,

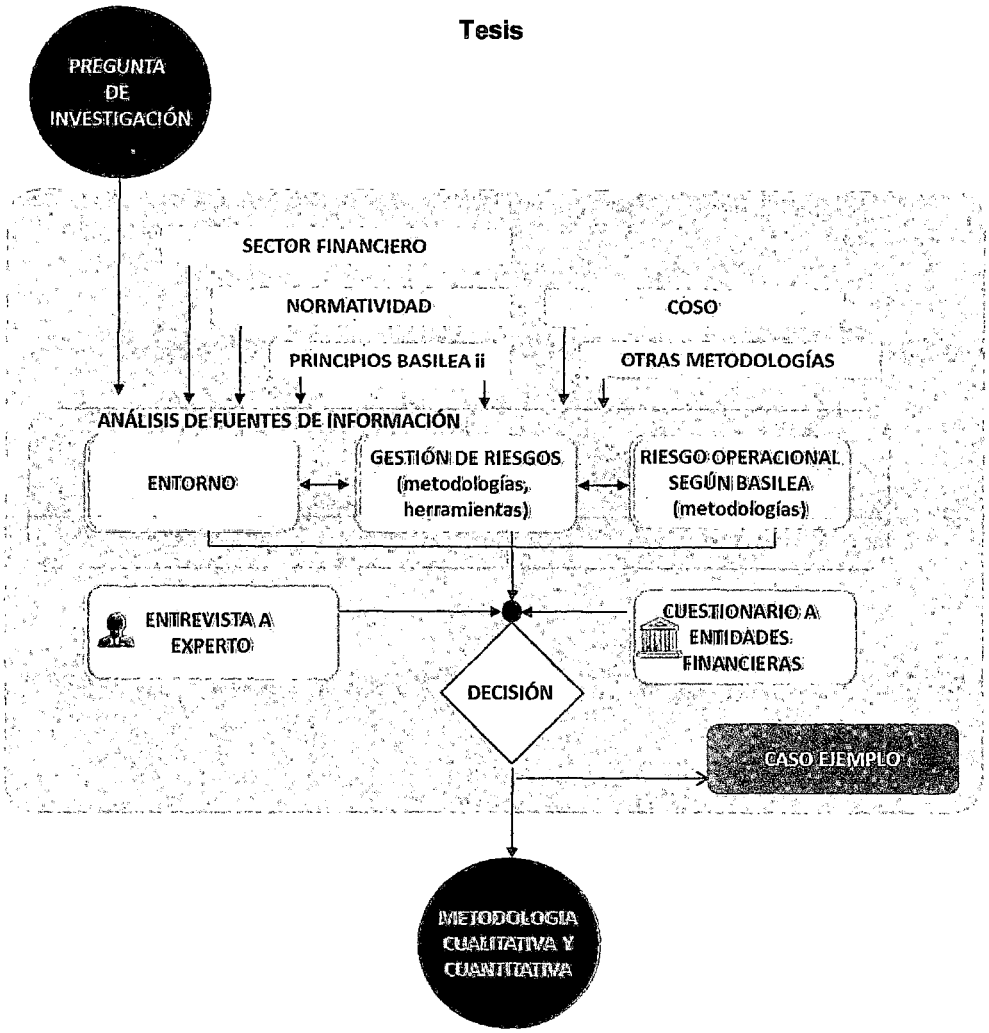
La forma investigación es aplicada ya que busca la obtención de un nuevo conocimiento técnico con aplicación inmediata a un problema determinado, el tipo de investigación que rigen la presente investigación es del tipo documental que por el carácter es cualitativo y cuantitativo y por la finalidad así como nivel de conocimientos que se adquiere en un inicio es correlacional, ya que se pretende combinar los diversos metodologías para la gestión de riesgos y en su etapa final será explicativos ya que buscará enunciar un marco metodológico conjunción de la combinación de diversas metodologías.

De esta manera, en primer lugar se realizó una identificación de las fuentes de información. Ello se logró a través de la identificación de las

fuentes secundarias, las mismas que están relacionadas a un análisis del entorno, a la gestión de riesgos y las metodologías asociadas a la gestión. Está información se identificó, se clasificó (descripción), se analizó (examen crítico); se extrajo de ella los aspectos que tienen relación con el tema de tesis (descomposición y enumeración), y luego se ordenaron y clasificaron los temas que son comunes a los objetivos del proyecto (ordenación y clasificación).

Finalmente, esta información se sintetizó y con la ayuda del experto se pudieron validar los elementos necesarios y comunes que debieran incorporar el producto resultante: una propuesta de metodología (cualitativa y cuantitativa) de gestión de riesgo operativo. La Figura I.3 resume el procedimiento metodológico seguido en el desarrollo de la Tesis.

Figura I.3 Descripción del Marco Metodológico para realizar el Desarrollo de la Tesis



Fuentes: Marco Metodológico de Tesis, Rosa Aurora Causal, Elaboración: Propia

1.8. Fuentes de Información

Esta tesis empleó fuentes de información secundarias documentales como una las fuentes del conocimiento. Dentro de la información se exploraron, entre los principales, los conceptos metodológicos siguientes: Gestión de Riesgos del Nuevo Acuerdo de Basilea II, el Marco integral de

Enterprise Risk Management (ERM) bajo el esquema COSO, los estándares de Riesgo Operativo de ORX (*Operational Risk Exchange*) la más importante plataforma internacional de eventos de riesgo operativo, y la norma ISO/IEC 17799:2005 publicado por la *International Organization for Standardization* y por la Comisión Electrotécnica Internacional, para ello, así como otras metodologías (Métrica), estas fuentes permitieron valida el marco metodológico de gestión de riesgos de una entidad financiera supervisada por la SBS cuya propuesta es objeto de la presente tesis.

Adicionalmente, por ser un tema nuevo, se ha analizado bibliografía reciente en la que destacan libros europeos, regulación local emitida por la SBS así como consulta de noticias en los medios de prensa locales.

1.9. Cuestionario

A través de este instrumento, cuyo diseño se puede apreciar en el Anexo A5, se obtuvo información del grado de madurez de la gestión de riesgos operativos en las entidades financieras locales

1.10. Entrevista

Se entrevistó a Jordi García Ribas, experto mundial en el tema de Riesgo Operativo, él es Ex Director Corporativo de Riesgo Operativo, Ex líder del Consorcio Español de Riesgo Operativo.

1.11. Resumen para el Desarrollo del Marco Metodológico

Tabla I.1 Resumen para el desarrollo del marco metodológico

Objetivos	Técnicas de Recopilación de Información		Método de Investigación	Herramientas, instrumentos	Entregables
	Fuente Secundaria	Entrevista Cuestionario	Analítico-Sintético		
Analizar los procesos de la gestión de riesgos identificación, evaluación, respuesta, seguimiento control de los riesgos utilizada en empresas no solo financieras	**Metodologías y Estándares:** - Buenas prácticas de administración y supervisión del RO propuestas por el Comité de Supervisión Bancaria de Basilea II - International Convergence of Capital Measurement and Capital Standards - ERM COSO - Operational Risk Reporting Standards -ISO 17799/2001 **Principales Libros:** La Gestión de Riesgo Operativo, de la teoría a la práctica (Ana Fernandez L.) - Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez) - Riesgo Operativo, enfoque de pérdidas e la práctica (Alberto Ferreras) **Buenas Prácticas y Normativas (Regulación)** - Buenas Prácticas según Basilea II - Normativa SBS **Cursos** - Curso Taller sobre de Base de Datos de Eventos por Riesgos Operativos` **Otros: Prensa, Investigaciones.**	- Jordi García, Ex-Director de Riesgo Operativo del Grupo BBVA (España) Vice Presidente de la organización ORX - Cuestionario de Preguntas abiertas al Sistema Financiero	- Observación - Descripción - Examen crítico - Descomposición del fenómeno; - Enumeración de sus partes - Ordenación; y - Clasificación	- Revisión de documentos - Recopilación de información - Análisis mediante lista de control - Análisis de supuestos - Diagramación	Diagnóstico de cómo se realiza la gestión de los riesgos operativos
Realizar una propuesta de procesos y herramientas a considerar para realizar la correcta identificación y evaluación cualitativa y cuantitativa de riesgos operativos				- Análisis cualitativo de riesgos - Matriz de Riesgos - Análisis Cuantitativo de Riesgos - Método de Medición según Basilea II	Propuesta metodológica para la gestión de riesgos
Aplicar la propuesta metodológica en un caso ejemplo					Aplicación Metodológica en un caso ejemplo

Fuente y Elaboración: Propia

CAPÍTULO II

MARCO TEÓRICO

En este capítulo se presentan las principales definiciones relacionadas con el tema tesis, el fin es situar al lector en el ámbito y campo de estudio de la presente tesis, para ello, se sitúa al lector dentro del sector financiero, bajo el cual recae este estudios, se explica el Principio del Nuevo Acuerdo de Capitales Basilea II y se describen las principales definiciones de Riesgo haciendo énfasis en el Riesgo Operativo.

2.1. El Sistema Financiero Peruano

2.1.1. Estructura

El sistema financiero está conformado por el conjunto de Instituciones bancarias, financieras y demás empresas e instituciones de derecho público o privado, debidamente autorizadas por la Superintendencia de Banca y Seguro, que operan en la intermediación financiera, como son: El sistema bancario, el sistema no bancario y el mercado de valores. El estado participa en el sistema financiero en las inversiones que posee en COFIDE como banco de desarrollo de segundo piso, actividad habitual

desarrollada por empresas e instituciones autorizada a captar fondos del público y colocarlos en forma de créditos e inversiones.

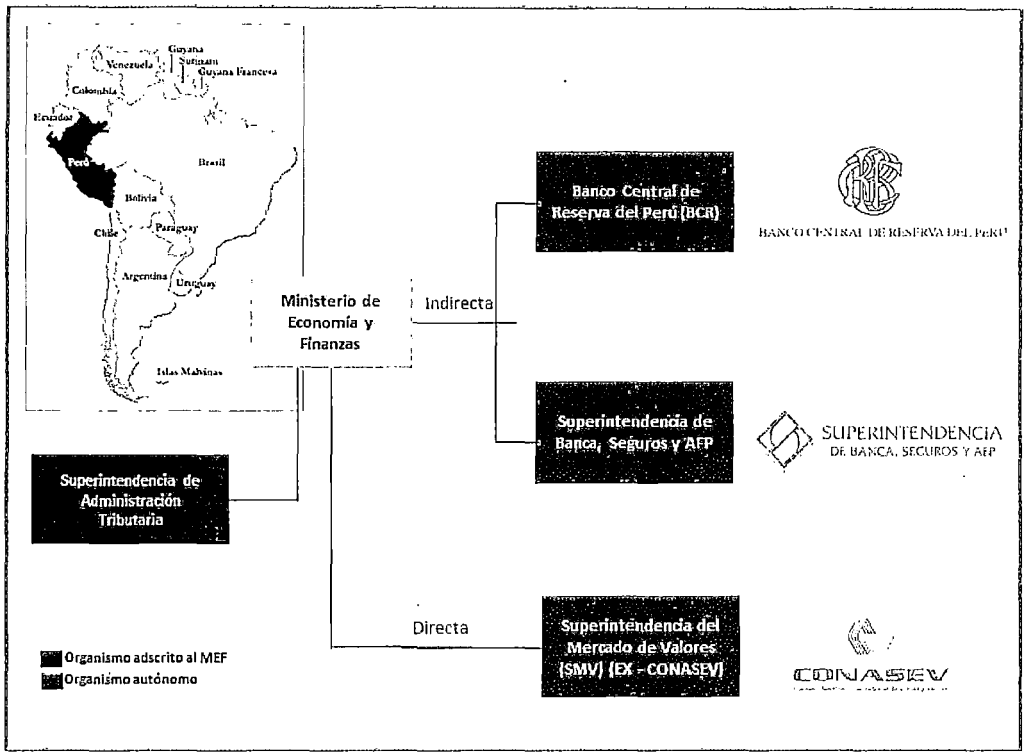
El conjunto de instituciones encargadas de la circulación del flujo monetario y cuya tarea principal es canalizar el dinero de los ahorristas hacia quienes desean hacer inversiones productivas son los denominados Intermediarios Financieros.

El sector financiero es un sector de servicios, intermedio entre la oferta y demanda de servicios financieros y ofrece a las partes del mercado involucradas la posibilidad de tra mitar sus transacciones financieras, de tal forma que un sector financiero bien desarrollado es prioritario para el desarrollo de la economía. En muchos países en vías de desarrollo la prestación de servicios financieros se limita a ciertos factores y a determinados grupos de clientes. La importancia del sector en el ámbito de la economía y en el ámbito político. Las intervenciones del gobierno o del banco central pueden adoptar diferentes formas y conciernen asuntos como: la estabilización o ajuste del tipo de cambio, la influenciarían del clima de las inversiones y la tramitación de las finanzas gubernamentales.

A. Organismos Supervisores

En el Perú, se distinguen diversos organismos rectores o supervisores que solicitan, obtienen, almacenan y analizan información económica-financiera de empresas jurídicas (financieras y no financieras), La Figura II.1 grafica la dependencia de los organismos supervisores.

Figura II.1 Organismos rectores o supervisores en el Perú



Fuente: Gráficos de Google Images, Elaboración: Propia

La definición y el rol que ocupan los organismos de la figura son mostrados a continuación:

- *Superintendencia de Banca, Seguros y AFPs (SBS):* Es el organismo supervisor y regulador de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, previene y detecta el lavado de activos y financiamiento del terrorismo, de allí que la SBS exige a sus supervisados la presentación de información financiera y registro de operaciones las cuales son transmitidas a través de los canales Submódulo de Captura y Validación Externa (SUCAVE) o bien a través del Portal del Supervisado.

- *Comisión Nacional Supervisora de Empresas y Valores (CONASEV):* Es el organismo encargado de promover la eficiencia del mercado de valores y productos, así como del sistema de fondos colectivos, a través de la regulación, supervisión y difusión de información; para los cuales su principal insumo es justamente la información de las empresas emisores peruanas la cual es transmitida a través del sistema electrónico de intercambio de información MVNET que incorpora tecnología de las firmas digitales.
- *Banco Central de Reserva (BCR):* Es el organismo encargado de regular la moneda y el crédito del sistema financiero, administrar las reservas internacionales, emitir billetes y monedas, e informar periódicamente al país sobre las finanzas nacionales, para ello solicita información del sistema de pagos Sistema de Liquidación Bruta en Tiempo Real (LBTR) que registra las transacciones entre los agentes del sistema financiero.
- *Superintendencia Nacional de Administración Tributaria (SUNAT):* Es el organismo que administra, fiscaliza y recauda los tributos internos cuyo sujeto tributario activo es el gobierno central peruano a través del Sistema SUNAT Operaciones en Línea (SOL). Adicionalmente se encarga de la administración y recaudación de los tributos aduaneros que percibe el estado peruano.
- *Ministerio de Economía y Finanzas (MEF):* Es el organismo gubernamental que coordina con todos los organismos anteriormente mencionados y que tiene por finalidad el de optimizar

la actividad económica y financiera del Estado, establecer la actividad macroeconómica así como lograr un crecimiento sostenido de la economía del país.

B. De la Superintendencia de Banca, Seguros y AFP (SBS)

La Superintendencia de Banca, Seguros y AFP es el organismo encargado de la regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SPP.

La SBS es una institución de derecho público cuya autonomía funcional está reconocida por la Constitución Política del Perú. Sus objetivos, funciones y atribuciones están establecidos en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP (Ley 26702).

B.1. Visión

Visión de la SBS
Ser una institución supervisora y reguladora reconocida en el ámbito mundial, que aplica estándares internacionales y las mejores prácticas, apoyada en las competencias de su capital humano.

Para el logro de su Visión la SBS focaliza sus esfuerzo en los siguientes:

- Realizar procesos de Benchmarking y recoger mejores prácticas de entidades similares, con la finalidad de compararse y establecer niveles mínimos de gestión y desarrollo institucional.
- Fomentar la innovación y motivación del personal, a través de mejoras en el clima organizacional, desarrollo de líneas de carrera que incluyan programas de capacitación, rotación de puestos, promociones entre otros, con el propósito de mejorar los mecanismos de motivación, incrementar la productividad y desempeño del personal y gerenciar el conocimiento institucional.
- Asignar con eficiencia los recursos de la Superintendencia, de tal manera de crear una cultura de ahorro y que premie la eficiencia.
- Consolidar y fortalecer la imagen institucional en dos frentes, el nacional e internacional. En el ámbito nacional, mantener la percepción positiva ante las diferentes audiencias (usuarios de los sistemas supervisados, líderes de opinión y gremio empresarial) sobre la gestión de la SBS y en el plano internacional, mejorar los vínculos de intercambio de información y áreas comunes de trabajo.
- Orientación a la Gerencia de la Calidad, es decir innovando y mejorando continuamente los procesos tanto para nuestros clientes internos como externos, de tal forma de generar un cambio en las acciones rutinarias y de comportamiento del personal en forma progresiva y sostenida.

B.2. Misión

Misión de la SBS
Velar por los intereses del público, cautelando la estabilidad, la solvencia y la transparencia de los sistemas supervisados, así como contribuir con el sistema de prevención y detección del lavado de activos y del financiamiento del terrorismo.

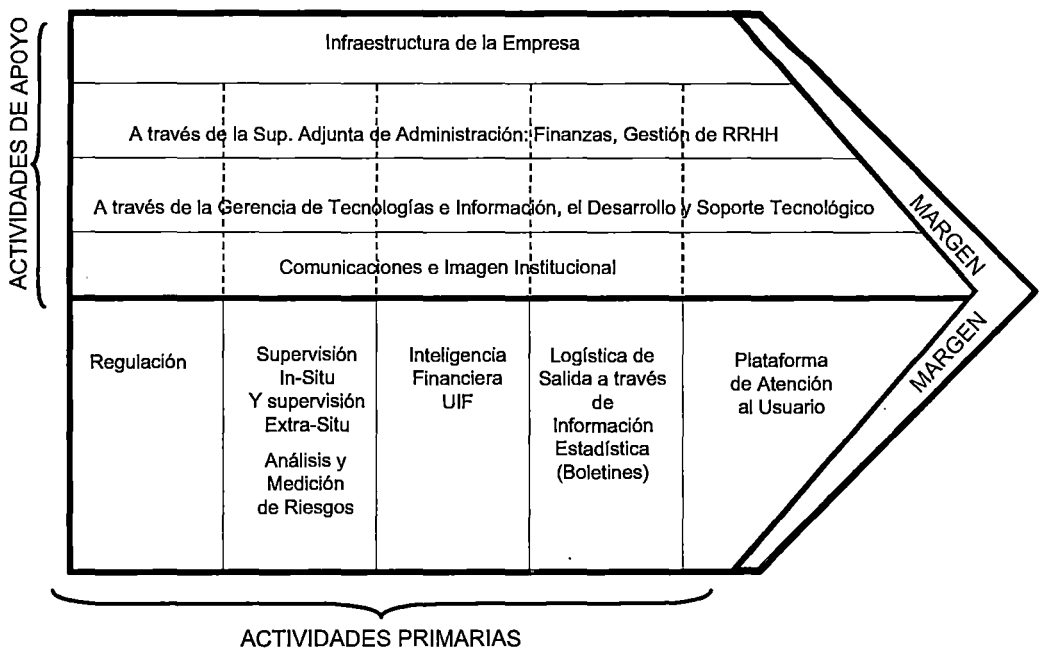
El desarrollo y consolidación de su misión significa:

- Mejorar y fortalecer los aspectos de supervisión, adecuándolos a estándares internacionales de supervisión y que promuevan recomendaciones en la generación y entrega de valor de las entidades supervisadas a los usuarios.
- Desarrollar un Sistema de Información Gerencial que incluya alertas tempranas para la toma de decisiones.
- Promover un marco regulatorio ágil y moderno, acorde con la realidad nacional, fortaleciendo el enfoque de proteger los intereses de público y que cautele la estabilidad de los sistemas supervisados.
- Y por último fomentar la transparencia y calidad de la información, es decir mejorando e innovando los servicios del Web Site, la Plataforma de Atención al Usuario de la SBS y realizando mayores acciones de difusión sobre las entidades supervisadas (boletines, reportes y publicaciones).

B.3. La cadena de Valor de la SBS

Las Figura II.2 ilustra la Cadena de Valor[2] de la SBS, luego del cual se explica tanto las actividades primarias como las actividades de apoyo.

Figura II.2 Cadena de Valor de la SBS



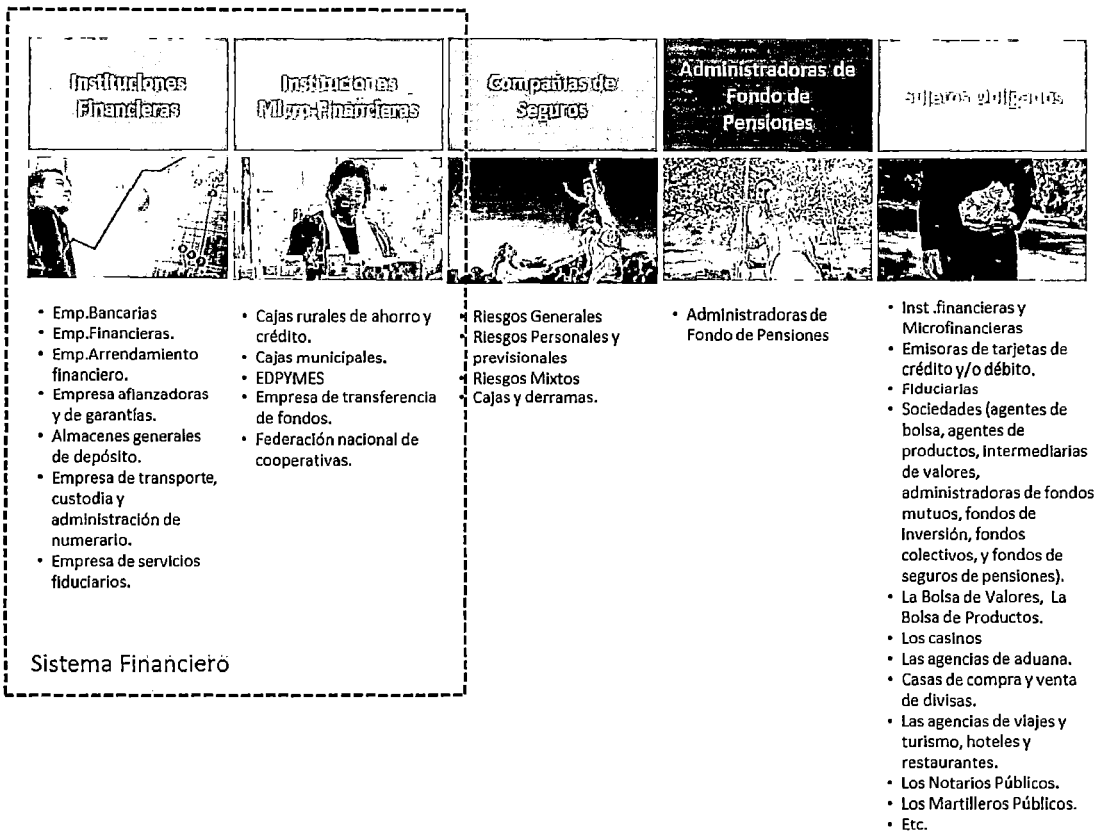
Fuente: SBS, Elaboración: Propia

B.3.1. Actividades Primarias de la Cadena de Valor

Las actividades de la SBS se centran en supervisar y regular las empresas bajo su supervisión. El gráfico II.3 nos detalla los tipos de empresas supervisadas por la SBS.

[2] La Cadena de Valor es un es un modelo teórico que permite describir el desarrollo de las actividades de una organización empresarial

Figura II.3 Empresas supervisadas por la SBS



Fuente y Elaboración: Propia

Estas actividades primarias, sugieren la creación de un sistema de incentivos que propicie que las decisiones privadas de las empresas sean consistentes con el objetivo de lograr que los sistemas bajo supervisión adquieran la solidez e integridad necesarias para mantener su solvencia y estabilidad en el largo plazo. Entre estas dos actividades primarias se destacan dos actividades medulares:

- ***Regulación*** La SBS confía en el mercado como mecanismo de organización y asignación de recursos, siempre que los incentivos dados por la regulación orienten a las empresas a internalizar los costos sociales en sus decisiones. Para que este enfoque se pueda

desarrollar en la práctica, la SBS se apoya sobre la base de cuatro principios básicos relacionados a (i) la calidad de los participantes del mercado, (ii) la calidad de la información y análisis que respalda las decisiones de las empresas supervisadas (iii) la información que revelan las empresas supervisadas para que otros agentes económicos tomen decisiones y (iv) la claridad de las reglas de juego es decir que las normas dictadas por la SBS sean de fácil comprensión, exigibles y que puedan ser supervisadas

- ***Supervisión*** Los principios de regulación arriba presentados demandan un estilo de supervisión dinámico y flexible, que se adecue a las características de cada empresa. En esta dirección la SBS busca poner en práctica una supervisión especializada, integral y discrecional. Una supervisión especializada significa que la SBS pretende implementar un enfoque de supervisión por tipo de riesgo. Ello implica contar con personal especializado en la evaluación de los diversos tipos de riesgo, tales como riesgo crediticio, de mercado, de liquidez, operativo y legal. Asimismo, la SBS se orienta hacia una supervisión integral que genere una apreciación sobre la administración de los riesgos por parte de las empresas supervisadas. Finalmente, una supervisión discrecional se refiere a que el contenido, alcance y frecuencia de la supervisión debe estar en función del diagnóstico de los riesgos que enfrenta cada empresa supervisada.

La estrategia de supervisión de la SBS se desarrolla en dos frentes. El primero consiste en la supervisión que ejerce directamente sobre las empresas y el segundo se basa en participación de los colaboradores externos, tales como los auditores, las empresas clasificadoras de riesgo, supervisores locales y de otros países.

Con relación a la supervisión directa, ésta se desarrolla bajo dos modalidades: la supervisión ***extra-situ,*** y la supervisión ***in-situ.*** La primera consiste en analizar en forma permanente la información brindada por las empresas supervisadas e identificar los temas que sean de preocupación y que merezcan un examen más profundo. La segunda se ocupa de verificar en la propia empresa supervisada los aspectos identificados previamente en la labor de análisis extra-situ. Respecto de la colaboración de agentes externos, desde su propia perspectiva estas entidades ejercen un cierto tipo de monitoreo de las empresas que se encuentran dentro del ámbito de la Superintendencia.

Otras actividades primarias son las siguientes:

- ***Unidad de Inteligencia Financiera*** (UIF) La Unidad de Inteligencia Financiera del Perú es la encargada de recibir, analizar y transmitir información para la detección del Lavado de Activos y/o del Financiamiento del Terrorismo; del mismo modo a través de sus supervisados detectar y reportar operaciones sospechosas de Lavado de Activos y/o Financiamiento del Terrorismo. Fue creada mediante Ley Nº 27693 de abril del año 2002, modificada por Leyes

Nº 28009 y Nº 28306 y reglamentada mediante el Decreto Supremo Nº 163-2002-EF modificado por Decreto Supremo Nº 018-2006-JUS. Ha sido incorporada como Unidad Especializada a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones mediante Ley Nº 29038 de junio del año 2007, y cuenta con autonomía funcional y técnica.

- ***Logística de salida a través de Información Estadística (boletines),*** A través de los Boletines es que se informa al mercado acerca de la salud de los supervisados por la SBS, este mercado incluye a los actores de la cadena de información financiera, desde los productores de información (instituciones públicas y compañías privadas) hasta quienes los reciben, analizan o transforman (auditores, gobiernos, otros reguladores públicos, analistas, inversores, mercados de capitales, entidades financieras, desarrolladores de tecnología entre otros).
- ***Plataforma de Atención al Usuario,*** La Plataforma de Atención al Usuario es el área de atención al público de la SBS, que orienta en forma gratuita las consultas de los usuarios de las empresas supervisadas pertenecientes al sistema financiero, de seguros y privado de pensiones. Asimismo, atiende las denuncias en contra de las empresas financieras, de seguros y del sistema privado de pensiones; así como los reclamos en el caso de las AFP.

B.3.2. Actividades de Apoyo en la Cadena de Valor

Como en la mayoría de las empresas públicas las actividades de apoyo en la cadena de valor son las siguientes:

- Infraestructura de la empresa, en las que se incluye a la gerencia de planeamiento que lleva a cabo las coordinaciones del plan estratégico institucional para su correcta formulación, ejecución y control, del mismo modo mantiene el inventario de procesos.
- La Superintendencia de Administración General, en el que se incluyen las actividades de las finanzas, la contabilidad, así como las actividades de adquisiciones y recursos humanos en el que prima al personal calificado.
- Tecnología. Incluye el desarrollo de tecnología para apoyar a las actividades de la cadena de valor. Por ejemplo: automatización de procesos, desarrollo de canales virtuales con sus supervisados, herramientas de *reporting*, análisis, inteligencia de negocios entre otros.
- Comunicaciones e Imagen Institucional. Apoya las actividades de difusión de información en todos sus aspectos, así mismo incorpora los lineamientos y estrategias de las actividades de inclusión financiera que las áreas de línea pueden desplegar como parte de sus funciones.

C. Sistemas Financieros Supervisados

Según señala la Superintendencia de Banca Seguros y AFP (Ver Tabla II.1), a diciembre de 2010, el ámbito de supervisión de la SBS comprendía a 153 entidades con un saldo en activos de 335,243 millones de nuevos soles (equivalente a 119,346 millones de dólares). Del total de activos, el 52,6% correspondía a empresas bancarias, el 26,2% a fondos de pensiones, el 5,2% a empresas de seguros y el 4,3% a instituciones microfinancieras no bancarias. Cabe señalar que el 8,9% de los activos que corresponde a entidades estatales está mayormente explicado por la participación del Banco de la Nación, encargado de administrar los fondos públicos.

Tabla II.1 Entidades Supervisadas por la SBS

	NÚMERO DE EMPRESAS	SALDO (S/. MILLONES)	PARTICIPACIÓN (%)
Empresas bancarias	**15**	**179 638**	**53,6**
Empresas financieras	**10**	**6 037**	**1,8**
Instituciones microfinancieras no bancarias	**33**	**14 336**	**4,3**
Cajas municipales (CM)	13	10 902	3,3
Cajas rurales de ahorro y crédito (CRAC)	10	2 282	0,7
Entidades de desarrollo de la pequeña y microempresa (Edpyme)	10	1 153	0,3
Entidades estatales	**4**	**29 768**	**8,9**
Banco de la Nación	1	21 165	6,3
Corporación Financiera de Desarrollo (COFIDE)	1	5 160	1,5
Banco Agropecuario (Agrobanco)	1	335	0,1
Fondo MiVivienda	1	3 108	0,9
Empresas de arrendamiento financiero	**2**	**132**	**0,0**
Empresas de seguros	**14**	**17 358**	**5,2**
Fondos de pensiones	**4**	**87 974**	**26,2**
Otras1/	**71**		
TOTAL	153	335 243	100,0

1/ Incluye 1 empresa de factoring, 2 empresas administradoras hipotecarias, 7 empresas de transferencias de fondos, 2 cajas y 2 derramas, 4 almacenes generales de depósitos, 2 empresas de servicios fiduciarios, 2 empresas de transporte, custodia y administración de numerario, 1 empresa afianzadora y de garantías, 45 Asociaciones de Fondos Regionales o Provinciales contra Accidentes de Tránsito, 1 Cooperativa de Ahorro y Crédito, la Federación Nacional de Cooperativas de Ahorro y Crédito del Perú y el Banco Central de Reserva del Perú.

Fuente: Memoria 2010 – SBS, Elaboración: SBS

En los últimos años, el sistema financiero a mostrado una significativa mejora en términos de acceso debido ya sea al incremento de la red de distribución de servicios (oficinas, cajeros automáticos y cajeros

corresponsales. Tal como se aprecia en la Tabla II.2, al 2010, el número de oficinas y cajeros del sistema se triplicaron las cifras del 2006, es así que el que el total de puntos de atención hoy en día representan aproximadamente el 61% por cada 100,000 habitantes

Tabla II.2 Número de Oficinas, Cajeros Automáticos y Corresponsales por Ubicación Geográfica

UBICACIÓN GEOGRÁFICA	OFICINAS		CAJEROS AUTOMÁTICOS		CAJEROS CORRESPONSALES*		TOTAL PUNTOS DE ATENCIÓN		VAR.
	2006	2010	2006	2010	2006	2010	2006	2010	2010/2006
Tumbes y Piura	105	209	93	210	93	405	291	824	533
Lambayeque, La Libertad y Áncash	210	415	196	509	168	840	574	1 764	1 190
Cajamarca, Amazonas y San Martín	106	193	68	153	56	339	230	685	455
Loreto y Ucayali	40	72	46	114	27	131	113	317	204
Huánuco, Pasco y Junín	105	198	78	167	58	525	241	890	649
Lima y Callao	798	1 406	1 797	3 198	1 012	5 012	3 607	9 616	6 009
Ica y Arequipa	141	266	157	381	165	1 308	463	1 955	1 492
Huancavelica, Ayacucho y Apurímac	64	108	29	64	18	128	111	300	189
Moquegua y Tacna	44	85	38	78	32	149	114	312	198
Cusco, Puno y Madre de Dios	96	219	117	248	60	367	273	834	561
Total Sistema Financiero	1709	3 171	2 619	5 122	1 689	9 204	6 017	17 497	11 480

*Corresponde al número de establecimientos que cuentan con puntos de caja.

Fuente: Memoria 2010 – SBS, Elaboración: SBS

Por otro lado, al cierre del 2010í a este mismo periodo el número de deudores bordea los 4.6 millones y el número de depositantes bordea los 14,9 millones.

2.2. El Nuevo Acuerdo de Basilea

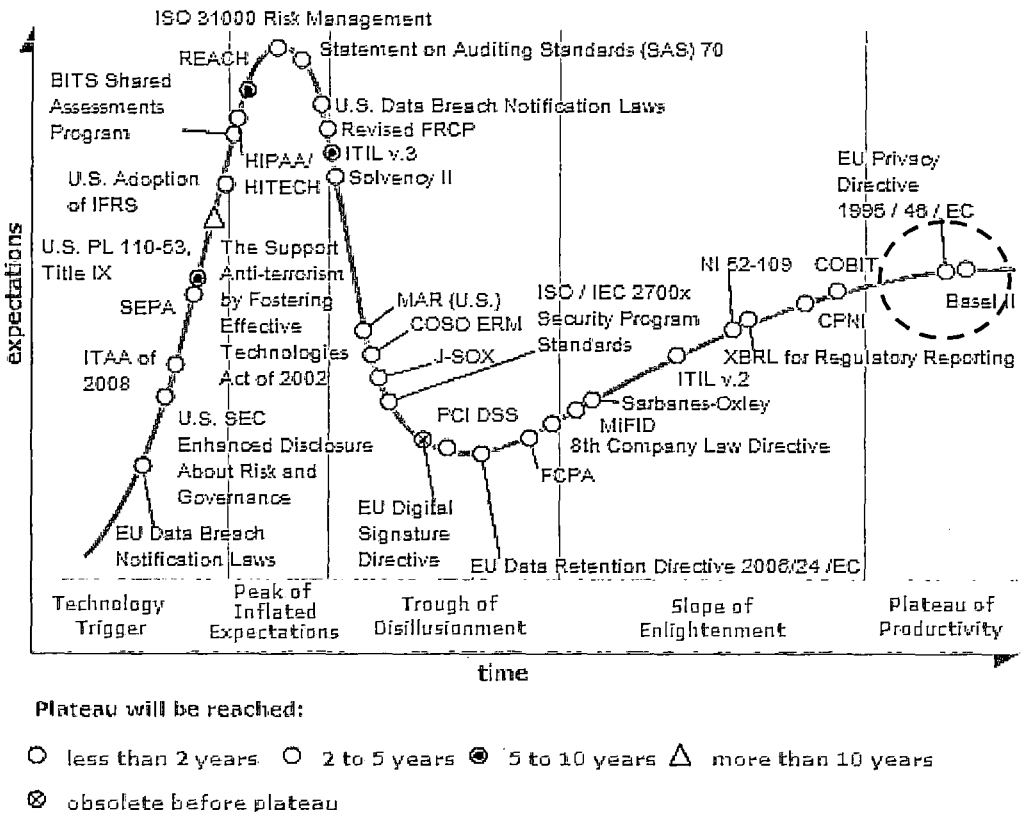
2.2.1. Definición

Como se mencionó anteriormente el Nuevo Acuerdo de Capitales Basilea II consisten en un conjunto de recomendaciones sobre la legislación y regulación bancaria, los cuales son emitidos por el Comité de Supervisión Bancaria de Basilea quien provee de estándares internacional

que sirva de referencia a los reguladores bancarios, en el caso peruano la SBS cumple el rol de regulador.

Según Gartner, tal como se muestra la siguiente Figura II.4 del *Hype Cycle*[3] Basilea II está localizado en el "plateau de productividad", es decir llego a su madurez por lo que es considerando ya un estándar.

Figura II.4 Hype Cycle de Estándares Financieros



Fuente y Elaboración: Gartner (Hype Cycle for Regulations and Related Standards, 2010)

[3] El Hype cicle es un gráfico que mide a las diversas tecnologías según un ciclo de vida que tiene como etapas el "disparador tecnológico" (cuando aparece el concepto en el mercado), "el pico de expectativa inflada" (cuando se habla mucho del concepto, pero está poco aplicado), "el valle de la desilusión" (cuando la herramienta está por debajo de lo que se esperaba de ella), "la pendiente de tolerancia" (el camino hacia la madurez) y el "plateau de productividad" (cuando alcanza la madurez).

2.3. Riesgo

En todo proceso de toma de decisiones, siempre se consideran los riesgos asociados a las decisiones, pero nunca tomamos se cuantifican. Pero, ¿Qué es el Riesgo?, de hecho existen muchas definiciones las cuales podemos detallar:

- Greenfacts[4] lo define como "Daño potencial que puede surgir por un proceso presente o suceso futuro",

- Kaplan y Garrick han discutido una infinidad de posibles definiciones de "riesgo". Así, se dice que: (i) Riesgo es una combinación de incertidumbre y daño. (ii) Riesgo es una relación de peligros y medidas de seguridad. (iii)

- Para Philippe Jorion el riesgo puede ser definido como "la volatilidad que los flujos financieros no esperados, generalmente derivada del valor de los activos y pasivos".

En ese sentido, según la bibliografía revisada se considera que el análisis de riesgo es inevitable en los procesos de toma de decisiones en general y en las decisiones de inversión en particular. El beneficio de tomar una decisión o de realizar una acción cualquiera, necesariamente debe asociarse con el riesgo inherente a esa decisión o acción. En finanzas, el concepto de riesgo está relacionado con el grado de incertidumbre de rendimientos esperados en el futuro. La medición efectiva y cuantitativa del riesgo está dada por la probabilidad asociada a

[4] www.greenfacts.org

una pérdida potencial. Por ello, la gestión de riesgos consiste en medir esas probabilidades en contextos de incertidumbre.

2.3.1. La Gestión de Riesgos

La gestión de riesgos consiste, principalmente en la definición de políticas de administración y control de riesgos con relación a la medición del riesgo, el desarrollo de modelos y el establecimiento de límites de tolerancia y la generación de reportes a la alta dirección que permitan monitorear y controlar las exposiciones.

Dicho proceso comprende una serie de etapas. El primer paso, es la identificación de los riesgos inherentes a la actividad de intermediación financiera; para ello, es necesario considerar las diferentes naturalezas de los riesgos que se presentan en las operaciones de la entidad y entender que en muchos casos puede ocurrir que diferentes tipos de riesgos se encuentren interrelacionados. Así por ejemplo, los riesgos de mercado están asociados a la volatilidad, la estructura de correlaciones y la liquidez, pero éstos no pueden estar separados de otros, tales como los riesgos operativos (riesgos de modelo, de fallas humanas o de sistemas) o riesgos de crédito (incumplimiento de contrapartes, riesgos en el degradamiento de la calificación crediticia o problemas con las garantías). En este contexto, una operación de crédito en moneda extranjera, implica un riesgo de crédito pero también uno de mercado y riesgos operativos al mismo tiempo.

Una siguiente etapa importante en el proceso de gestión de riesgos es el que se refiere a la cuantificación, para lo cual existe una serie de

metodologías y modelos de medición. Para el caso del riesgo de crédito, por ejemplo, existen metodologías que permiten la cuantificación a partir del cálculo de la probabilidad de incumplimiento y de las pérdidas esperadas e inesperadas. En el caso de los riesgos de mercado, existen metodologías de cuantificación basadas en el VaR, duración, convexidad, peor escenario, análisis de sensibilidad, beta, delta, etc. Las entidades supervisadas por la SBS son tomadoras de riesgo por naturaleza. En ese contexto, aquellas que tienen una cultura de riesgos crean una ventaja competitiva frente a las demás; asumen riesgos más conscientemente, se anticipan a los cambios adversos, se protegen o cubren sus posiciones de eventos inesperados y logran experiencia en el manejo de riesgos.

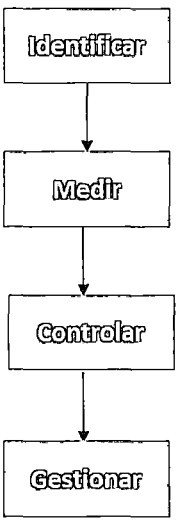
En el caso de, las instituciones que no tienen cultura de riesgos, posiblemente ganen más dinero en el corto plazo pero en el largo plazo convertirán sus riesgos en pérdidas importantes que pueden significar inclusive, la quiebra.

Los avances logrados hasta el momento en materia de gestión de riesgos, están posibilitado un mayor grado de sofisticación de los sistemas de medición de aspectos cuantitativos en base a modelos matemáticos y técnicas estadísticas apoyadas en tecnologías de la información- pero también de estándares cuantitativos. Las entidades vienen ajustando sus estructuras organizacionales de forma que se implementen las unidades o dependencias, cuyas funciones y responsabilidades posibiliten una óptima gestión de los riesgos. Sin duda

que éste es un proceso altamente dinámico y las entidades seguirá evolucionando en este sentido.

Por otro lado, según el Grupo Financiero Acobo, el objetivo de la Gestión de Riesgos es "Crear valor para la empresa y para los clientes por medio de un manejo eficiente de los recursos disponibles, tomando en cuenta la rentabilidad que se obtiene asociada a un determinado nivel de riesgo, de manera que permita el crecimiento" de allí que este grupo establece las etapas descritas de la Figura II.5 para gestionar el riesgo:

Figura II.5 Etapas de Gestión de Riesgo



Conocer detalladamente a cada uno de los riesgos que enfrente la empresa en su operativa diaria.

Evaluar el posible impacto monetario que la ocurrencia de un evento negativo pueda tener sobre la empresa y si esto afecta o no de manera significativa la situación financiera del negocio.

Conlleva el uso de herramientas y la búsqueda de acciones tales que permitan mitigar el impacto de un evento de riesgo cuando este ocurra.

Adecuada combinacion de actividades de negocio tales que, se puedan determinar las proporciones optimas de recursos destinados a cada una de ellas tales que minimicen el riesgo en la empresa

Fuente y Elaboración: Acobo

2.3.2. Tipos de Riesgos

Según Jorion, podemos señalar que las empresas están expuestas a tres tipos de riesgo: de negocios u operativos, estratégicos o sistémicos y financieros. A continuación se resume cada uno de los tipos de riesgo.

Los riesgos de negocios son aquellos que la empresa está dispuesta a asumir para crear ventajas competitivas y agregar valor para los

accionistas. Los riesgos de negocios, o riesgos operativos, tienen que ver con el mercado del bien o servicio en el cual opera la empresa y comprenden innovaciones tecnológicas, diseño del bien o servicio y mercadotecnia. En cualquier actividad de negocios, la exposición racional a este tipo de riesgo es considerada como una .habilidad interna o ventaja competitiva. de la propia empresa.

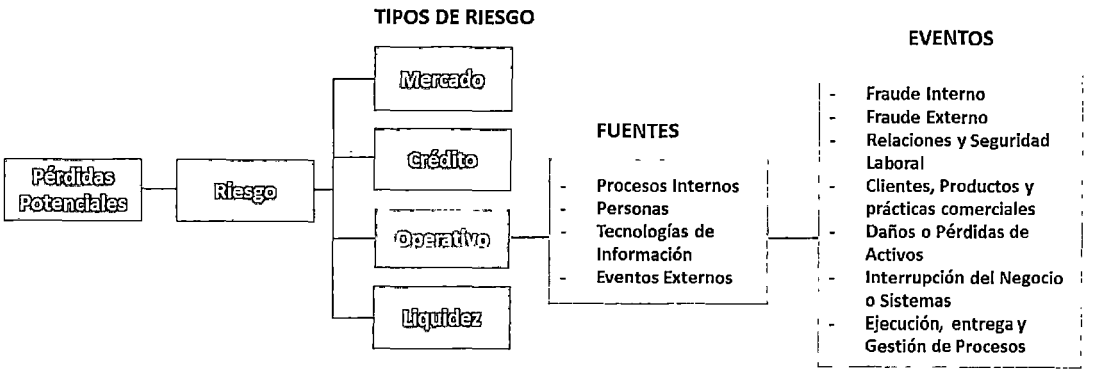
Los riesgos estratégicos o sistémicos son resultantes de cambios fundamentales en la economía o en el entorno político. Estos riesgos difícilmente se pueden cubrir, a no ser por la diversificación a través de distintas líneas de negocios y de distintos países.

Los riesgos financieros están relacionados con las posibles pérdidas en los mercados financieros. Los movimientos en las variables financieras, tales como las tasas de interés y los tipos de cambio, constituyen una fuente importante de riesgos para la mayoría de las empresas. La exposición a riesgos financieros puede ser optimizada de tal manera que las empresas puedan concentrarse en lo que es su especialidad: administrar su exposición a los riesgos del negocio.

2.3.3. Acerca del Riesgo Financiero

Según Wilson Paul Falen Lara, en su tesis "*Gestión de Riesgos en las Casas de Bolsa*" (ver Figura II.6) los riesgos financieros consideran principalmente los riesgos de mercado, riesgo de crédito, riesgo de liquidez, riesgo operativo (incluye al riesgo legal)

Figura II.6 Tipos de Riesgo



Fuentes: "Gestión de Riesgos en las Casas de Bolsa" de Wilson Paul Falen Lara y Gestión de Riesgos

Operativo de ASBA. Elaboración Propia.

A. Riesgo de Mercado

El riesgo de mercado se debe a variaciones (volatilidad) de los precios/tipos negociados en los mercados financieros. La evaluación del riesgo de mercado se basa en la inestabilidad de tasas de interés, los cambios bursátiles y los cambios de divisa. Dicha estabilidad se mide mediante las volatilidades de mercado. La desviación de valor de la posición se calcula a partir de la variabilidad del instrumento frente a los cambios de precio, en términos de volatilidad.

B. Riesgo de Crédito

El riesgo de crédito se presenta cuando las contrapartes están poco dispuestas o imposibilitadas para cumplir sus obligaciones contractuales. Su efecto se mide por el costo de la reposición del flujo de efectivo si la otra parte incumple. En términos generales, el riesgo de crédito también puede conducir a pérdidas cuando los deudores son clasificados con un

mayor nivel de riesgo por las agencias crediticias, generando con ello una caída en el valor de mercado de sus obligaciones. El riesgo de crédito es realmente crítico, ya que el incumplimiento ó *"default"* simultáneo de un pequeño número de clientes corporativos puede ocasionar fuertes pérdidas, e incluso la total insolvencia del banco o fondo de inversión. En la gestión de este riesgo juega un papel importante la normativa interna sobre la diversificación.

C. Riesgo Operativo

El riesgo de operativo se refiere a las pérdidas potenciales resultantes de sistemas inadecuados, fallas administrativas, controles defectuosos, fraude, o error humano. Esto incluye riesgo de ejecución, es decir, cualquier problema en las operaciones de compensación y liquidación (back office), que está a cargo del registro de las operaciones y la reconciliación de transacciones individuales con la posición agregada de las empresas.

Este tipo de riesgo también incluye los fraudes o situaciones donde se falsifican intencionalmente información, y el riesgo tecnológico, que se refiere a la necesidad de proteger los sistemas del acceso no autorizado y de la interferencia.

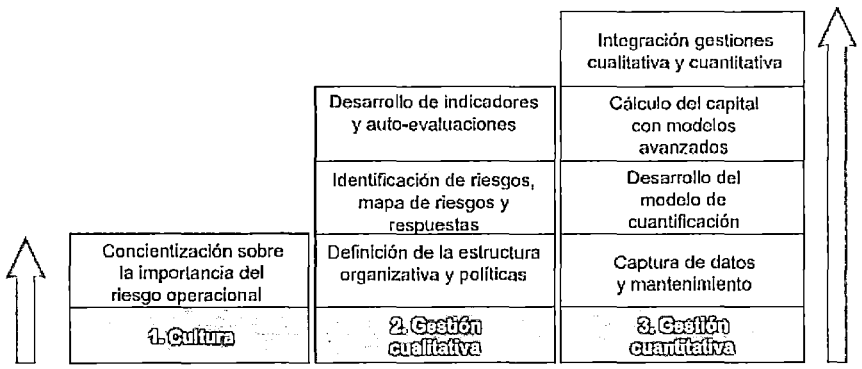
D. Riesgo Legal

Se presenta cuando una contraparte no tiene la autoridad legal o regulatoria para realizar la transacción. El riesgo legal incluye el riesgo regulatorio, el cual hace referencia a actividades que podrían quebrantar

regulaciones gubernamentales, tales como la manipulación del mercado, la operación con información privilegiada y restricciones en convenciones.

Según Norberto Rodríguez y Claudio Corbetta, ambos de PricewaterhouseCoopers el marco regulatorio para la gestión de riesgo operativo puede ser enmarcada dentro del esquema que se presenta en la Figura II.7:

Figura II.7 Marco para la gestión de riesgo operativo según PWC



Fuentes y Elaboración: PriceWaterhouseCoopers (Revista Electrónica CEO, Responsabilidad Social Corporativa, Año 3 Edición Especial 2007)

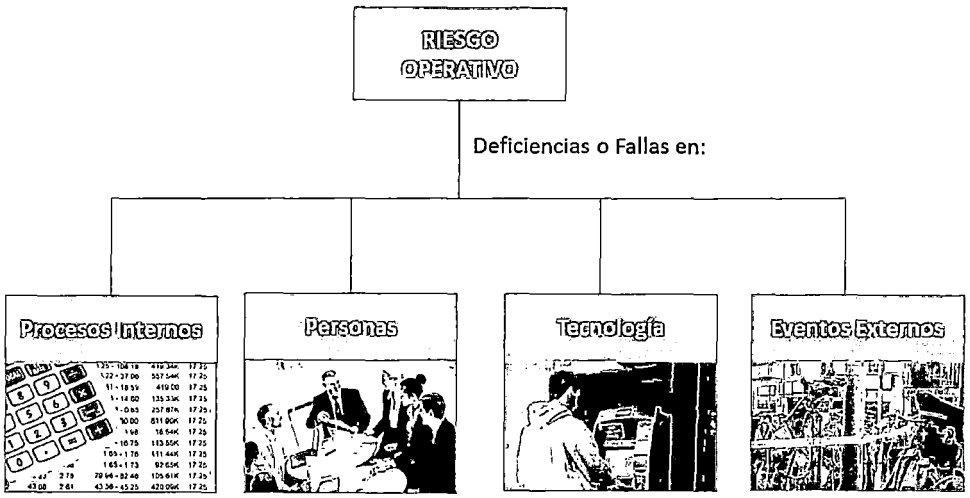
E. Riesgo de Liquidez

El riesgo de liquidez se refiere a la incapacidad de conseguir obligaciones de flujos de efectivo necesarios, lo cual puede forzar a una liquidación anticipada, transformando en consecuencia las pérdidas en papel en pérdidas realizadas.

2.3.4. Fuentes de Riesgo Operativo

La Figuera II.8 esquematiza las fuentes de riesgo operativo, las mismas que son detalladas a continuación:

Figura II.8 Fuentes de Riesgo Operativo



Fuentes y Elaboración: SBS.

A. Procesos Internos

Esta dada por la posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

Se consideran los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y presupuestos planeados.

B. Personas

Esta dada por la posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores. Se puede también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación. Un caso es el de Cronwell Gálvez, ex-empleado del Banco Continental quien robaba a dicho banco.

C. Tecnología de Información

Esta dado por la posibilidad de pérdidas financieras derivadas del uso de inadecuados de las tecnologías de información y comunicaciones, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Las instituciones pueden considerar de incluir en ésta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas TI, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear la TI con los objetivos de negocio, con entre otros aspectos. Otros riesgos incluyen la

falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

Todos los bancos que realizan transacciones electrónicas via Internet y que no ofrecen a los usuarios teclados virtuales son más vulnerables que aquellos que si lo ofrecen.

D. Eventos Externos

Esta dada por la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

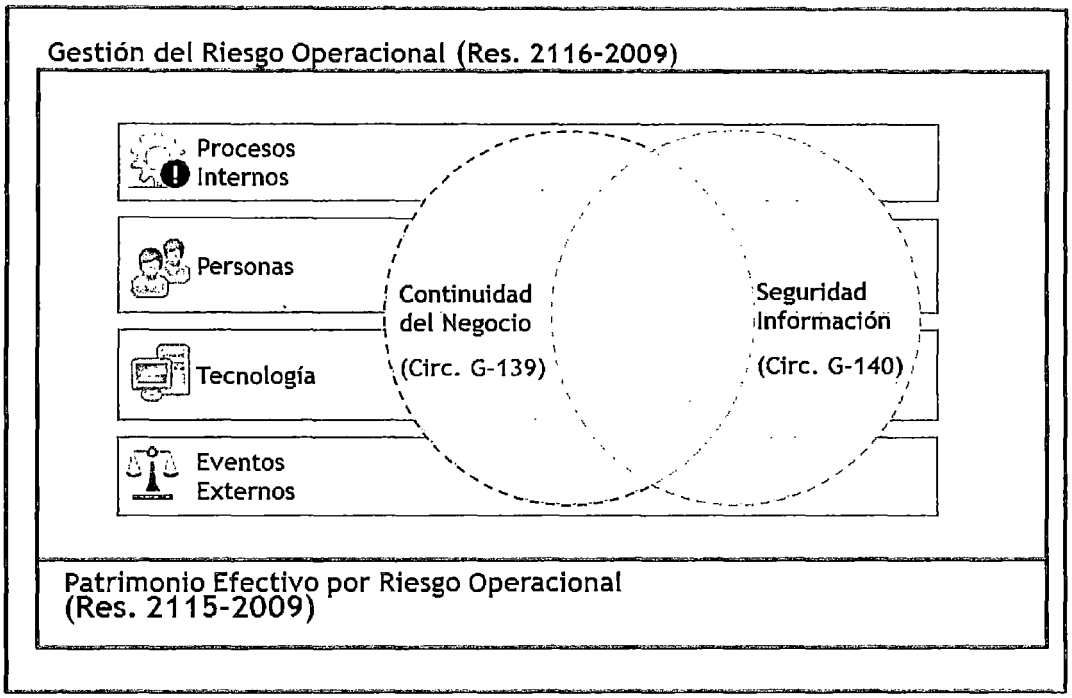
El terremoto ocurrido en Pisco es un ejemplo de cómo un desastre puede afectar operativamente a las entidades financieras..

2.3.5. De su relación con la Gestión de la Seguridad de Información

Una adecuada Gestión de la Seguridad de la Información permitiría a las entidades financieras proteger los activos de información más importantes, es así que desde ese punto de vista de la gestión de riesgos financieros y tal como se aprecia en la Figura II.9, la Gestión de la

Seguridad de la Información es uno de los componentes de la Gestión de Riesgos Operativo.

Figura II.9 Marco para la gestión de riesgo operativo según SBS



Fuente y Elaboración: Jorge Domínguez, Supervisor Principal de Riesgo Operativo de la SBS, 2009

Es así que la SBS Mediante la Circular N° G-140-2009, la SBS establece los criterios mínimos para una adecuada Gestión de la Seguridad de la Información (GSI), la misma está basada en los estándares internacionales como el ISO 17799 e ISO 27001. Adicionalmente al marco de Gestión de la Seguridad de la Información la SBS la SBS considera criterios para la continuidad del negocio.

Mediante la Circular N° G-140-2009, la SBS se exige que todas las Instituciones Financieras del Perú implanten un sistema orientado a controlar el riesgo operativo de las instituciones, a través de un Sistema

de Gestión de Seguridad de Información (SGSI). De esta manera las empresas deben realizar los siguientes puntos:

Las empresas deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

A. Del Sistema de Seguridad de Gestión de Seguridad de Información

El Sistema de Gestión de la seguridad de la Información (SGSI) es el conjunto de controles de administración de la información, que busca minimizar los riesgos y asegurar la confidencialidad, integridad y disponibilidad de los activos de información. Adicionalmente, el SGSI debe incorporar un sistema de comunicación de incidentes de seguridad.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno, para lo cual cuenta con una política de seguridad de la información aprobada por el más alto nivel de dirección de la organización.

Según la Circular N° G-140-2009 las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

- Definición de una política de seguridad de información aprobada por el Directorio.
- Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operativos de la empresa.

- Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Por otro lado, las empresas deben contar con una estructura organizacional que les permita implementar y mantener el SGSI y que puedan desarrollar las funciones siguientes:

- Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.
- Coordinar y monitorear la implementación de los controles de seguridad de información.
- Desarrollar actividades de concientización y entrenamiento en seguridad de información.
- Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas.

B. De la Norma ISO 27001

La Norma ISO 27001 es la principal norma que agrupa los requisitos del SGSI. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002 (nueva denominación a partir del 1 de Julio 2007 para ISO 17799:2005), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la norma considera que la organización

deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

La norma es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

En Perú la ISO/IEC 17799 es de uso obligatorio también en todas las instituciones públicas desde agosto del 2004, de esta manera, se estandarizan los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales, la supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI

CAPÍTULO III

ANÁLISIS DEL ENTORNO

El objetivo de este capítulo es desarrollar un análisis de la situación actual de la gestión de riesgo operativo del país, de mismo modo explorar cual es el marco regulatorio que rige bajo este riesgo.

3.1. El Marco Regulatorio en el Caso Peruano

En el Perú, con la modificación a la Ley de Bancos en el 2008 (ver Figura III.1), el marco regulatorio de Basilea II entró en vigencia en julio del 2009. Es así que a lo largo del año 2009, se publicaron los reglamentos para el requerimiento de patrimonio efectivo por riesgo de crédito, riesgo de mercado y riesgo operativo. En estos reglamentos, se establecen las distintas metodologías que podrán utilizar las empresas del sistema financiero para el cálculo del capital regulatorio y las condiciones que deberán cumplir para hacer uso de las mismas. En particular, para la utilización de modelos internos, las empresas deberán realizar su aplicación formal a la Superintendencia, así como aprobar el proceso de validación que llevará a cabo el supervisor.

La SBS genera las disposiciones del para la Gestión Integral de Riesgos, en el caso de la administración del riesgo operativo así como

a los desarrollos recientes sobre el citado riesgo, mediante Resolución SBS N° 2116-2009 del 2 de abril, se aprueba un nuevo Reglamento para la Gestión del Riesgo Operativo, cuya aplicación se hace extensiva también a las Administradoras Privadas de Fondos de Pensiones (AFP).

Figura III.1 Nota Periodística del Comercio que anuncia la adecuación de gestión de riesgos de Basilea II

CUERPO B — CONTÁCTENOS • editoreconomia@comercio.com.pe — LIMA martes 24 de junio del 2008 — El Comercio

ECONOMÍA& Negocios

SEGÚN ACCEP [96]
Restricciones en las licencias podrían paralizar proyectos comerciales

CASELLA MORENA, LA CABRITA [82]
"La educación nos dio otra visión, sino seríamos 'chivateros' tradicionales"

DÓLAR: Paralelo ⊃ Compra 2,920 Venta 2,950 • Interbancario ⊃ Compra 2,938 Venta 2,941 • Bancario ⊃ Compra 2,870 Venta 3,000 • EURO: Interbancario ⊃ Compra 4,312 Venta 4,575

EMPIEZA A REGIR PARCIALMENTE DESDE EL 1 DE JULIO PRÓXIMO

SBS: Modificaciones a la ley de bancos mejorará la competencia

■ Estiman que la mayor flexibilización de la ley promoverá la competencia

■ La adecuación de gestión de riesgos de Basilea II regirá desde julio del 2009

LUIS DAVID LUQUE LLANOS

Las modificaciones a la Ley General del Sistema Financiero (Ley 26702) promulgadas el domingo por el Ejecutivo (a través del Decreto Legislativo 1028-2008) promoverán la competencia entre los actores del sistema, al uniformizar las reglas de juego, afirmó Javier Poggi Campodónico, gerente de estudios económicos de la Superintendencia de Banca, Seguros y AFP (SBS) y presidente del comité de esa institución que se encargó de proponer la modificación a la ley.

En efecto, hasta ahora la oferta de productos de las instituciones del sistema financiero peruano estaba orientada a obtener una autorización de la SBS. Esta exigía cumplir con una serie de requisitos que permitiera a la entidad operar dentro de un determinado módulo o paquete de operaciones. "Nunca ninguna institución pudo calificar por lo complicado que resultaba el cumplimiento de los parámetros", explica el superintendente adjunto de banca de la SBS, Diego Cisneros.

Por ejemplo, el número de operaciones que puede realizar la banca es mucho mayor que las que pueden efectuar las instituciones microfinancieras cuando, en la práctica, no tiene una razón de ser desde el punto de vista del riesgo. "Que las cajas no puedan otorgar tarjetas de débito no tiene sentido cuando pueden ofrecer créditos hipotecarios", agregó Cisneros.

Con esta medida, vigente desde el 1 de julio, las instituciones microfinancieras podrán realizar operaciones de comercio exterior, negociar papeles del Estado Peruano y facturas, generar créditos para la titulación de hipotecas a través de mecanismos de financiamiento adicionales que les permitirán crecer, entre otros.

Y para ello no deberá calificar a un rango o módulo de operaciones; podrá aplicar ante la SBS para obtener las autorizaciones para realizar cada una de estas operaciones una por una. Así –explica Poggi–, se nivelan las reglas de juego y se logra que las instituciones microfinancieras se fortalezcan y puedan competir en mejores condiciones. A la larga, este incremento de la competencia debería obligar a los actores del mercado a reducir sus márgenes de utilidad, lo que repercutirá en el consumidor con precios más bajos y se favorecerá la bancarización, tarea en la que estas instituciones no bancarias son más activas.

"Al hacer más flexible el acceso, el costo financiero debe bajar por la mayor oferta y competencia", sostuvo Poggi.

TAMBIÉN BASILEA II

Las modificaciones, emitidas como parte de las facultades legislativas delegadas al Ejecutivo por el Congreso para la implementación del TLC con EE.UU., también contemplan la adecuación a los estándares de regulación, capital, evaluación y gestión de riesgos de Basilea II, un conjunto de prácticas que se recomienda adoptar los países para fortalecer sus sistemas financieros.

En ese sentido, las instituciones financieras tienen hasta julio del 2009 para adecuarse a un límite mínimo de capitalización sobre colocaciones de 9,5% (el 2011 debe ser 10%). Actualmente el límite es 9.1%, pero el promedio del mercado es 12.8%. "Esta acción preventiva no generará perturbaciones en el mercado; nos protegerá frente a las vaivenes de los ciclos económicos", explicó Poggi.

Según Cisneros, la SBS viene trabajando en ello desde el 2002, de manera que el estándar internacional pueda ajustarse a la realidad del Perú. Además, estos ajustes "hacen mejores a las instituciones y proveen de mayor protección al ahorrista", concluyó Poggi.

Según ambos funcionarios, la ley es ahora más flexible y menos reglamentarista, para enfrentar una realidad más dinámica. Eso sí, para evitar excesos, se obliga a la SBS a presentar con 90 días de anticipación los cambios que se propongan realizar. ■

Todavía por encima

Actualmente, el capital de los bancos y con creces el de las instituciones microfinancieras sobrepasa los requerimientos mínimos de la SBS. No obstante, el regulador siempre estará más cómodo con el exceso.

Patrimonio Efectivo/ Activos y créditos contingentes ponderados por riesgo *En porcentaje*

Patrimonio Efectivo/ Activos y créditos contingentes ponderados por riesgo *En porcentaje*

Fuente: SBS — EL COMERCIO

Tipos de riesgo y gestión

Basilea II incorpora un nuevo tipo de riesgo a los que ya venían manejándose en el sistema financiero peruano: el riesgo operativo o operacional que se refiere al caso nada deseable de que se produzca, por ejemplo, una caída de los sistemas o el soporte tecnológico de la institución o, peor aun, el eventual riesgo de que un empleado pueda burlar los parámetros de seguridad de la entidad y producir un problema como el que quebró al banco más antiguo y prestigioso de Inglaterra, Barings (adquirido por ING) en la década de 1990 o, recientemente, la Société Generale Francés.

Los otros dos tipos de riesgos están asociados a las colocaciones: riesgo crediticio y a la eventualidad de un incumplimiento de pago masivo causado por una ola de desempleo, por ejemplo. El tercero es el riesgo de mercado, que tiene que ver con la valorización de los activos en los cuales invierten los bancos y la volatilidad que puedan tener sus precios en los mercados.

En un primer momento, los bancos se adecuarán a un método estándar de medición y gestión de riesgos y, más adelante, podrán generar sistemas o modelos más avanzados e individuales de gestión, siempre bajo la supervisión de la SBS.

Fuente: Diario El Comercio

La SBS genera las disposiciones del para la Gestión Integral de Riesgos, en el caso de la administración del riesgo operativo así como a los desarrollos recientes sobre el citado riesgo, mediante Resolución SBS N° 2116-2009 del 2 de abril, se aprueba un nuevo Reglamento para la Gestión del Riesgo Operativo, cuya aplicación se hace extensiva también a las Administradoras Privadas de Fondos de Pensiones (AFP).

Por otro lado, Para la adecuada aplicación del artículo 194° de la Ley General, modificado por el Decreto Legislativo N° 1028, mediante Resolución SBS N° 2115-2009 del 2 de abril, se aprueba el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operativo, estableciéndose la metodología que deberá aplicarse, así como los requisitos que deberán cumplirse para efectuar el cálculo de dicho requerimiento.

Es así que, a partir de julio del 2009, las empresas tuvieron que considerar un nuevo componente: el riesgo operativo, bajo tres de los métodos recomendados por el NAC: del indicador básico, estándar alternativo o los métodos avanzados. De éstos, los dos más complejos requieren autorización previa de la Superintendencia, por lo que desde abril del 2009 se recibieron solicitudes de varias empresas para realizar el cálculo de capital por riesgo operativo mediante el método estándar alternativo.

Es bueno mencionar todas las normas relacionadas directa o indirectamente al tema de riesgo operativo, a continuación dichas normas:

- Resolución SBS N° 037-2008 de fecha 10.01.2008 que aprueba el Reglamento de Gestión Integral de Riesgos.
- Resolución SBS No 2115 – 2009 de fecha 02.04.2009 que aprueba el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operativo. (ver Anexo A1)
- Resolución SBS No 2116 – 2009 de fecha 02.04.2009 que aprueba el Reglamento para la Gestión del Riesgo Operativo (ver Anexo A2)
- Circular SBS No G-139-2009 de fecha 02.04.2009 Gestión de la Continuidad del Negocio. (ver Anexo A3)
- Circular SBS No G-140-2009 de fecha 02.04.2009 Gestión de Seguridad de la Información. (ver Anexo A4)
- Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.- Ley 26702 y sus modificatorias.

3.1.1. Análisis de la Normativa de Riesgo Operativo

A. Alcance

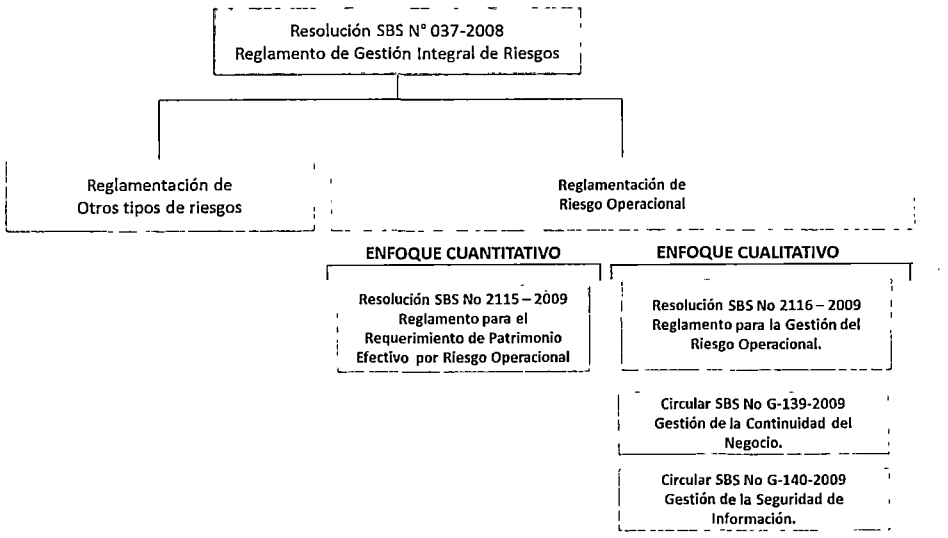
Según la SBS, el reglamento de la gestión del riesgo operativo es aplicado a las empresas señaladas en el artículo 16.° de la Ley General de Bancos, así como a las AFP, en adelante empresas.

También es aplicado a las CMAC, la Caja Municipal de Crédito Popular, el Fogapi, el Banco de la Nación, el Banco Agropecuario, Cofide, el Fondo Mivivienda S.A., y las derramas y cajas de beneficios bajo control de la SBS, en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas. Las empresas de servicios complementarios y conexos señaladas en el artículo 17.º de la Ley General de Bancos se sujetarán para la gestión de su riesgo operativo a lo establecido en sus normas específicas. Asimismo, podrán tomar en consideración las disposiciones señaladas en el mencionado reglamento en función de su tamaño y complejidad.

B. Enfoques

Tal como lo señala la Figura III.2, la reglamentación tiene dos enfoques: el de cuantitativo y el de cualitativo.

Figura III.2 Enfoque de la Regulación relacionada con Riesgo Operativo



Fuente: SBS, Elaboración: Propia

B.1. Enfoque Cuantitativo: Resolución SBS No 2115 – 2009, Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operativo

El enfoque cuantitativo, que se rige esta resolución establece que las empresas deberán destinar patrimonio efectivo para cubrir el riesgo operativo que enfrentan. Para el cálculo de dicho requerimiento patrimonial, se tendrá que aplicar uno de los siguientes métodos:

- Método del indicador básico: Este método considera como base de cálculo el margen operativo bruto anualizado de la empresa.
- Método estándar alternativo: Este método considera como base de cálculo, una combinación de margen bruto y saldos de créditos, sobre la base de la identificación de seis (06) líneas de negocios de la empresa.
- Métodos avanzados: Este método permite que la empresa determine el procedimiento apropiado para establecer el requerimiento de patrimonio efectivo por riesgo operativo. Básicamente se aplica a empresas de gran tamaño y que cuentan con herramientas eficientes para la identificación y mitigación del riesgo operativo.

Asimismo, para la aplicación de los métodos b y c será necesario contar con autorización previa y expresa de la SBS, para ello, previamente deberán cumplirse los requisitos que dicho organismo exige. Así, las entidades financieras tienen que aplicar el método del

indicador básico en tanto no cuenten con autorización para la aplicación de los otros dos métodos.

Bajo este enfoque, el patrimonio efectivo constituye un límite operativo dentro del cual las empresas determinarán sus objetivos estratégicos, los perfiles de riesgo y los controles necesarios. El riesgo operativo, además del riesgo crediticio es una innovación necesaria, por cuanto, las pérdidas que se generan por errores o fraudes u otros factores relacionados con el manejo o gestión de la empresa también inciden de manera gravitante en los resultados de la misma, pudiendo incluso poner en riesgo la marcha de la empresa, en caso la cuantía de las pérdidas supere el patrimonio de la misma.

B.2. Enfoque Cualitativo: Resolución SBS No 2116 – 2009, Reglamento para la Gestión del Riesgo Operativo.

En este caso el Reglamento contempla criterios mínimos que las empresas deberán tener en cuenta para realizar una gestión adecuada del riesgo operativo que enfrentan, los principales factores detonantes del Riesgo Operativo contemplados en el Reglamento son los siguientes:

- Procesos internos, implementados para la realización de las operaciones y servicios: Son aquellos relacionados con el diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que produzcan un desarrollo deficiente

de las operaciones y servicios, al extremo de provocar la interrupción de los mismos.

- Personal: Se considera factor de riesgo la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.
- Tecnología de información: Este factor de riesgo comprende las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.
- Eventos externos: Son aquellos eventos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

En este enfoque también se considera a la gestión del riesgo legal que es considerado dentro de la mitigación de los factores antes mencionados, especialmente la administración de los procesos internos, la gestión del personal y el uso de tecnologías de información.

El mismo modo, entre los eventos de pérdidas por riesgo operativo previstos en el Reglamento se encuentra los siguientes:

- Fraude interno: Pérdidas por actuaciones encaminadas a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se

encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

- Fraude externo: Pérdidas por actuaciones encaminadas a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.
- Relaciones laborales y seguridad en el puesto de trabajo: Pérdidas por actuaciones incompatibles con la legislación o acuerdos laborales, así como sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.
- Clientes, productos y prácticas empresariales: Pérdidas por el incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos, o derivados de la naturaleza o diseño de un producto.
- Daños a activos materiales: Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos. Interrupción del negocio y fallos en los sistemas: Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.
- 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.

B.3. Enfoque Cualitativo: Circular SBS No G-139-2009, Gestión de la Continuidad del Negocio

También como enfoque cualitativo, se establecen los criterios mínimos para la gestión de la continuidad del negocio financiero, que forma parte de una adecuada gestión del riesgo operativo que enfrentan las empresas supervisadas por la SBS. Esta circular contiene disposiciones, que toman como referencia estándares internacionales como la BS-25999.

Esta norma pretende asegurar que los productos o servicios de la empresa financiera continuarán brindándose en el tiempo a pesar de la ocurrencia de un evento o incidente que pudiera interrumpir los procesos esenciales del negocio.

B.4. Enfoque Cualitativo, Circular SBS No G-140-2009 - Gestión de la Seguridad de Información

Mediante esta regulación se exige que todas las Instituciones Financieras del Perú implanten un sistema orientado a controlar el riesgo operativo de las instituciones, a través de un Sistema de Gestión de Seguridad de Información (SGSI). Esta reglamentación plantea que el ISO 27001:2005 debiera tomarse como referencia.

C. Necesidades

Las necesidades que se plantean en las normas pasan por establecer algunas de las consideraciones siguientes:

- *El Rol del Directorio y la Gerencia*, de acuerdo al Reglamento, los estamentos responsables de la gestión del riesgo operativo son cuatro: el directorio, la gerencia, el comité de riesgos y la unidad de riesgos. De los cuatro, el Directorio es la máxima instancia responsable en la conducción de dicha gestión, siendo entre sus funciones principales las de definir la política general para la gestión del riesgo operativo así como el de asignar los recursos necesarios para la adecuada gestión del riesgo operativo.
- *El Apetito al Riesgo*, corresponde a cada entidad determinar cuál es su apetito por el riesgo y en atención a ello elaborar su estrategia de identificación y mitigación del riesgo operativo.
- *Mejora de los procesos internos*, lo cual comprende las actividades propias del negocio así como las actividades ajenas al negocio, la idea es generar procedimientos sencillos, de fácil comprensión para los usuarios internos y externos, estandarizados e integrados. Una buena administración de los procesos conlleva una reducción del riesgo operativo y de los costos operativos.
- *Adquisición de tecnología*, que faciliten el suministro de información entre las diversas áreas, así como centralizar y depurar las bases de datos.
- *Construcción de una Base de Datos de Eventos de Pérdidas Operativo,* las entidades deberán contar con una base de datos de los eventos de pérdida por riesgo operativo, para ello se debe tener en cuenta que un evento puede tener como efecto una o

más pérdidas, por lo cual las empresas deberán estar en capacidad de agrupar las pérdidas ocurridas por evento.

D. Limitaciones

La regulación ha seguido parámetros y lineamientos similares a los que dictan otros reguladores internacionales, en el caso peruano, para el Instituto Peruano de Auditores (IPAI), existe la limitante en cuanto a las actividades de auditoría y control interno, en efecto, en el Comunicado IPAI N° 02-2010 el IPAI manifiesta que "*si bien la SBS ha emitido el reglamento para que las empresas del sistema financiero den cumplimiento a las normas sobre evaluación de la gestión de riesgo operativo; éste no establece los procedimientos de auditoría y los alcances que las firmas de auditoría externa deben aplicar para satisfacer los requisitos de la norma y verificar su cumplimiento por parte de las empresas supervisadas*" Es así que en vista de que no existen esos alcances y ya que de acuerdo con las normas de la SBS, el informe de cumplimiento sobre la evaluación de la gestión de riesgo operativo debe resultar de un trabajo independiente a la auditoría de los estados financieros, estableciendo que el trabajo debe ser realizado por un equipo de auditoría diferente o una sociedad de auditoría diferente a la que realiza dicha auditoría externa, han convenido seguir los parámetros que en el comunicado IPAI N° 02-2010 se establecen.

Adicionalmente, otra limitante es que la SBS si bien en el 2009 ha dictado las normas de gestión de riesgos operativo la misma que ha ido

de la mano con un sistema que les permita recibir pruebas de que las entidades están adecuándose al enfoque de riesgo operativo, lo cierto es que recién este año están implementando los sistemas de información que permitan recibir información de eventos de pérdidas de riesgo operativo y que serviría para disponer de una central de eventos de riesgo operativo, necesaria en el mercado peruano.

3.1.2. Estado Situacional de Riesgo Operativo en el País

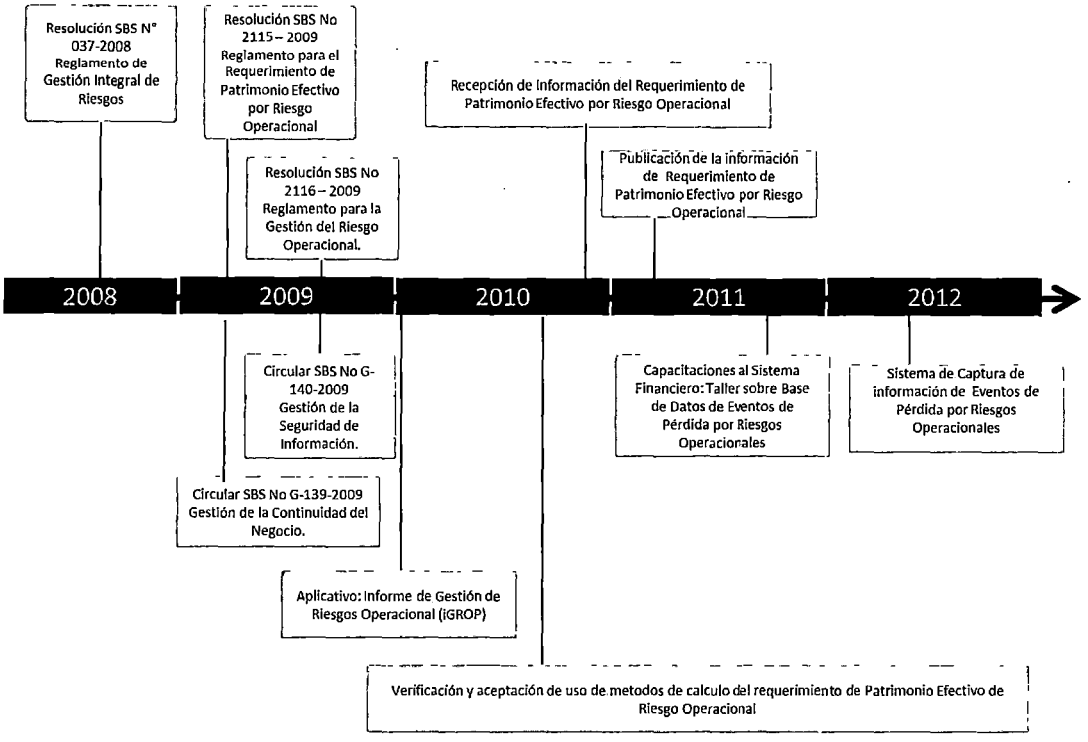
A. Línea de acción del Supervisor SBS

El órgano supervisor del sistema financiero peruano es la SBS, en su rol supervisor y siguiendo directrices del NAC Basilea II viene haciendo posible que la gestión del riesgo operativo cobre importancia en los últimos años para las empresas del sistema financiero, para ello se basa en los mismos justificantes del NAC: la mayor complejidad operativa de las operaciones financieras, los lineamientos para la gestión de este riesgo y los eventos ocurridos en los últimos años asociados con riesgos operativos que han generado pérdidas significativas a algunas empresas.

Para ello, como se pudo apreciar, la SBS ha emitido por un lado una serie de normas por el cual las entidades financieras tienen que gestionar el riesgo operativo y el realizar el cálculo de los requerimientos de capital asociados al riesgo operativo y por otro viene implementando una serie de acciones (solicitud de información y proyectos) para mejorar la gestión del sistema en su totalidad.

El conjunto de acciones y normativa que se han venido desde que se dio la normativa en el 2009 son reflejadas en la línea de tiempo de la Figura III.3

Figura III.3 Línea de Tiempo de las Acciones Tomadas por la SBS en el Ámbito del Riesgo Operativo

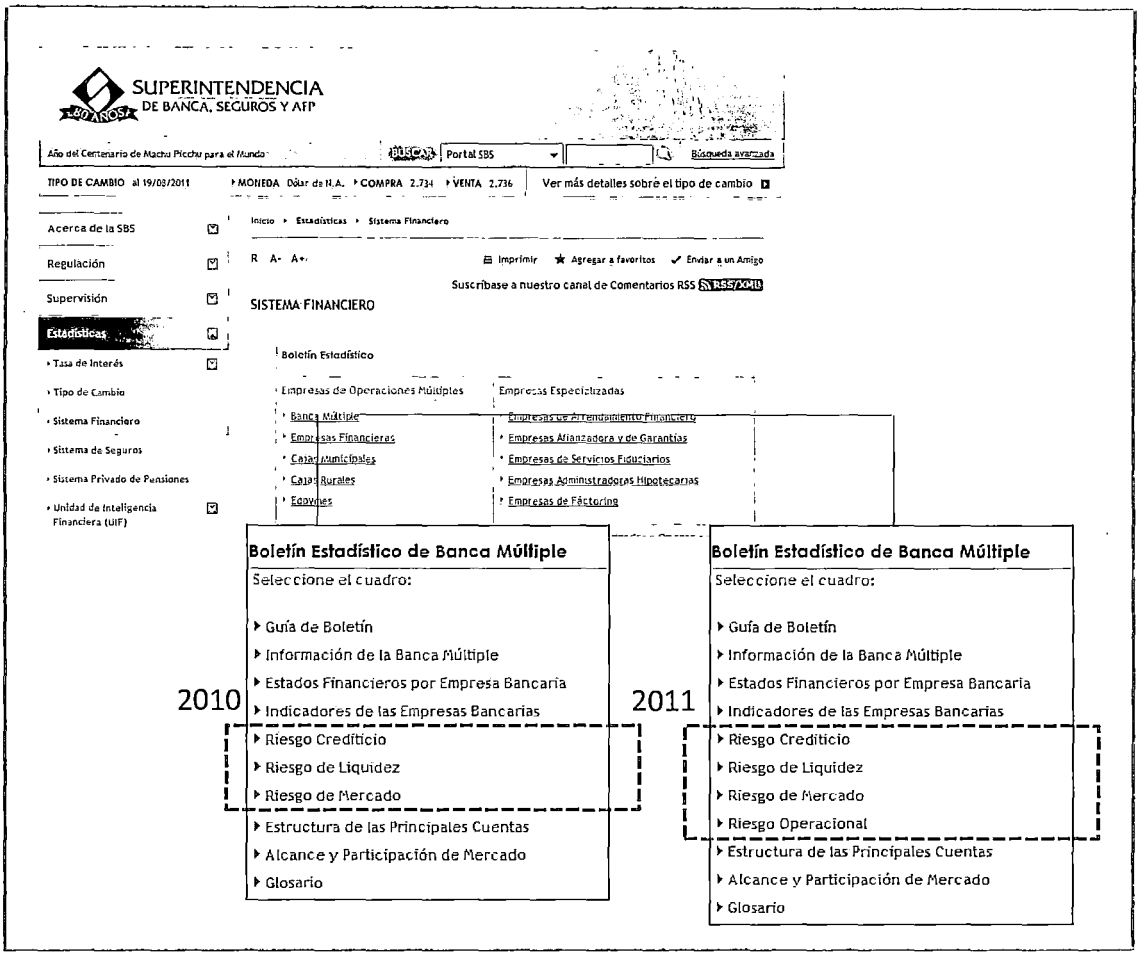


Fuente: SBS, Elaboración: Propia

Como se pueden apreciar, si bien la normativa se dio el año 2009, es recién en el 2010 que la SBS supervisa que la adecuación de las entidades en este enfoque, un ejemplo de ello es que a finales del 2010 el Portal de la SBS (ver Figura III.4) no mostraba información de Riesgo Operativo esto no sucedía con los otros tipos de riesgo (crediticio, liquidez y mercado) que si eran presentados. Al 2011, la información

mostrada hace referencia al Requerimiento de Patrimonio Efectivo por Riesgo Operativo

Figura III.4 Estadísticas de Riesgo

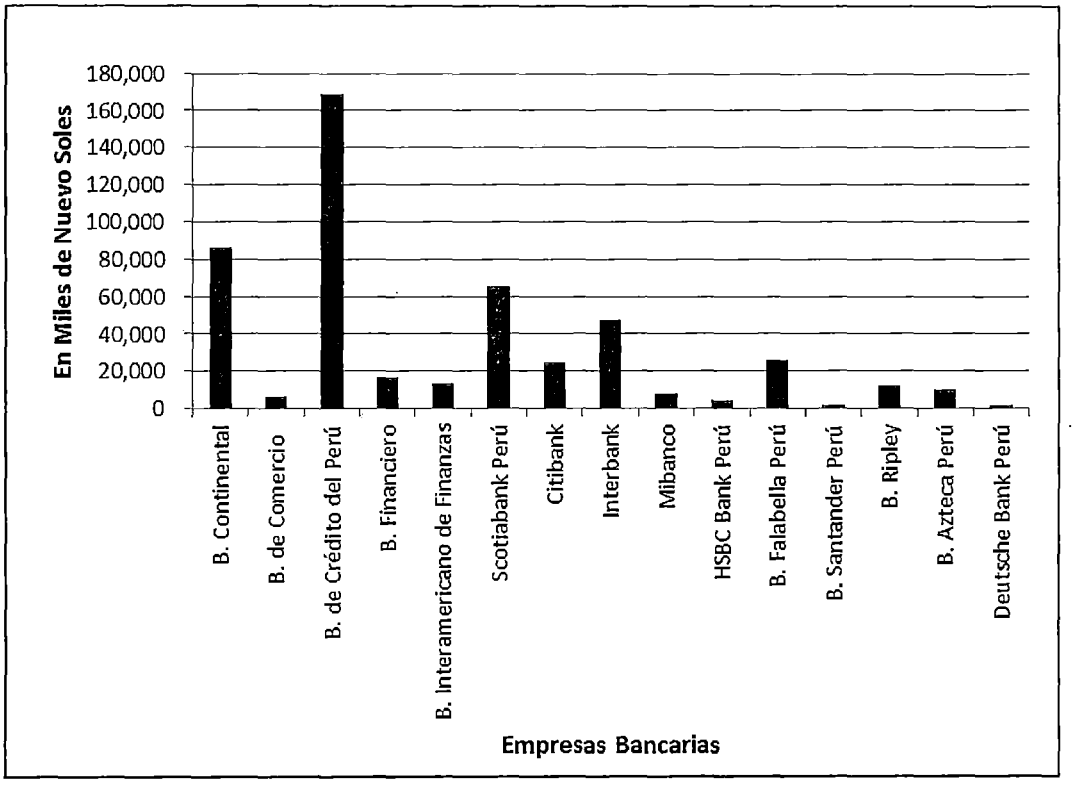


Fuente y Elaboración: SBS

Según la SBS, el 2009 comenzó la constitución del Requerimiento de Patrimonio Efectivo por Riesgo Operativo y se encuentra en proceso gradual de ajuste y que debe terminar a mediados de año del 2012. Es así que a diciembre del 2010, el 4.5% del total del patrimonio requerido al sistema financiera corresponde al riesgo operativo.

De esta manera, tal como se aprecia en la Figura III.5 según la SBS y a Junio de 2011 el Requerimiento de Patrimonio Efectivo por Riesgo Operativo de las Empresas Bancarias asciende a un total de 495,427 miles de nuevos soles y en donde el Banco de Crédito se diferencia de las otras significativamente.

Figura III.5 Requerimiento de Patrimonio Efectivo de Riesgo Operativo, Junio de 2011



Fuente y Elaboración: SBS

Del mismo modo esto va de la mano con la adecuación y la necesidad de las entidades por construir un marco metodológico en la evaluación de la gestión de riesgo operativo en las empresas, así como en la continuidad de los negocios y la gestión de riesgo operativo.

En la actualidad, si bien ya existe el marco normativo no existen estudios de los estados de situación en la adopción de la gestión de riesgo operativo (por ende hay información limitada) que indique el grado de concientización de los directivos, de buscar ventajas competitivas, de los problemas que tienen, por ello, como toda adopción de un nuevo estándar o marco regulatorio se prevé que en los próximos años que exista información situacional.

B. Estudio de Posicionamiento del Riesgo Operativo en las Entidades Financieras Peruanas

Teniendo como instrumento de recolección de información el cuestionario y en base a preguntas los estudios empíricos de "Riesgo Operativo" elaborado por Pricewaterhouse Coopers y el de Universidad de Cantabria, ambos en el 2006 se elaboró un estudio de posicionamiento de riesgo operativo

B.1. Objetivo e Hipótesis

Los objetivos se centran en analizar el grado de madurez y desarrollo de las entidades encuestadas en la Gestión del Riesgo Operativo y la hipótesis de este estudio corresponde a la misma de la presente tesis.

B.2. Población y Muestra

La población incluida en el estudio incluyó a las empresas del Sistema Financiero excluyéndose a las Microfinancieras, esto

comprende a los Bancos (Grupo A) y a las Financieras (Grupo B) y en donde se excluye a las Microfinancieras (Cajas Municipales, Cajas Rurales y Edpymes) as;i como a Entidades Estatales, como es el caso del Banco de la Nación.

En este sentido la población objeto del estudio involucra a 25 entidades, donde a diciembre del 2010 representaban el 54.6% del saldo de activos los bancos representan el 85% del saldo total de créditos y el 80% de saldos del sistema financiero y las financieras el 4% del saldo total de créditos y el 1% respectivamente. En suma, hablando financieramente la muestra representa el 89% de saldo total de créditos y al 81% del total de saldos. Estadísticamente hablando debido a que la muestra es menor a 30 se infieren los siguientes parámetros de intervalos de confianza: Z=1.96, Nivel de confianza de 95%, n=25, Margen de error=29%, p=q=0.5.

La siguiente tabla muestra la población objeto de estudio:

Tabla III.1 Muestra de Población de Entidades

Grupo A: Bancos	B. Continental
	B. de Comercio
	B. de Crédito del Perú
	B. Financiero
	B. Interamericano de Finanzas
	Scotiabank Perú
	Citibank
	Interbank
	Mibanco
	HSBC Bank Perú
	B. Falabella Perú
	B. Santander Perú
	B. Ripley
	B. Azteca Perú
	Deutsche Bank Perú
Grupo B: Financiera	Crediscotia Financiera
	Financiera TFC

	Financiera Edyficar
	Financiera Crear
	Financiera Confianza
	Financiera Efectiva
	Financiera Universal
	Financiera UNO
	Amérika Financiera
	Mitsui Auto Finance

Fuente: SBS, Elaboración: Propia

B.3. Instrumento: Cuestionarios

El instrumento utilizado para obtener información ha sido a través de cuestionarios, para ello el cuestionario fue configurado con un total de ocho preguntas, los cuestionaron plantearon totalmente anónimas y cuyo diseño se puede apreciar en el Anexo A5.

B.4. Tratamiento de los datos

Para el análisis y representación se ha empleado fundamentalmente la estadística descriptiva.

B.5. Nivel de Respuestas

Las respuestas recibidas se detallan en la tabla siguiente, se proporcionan un nivel de respuesta satisfactorio teniendo en cuenta el que el 60% ha contestado

Tabla III.2 Estadística de Envíos y Recepción de Cuestionarios

	Grupo A	Grupo B	
Enviadas	15	10	25
Recibidas	9	6	15
	60%	60%	

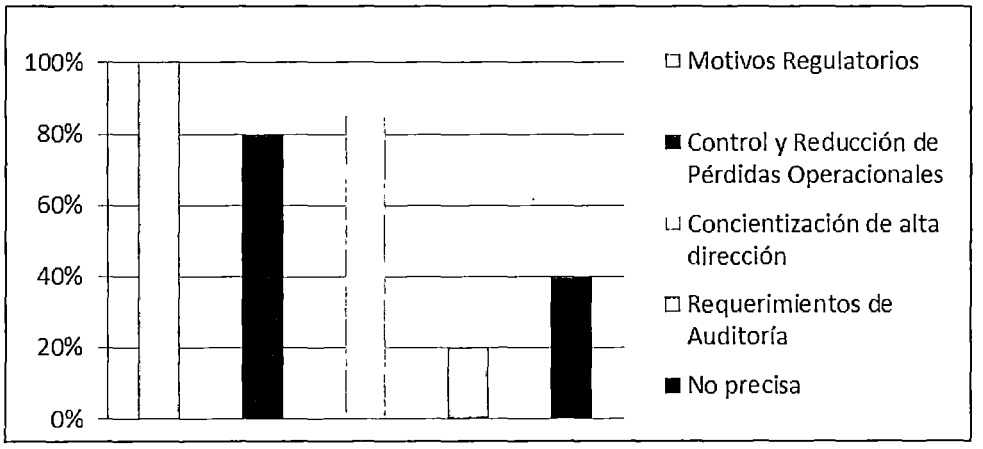
Fuente y Elaboración: Propia

B.6. Resultados

B.6.1. Definición y motivos de adopción

Como era de esperarse las entidades comenzaron a avanzar con la gestión del riesgo operativo debido a que es una exigencia por parte del regulador SBS, todos los encuestados, sin excepción, salvo los que no contestaron, habían adoptado a la fecha del estudio la definición del NAC por motivos regulatorios.

Figura III.6 Motivos por los cuales se comenzó a trabajar en la gestión de Riesgo Operativo



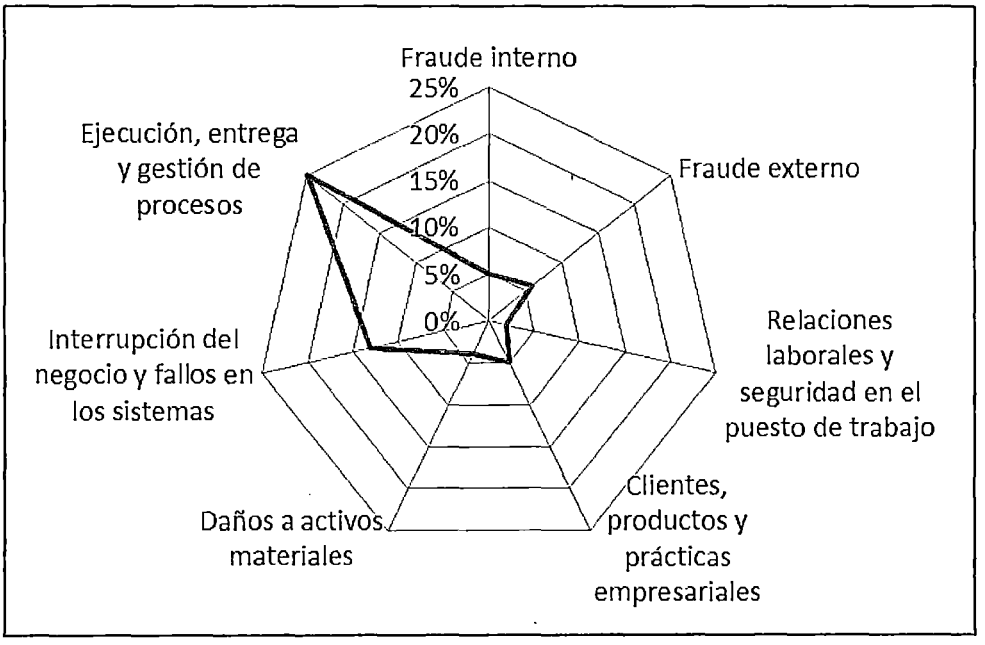
Fuente: Cuestionario, Elaboración: Propia

B.6.2. Tipos de Evento

Respecto a cuáles son los tipos de evento más importantes, sin distinguir la frecuencia o severidad de los eventos, destacan con 25% la ejecución, entrega y gestión de los procesos, le siguen, la

interrupción del negocio y fallo en los sistemas con 13%, los niveles más bajos hacen referencia a el fraude externo, fraude interno, Clientes, productos y prácticas empresariales, daño a activos materiales, y las relaciones laborales y seguridad en el puesto de trabajo. El 40% no precisa.

Figura III.7 Tipos de más Importantes de Riesgo Operativo en las Entidades Financieras



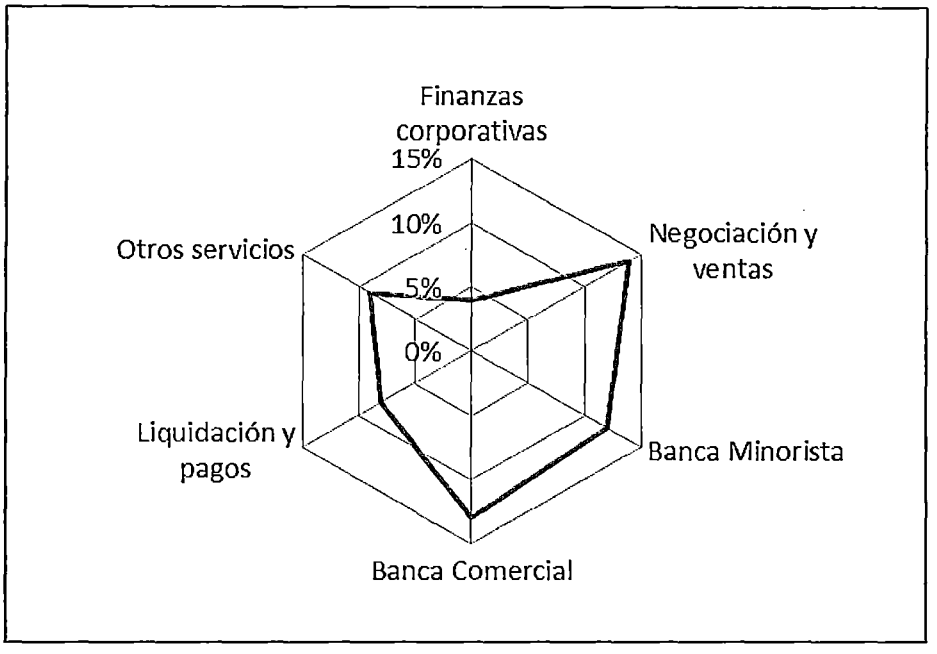
Fuente: Cuestionario, Elaboración: Propia

B.6.3. Líneas de Negocio

Respecto a cuáles son las líneas de negocio más importantes, sin distinguir la frecuencia o severidad, destacan con 14% Negociación y ventas, le siguen Banca Comercial con 13%, Banca Minorista con 12%, Otros servicios (no se precisa el detalle) con 9%, Liquidación y pagos

con 8% y finanzas corporativas con 4%.. El 40% de las empresas encuestada no precisa.

Figura III.8 Líneas de Negocio más Importantes de Riesgo Operativo en las Entidades Financieras



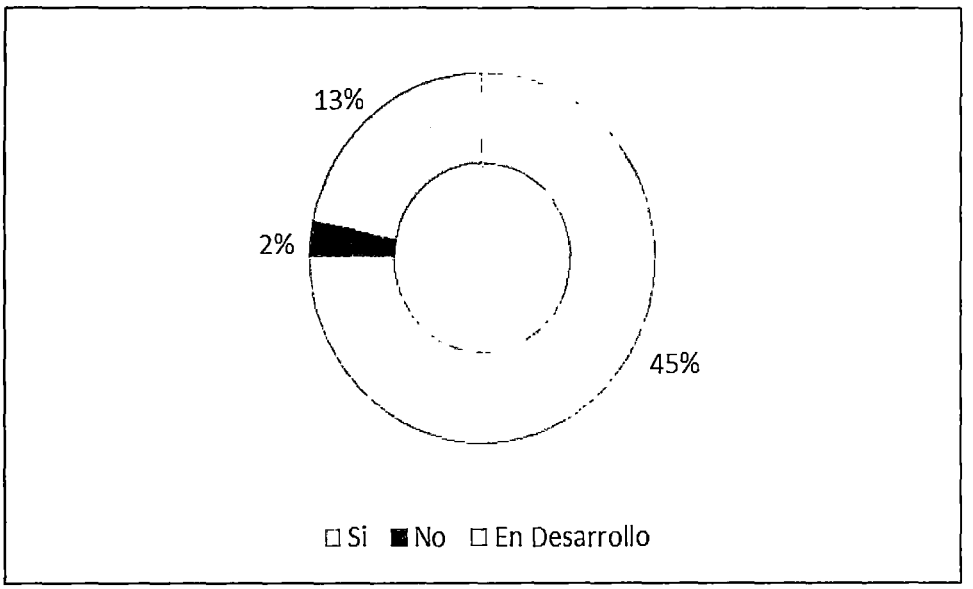
Fuente: Cuestionario, Elaboración: Propia

B.6.4. Organización

El reto de las entidades es la de crear un modelo organizativo que fomente la gestión de riesgos operativos dentro de la entidad y que cuenten con una unidad centralizada de gestión del riesgo operativos. A sabiendas que todas las entidades encuestadas ya han incorporado la gestión del riesgos operativo, los resultados del cuestionario arrojan que el 45% de las entidades cuentan con un área independiente de riesgos de operación, el 13% está en desarrollo y el 2% cuenta con un área independiente de riesgos de operación. Entre las que si cuentan

con un área independiente se aprecian diferencias en el número de personal que labora en ellas, se han entidades que tienen únicamente a tres personas hasta una entidad con 15 personas, se entiende que esto redunda en el gran desarrollo alcanzado por dicha entidad.

Figura III.9 ¿Cuentan con un área independiente de Riesgos de Operación?



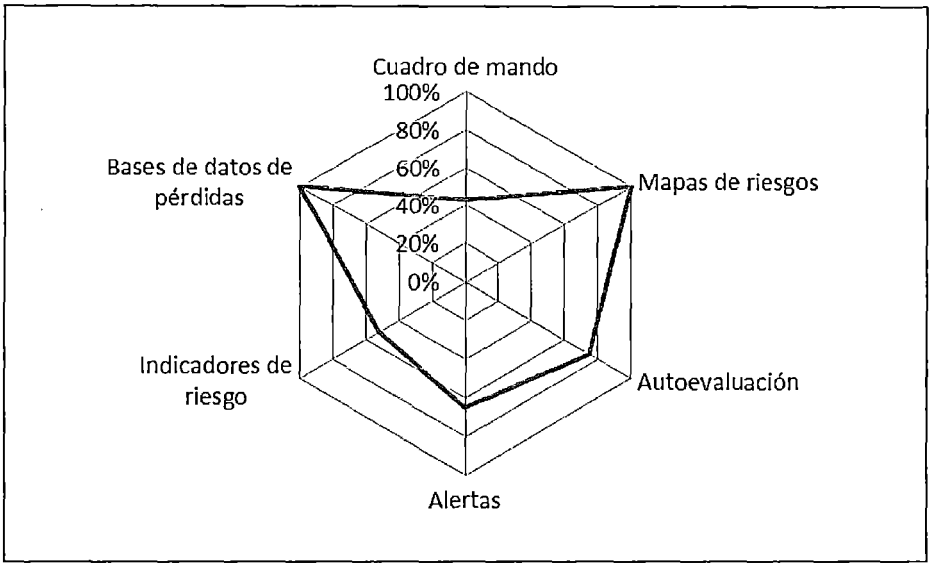
Fuente: Cuestionario, Elaboración: Propia

B.6.5. Herramientas y Metodología

El uso de herramientas es vital para identificar y capturar las pérdidas operativas, así como la evaluación, seguimiento, control y reporting de los riesgos. Tal como se aprecia en el gráfico siguiente las herramientas más utilizadas son por un lado las bases de datos de eventos de pérdida, previsible en el estudio por ser una exigencia del regulador y por el otro lado, las matrices de riesgos, ambas con un uso del 100%, otras herramientas que hacen alusión son la autoevaluación con 75%, las alertas con 65% y los indicadores de riesgo con 52%,

finalmente un hecho real es que solo el 43% de los que respondieron usan un cuadro de mando integral. Respecto

Figura III.10 Herramientas de Gestión de riesgos de Operación



Fuente: Cuestionario, Elaboración: Propia

B.6.6. Componentes de la Metodología Integral de Gestión de Riesgos Operativo

Los componentes que se incluyeron en la encuesta se basan en la previsión de los elementos que se creen necesarios deba de tener la metodología de gestión de Riesgos Operativo.

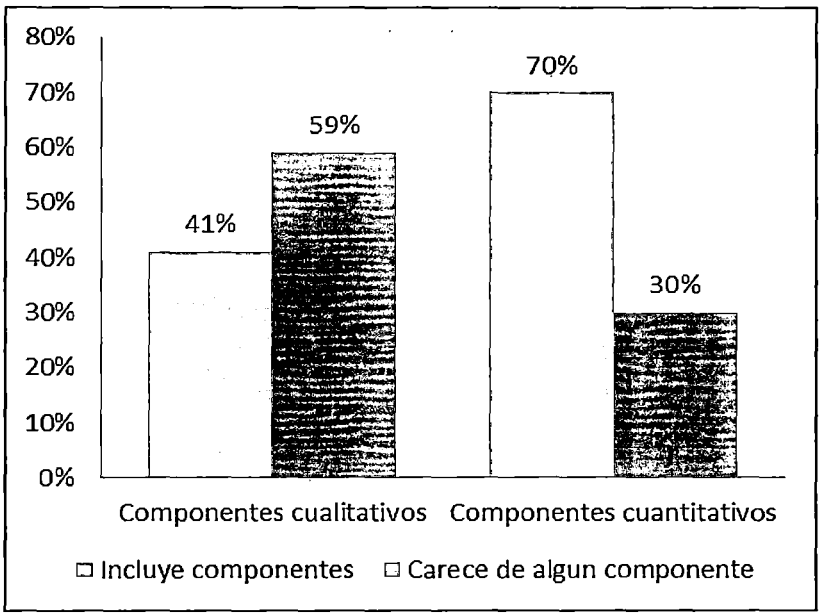
En el caso de la parte cualitativa se consideraron los componentes siguientes: la estructura organizativa, modelo general, políticas, requisitos, marco legal, mapeo de procesos, herramientas informáticas (software) y documentales que cubren las diferentes etapas de gestión de riesgos cualitativo, identificación de eventos de pérdida.

En el caso de la parte cuantitativa se consideraron los métodos de medición de cálculo para los diferentes tipos de riesgo según Basilea y

que esté(n) integrado(s) con el sistema informático financiero y contable de empresa.

Los resultados obtenidos denotan que hay una carencia de componentes cualitativos y cuantitativos, esto comprueba que la metodología para gestión de riesgos no es lo suficientemente madura y que se esta tesis se justifica.

Figura III.11 Nivel de Componentes que incluyen la Metodología Integral de Gestión de Riesgos Operativo



Fuente: Cuestionario, Elaboración: Propia

B.6.7. Metodología Cualitativa según Principios de Basilea II

Los criterios cualitativos que son tomados en cuenta para la gestión de riesgos de operación según los principios de Basilea tienen el nivel de cumplimiento aproximado siguiente:

Tabla III.3 Nivel de cumplimiento de Metodología Cualitativa según Principios de Basilea II

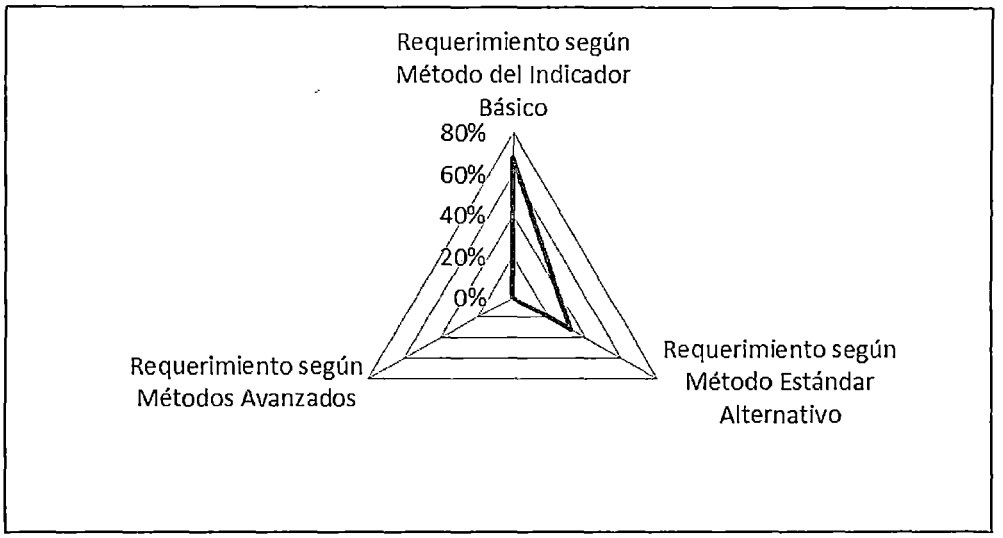
Tener un sistema de gestión del Riesgo Operativo (RO) que asigne responsabilidades claras a la unidad de gestión del RO.	40%
Tener un sistema de evaluación del RO perfectamente integrado dentro de los procesos de gestión del riesgo de la entidad.	48%
Analizar de forma sistemática la información sobre el RO, incluidas las perdidas relevantes sufridas en cada una de las líneas.	52%
Contar con un sistema periódico de información sobre las exposiciones al RO, incluidas las pérdidas operativos más relevantes, dirigido al Consejo de Administración, la Alta Dirección y las diferentes unidades de negocio.	28%
Contar con un sistema periódico de información sobre el historial de pérdidas por RO, dirigido al Consejo de Administración, la Alta Dirección y las diferentes unidades de negocio.	39%
Definir procedimientos destinados a adoptar las acciones necesarias según la información aportada por los informes de la gestión del RO.	48%
Documentar correctamente todo el sistema de gestión del RO.	55%
Validar y examinar de forma periódica e independiente los procesos de gestión y el sistema de evaluación del RO.	57%
Que los auditores internos y/o externos realicen exámenes periódicos de los procesos de gestión y de los sistemas de evaluación del RO.	18%
Implantar técnicas que asignen los ingresos brutos o el capital, según el método, a las diferentes líneas de negocio y que generen incentivos para la mejora de la gestión del RO en toda la entidad.	62%

Fuente: Cuestionario, Elaboración: Propia

B.6.8. Métodos de Medición del Requerimiento de Patrimonio Efectivo por Riesgo Operativo

Al cierre del cuestionario, de los que respondieron el cuestionario, el 68% de las entidades usan el método de indicador básico y el 32% el estándar alternativo, en el caso de este último es un hecho que han presentado a la SBS una solicitud de autorización, la SBS ha evaluado el método de cálculo y ha autorizado el uso del método. En caso del método avanzado, se distingue que ninguna entidad que respondió el cuestionario ha empleado dicho método.

Figura III.12 Métodos de Medición del Requerimiento de Patrimonio Efectivo por Riesgo Operativo

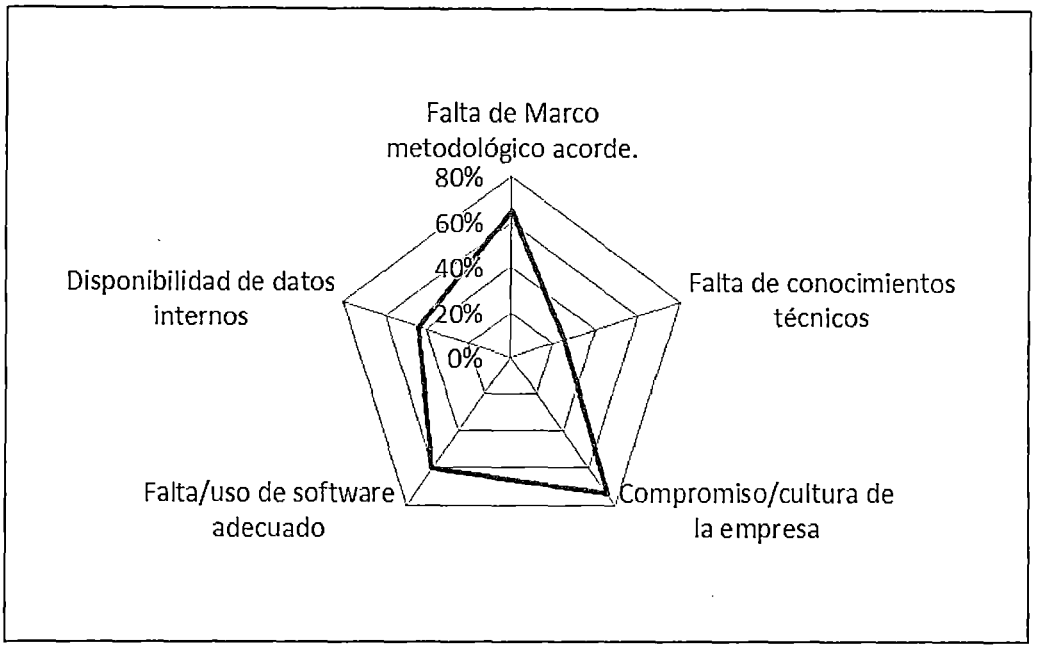


Fuente: Cuestionario, Elaboración: Propia

B.6.9. Principales Dificultades en la Gestión de Riesgos Operativo

Por otro lado, si bien el mercado de riesgo operativo está en desarrollo y en etapa de madurez existen dificultades e inconvenientes en su implementación, entre ellos el compromiso o la cultura de la empresa representa un 74% de dificultad, le sigue con un 65% la falta de un marco metodológico acorde, con 60% la falta/el uso de software adecuado, con 44% la disponibilidad de datos internos y finalmente con 25% la falta de conocimientos técnicos.

Figura III.13 Principales Dificultades para Gestionar el riesgo Operativo



Fuente: Cuestionario, Elaboración: Propia

C. Panorama de la Gestión de Riesgos: Entrevista a Jordi García Ribas

Jordi García Ribas es experto mundial en el tema de Riesgo Operativo, el es Ex Director Corporativo de Riesgo Operativo, Ex líder del Consorcio Español de Riesgo Operativo y Vicepresidente de la organización internacional ORX (Operational Risk Exchange)

Tipo de Entrevista : Presencial

Fecha de la Entrevista : 15 de Setiembre de 2011

Ricardo Berrospi:	***¿Cuál es su opinión respecto a la proyección en los 5 años próximos respecto a la evolución de la gestión de riesgo operativo?***

Jordi Garcia:	Mi opinión es que el modelo de gestión de riesgo operativo va a evolucionar en la medida que evolucione la contabilidad , haciendo un paralelismo al riesgo de crédito, el cual posee cuentas específicas en un plan contable, se requiere que los riesgos de operación tengan cuentas específicas de modo que el impacto económico de los diversos tipos de pérdidas se encuentren registrados en la cuentas específicas de riesgos de operación.
Ricardo Berrospi:	***¿Qué opina del uso de las metodologías cualitativas para gestionar los riesgos operativos como COSO y la ISO-17799?***
Jordi Garcia:	Mi opinión es que COSO es más bien una metodología útil en tareas de Auditoría o Control Interno, un buen documento de definiciones de los conceptos acerca de gestión de riesgo operativo es el OPERATIONAL RISK REPORTING STANDARDS (ORRS) del Operational Riskdata eXchange Association (ORX), este es un libro de aproximadamente 300 páginas que puede servir a los reguladores y empresas financieras.
Ricardo Berrospi:	***¿Qué papel cobran las base de datos de eventos de pérdida?***
Jordi Garcia:	La gestión de riesgos de operación se puede hacer de dos formas: cualitativa y cuantitativa, bueno, la base de datos de eventos de pérdidas aporta la información necesaria para realizar la gestión cuantitativa, tal como se hace con el riesgo de crédito, aporta aspecto necesarios para la gestión de procesos en las líneas de negocio y aporta datos para el cálculo de capital en riesgo.

	Las base de datos aportan información muy valiosa, tu sabes que el ser humano aprende por sus experiencia, es más fácil conocer la exposición al riesgo operativo por los eventos ocurridos que por factores cualitativos que aún no se han manifestado en forma de eventos. Las bases de datos son útiles en la medida en que las entidades se preguntan qué lagunas en la gestión hay detrás de los eventos que ocurren.

Ricardo Berrospi:	***¿Cuáles cree que son los requisitos, factores de decisión o limitaciones que una entidad elija entre uno u otro método de medición de riesgo operativo (Básico, Estándar y Avanzado)?***
Jordi Garcia:	Esto dependerá de cuan refinado sea su modelo, hay que tener en cuenta el grado de complejidad y exigencia, nótese que en caso del método estándar se incorpora el concepto de líneas de negocio y que además de que las entidades tienen que calificar para este modelo, tienen que cumplir no solo requisitos cuantitativos sino también requisitos cualitativos en donde resalta el hecho de tener una estructura que incentive y promueva la gestión del riesgo operativo. En cambio en el avanzado, la entidad utiliza su propio modelo interno de cálculo e igual tiene que calificar para el uso de su modelo. En cuanto a los requisitos, estos los puedes encontrar en el propio documento de Basilea II, un libro muy recomendado es el de mi colega Alberto Ferreras, te recomiendo leerlo.

CAPÍTULO IV

METODOLOGÍA PARA LA GESTIÓN DEL RIESGO OPERATIVO

El objetivo de este capítulo es describir la metodología propuesta para la gestión de riesgo operativo en una entidad financiera.

4.1. De la Metodología de Gestión del Riesgo Operativo

Dado que las empresas gestionan el riesgo operativo de diversas maneras, se propone y sugiere elaborar en lo posible una metodología que integren los procedimientos y herramientas que permitan a las entidades gestionar sus riesgos operativos de modo que puedan cumplir las mejores prácticas establecidas en los escenarios financieros así como cumplir con los requerimientos normativos de la SBS, entre ellos el Reglamento de Gestión Integral de Riesgos (Resolución SBS N° 037-2008), Reglamento para el Requerimiento de Patrimonio Efectivo Por Riesgo Operacional (Resolución SBS No 2115-2009) y Reglamento para la Gestión del Riesgo Operativo (Resolución SBS No 2116-2009).

En ese sentido, se debe considerar que la metodología esté documentada y que se implemente en toda la empresa en forma

consistente, para lo cual la empresa asignará los recursos suficientes para la aplicación de la misma, la cual debe de estar integrada a los procesos de gestión de riesgos de la empresa en todas las líneas de negocio, de control y de apoyo. Para ello, la empresa debe de establecer incentivos y procedimientos que permitan mejorar y dar cumplimiento a la metodología.

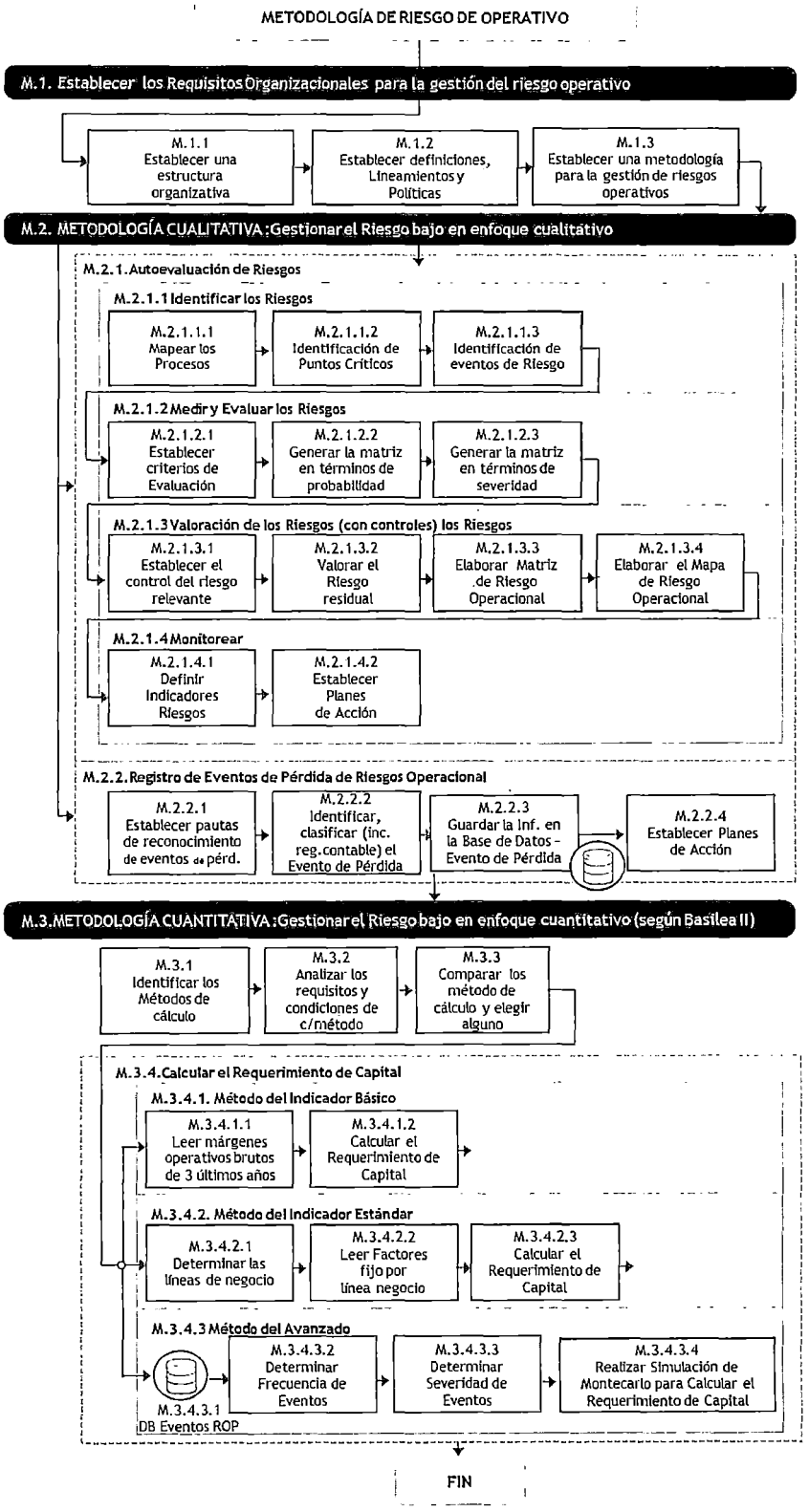
La Figura IV.1. a manera de diagrama de flujo, muestra la secuencia de pasos de la metodología propuesta, para ello, se considera como paso inicial el establecimiento de requisitos organizacionales para lo cual explorar las actividades y herramientas tanto de la metodología cualitativa como la metodología cuantitativa.

4.2. (M.1) Establecer los Requisitos Organizacionales para la gestión del riesgo operativo

4.2.1. (M.1.1) Establecer una Estructura Organizativa para la Gestión del Riesgo Operativo

El enfoque tradicional necesitaba una serie de departamentos centralizados que velaban por determinadas tipologías de riesgo en donde el riesgo operativo era gestionado por cada línea de negocio. Esta gestión se buscando soluciones a problemas que han puesto de manifiesto a través de controles internos o auditorías. Las soluciones, en muchos casos implicaba la contratación de seguros o realizar inversión en tecnología, pero siempre enfocándose en el problema concreto que había dado lugar a la pérdida sin tener una visión global.

Figura IV.1 Metodología para la Gestión del Riesgo Operativo



Fuente: Jordi García Ribas (BBVA), SBS, PricewaterhouseCoopers, COSO.

Elaboración: Propia.

De hecho el enfoque tradicional ha mostrado inconvenientes tales como la ausencia de una visión global, la ausencia de una medida para valoración de riesgo, la ausencia de información para una gestión eficaz y la ausencia de un único responsable

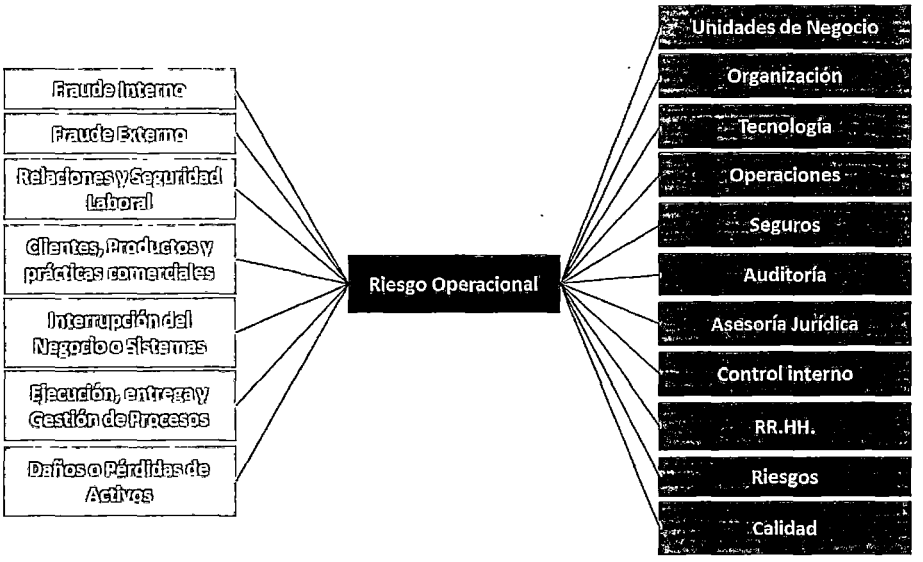
En ese contexto, la NAC como impulsores del cambio refieren aspectos organizativos de la función del riesgo operativo en sus tres primeros principios básicos:

> *"Principio 1: El Consejo de administración deberá conocer cuáles son los principales aspectos de los riesgos operativos para el banco, en tanto que categoría de riesgo diferenciada, y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo.*
>
> *Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operativo en el banco esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operativo.*
>
> *Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco"*

La gestión derivada del NAC es una gestión Ex – ante, que pretende identificar las debilidades de los controles y procedimientos optimizando el riesgo operativo que la entidad debe asumir.

Por ello, lo aconsejable es poner en marcha un departamento de riesgo operativo que asuma las funciones descritas en el NAC y que lleve a cabo una gestión global, si bien es cierto tendría como competencias la gestión de dicho riesgo la responsabilidad sería compartida ya que el Reglamento de la SBS estipula que los estamentos responsables de la gestión del riesgo operativo son cuatro: el directorio, la gerencia, el comité de riesgos y la unidad de riesgos. La Figura IV.2 muestra las interacciones de este departamento con las otras unidades de la organización.

Figura IV.2 La gestión del Riesgo Operativo en el enfoque NAC



Fuente: Virginia Gonzales Sierra y Estebaliz López Fernández, en el libro de "La gestión de Riesgo Operativo, de la teoría a su aplicación" Elaboración propia.

Los beneficios que trae este enfoque permitiría:

- Disponer de información consolidada del riesgo operativo, y que permita coordinar los esfuerzos de la organización en

este materia de modo que se evite la duplicidad y solapamientos

- Gestión integral e independiente cubriendo las brechas que produciín la gestión departamental
- Reducción de costos y del consumo de capital producto de la gestión y aplicación de las metodologías.
- Optimización de los elementos de mitigación

No existe un único modelo válido de estructura organizativa del riesgo operativo para todas las organizaciones pero si debe reflejar tres importantes objetivos:

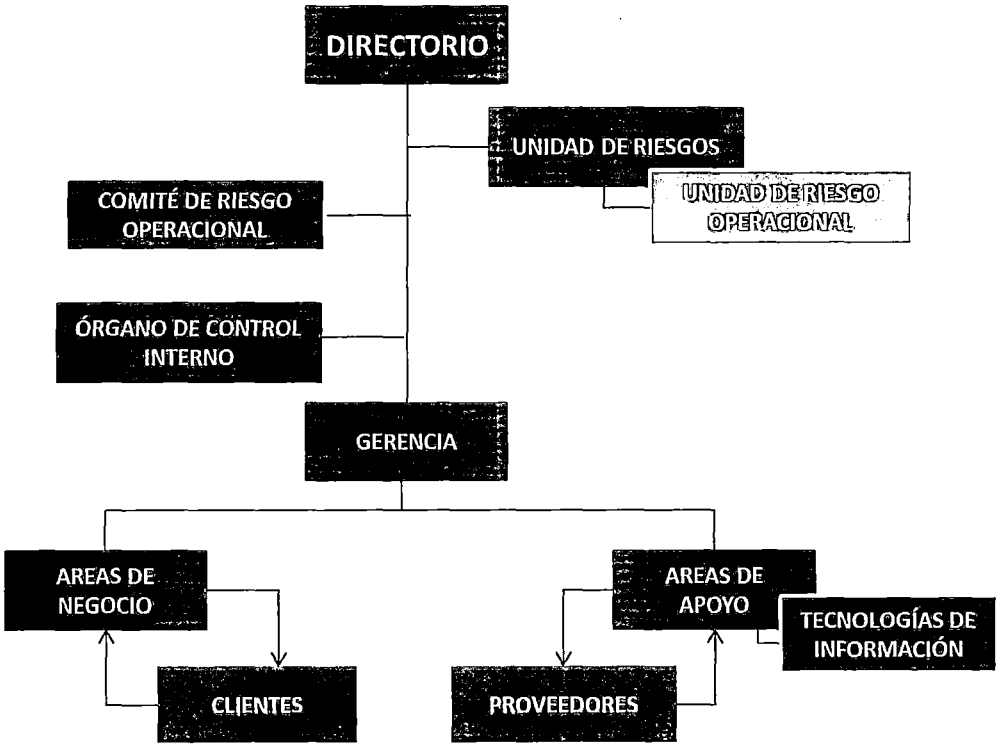
- El riesgo operativo no puede ser limitado a unidades organizativas específicas sino que es en gran medida responsabilidad de toda la entidad
- Es necesario que existe una clara división de funciones entre el riesgo operativo y el área de auditoría interna. El departamento de riesgo operativo debe ser independiente del área de auditoría interna.
- El comité de riesgo operativo debe de tener un papel fundamental en esta estructura, como órgano independiente o como un subgrupo dentro del comité de riesgos de la entidad.

Al diseñar la estructura organizativa de la gestión del riesgo operativo es importante tener en cuenta la estructura general de la

gestión de riesgos, ya que la solución adoptada debe ser coherente con las necesidades de la gestión global de riesgos,

La figura siguiente muestra la estructura organizativa de área de gestión de riesgo operativo sugerida.

Figura IV.3 Estructura Organizacional sugerida



Fuente: "La gestión de Riesgo Operativo, de la teoría a su aplicación", Elaboración propia.

La descripción de las actividades de cada componente de la estructura organizacional es la siguiente:

A. El Directorio y la Gerencia General

El Directorio es la máxima instancia responsable final de la administración de los riesgos asociados a los productos y servicios ofrecidos en los diversos mercados en los que opera la organización, siendo sus responsabilidades las siguientes:

- Aprobar las políticas generales que guíen las actividades del banco en la gestión de los riesgos operacionales que enfrenta.
- Aprobar los recursos necesarios para el adecuado desarrollo de la Gestión de Riesgo Operativo, a fin de contar con la infraestructura, metodología y personal apropiado.
- Establecer un sistema de gestión que fomente el adecuado funcionamiento de una gestión integral de riesgos y que favorezca la toma apropiada de riesgos.
- Asegurar razonablemente que el patrimonio contable de la empresa sea suficiente para enfrentar los riesgos a los que está expuesto

Por su parte la Gerencia tiene como responsabilidades los siguientes:

- Implementar la Gestión de Riesgo Operacional conforme a las disposiciones del Directorio y Comité de Gestión Integral Riesgos.
- Velar por el cumplimiento del marco regulatorio y las normas relacionadas a la Gestión de Riesgos.

- Promover la cultura de riesgos en la organización, asegurándose de que exista un marco de trabajo adecuado para la administración de los mismos.
- Implementar las políticas y procesos generales establecidos por el Directorio y Comité de Gestión Integral de Riesgos, promoviendo conciencia de la necesidad de la administración de los riesgos operacionales en la organización.
- Garantizar el cumplimiento de los niveles de exposición al riesgo operacional aprobados en la política de apetito y la tolerancia al riesgo y los planes de negocios aprobados.
- Obtener aseguramiento razonable que exista un marco de trabajo adecuado para identificar, medir, monitorear y reportar los riesgos operacionales en el Banco.
- Proponer mejoras que fomenten la adecuada administración de riesgos operacionales.
- Autorizar y/o priorizar los recursos para implementar los planes de acción aprobados.
- La responsabilidad es delegada por el Directorio a la Gerencia General, quién a su vez cumple con sus responsabilidades a través de la Vicepresidencia de Riesgos y específicamente la Gerencia de Riesgo Operativo.

B. Unidad de Riesgos - Comité de Gestión Integral de los Riesgos

La Unidad de Riesgos está integrada por un Jefe, que depende del Directorio y cuenta con la colaboración de las distintas unidades de Riesgos de Créditos, Riesgos Mercado, Riesgos Operativos y Tecnología de la Información. Dependiendo de la estructura elegida se recomienda conformar el Comité de gestión Integral de Riesgos, en cualquiera de los dos casos las responsabilidades serían los siguientes:

- Obtener aseguramiento razonable de la implementación dea dministración de riesgos operacionales que resulte acorde a la dimensión y naturaleza de sus operaciones y servicios.
- Asistir al Directorio en la responsabilidad de proveer un esquema de administración de riesgos operacionales a través de la organización.
- Aprobar la organización y las políticas generales de Riesgos, así como las modificaciones que se realicen a los mismos.
- Definir el nivel de apetito por el riesgo operacional a asumir para el desarrollo del negocio.
- Verificar que el nivel de exposición a los riesgos operacionales afrontados este dentro del apetito y la tolerancia al riesgo y los planes de negocios aprobados.
- Decidir las acciones necesarias para la implementación de las acciones correctivas requeridas, en caso existan desviaciones con

respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.

- Aprobar la sub-contratación significativa de servicios.
- Reportar semestralmente al Directorio respecto a la gestión realizada para la administración de los riesgos operacionales.
- Asegurar que la implementación de la administración de riesgos operativos proporcione aseguramiento razonable del logro delos objetivos y prevenga las pérdidas.
- Autorizar y/o priorizar los planes de acción, para mitigar los riesgos o eventos que lo requieran.
- Evaluar los avances de las auto evaluaciones, informes, medidas de mitigación, y tratamiento de los riesgos operacionales.
- Reportar las pérdidas/contingencias y riesgos operacionales que se han materializado al Directorio.

C. Unidad de Riesgos Operativo (Gerencia de Riesgo Operacional)

Es la unidad que dependiendo del modelo de estructura organizativa adoptada puede depender del Directorio o bien ser parte integrante de la Unidad de Riesgos y debe tener las siguientes funciones:

- Implementar la gestión de riesgos operacionales conforme a las disposiciones de la Unidad de Riesgos o el Comité de Gestión Integral de Riesgos (según sea el caso).

- Asistir a las unidades de negocio y soporte en la administración de los riesgos operacionales a lo largo de la empresa.
- Velar por el cumplimiento de las políticas y procedimientos de gestión de riesgos, comprendidas en las diferentes normas de la empresa.
- Reportar a la Unidad de Riesgos o el Comité de Gestión Integral de Riesgos (según sea el caso) la situación sobre la gestión de riesgo operacional en la organización.
- Proponer las políticas de administración de riesgos operacionales mismas.
- Desarrollar y proponer la metodología para la administración de riesgos operacionales en la organización.
- Apoyar en la validación del entendimiento de los productos y procesos
    - Velar porque el análisis correspondiente al entendimiento del producto refleje objetivamente su situación
    - Definir los procedimientos críticos y su prioridad para la evaluación de riesgos operacionales.
- Autoevaluación de Riesgos
    - Realizar un seguimiento continuo al grado de avance de las autoevaluaciones vía cuestionarios, desde su generación hasta su cierre.
    - Definir los criterios para efectuar la autoevaluación cualitativa de la eficacia de los controles y medidas de mitigación.

- Asistir a las áreas de la empresa en las autoevaluaciones de los riesgos ante el lanzamiento de nuevos productos ó cambios significativos en el ambiente operativo y/o informático.

- Recolección de Eventos
  - Velar por la correcta identificación, clasificación y registro de los eventos de pérdida reportados por las áreas de negocio y soporte, así como del correcto análisis de su criticidad.
  - Verificar la calidad de la información de los eventos de pérdida recolectados.
  - Reportar los eventos de pérdidas operacionales que se han materializado al Unidad de Riesgos o el Comité de Gestión Integral de Riesgos (según sea el caso) así como al Directorio.
- Indicadores de Riesgos
  - Asistir a los Gerentes de Producto y Coordinadores de Riesgo Operativo, en la definición de los indicadores de riesgo y sus límites asociados
  - Analizar e informar periódicamente los niveles de exposición, valor de los indicadores y cumplimiento de límites establecidos
- Planes de Acción
  - Realizar seguimiento al grado de avance de los planes de acción aprobados. o Evaluar y comunicar el impacto de ampliar los plazos de implementación de los planes de acción solicitados por los responsables de los productos.
- Reporte

- Realizar seguimiento e informar los avances en la administración de riesgos operacionales en la empresa
- Administrar los riesgos de los procesos de negocio que trascienden las fronteras de las funciones de negocio, y en los cuales no es posible asignar un responsable de los mismos.
- Administrar el sistema de información (accesos, mantenimiento, etc.).

D. Gerente de Producto ó Gerente de Área

De producto o de área dependerá del enfoque con el que se estructures la empresa, tiene las siguientes responsabilidades:

- Garantizar el cumplimiento de las políticas, lineamientos y metodología de gestión de los riesgos operacionales para los productos bajo su responsabilidad.
- Velar por que las políticas, procesos y controles, y contratos de servicios críticos del producto o proceso bajo su responsabilidad, se encuentren actualizados.
- Garantizar que los riesgos legales relacionados a los procesos, productos y servicios que administra, se encuentren debidamente mitigados.
- Establecer los niveles de servicios requeridos para los servicios de terceros relacionados a los productos bajo su gestión.
- Autoevaluación de riesgos

- Conjuntamente con el área de Planeamiento identificar los procesos asociados a los productos y actividades.
- Garantizar la veracidad de la identificación, evaluación, seguimiento y mitigación de los principales riesgos operacionales de todos sus productos, actividades, procesos y sistemas.
- Gestionar la evaluación de las subcontrataciones significativas con la asistencia de Legal y la Gerencia de Riesgo Operativo; así mismo garantizar que los contratos de dichas subcontratación cuente con cláusulas que aseguren la mitigación de sus riesgos y cumplimiento de normas vigentes.
- Gestionar los riesgos de forma previa al lanzamiento de nuevos productos o a la realización de cambios significativos en el ambiente operativo y/o informático.

- Recolección de Eventos
  - Liderar la identificación y reporte de los eventos de pérdida, así como la recolección de la información mínima requerida en las políticas del presente manual.
  - Informar a la Gerencia de Riesgo Operativo todos los eventos de pérdidas identificados bajo su gestión.
- Indicadores de Riesgos
  - Definir conjuntamente con la Gerencia de Riesgo Operativo, los indicadores de riesgo operacional, niveles de exposición y límites para cada indicador.

- Verificar la calidad y consistencia de la información de los indicadores de riesgo, y que en caso de exceso en los límites se tomen las acciones de mitigación pertinentes.

- Planes de Acción
  - Implementar los planes de acción de manera oportuna y coherente con los riesgos a tratar
  - Revisar periódicamente la efectividad de los planes de acción implementados.
- Gestionar los riesgos operacionales asociados a la interrupción de los servicios, de acuerdo a las políticas y procedimientos de gestión de la continuidad.
- Gestionar los riesgos asociados a seguridad de información para los productos y servicios a su cargo.

E. Coordinador de Riesgo Operacional

Sus responsabilidades son las siguientes:

- Asistir al Gerente en la administración de los riesgos operacionales.
- Autoevaluación de riesgos
  - Gestionar la autoevaluación a través de cuestionarios con los expertos en el proceso.
  - Gestionar la autoevaluación de los riesgos de forma previa al lanzamiento de nuevos productos o a la realización de cambios significativos en el ambiente operativo y/o informático.

- Garantizar la veracidad e integridad de los resultados de las autoevaluaciones.
- Velar por el cumplimiento de la política de apetito de riesgo.

- Recolección de Eventos
  - Gestionar la identificación, valoración y reporte de los eventos de pérdida así como garantizar la integridad y disponibilidad de la información en el sistema.
  - Monitorear e informar a la Gerencia de Riesgo Operativo, respecto a cada evento de pérdida encontrado.
  - Velar por el cumplimiento de la política de tolerancia al riesgo y custodiar sus respectivos expedientes.
- Indicadores de Riesgos
  - Valorar y registrar en el sistema mensualmente los indicadores de riesgos (KRI) reflejando la situación actual, informando al respectivo Gerente de Producto.
  - Asistir a la Gerencia de Riesgo Operativo, en la definición de los límites niveles de alerta y críticos para cada indicador de riesgo.
  - Analizar y gestionar la información generada por los indicadores con la finalidad de mitigar los riesgos operacionales asociados a estos en sus negocios.
- Planes de acción
  - Identificar los riesgos que necesitan mitigaciones adicionales de acuerdo a las políticas del banco. o Realizar el seguimiento a la ejecución de los planes de acción, informando periódicamente

al Gerente de Producto y Gerencia de Riesgo Operativo a través del sistema.

- Comunicar los cambios significativos en el plazo o forma de implementar los planes.

- En caso de ausencia temporal o permanente (vacaciones, licencias, cambio de áreas, entre otros) coordinar su reemplazo.

F. Otras Áreas y Roles

Se incluyen las responsabilidades de cada área o rol.

F.1. Investigador de Eventos

- Capturar la información de los eventos de pérdida, montos, fechas, sus recuperaciones y los costos asociados a los mismos.
- Documentar la información vertida sobre el evento de pérdida presentando información que sustenten el registro.

F.2. Prevención de Fraude

- Gestión y seguimiento de las operaciones relacionadas al riesgo de fraude externo para los productos y servicios dentro de su ámbito.
- Gestionar la implementación de políticas y procedimientos para prevenir el riesgo de fraude.
- Informar los eventos de pérdida relacionados al fraude a la Gerencia de Riesgo Operativo.
- Desarrollar y proponer la metodología para prevenir el riesgo

F.3. Tecnología de Información

- Velar por que durante el desarrollo de los proyectos e iniciativas de mejora de procesos que se llevan a cabo en el Banco, se tomen en consideración las políticas y lineamientos definidos para la administración de los riesgos operacionales.
- Poner en conocimiento de la Gerencia de Riesgo Operativo aquellos procesos que pudiesen verse afectados por un cambio significativo, previo a la implementación de los mismos.

F.4. Seguridad de Información

Dependiendo de la estructura puede ser un área o rol dentro de la gerencia de Tecnologías, tiene las responsabilidades son las siguientes:

- Implementar el Sistema de Gestión de la Seguridad de Información.
- Gestionar la implementación de políticas y procedimientos de Seguridad de Información.
- Informar los eventos de pérdida relacionados al fraude a la Gerencia de Riesgo Operativo.
- Apoyar en el proceso de identificación y valoración de riesgos operacionales.

F.5. Auditoría Interna

- Compartir información relativa a eventos de pérdida y otras situaciones de potencial riesgo operacional con la Gerencia de Riesgo Operativo.
- Coordinar con la Unidad de Riesgos aspectos relevantes relacionados con la evaluación de los riesgos operacionales del Banco.
- Realizar anualmente un proceso de auditoría independiente a la Gestión del Riesgo Operacional, con la finalidad de comprobar que las políticas y procedimientos operativos están siendo realizados eficazmente.

F.6. Planeamiento

- Velar por que durante el desarrollo de los proyectos e iniciativas de mejora de procesos que se llevan a cabo en la empresa, se tomen en consideración las políticas y lineamientos definidos para la administración de los riesgos operacionales.
- Identificar e incluir en los documentos normativos, puntos de control que hagan referencia a las validaciones que las áreas de negocio deben realizar para cerciorarse de la conformidad operativa de cada proceso.
- Gestionar el programa de continuidad de negocio, de acuerdo a las políticas y procesos vigentes.

- Asistir al Gerente de Producto en su coordinación con la Gerencia de Riesgo Operativo sobre los nuevos productos y/o servicios a ser ofrecidos por la empresa, previo a la realización de dichos lanzamientos.
- Poner en conocimiento de la Gerencia de Riesgo Operativo aquellos procesos que pudiesen verse afectados por un cambio significativo, previo a su implementación.

F.7. Legal

- Gestionar la implementación de políticas y procedimientos para prevenir el riesgo legal.
- Informar los eventos de pérdida a la Gerencia de Riesgo Operativo relacionados a las relaciones laborales y seguridad en el puesto de trabajo o demandas y juicios contra el banco.
- Verificar que los contratos incluyan las cláusulas estándar en los casos de subcontratación significativa.
- Verificar que los contratos incluyan las cláusulas

F.8. Seguros

- Definir los criterios y niveles de cobertura de los activos de la empresa y de los activos de sus clientes que respaldan operaciones.
- Asesorar en el desarrollo de las alternativas para la reducción de pérdidas por riesgos operacionales, asegurables y no asegurables.

- Mantener un inventario actualizado de los contratos de seguros de la empresa „

F.9. Colaborador

- Informar los riesgos y eventos de pérdida al Jefe inmediato, coordinador de riesgo y a la Gerencia de Riesgo Operativo.
- Participar de la identificación y valorización de los riesgos operativos inherentes a sus funciones y a los procesos en los que intervienen.
- Asegurar que las medidas de mitigación implantadas en su unidad de negocio o soporte funcionen en forma adecuada.

4.2.2. (M.1.2) Establecer las Definiciones, Lineamientos y Políticas de la Gestión del Riesgo Operativo

A. Definiciones

Para establecer los lineamientos y políticas de la gestión del riesgo operativo es necesario establecer una serie de definiciones, similar a un diccionario de términos, a continuación.

A.1. Generales

Tabla IV.1 Principales Definiciones para la gestión de Riesgo Operativo

TÉRMINO	DEFINICIÓN
Administración de riesgos	Proceso que consiste en identificar, medir, controlar y reportar los riesgos que la empresa enfrenta
Apetito por el riesgo	El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor
Directorio	Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente

TÉRMINO	DEFINICIÓN
Exposición al Riesgo	Medida que representa el grado de posibilidad de ocurrencia de un evento negativo o adverso, así como el impacto del mismo en el Banco al momento de materializarse
Línea de Negocio	Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento de mercado objetivo definido en la planificación estratégica
Mapa de Procesos	Herramienta que ayuda a visualizar la institución desde un enfoque basado en procesos
Mapeo de Procesos	Estructurar la información de los productos y servicios, asociándoles la División responsable del Producto (Unidad de Negocio), procesos que lo soportan
Proceso	Conjunto de actividades, tareas y procedimientos organizados y repetibles
Proceso crítico	Proceso considerado indispensable para la continuidad de las operaciones y servicios del Banco
Reglamento de la Gestión Integral de Riesgos	Reglamento de la Gestión Integral de Riesgos aprobado mediante la Resolución SBS N° 37-2008 del 10 de enero de 2008.
Riesgo	La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa
Riesgo Operativo	Entiéndase por riesgo operativo a la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación
Riesgo legal	Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.
Subcontratación	Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante
Superintendencia (o SBS)	Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. (SBS)
Tolerancia al riesgo	El nivel de variación que la empresa está dispuesta a asumir en caso de desviación de los objetivos empresariales trazados
Tecnología de información	Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas

Fuente: La Gestión de Riesgo Operativo, Ana Fernández-Laviada. Elaboración y adaptación: propia.

A.2. Definiciones de Autoevaluación de Riesgos

Tabla IV.2 Principales Definiciones para la Autoevaluación de Riesgos

TÉRMINO	DEFINICIÓN
Aceptación de riesgo	Es la decisión bajo la cual se aceptan las consecuencias de un riesgo en particular
Control	Acciones que son parte de un proceso o actividad, y que tiene por objetivo la reducción de la probabilidad de ocurrencia de eventos asociados a los riesgos inherentes de dicho proceso o actividad
Mitigante	Acción o mecanismo que permite disminuir el impacto de un riesgo sobre los resultados, operaciones o competitividad del Banco
Frecuencia	Es el número de ocurrencias de un evento en un periodo dado
Severidad	Consecuencia o consecuencias de un evento, expresado en términos cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. También es llamado impacto

Fuente: La Gestión de Riesgo Operativo, Ana Fernández-Laviada. Elaboración y adaptación: propia.

A.3. Definiciones de Registro de Eventos de Pérdida

Tabla IV.3 Principales Definiciones para los Eventos de Pérdida

TÉRMINO	DEFINICIÓN
Base de Datos de Eventos de Pérdida	La recopilación sistemática de los eventos de pérdida y la información relacionada a estos, como son: descripción, causas, recuperos y consecuencias se almacenará en una base de datos.
Evento	Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
Evento de pérdida por riesgo operativo	El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operativo (ver Anexo 7)
Información	Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
Pérdida Operativo	Todo impacto negativo o reducción en la cuenta de resultados o en la situación patrimonial del banco susceptible de tener reflejo contable, cuyo origen sea un evento de pérdida por riesgo operativo.
Recuperación	Porción de la pérdida que logra ser recuperada (por ejemplo, monto reconocido por compañía de seguros).

Fuente: La Gestión de Riesgo Operativo, Ana Fernández-Laviada. Elaboración y adaptación: propia.

A.4. Definiciones de Indicadores de Riesgo

Tabla IV.4 Principales Definiciones para los Indicadores de Riesgo

TÉRMINO	DEFINICIÓN
Indicador de riesgo operativo (KRI)	Medida utilizada para indicar que tan riesgosa es una actividad, permitiendo representar la dimensión teórica o específica de un factor de riesgo considerado clave. Dicho valor es calculado en base a datos reales de las operaciones de la empresa.
Nivel de alerta / Nivel Crítico	Umbral establecido para identificar si el valor del KRI se está moviendo en los niveles previstos. Estos límites permiten identificar con antelación cuando el nivel de exposición se está incrementando, al punto que pudiese traducirse en pérdidas futuras para la empresa.

Fuente: La Gestión de Riesgo Operativo, Ana Fernández-Laviada. Elaboración y adaptación: propia.

A.5. Definiciones de Cálculo de Capital

Tabla IV.5 Definiciones para el Cálculo de Capital

TÉRMINO	DEFINICIÓN
Cálculo de Capital Regulatorio	En riesgo operativo, Basilea II establece que se deben de calcular los requerimientos de capital como la suma de pérdidas esperadas e inesperadas, para ello deberá usar alguno de los métodos sugeridos y aceptados por el supervisor.

Fuente: La Gestión de Riesgo Operativo, Ana Fernández-Laviada. Elaboración y adaptación: propia.

A.6. Definiciones de Componentes Relacionados

Tabla IV.6 Definiciones de Componentes Relacionados

TÉRMINO	DEFINICIÓN
Plan de Continuidad del negocio	Es el documento que refleja el proceso continuo que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable ante todo tipo de escenarios de riesgos, con el

TÉRMINO	DEFINICIÓN
	objetivo de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de evento que puedan crear una interrupción o inestabilidad en las operaciones de la organización.
Gestión de la Seguridad de Información	Es el proceso que se basa en las normas NTP 17799 e ISO 27001, define los criterios mínimos para la Gestión de la Seguridad de la Información en éste tipo de organizaciones, el objetivo es establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

Fuente: La Gestión de Riesgo Operativo, Ana Fernández-Laviada. Elaboración y adaptación: propia.

B. Políticas

Las políticas dependerán tanto de la estructura organizacional como el *core* de negocio de la empresa. A continuación, se presentan una serie de políticas que debieran ser tomadas como un modelo mas no una regla a seguir:

B.1. Políticas Generales

- La gestión de riesgo operativo es integral y abarca a toda la organización
- La gestión de riesgo operativo tiene como base a los responsables a las diversas unidades de negocio y soporte que la componen.
- El Directorio aprobará y revisará periódicamente la estrategia de riesgo operativo implementada por la empresa.
- La Gerencia tiene la responsabilidad de implementar la estrategia de riesgo operativo aprobada por el Directorio. Dicha estrategia será desarrollada de forma sistemática en toda la organización.

- El Directorio y la Gerencia General, en sus respectivos niveles de responsabilidad comunicarán que la Gestión de los Riesgos Operativos constituye una prioridad institucional.
- El Directorio y la Gerencia General, propiciará una eficiente gestión del riesgo operativo y un ambiente interno que facilite su desarrollo adecuado, delegando las facultades necesarias a las áreas correspondientes.
- La Gerencia de Riesgo Operativo deberá proponer las políticas, procedimientos y metodologías apropiadas para la Gestión del Riesgo Operativo en la empresa, incluyendo los roles y responsabilidades.
- Los Gerentes de División, Coordinadores de Riesgo Operativo y personal involucrado en los procesos de negocio y soporte, deberán gestionar el riesgo operativo en los procesos y productos bajo su responsabilidad.
- La Gerencia de Riesgo Operativo es responsable de evaluar la Gestión del Riesgo Operativo, medida por el indicador de cumplimiento en la aplicación de la metodología por los responsables de cada producto o proceso de la empresa.
- La Gerencia de Riesgo Operativo reportará periódicamente los resultados de gestión y riesgos operativos identificados mediante el "Informe de Gestión de Riesgo Operativo para el Directorio".
- Los casos de incumplimiento de las políticas serán informados Gerencia de Riesgo Operativo; a la Gerencia Genera quien tomará

las acciones pertinentes. Se considerarán incumplimientos de las políticas de Riesgo Operativo lo siguientes puntos:

- Omitir informar sobre eventos de pérdida de Riesgo Operativo.
- Omitir comunicar/gestionar la autoevaluación de riesgos operativos de forma previa al lanzamiento de nuevos productos o cambios significativos en el ambiente operativo e informático.
- Omitir informar los indicadores de riesgos.
- No gestionar u omitir informarla situación de mitigación de los riesgos considerados dentro de planes de acción.
- No implementación de acciones de mitigación por parte de las Divisiones de Soporte; en el caso los planes para tratar los riesgos o pérdidas operativos requieran de su participación.
- Incumplimiento en informar de manera previa a la subcontrataciones de procesos o funciones significativas según las normas internas.

- La empresa evaluará los costos y beneficios de las estrategias alternativas de control y mitigación del riesgo operativo, y ajustará su exposición al riesgo empleando estrategias apropiadas, tomando en consideración su perfil integral de riesgo.
- La empresa gestionará los riesgos operativos asociados a nuevos productos, servicios o cambios significativos en el ambiente operativo y/o informático.
- La empresa gestionará los riesgos asociados a la subcontratación significativa, considerando normas y procedimientos relacionados

a la evaluación de proveedores, mecanismos de subcontratación y procedimientos del nivel de prestación de servicios.

- La empresa aplicará un sistema de incentivos que permita el cumplimiento y mejora de la gestión de riesgos operativos de la empresa.
- La empresa ejecutará programas de capacitación sobre mecanismos de gestión de riesgos con el objetivo de asegurar que el personal cuente con las habilidades y experiencia apropiadas y optimizar las actividades de gestión de riesgos operativos.
- La empresa establecerá planes de contingencia y de reanudación de negocio para los procesos, sobre todo en aquellos con alta dependencia de tecnología de información; con la finalidad de garantizar nuestra capacidad de operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio. Los planes de contingencia y de continuidad serán revisados periódicamente para asegurar que sean consistentes con las actuales operaciones y estrategias de empresa.
- La empresa llevará a cabo de manera directa o indirecta, una evaluación periódica de las estrategias, políticas, procedimientos y prácticas que se relacionan con los riesgos críticos de la empresa. Asimismo, se implementarán mecanismos eficaces de reporte, que permitirán mantenerse informado de los avances que se realizan.
- La empresa deberá definir indicadores que busquen reflejar fuentes potenciales de riesgos de operación.

- Los resultados de las actividades de monitoreo deben ser incluidos en los informes a la Gerencia General, así como las revisiones de cumplimiento de la Gerencia de Riesgo Operativo.
- La empresa, adaptará alguno de los métodos de indicador para el cálculo del requerimiento de patrimonio efectivo por riesgo operativo de acuerdo a lo dispuesto con la SBS.

En algunos casos, si la empresa cuenta con el Comité de Riesgos muchas de las actividades macro de gestión de riesgos puede ser asumida por el Comité y no por la Gerencia de Riesgo Operativo.

B.2. Políticas relacionadas al apetito y tolerancia por riesgo operativo

- El Comité Gestión Integral de Riesgos/la Gerencia de Riesgo Operativo definirá anualmente el perfil de riesgos de la empresa, la exposición acumulada al riesgo operativo y el nivel de exposición a pérdidas, teniendo en cuenta la complejidad y tamaño de la empresa, las necesidades de patrimonio efectivo.
- El apetito y tolerancia por riesgo operativo se expresa en los productos de la empresa, con el fin de facilitar su entendimiento han sido clasificados según el siguiente cuadro:

Tabla IV.7 Modelo de Tipos de Producto en una empresa financiera

Tipo de Producto	DEFINICIÓN
A	Grupo de Productos A
B	Grupo de Productos B
C	Grupo de Productos C
...	
N	Grupo de Productos N

Fuente: SBS,. Elaboración y adaptación: propia.

Donde Grupo de Productos puede ser la agrupación de los productos siguientes:`

Tarjeta de Crédito, Inversiones en Mercado, Cambio de Divisas, Derivados (forward, swap) y Pagares, Convenios, Tarjeta de Débito, Depósitos de Banca Personal, Créditos Hipotecarios, Descuentos de letras y facturas, Captaciones en Mercado. Créditos Indirectos, Arrendamiento Financiero, Negocio Inmobiliario, Cuenta Corriente PJ, Cartas Fianzas, Switching y Foráneas, canales de atención (Directo, Tiendas y ATM´s), Finanzas Corporativas, Factoring, Depósitos PJ, Servicios de Recaudación, Servicios de Pagos, Servicios de Comercio Exterior y Créditos a Pequeña Empresa, Remesas, Banca Seguros, Préstamo Fácil y Efectivo, Préstamo Vehicular, entre otros.

- El Gerente de Producto es responsable de garantizar que los riesgos operativo es cumplan con aplicar la política de apetito, estos son identificados y valorados dentro de las autoevaluaciones periódicas para los productos y productos nuevos / cambios importantes en el ambiente operativo e informático.
- El apetito por riesgo operativo se manifiesta en las decisiones de aceptar la situación encontrada de exposición al riesgo operativo en el momento de evaluación; sin necesidad de establecer acciones adicionales para mitigarlos. Se considera parte activa del apetito la decisión de reducir la exposición mediante acciones de mitigación.
- Los niveles de autonomía del apetito son expresados como la exposición anual a posibles pérdidas operativo es; y permiten tomar la decisión de aceptar los riesgos asociados a las actividades de un producto y/o línea de negocio, como sigue continuación:

Tabla IV.8 Niveles de Autonomía para Tolerancia a Riesgo

Niveles de Autonomía	Importe de Evento de Pérdida a<b	Importe Anual Acumulado por Perdidas por Niveles de Tipo de Producto				
		A	B	C	...	N
Gerente de Producto	<=a	mA1	mB1	mC1	...	mN1
Gerente de División	>a y <=b	mA2	mB2	mC2	...	mN2
Gerente General	>b	mA3	mB3	mC3	...	mN3

Fuente: SBS,. Elaboración y adaptación: propia.

B.3. Políticas Relacionadas a la Autoevaluación de Riesgos

- La Gerencia de Riesgo Operativo, periódicamente (se recomienda anualmente) deberá preparar y ejecutar un plan de autoevaluación de riesgos y controles en los principales productos asegurando su consistencia con las políticas de apetito y tolerancia al riesgo aprobadas.
- El Gerente de Producto será el responsable de la coherencia, calidad y veracidad de los resultados de la autoevaluación, y así mismo de la gestión de los riesgos identificados de acuerdo a las políticas.
- Los principales aspectos de la gestión de cada producto y los avances y resultados del proceso de autoevaluación de riesgos y controles deberán ser informado a los niveles correspondientes.
- La autoevaluación de riesgo operativo permitirá identificar y valorar los riesgos inherentes a las actividades del producto, por lo cual se deberán identificar los factores claves que podrían generar futuros eventos de pérdida, con la finalidad de reconocer de manera oportuna el perfil de riesgo.

- Los criterios utilizados en las autoevaluaciones para evaluación cualitativa de la efectividad y calidad de los controles y medidas de mitigación, serán definidos y comunicados por la Gerencia de Riesgo Operativo.

B.4. Políticas Relacionadas a la Recolección de Eventos de Pérdida

- Todo evento de pérdida informado al Coordinador de Riesgo Operativo, deberá ser reportado a través del sistema de riesgo operativo (propio en cada entidad).
- Los eventos que sean identificados por áreas de soporte que afecten a los productos y servicios, deberán ser reportados a los Coordinadores de Riesgos y la Gerencia de Riesgo Operativo. En caso no se pueda identificar los productos afectados por el evento de pérdida se comunicará directamente a la Gerencia de Riesgo Operativo, para su análisis.
- Las áreas de soporte deberán asistir a los coordinadores de riesgo e investigadores de eventos en la cuantificación, análisis y sustento de la información de los eventos de pérdida, proporcionándoles toda la documentación necesaria. El monto mínimo para el registro de eventos de pérdida es definido por cada entidad.
- Todo evento que pudiera generar una pérdida directa, deberá documentarse por la Unidad de Negocio responsable del producto,

inclusive en los casos en que el monto de la pérdida fuera recuperado en su totalidad.

- Los eventos de pérdida operativo neta cuyos valores sean mayores a un monto a ser definido por la entidad, deberán ser documentados por la Unidad de Negocio responsable y además, por la Gerencia de Riesgo Operativo, la cual deberá custodiar una copia electrónica idéntica a los expedientes originales, pudiendo ser esta almacenada de forma electrónica o física.
- Los eventos de pérdida relacionados a riesgos operativos, deberán ser asignados a las líneas de negocio de acuerdo a los productos y servicios asociados. En caso una pérdida se relacione a más de un producto, la Gerencia de Riesgo Operativo definirá el producto al cuál se asignará la pérdida, basándose en la mayor relación del evento.
- En caso los eventos de pérdida se asocien a más de un producto o línea de negocio, el impacto será distribuido de manera proporcional al total de las pérdidas registradas en el año, por cada producto o línea vinculada para fines de gestión.
- En caso los eventos de pérdida sean originados por procesos de apoyo no vinculados directamente a los productos del banco; el impacto será distribuido de manera proporcional al total de las pérdidas registradas en el año, por cada uno de los productos para fines de gestión.

- Los eventos de pérdida que ocurran en áreas de soporte deberán ser reportados tanto al Coordinador de Riesgo Operativo correspondiente como a la Gerencia de Riesgo Operativo.
- Los eventos de pérdida relacionados a un canal o a toda la institución deberán ser gestionados a nivel de toda la empresa, siendo la Gerencia de Riesgo Operativo quien defina el área que realizará la investigación y seguimiento del evento.
  - Las pérdidas de riesgo de crédito, cuya causa u origen se relaciona a eventos de riesgo operativo, deben registrarse en la base de eventos de pérdida de riesgo operativo y ser diferenciados en dicha base de datos.
  - Las pérdidas de riesgo de mercado, cuya causa u origen se relacionan a eventos de riesgo operativo deben registrarse como eventos de pérdida de riesgo operativo para todos los fines.
  - Los eventos de pérdida se podrán cerrar en los casos donde ocurra lo siguiente:
    a) El evento no generó perdida efectiva de dinero, siendo que se evitó la salida real del efectivo de la empresa. En este caso no deberá quedar ninguna posibilidad que el dinero sea exigido por un tercero.
    b) El evento generó un perjuicio económico para la empresa y dicho perjuicio es susceptible de ser reflejado en los estados financieros; los recuperos (seguros, indemnizaciones y otras gestiones), han sido agotados por el Banco y se encuentran

contabilizados en cuentas de resultados al igual que las pérdidas.

c) El evento generó un perjuicio económico para la empresa que no es susceptible de reflejo contable, sin embargo se ha cuantificado y bloqueado la posibilidad de futuros impactos económicos o recuperos asociados al evento.

B.5. Políticas Relacionadas a los Planes de Acción

- Todo plan de acción definido deberá estar siempre asociado al menos a un riesgo con exposición no aceptada de acuerdo a las políticas de apetito y tolerancia al riesgo, así como un riesgo podrá estar sujeto a varios planes de acción, a fin de lograr su mitigación.
- Los Gerentes de producto son responsables, de gestionar los planes de acción y los recursos necesarios para su ejecución; en caso un plan de acción constituya un "proyecto" (duración mayor a tres meses), deberá gestionar con la aprobación del nivel de aprobación correspondiente.
- Los Gerentes de producto tienen como plazo para el análisis, evaluación y registro en el sistema de las medidas que se adoptarán para llevar a cabo el plan de acción, este plazo comienza una vez tomada la decisión de mitigar el riesgo y no deberá ser mayor a los plazos definidos por la empresa.

B.6. Políticas Relacionadas a la Definición de Indicadores de Riesgo

- Los Gerentes de productos son responsables del cumplimiento de las políticas de tolerancia al riesgo, para este fin los indicadores de riesgos son herramientas para el seguimiento; el cumplimiento de la tolerancia se realiza en cada indicador al no exceder los límites establecidos en su definición.
- Los Gerentes de producto y Coordinadores de Riesgo Operativo deberán gestionar los procesos de acuerdo a información generada por los indicadores, con la finalidad de garantizar que los riesgos operativos asociados a éstos se encuentren dentro de los límites o se tomen las acciones del caso.
- La Gerencia de Riesgo Operativo y los Gerentes de producto deberán establecer los indicadores de riesgos adecuados para cada proceso; con el fin de monitorear la exposición al riesgo.
- Los productos y procesos donde se identifiquen riesgos operativos, cuya exposición se considere crítica o exceda el monto definido por la entidad y no se establezcan mitigaciones adicionales deberán contar con indicadores de riesgos.
- El Gerente de producto revisará los excesos de límites en la medición de los indicadores; aplicará acciones para su mitigación (planes de acción) en caso sea necesario y de acuerdo a las políticas establecidas para apetito y tolerancia al riesgo.

B.7. Políticas Relacionadas al Lanzamiento de Nuevos Productos y los relacionados en la Gestión de Cambios

- Los Gerentes de producto y coordinadores son responsables de gestionar los riesgos operativos de todos los productos nuevos y cambios importantes en el ambiente operativo o informático; para su implementación es necesario cumplir con aplicar las políticas de apetito y tolerancia.
- La mejora continua de procesos y el diseño de nuevos productos y servicios deberán considerar la evaluación de los aspectos relacionados al riesgo operativo y deberán cumplir con las políticas y lineamientos del presente manual.
- Se consideran lanzamientos de nuevos productos para la evaluación de riesgos operativos, los productos que introducen nuevos riesgos o generen cambios negativos e importantes en el nivel de exposición al riesgo operativo.
- Las políticas del banco no permiten aceptar los riesgos de incumplimiento expreso de las normas de los reguladores bancarios, políticas internas y estándares de operación establecidos para el sistema financiero en el diseño de nuevos productos y cambios significativos en el ambiente operativo e informáticos.
- Se consideran cambios significativos en los procesos operativos, los siguientes:

- Introducción de nuevos riesgos o cambios importantes que afecten negativamente el nivel de exposición al riesgo operativo. Incluye cambios en la forma de realizar las actividades de control.
- Implementación de nuevos canales para los productos (en caso donde no existan en productos semejantes).
- Cambio en las actividades de control que afecten negativamente la segregación de funciones.
- Eliminación de actividades de control.
- Subcontratación significativa de procesos que soporten a productos y/o servicios.
- Proyectos de rediseño de procesos o reingeniería de productos y/o servicios de la empresa.

• Se consideran cambios significativos en el ambiente informático de la empresa, los siguientes:

- Proyectos de tecnología de información (administrados por la Gerencia de Tecnología y/o Banca Electrónica).
- Implementación de nuevas aplicaciones o actualizaciones de versiones con nuevas funcionalidades relacionadas al soporte de los productos y/o servicios del Banco.

• Se consideran cambios de menor magnitud o no significativos que no requieren de la evaluación de riesgos operativos en el ambiente operativo e informático, los siguientes:

- Incrementos de planta.

- Pilotos comerciales o crediticios, sin impacto en procesos o sistemas.
- Cambios en tasas/precios.
- Lanzamiento de producto con características y procesos iguales / semejantes a los existentes.
- Campañas comerciales de productos / relanzamiento comercial de productos sin cambios significativos operativos e informáticos.
- Nuevos servicios sin cambios en el proceso y que utilicen el mismo canal.
- Canales adicionales para un producto ya existente (donde el canal ya existe para productos semejantes)
- Cambios en los sistemas operativos y actualizaciones de los proveedores en las aplicaciones, tareas de mantenimiento y desarrollos menores de sistemas no considerados como proyectos sino como Tareas dentro de la Tipología de Pedidos a Sistemas, de la Gerencia de Tecnología.
- Actividades de desarrollo de sistemas orientadas a solucionar cancelaciones y/o errores que afectan la operativa normal del Banco categorizadas como Urgencias dentro de la Tipología de Pedidos a Sistemas, de la Gerencia de Tecnología.
- Cambios rutinarios en el ambiente informático realizados en los procesos de Tecnología (configuración de servidores, cambios de equipos e infraestructura).

- Los Líderes y Gerentes de Proyectos son los responsables de identificar y mitigar (controlar) los principales riesgos operativos de los proyectos, así como velar porque se cuente con la información mínima para evaluar los riesgos operativos y tecnológicos en la implementación del proyecto.
- Los riesgos asociados a la integridad, consistencia y eficiencia de la información, producto de cambios en procesos y/o aplicaciones críticas, serán mitigados mediante el proceso de pruebas, cuyo cumplimiento es responsabilidad del Administrador del Producto. Lineamientos para la Gestión de Riesgos

C. Lineamientos

C.1. Personas

- La Gerencia General deberá garantizar que la empresa cuente con personal calificado que ofrezca la necesaria experiencia, aptitudes técnicas y acceso a recursos, y que la autoridad del personal encargado de controlar y asegurar el cumplimiento de las políticas para la gestión del riesgo no procede de las unidades que vigila.
- Los procesos de administración de personal, incluyendo su selección, evaluación y retención deberán considerar los valores de transparencia, honestidad, integridad y otros factores, mitigando así los riesgos operativos que puedan originarse por las personas.

- La empresa deberá promover el desarrollo de las habilidades necesarias para garantizar el buen desempeño de los colaboradores.
- Los colaboradores de la empresa desarrollarán sus funciones dentro de la normativa establecida incorporando las políticas y lineamientos de Riesgo Operativo y manteniendo una actitud proactiva en la gestión de los mismos.

C.2. Procesos

- Las Divisiones de la empresa y sus colaboradores deberán tener claramente definidas las responsabilidades y funciones del puesto que desempeñan con una segregación defunciones adecuada para que no se generen conflicto de intereses y minimizar la exposición a riesgos operativos.
- Los procesos deberán contar con las mitigaciones necesarias para los principales riesgos inherentes, que garanticen el cumplimiento de las políticas de apetito y tolerancia al riesgo.
- Para considerar como mitigadores a los controles definidos en los procesos deberán estar definidos formalmente como políticas o procedimientos, específico donde se describa la actividad a realizar, periodicidad y responsable de realizarla.
- Los riesgos asociados a la suspensión de servicios, se gestionarán de acuerdo a las políticas de gestión de la continuidad y a través de los planes de continuidad de negocio establecidos por ésta.

- Los riesgos legales relacionados a los contratos o complejidad de los productos y servicios del banco, se administrarán de acuerdo a los procesos internos para la adquisición de bienes y servicios, así como los procesos de contratación aprobados por el banco.
- Las políticas y lineamientos para definir los servicios de terceros considerados como críticos, se establecerán dentro de la gestión de la continuidad.
- Los servicios críticos provistos por terceros no considerados como sub contrataciones significativas, deberán considerar en sus contratos los aspectos relacionados a los riesgos operativos que podrían originarse por la prestación de los mismos.

C.3. Tecnología de Información

- La prudente gestión de los riesgos asociados a la seguridad de información, sea dministran a través de las políticas y procedimientos para la Gestión de la Seguridad de Información.
- Los riesgos asociados a la tecnología de información cuya materialización conlleve pérdidas operativos atribuibles a un producto y/o proceso en particular forman parte del riesgo operativo y por tanto su gestión es responsabilidad del Gerente de producto.
- Los riesgos asociados a la tecnología de información cuya materialización conlleve pérdidas operativas no relacionados a un producto y/o proceso en particular, son responsabilidad de la

División/Gerencia de Tecnología que administren el proceso afectado.

- Los riesgos asociados a la interrupción de los servicios de tecnología, serán administrados de acuerdo a las políticas de gestión de la continuidad de negocio.

C.4. Eventos Externos

- El área de Seguridad de Información establecerá las condiciones mínimas a cumplir por los proveedores para asegurar el cumplimiento de las políticas y lineamientos de seguridad de información en la subcontratación significativa.
- Los eventos de la naturaleza, atentados, y otros desastres razonablemente factibles de ocurrencia, deberán mitigarse, en caso un análisis costo/beneficio lo amerite, a través del uso de Seguros, Plan de Continuidad de Negocios, o combinación de éstos según sea la necesidad de la empresa.
- Los contratos de seguros de los activos de la empresa y de los activos de sus clientes que respalden operaciones, se establecer se establecerán de acuerdo a los criterios y niveles de cobertura definidos por la División/Gerencia de Seguros

4.2.3. (M.1.3) Establecer una metodología para la Gestión del Riesgo Operativo

Para efectos de la tesis este punto está comprendido por todo el Capítulo IV descrito en este documento.

4.3. (M.2) METODOLOGÍA CUALITATIVA

El enfoque cualitativo tiene por objeto, la identificación, control y la gestión de los riesgos operativos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de procesos críticos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos. Considerar que esta parte de la metodología considera el siguiente marco legal:

- Resolución SBS N° 037-2008 de fecha 10.01.2008 que aprueba el Reglamento de Gestión Integral de Riesgos.
- Resolución SBS No 2116 – 2009 de fecha 02.04.2009 que aprueba el Reglamento para la Gestión del Riesgo Operativo (ver Anexo A2)
- Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.- Ley 26702 y sus modificatorias.

4.3.1. (M.2.1) Autoevaluación de Riesgos

Con ayuda de la Gerencia de Riesgo Operacional, las autoevaluaciones son llevadas por las propias gerencias de producto o unidades de negocio y tiene por finalidad tratar de evaluar el grado de adecuación sobre el control de riesgo y determinar los puntos de

control que se debe de mejorar, en esta metodología se plantea un enfoque mixto en el que las herramientas de mapas de riesgos que permite advertir donde están las debilidades críticas donde es necesario actuar en forma prioritaria.

Este enfoque considera como base los procesos de una gerencia de producto y siguen un esquema como el siguiente:

Tabla IV.9 Ejemplo de Información de Riesgo en una Empresa en Base a Procesos

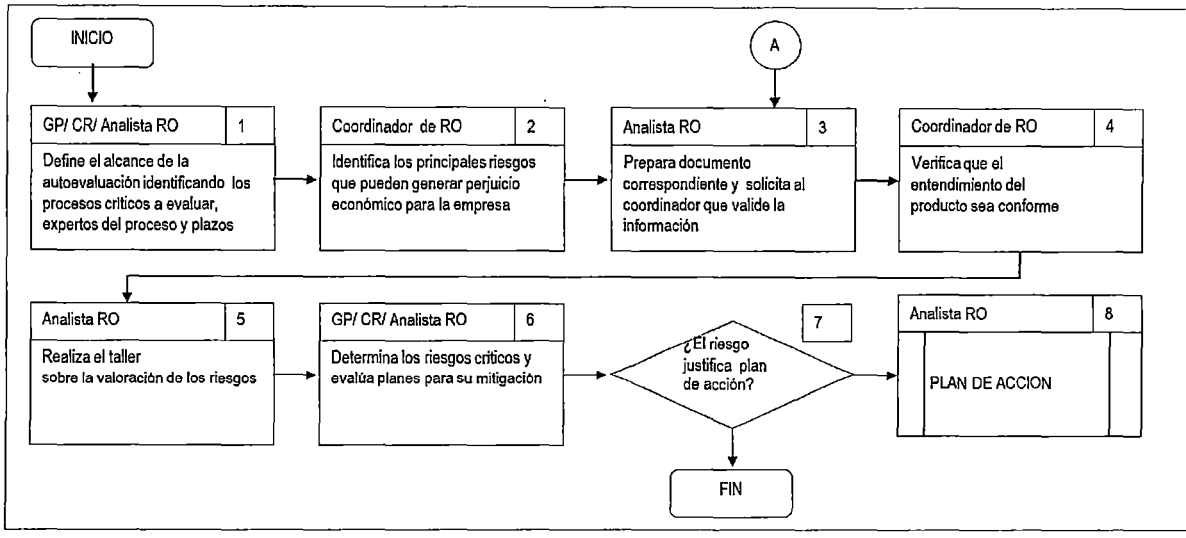
Producto	Proceso	Actividad	Riesgo	Control	Riesgo Residual	Plan de Acción	Responsable	Previsto
Producto A	Proceso A	Tarea 1	Riesgo 1	Control 1	Bajo	N.A.		
				Control 2	Medio	abc...	Carlos	jul-12
			Riesgo 2	Control 3	Alto	N.A.		
				Control 4	Medio	abc...	Ernesto	jul-12
....	....	....	....	....	....	....	....	....
Producto X	Proceso Y	Tarea N	Riesgo 1	Control 1	Alto	abc..	Sofía	jun-12
				Control 2	Medio	abc...	Vicente	jul-12
			Riesgo 2	Control 3	Alto	N.A.		
				Control 4	Medio	abc...	Ernesto	jul-12

Fuente: Curso Taller sobre de Base de Datos de Eventos por Riesgos Operativos, SBS

Elaboración: propia

Otro enfoque a considerar podría ser aquel basado en unidades de negocio, este enfoque tiene como críticas que estas manejan cierto nivel de discrecionalidad, si ese es el caso, auditoría puede ayudar en la labor.

Figura IV.4 Procedimiento para la Autoevaluación de Riesgos



Fuente: El Riesgo Operacional, Metodologías para su medición y control, Enrique Jiménez Rodríguez

Elaboración: propia.

Tabla IV.10 Principales Definiciones para la gestión de Riesgo Operativo

Nro	Responsable	Descripción
1	**Gerente de Producto/ Coordinador de Riesgo/ Analista de Riesgo Operativo**	Define el alcance de la autoevaluación identificando lo siguiente: • Procesos críticos a evaluar • Expertos de los procesos críticos a consultar. • Plazos para realizar el proceso de autoevaluación En este sentido es recomendable utilizar un mapa de procesos actualizado
2	**Coordinador de Riesgo**	Revisa los productos y procesos críticos a evaluarse e identifica los principales riesgos que pueden generar perjuicios económicos para la empresa. La identificación de los riesgos está basada en la información existente de normativa y haciendo un levantamiento en entrevistas con los Expertos del Producto, cuando el caso lo requiere.
3	**Analista de Riesgo Operativo**	Prepara la documentación correspondiente al entendimiento del producto y solicita al Coordinador de Riesgo, validar lo siguiente: • Relación de los procesos que soportan al producto. • Diagramas de flujo de los procesos críticos. • Relación de riesgos asociados a los procesos a evaluar (similar a la tabla 6.3) La documentación del entendimiento del producto se elabora en base a la información de la normativa vigente que lo soporta y de ser el caso, mediante entrevistas con los Expertos del Producto
4	**Coordinador de Riesgo**	Verifica que la documentación del entendimiento del producto refleje la situación real del mismo y que se hayan identificado los riesgos críticos del proceso en evaluación. Evidencia: Conformidad

Nro	Responsable	Descripción
		emitida del coordinador
5	**Analista de Riesgo Operativo**	Realiza el taller sobre la evaluación de los riesgos, esto consiste en Capacitar al coordinador de riesgos y colaboradores que participaran sobre el llenado del cuestionario que incluya información sobre la metodología y conceptos, entre otros temas.
6	**Gerente de Producto / Analista de Riesgo Operativo**	Se realiza la identificación y validación de los riesgos operacionales. • Revisar que la descripción se ajuste a riesgos operacionales. • Clasifica los riesgos identificados para el producto. • Registra la información de los riesgos • Se realiza el mapeo del producto en evaluación • Se realiza la evaluación del riesgo Se Verifica la criticidad de los riesgos identificados y si éstos se encuentran dentro de los límites establecidos o si cuentan con la aprobación de los niveles establecidos según las políticas Se evalúa los planes de mitigación Nota: Los niveles de aprobación de riesgos y límites establecidos se señalan en las Políticas
7	**Analista de Riesgo Operativo**	¿El riesgo justifica la generación de Plan de Acción? Sí, procede con la actividad 8 No, da por terminado el proceso
8	**Analista de Riesgo Operativo**	Procede según lo establecido en el procedimiento de Planes de Acción

Fuente y Elaboración: propia

A. (M.2.1.1.) Identificar los Riesgos

A.1. (M.2.1.1.1) Mapear los Procesos

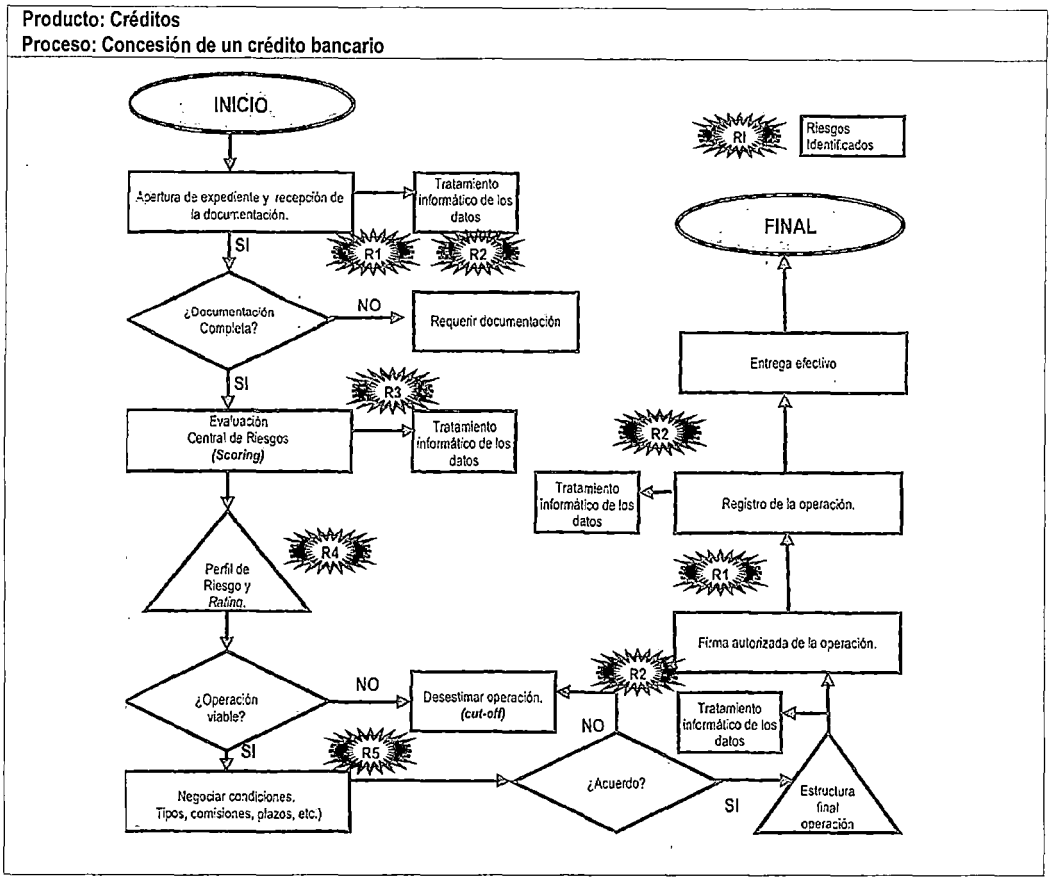
La autoevaluación de riesgos considera como inputs los procesos del negocio, para ello es necesario contar con un mapa de procesos, esto es contar con una clasificación de procesos (desde macro procesos a micro procesos) que puede variar debido al crecimiento en servicios y productos financieros de la Entidad Financiera, el responsable de mantener el mapa de Procesos es la Gerencia de Planeamiento quien levanta esa información con el Gerente de Producto, dentro de cada macro proceso, deberán estar identificados

los dueños de los procesos, quienes son responsables del desempeño del proceso y cuales son críticos.

A.2. (M.2.1.1.2) Identificar los Puntos Críticos

Considerar que un proceso lo consideramos crítico cuando la ocurrencia de un hecho o incidente sobre este proceso puede dañar: personas, equipos, materiales o ambientes, afecta el normal desarrollo de las operaciones, afecta la calidad del servicio que se entrega a nuestros clientes, afecta negativamente en los costos, provocando un aumento de ellos. Todo mapa de procesos, parte de un flujograma, respecto a dicho diagrama no existe una simbología homogénea, de hecho, existen esquemas distintos, a continuación, teniendo como ejemplo el proceso de Concesión de un Crédito Bancario e identificación de riesgos se opta por una estructura propia.

Figura IV.5 Flujograma del Proceso de Concesión de un Crédito Bancario e Identificación de Riesgos



Fuente y Elaboración: Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez),

A.3. (M.2.1.1.2) Identificación de los Eventos de Riesgo

Así de esta maneta los riesgos identificados pueden resumirse en una tabla como la siguiente:

Tabla IV.11 Ejemplo de Listado de Riesgo y sus Categorías Según Basilea

Riesgo	Descripción	Categoría (Nivel 1 BIS)	Categoría (Nivel 2 BIS)
R1	Falsificación	Fraude Externo	Robo y Fraude
R2	Errores de introducción de datos	Prácticas con clientes, productos y de negocio	Productos defectuosos

R3	Ausencia de investigación a clientes conforme a directrices	Prácticas con clientes, productos y de negocio	Selección, Patrocinio y exposición
R4	Comunicación defectuosa	Ejecución, entrega y gestión de procesos	Captura de transacciones, ejecución y mantenimiento
R5	Prácticas inadecuadas de gestión	Prácticas con clientes, productos y de negocio	Prácticas inadecuadas de negociación

Fuente: Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez),

Elaboración: Propia

B. (M.2.1.2) Medir y Evaluar los Riesgos

B.1. (M.2.1.2.1) Establecer Criterios de Evaluación

La evaluación de Riesgo Operativo se realiza a través de dos perspectivas: Impacto y Probabilidad, establecer los criterios de evaluación tienen que ver con la fijación de parámetros tanto de impacto en términos monetarios así como de probabilidad en términos de porcentaje y mediante el cual se establecen los valores monetarios para cada nivel de rango en ambos casos.

B.2. (M.2.1.2.2) Generar la Matriz de Probabilidad

A sabiendas que la **probabilidad (frecuencia)** es la posibilidad de que un evento dado ocurra, la empresa debe definir los principales criterios para evaluar la probabilidad de un evento de riesgo operativo, siendo estos los siguientes:

Tabla IV.12 Criterios de Probabilidad

PROBABILIDAD					
NIVEL	**RANGO**	**ESTADÍSTICA (Ejemplo)**	**DESCRIPCIÓN**	**A NIVEL DE ENTIDAD (Ejemplo)**	**A NIVEL DE PROCESO (Ejemplo)**
5	Muy Alta	>75%	El evento ocurre frecuentemente en nuestra entidad.	Una vez o más al año.	Una vez por hora.
4	Alta	50% a 75%	Un evento así ha ocurrido varias veces en nuestra entidad.	Una vez cada 3 años.	Una vez por día.
3	Moderada	10% a 50%	Un evento así ocurrió en nuestra entidad una vez.	Una vez cada 10 años.	Una vez por semana
2	Baja	1 % a 10%	El evento ocurrió alguna vez en otra entidad, pero nunca en la nuestra.	Una vez cada 30 años.	Una vez por mes
1	Muy Baja	< 1%	El evento es teóricamente posible pero nunca ha ocurrido en nuestra entidad ni en otras similares.	Una vez cada 100 años.	Una vez por año

Fuente: Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez),

Elaboración: Propia

B.3. (M.2.1.2.3) Generar la Matriz de Severidad

A sabiendas que la **severidad (impacto)** es la magnitud de la consecuencia si se materializa el riesgo, la empresa debe definir los principales criterios para evaluar el impacto de un evento de riesgo operativo, siendo estos los siguientes:

Tabla IV.13 Criterios de Impacto

IMPORTANCIA			
NIVEL	**RANGO**	**FINANCIERO (Ejemplo)**	**DESCRIPCION**
5	CATASTRÓFICO (Muy Alta)	> $ 15,000,000	Pérdida catastrófica, inaceptable en el sector, intervención regulatoria y multas, pérdida total del mercado, quiebra de la entidad o pone en peligro su continuidad.
4	MAYOR (Alta)	> $ 500 000 y <= $ 15,000,000	Pérdida o daño mayor, inaceptable en el sector, cobertura de medios locales y nacionales sostenida, investigación formal del regulador y multas(SBS), pérdidas elevadas del mercado.
3	MODERADO	> $ 40 000 y <= $ 500,000	Pérdida significativa, inusual del sector, reclamos de clientes a gran escala, indagaciones del regulador (SBS), potencialmente pérdida del mercado.
2	MENOR (Baja)	> $ 5,000 y <= $ 40,000	Pérdida o daño menor, aceptable en el sector, aumentan las quejas de los clientes, no hay impacto negativo en el negocio.
1	INSIGNIFICANTE (Muy Baja)	Nivel entidad pérdida > = $1 y <=$5,000	Pérdida o daño insignificante; aceptable en el sector, no aumentan las quejas de los clientes.

Fuente: Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez), Elaboración: Propia

Sin embargo es importante definir que estos criterios no son mandatorios, la evaluación a nivel de procesos y sub procesos básicamente estará sustentada en el buen criterio de cada uno de los dueños de los procesos, que son quienes conocen directamente su probabilidad y su impacto.

C. (M.2.1. 3) Valoración de los Riesgos

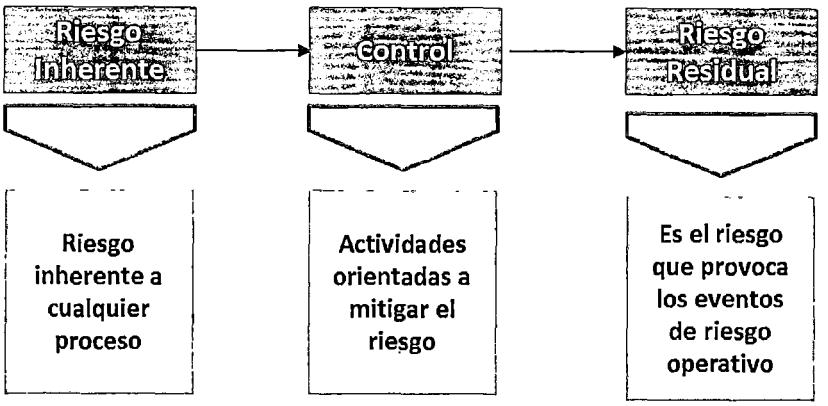
C.1. (M.2.1.3.1 y M.2.1.3.2) Riesgo Inherente y Riesgo Residual

Los riesgos operativos se clasifican en dos categorías:

- **Riesgo Inherente**, es aquel al que se enfrenta la organización en ausencia de acciones de la Gerencia para modificar su probabilidad y su impacto.

- **Riesgo Residual,** es aquel que permanece después de que la Gerencia desarrolle sus respuestas a los riesgos.

Figura IV.6 Riesgo Inherente y Riesgo Residual



Fuente y Elaboración: Curso Taller sobre de Base de Datos de Eventos por Riesgos Operativos, SBS

Una vez relativizado en riesgo en función de la cobertura establecida, se realiza una nueva clasificación de riesgos – más afinada – en la que la valoración resultaría la combinación de tres factores: impacto, frecuencia y controles implantados. A este clasificación se le denominará Nivel de Riesgo y ahora se ordenaría en cuatro rangos:

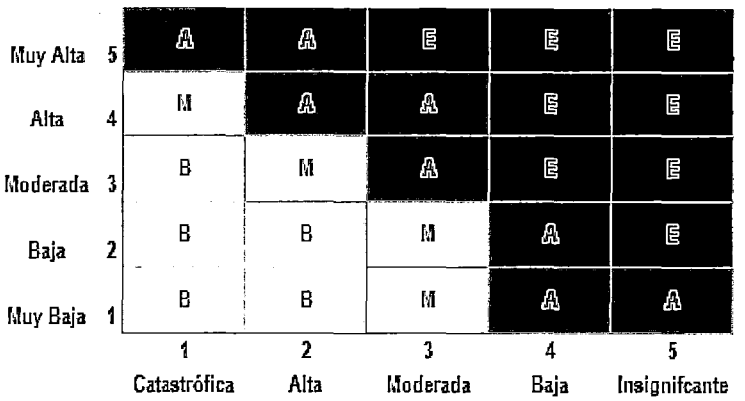
$$NR = f(I,P,C)$$

	Extremo (E):	Conlleva acción inmediata
	Alto (A) :	Requiere atención de la alta dirección
	Medio (M)	Aceptable, debe ser controlado en procedimientos normales
	Bajo (B)	Se gestiona con procedimientos rutinarios, riesgo significante

C.2. (M.2.1.3.3) Elaborar la Matriz de Riesgos Operacionales

La nueva jerarquía se extrapola en una matriz de riesgos que nos permite visualizar, según la posición que ocupe el riesgo en la misma.

Tabla IV.14 Esquema de Clasificación del Niveles de Riesgo



Fuente: COSO.

Para clarificar esta herramienta se retoma al Flujograma del Proceso de Concesión de un Crédito Bancario e Identificación de Riesgos, aquí se valora el riesgo con la conjunción de datos de control para generar la clasificación de riesgo residual.

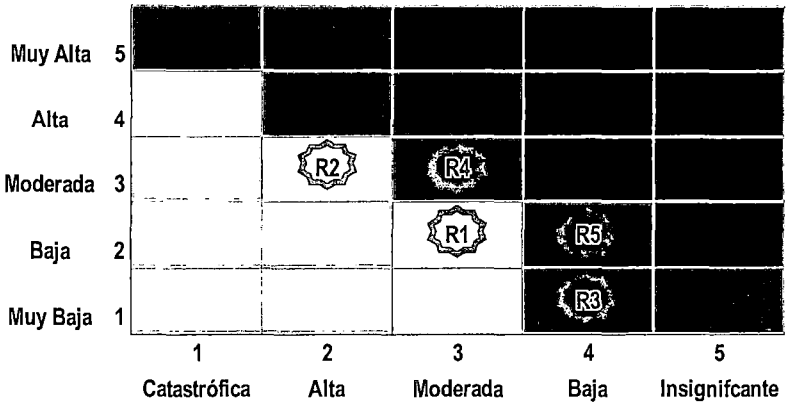
Tabla IV.15 Ejemplo de Clasificación de Riesgo Residual

Riesgo	Descripción	Impacto (1-5)	Frecuencia (1-5)	Riesgo
R1	Falsificación	3	2	MODERADO
R2	Errores de introducción de datos	2	3	MODERADO
R3	Ausencia de investigación a clientes conforme a directrices	4	1	ALTO
R4	Comunicación defectuosa	3	3	ALTO
R5	Prácticas inadecuadas de gestión	4	2	ALTO

Fuente: Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez), Elaboración: Propia

Una vez ajustado el riesgo residual de cada factor, para obtener una perspectiva gráfica de la criticidad de estos, se extrapola el cálculo realizado a la matriz frecuencia/impacto en la siguiente figura:

Tabla IV.16 Matriz de Riesgo Operacionales



Fuente: Riesgo Operacional, metodologías para su medición y control (Jimenez Rodriguez), Elaboración: Propia

C.3. (M.2.1.3.4) Elaborar el Mapa de Riesgos Operacional

Para concluir el desarrollo del mapa de riesgos se agregan los factores identificados en cada proceso por categoría de riesgo operacional. finalizado este proceso habremos obtenido la exposición para cada una de las áreas y tipos de riesgo, para llevar a cabo esta operación no existe una metodología estandarizada, por lo que se propone un ejemplo:

- Si el 25% de los factores de riesgo son evaluados como riesgo alto, el tipo de riesgo analizado se evalúa en conjunto como riesgo alto; si no se cumple esta condición se evalúa el siguiente intervalo.

- Si los factores de riesgo evaluados como riesgo alto o medio alto, son más del 25%, el tipo de riesgo analizado se evalúa en conjunto como riesgo medio alto; si no se cumple esta condición se evalúa el siguiente intervalo.
- Si los factores de riesgo evaluados como riesgo alto, medio alto o medio, son más del 50%, el tipo de riesgo analizado se evalúa en conjunto como riesgo medio
- Si no se han cumplido ninguna de las condiciones anteriores el tipo de riesgo analizado se evalúa en conjunto como riesgo bajo.

Tabla IV.17 Mapa de Riesgo Operacional

Area (producto)	Riesgos						
	Fraude interno	Fraude externo	Relaciones laborales y seguridad en el puesto de trabajo	Clientes, productos y prácticas empresariales	Daños a activos materiales	Interrupción del negocio y fallos en los sistemas	Ejecución, entrega y gestión de procesos
Área 1	■	■	■	■	■		
Área 2	■			■			
Área 3			■				■
Área 4	■					■	
Área 5			■			■	■
...							
Área n	■		■		■	■	

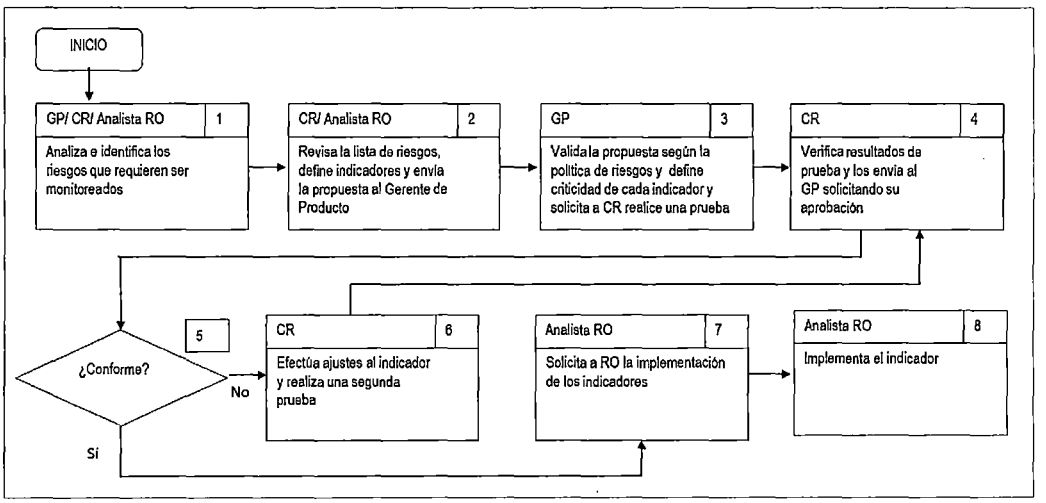
Fuente: La gestión de Riesgo Operacional, de la teoría a la Aplicación (Ana Fernández Laviada), Elaboración: Propia

C.4. (M.2.1.4) Monitorear

C.4.1. (M.2.1.4.1) Definir Indicadores de Riesgo

Los indicadores de riesgo operación funcionarían como un termómetro del comportamiento del riesgo operacional en la empresa. Los indicadores son variables representativas del funcionamiento de la entidad en aquellos puntos que puedan derivar en pérdidas operacionales, permitiendo la identificación, control y seguimiento del riesgo. A continuación en la Figura IV.7 y la Tabla IV.18 sugiere un procedimiento para la definición de indicadores:

Figura IV.7 Procedimiento para la Definición de Indicadores de Riesgos



Fuente: El Riesgo Operacional, Metodologías para su medición y control, Enrique Jiménez Rodríguez. Elaboración: Propia.

Tabla IV.18 Descripción del Proceso de Identificación de Indicadores

Nro	Responsable	Descripción
1	**Gerente de Producto / Coordinador de Riesgo/ Analista de Riesgo Operativo**	Analiza los riesgos basándose en la información de las siguientes fuentes de información: • Eventos de pérdida • Autoevaluaciones Identifica los riesgos que requieren ser monitoreados y los lista
2	**Coordinador de Riesgo/ Analista de Riesgo Operativo**	Revisa la lista de riesgos y define los indicadores (KRI) a monitorear, especificando lo siguiente: • Mapeo del KRI al Producto respectivo • Información básica del indicador o KRI: Nombre,Descripción, Categoría de Evento y Categoría del Riesgo, entre otros. • Forma y periodicidad para la medición del KRI. • Comunica la propuesta de KRI al Gerente de Producto.
3	**Gerente de Producto / Coordinador de Riesgo Operativo**	Valida que la propuesta de indicadores permita monitorear los riesgos críticos del producto de acuerdo a la política de riesgos de la Empresa. Define con el apoyo del Coordinador de Riesgo y Analista de Riesgo Operativo, los niveles de criticidad por cada KRI (límite superior, límite inferior, nivel de alerta y nivel crítico). Solicita al Coordinador de Riesgo revisar la factibilidad de implementar dichos indicadores.
4	**Coordinador de Riesgo**	Analiza y verifica los indicadores midan efectivamente los riesgos y permitan su gestión. De ser el caso, propone mejoras para cada indicador, las cuales hace llegar tanto al Gerente del Producto como al Analista de Riesgo Operativo, solicitando su conformidad para la implementación. Nota: En caso no estar de acuerdo el análisis se realizará con la gerencia de Riesgo Operativo.
5	**Coordinador de Riesgo**	¿Resultado de indicadores es conforme? Sí, procede con la actividad 7. No, procede con la actividad 6.
6	**Coordinador de Riesgo**	Efectúa ajustes al indicador y validar los cambios efectuados al indicador. Regresa a la actividad 4.
7	**Coordinador de Riesgo**	Solicita la implementación de los indicadores aprobados.
8	**Analista de Riesgo Operativo**	Implementa el indicador

Fuente y Elaboración: propia

Para la definición de los indicadores se sugiere que al Cuadro de Mando en entidades financieras tradicional se incorpore un conjunto de indicadores de riesgo. Para ello, a las cuatro perspectivas tradicionales (pero no necesariamente las únicas) propuestas por Kaplan y Norton (clientes, proceso interno, aprendizaje y crecimiento y financiera) debe sumarse una más referida al riesgo o, alternativamente, incluir indicadores al respecto en las ya existentes, pudiendo identificarlos para las cuatro fuentes de eventos de riesgo citados en Basilea-II. La Tabla IV.19 sugiere algunos indicadores por cada fuente de riesgo.

La presentación de estas variables puede ser heterogénea, dependerá de la herramienta tecnológica que se utilice y de la forma como se ha estructurado el tablero de control. A continuación la Figura IV.8 sugiere una forma de organización de estos indicadores, en la misma se ingresan las líneas de negocio y los diversos riesgos y como se han comportado en un periodo de tiempo.

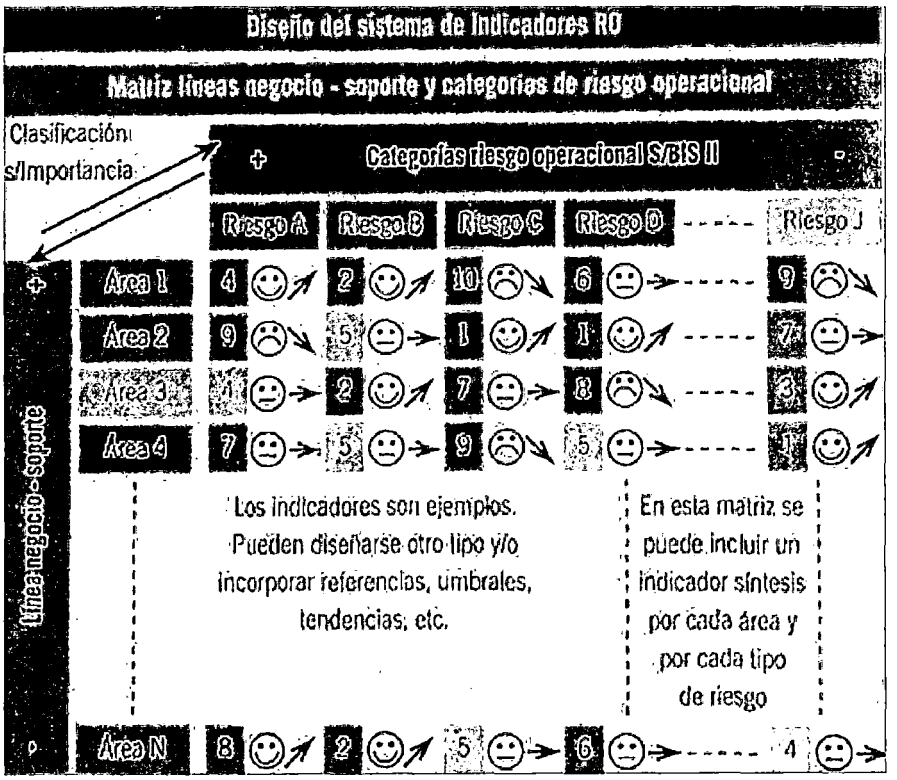
Tabla IV.19 Indicar

Riesgo	Indicador
Procesos	Porcentaje de incidencias
	Segregación funcional
	Manualidad de procesos
	Transacciones no completadas
RR.HH.	Cualificación staff
	Rotación staff
	Procedimiento ante quejas
	Temporalidad staff
	Cualificación de staff
Tecnología	Capacidad procesar

	Fallos en aplicaciones
	Éxito de las transacciones
	Caídas del sistema
	Seguridad en internet
	Denegación del Servicio
	Tiempo del Sistema
	Nivel de recuperación ante fallos
Factores Externos	Planes de Contingencia
	Seguridad de Edificios
	Planes de Evacuación
	Custodia de documentos

Fuente: Riesgo operacional: el nuevo reto para el sector financiero (Navactiva),

Figura IV.8 Procedimiento para la Definición de Indicadores de Riesgos



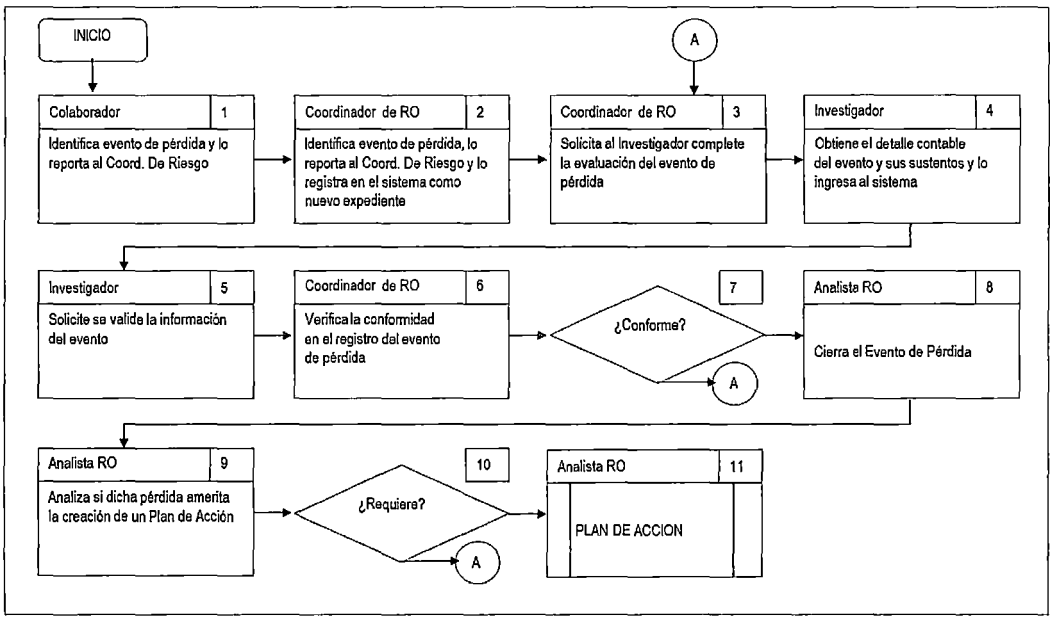
Fuente y Elaboración: Indicadores de Riesgo (Manuel Rodriguez López, José Pedro Arranz Alamo).

4.3.2. (M.2.2) Registro de Eventos de Pérdida de Riesgo Operacional

Se cuantifican las pérdidas de eventos de riesgo operativo que ya se han materializado, para lo cual, se deberán registrar usando un sistema informático que se haya implementado para tal efecto y la recolección de los eventos deberán estar ceñidas estrictamente a las políticas de registro de eventos de pérdida tal como lo señala el punto "4.3.4. Políticas Relacionadas a la Recolección de Eventos de Pérdida"

Un procedimiento en detalle para realizar de registro de pérdidas es descrito en la figura 5.7 y tabla 5.18 siguientes:

Figura IV.9 Procedimiento para el Registro de Pérdidas



Fuente y Elaboración: El Riesgo Operacional, Metodologías para su medición y control, Enrique Jiménez Rodríguez

Tabla IV.20 Descripción del Proceso de Registro de Pérdidas

Nro	Responsable	Descripción
1	**Colaborador Personal Clave**	Identifica un posible evento de pérdida y lo reporta al Coordinador de Riesgo del respectivo producto, una copia del evento llega a la Gerencia de Riesgos , la información a contemplar deberá considerar: • Proceso • Fecha de ocurrencia • Nombre del Evento • Descripción del Evento En caso se presenten dudas respecto a la validez de un evento de pérdida, el Colaborador podrá realizar sus consultas directamente la Gerencia de Riesgo Operativo
2	**Coordinador de Riesgo Riesgo**	Revisa las características del evento y basándose en las Pautas para el Reconocimiento de Eventos de Pérdida (Anexo 6) valida que el evento corresponda a un caso de riesgo operacional. Se registra en el Sistema el evento abre el expediente electrónico del nuevo evento de pérdida relacionándolo al mapeo del producto que está afectando. Completa la siguiente información básica del evento: • Nombre del evento de pérdida • Descripción del evento de pérdida • Investigador de Eventos • Fecha de identificación Para el caso que no corresponda y lo reporta al Coordinador de Riesgo del respectivo producto, una copia del evento llega a la Gerencia de Riesgos. Evidencia: Reporte o registro del Evento de pérdida.
3	**Coordinador de Riesgo**	Remite el evento de pérdida al Investigador de Eventos designado para que complete la evaluación del caso.
4	**Investigador de Eventos**	Recibe el requerimiento de información y coordina para obtener el detalle del evento de pérdida con las distintas áreas involucradas así como a través de consultas a los aplicativos correspondientes. La presente actividad implica realizar las siguientes acciones: • Valorar la pérdida total. • Valorar la pérdida directa. • Clasificar el evento según la categoría a la que pertenece, basándose en el cuadro de Tipos de Eventos de Pérdida (Anexo 7) • Clasificar el evento de pérdida según la causa que lo originó, basándose en el cuadro de Categorías de Riesgo (Anexo 8) • Identificar los gastos asociados. • Identificar las fechas críticas asociadas al evento. • Identificar si se produjeron recuperaciones relacionadas al evento. Luego de contar con la información contable del evento

Nro	Responsable	Descripción
		de pérdida, registra la siguiente información: • Cuenta • Cuentas relacionadas • Gastos asociados • Fechas asociadas • Recuperaciones asociadas Procede a relacionar los documentos de sustento al respectivo evento de pérdida al cual soportan, utilizando la opción "adjuntar documentos" donde se ubica el nombre del archivo cargado en Reveleus, y luego, se graba la actualización del evento de pérdida. Nota: El registro de cada recuperación en el sistema se dará de forma independiente, esto significa, que a medida que se vayan obteniendo recuperos, éstos se irán registrando dentro de la información del evento de pérdida hasta que se cierre.
5	**Investigador de Eventos**	Solicita al Coordinador de Riesgo validar y aprobar la información del evento de pérdida.
6	**Coordinador de Riesgo**	Verifica que el evento de pérdida se encuentre debidamente registrado, validando: • La información relacionada a la descripción, cuentas, gastos y fechas asociadas al evento. • La clasificación ingresada para el evento de pérdida. • Que los documentos que sustenten el evento de pérdida solventen la información mostrada. • Que se hayan registrado las recuperaciones asociadas al evento, de ser el caso. Evidencia: Solicitud de aprobación dirigida al Analista de Riesgo Operacional
7	**Coordinador de Riesgo**	¿Información conforme? Sí, procede con la actividad 8. No, regresa a la actividad 3
8	**Analista de Riesgo Operativo**	Verifica que el evento de pérdida se encuentre "cerrado", según las políticas de riesgos del presente manual. • La información está completa • Sustentos • Clasificación
9	**Analista de Riesgo Operativo**	Analiza si la criticidad del evento de perdida justifica la creación de un Plan de Acción.
10	**Analista de Riesgo Operativo**	¿Pérdida requiere Plan de acción? Sí, procede con la actividad 11. No, da por terminado el proceso
11	**Analista de Riesgo Operativo**	Procede según lo establecido en el procedimiento de Planes de Acción

Fuente y Elaboración: propia

Si bien se ha detallado el procedimiento en detalle considerar que éste puede variar, sin embargo hay pasos que no se deben de dejar de pasar como son los siguientes:

A. (M.2.2.1) Establecer pautas de reconocimiento de eventos de pérdida

Para reconocer si un evento corresponde a un evento de riesgo operacional, es necesario que se establezcan pautas para el reconocimiento de eventos de pérdida, para ello se deben de basar en la información del Anexo 6 "Pautas para el Reconocimiento de Eventos de Pérdida" el cual permite valida que el evento corresponda a un caso de riesgo operacional.

B. (M.2.2.2) Identificar, clasificar el evento de Pérdida

Establecido las pautas y validada la correspondencia de que un evento es de riesgo operacional, el siguiente paso es identificar y clasificar el evento de pérdida, para ello se deben de basar en la información del Anexo 7 "A7. Tipos de Eventos de Pérdida" y A8. "Categorías de Riesgo Operacional".

C. (M.2.2.2) Guardar la información en la Base de Datos de Evento de Pérdida

Se tiene que considerar que la Base de Datos de Eventos de Pérdida es un requisito de la Superintendencia quien en los próximos años plantea la creación de una Central de Riesgos de Eventos de Pérdida, por ello es

necesario plantear un esquema de registro de información. Para ello, se recomienda que el registro de la información se realice empleando un sistema informático y cuyo formulario debiera tener al menos la información del evento así como su contraparte contable, une ejemplo de que campos deberá tener el sistema de registro se muestran en el ejemplo siguiente:

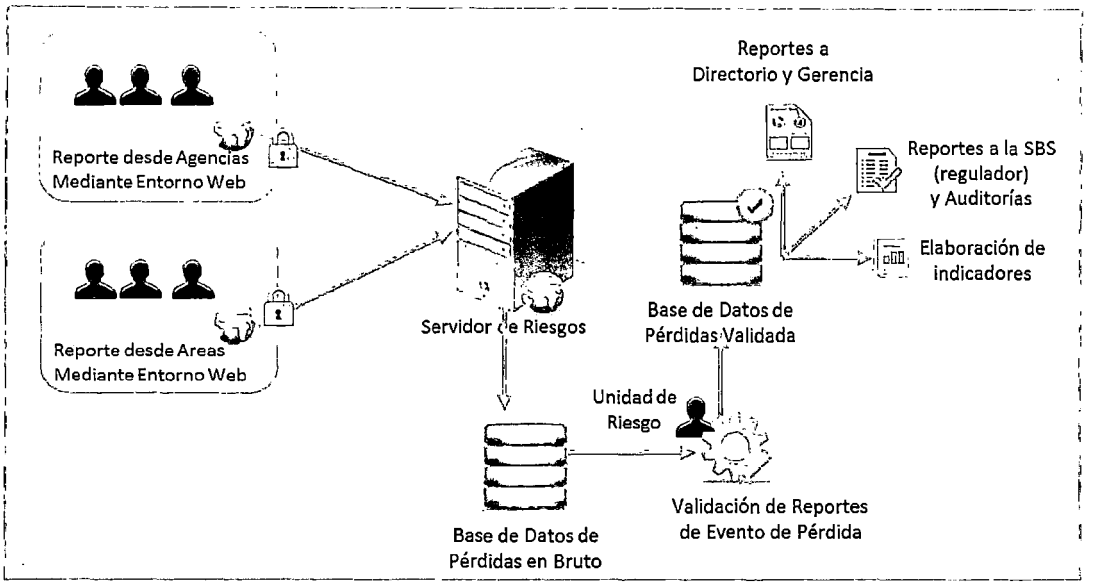
Figura IV.10 Procedimiento para el Registro de Pérdidas

Entidad Legal	Banco XXX						
Unidad	Banca Minorista					Nro de Evento	24/04/1907
SubUnidad	Red Oficinas					Fecha de Alta	15/06/2011
Proceso (N1)	RRHH					Proceso (N2)	Nóminas
Producto (N1)	N/A					Producto (N2)	NA
Clase de RO (N1)	Ejecución, entrega y gestión de procesos					Clase de RO (N2)	Error Humano
Referencia	247/10	Contabilización	40770			Ocurrencia	15/05/2011
Tipo de Evento		Ref Mutiple	NA			Descubrimiento	15/04/2011
Importe	1,000,000		Cuenta	123456		Causa 1	Error humano
Importe Recuperado	200,000		Cuenta	9955		Causa 2	Falta de Capacitación
Recuperado por Seguro	0		Cuenta	NA		Causa 3	NA
Descripción Breve	error de cálculo					Riesgo de Crédito	N
Observaciones	Error en el cálculo de la retención de beneficios en especie practicada por el CAR						
Factor de Riesgo Identificado previamente			Conforme	S		Abierto/Cerrado	C
Categoria Nivel I	Ejecución de Procesos				Categoria Nivel	Ejecución de Procesos	
Frecuencia Ajustada			Conforme	S		Evento Externo	N

Fuente y Elaboración: Curso Taller sobre de Base de Datos de Eventos por Riesgos Operativos, SBS,

Adicionalmente, es necesario tener en consideración que además del sistema de registro debiera existir un sistema o mecanismo por el cual se captura los eventos de pérdida desde las agencias y áreas, hasta su validación por la Gerencia de Riesgos y los reportes que se envían al Directorio, la Gerencia, el órgano supervisor y el órgano de control. La figura IV.11 plantea un modelo de flujo de información mediante el cual viaja la información relacionada a los eventos de pérdida de riesgo operacional.

Figura IV.11 Flujo de Información



Fuente: Gráficos e Íconos de Google Images y Elaboración: Propia

Por otro lado, es necesario plantear algunas consideraciones adicionales para realizar la estimación de las pérdidas, que dependerá de caso:

- En el caso de eventos con pérdidas múltiples, la Entidad Financiera podrá registrar la información mínima requerida por cada pérdida, y se agruparán tomando en cuenta el mismo evento que las originó, al cual se le debe haber asignado un código.
- También se podrá registrar información parcial de un evento, en tanto se obtengan los demás datos requeridos, como es el caso de las recuperaciones que se dan posteriormente a ocurrido el evento.
- Un evento podrá estar asociado a más de una línea de negocio.
- El monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos es de 3,000 nuevos soles para los bancos, otros tipos de entidades tienen como monto mínimo 1,000 nuevos

soles para el resto de empresas Se debe tomar en cuenta que la SBS podrá actualizar el monto mínimo definido por medio de Circular.

- El área de Contabilidad, debe reportar como pérdida por riesgo operativo los montos y detalle de las cuentas 271202 Provisiones para litigios y demandas, y la 271209 otras provisiones, dado que estas cuentas pertenecen al gasto y afectan los resultados del mes. En caso haya alguna reversión de esta provisión que afecta resultados, se considerará como una recuperación, en el mes que sea reportado.
- En lo que se refiere al área de Seguridad y Continuidad, ésta deberá enviar la documentación de las investigaciones efectuadas respecto de eventos de pérdida que afectan la seguridad y continuidad de las operaciones. Es importante indicar que la documentación a presentar por esta área, deberá dar importancia no solo a eventos con pérdida monetaria, sino también a eventos que aún no habiendo significado una pérdida monetaria real, si se ha visto comprometida la confidencialidad de la información de nuestros clientes, la continuidad de las operaciones en el centro de cómputo de principal y en el alterno, la continuidad de las operaciones en una agencia por más de un día, el intento de fraude ya sea este efectuado por personal interno, externo o por una combinación de ambos.
- El área legal, deberá enviar un informe con la documentación sustentatoria de los juicios perdidos por la institución en ese un

periodo establecido, si los hubiera, así mismo deberá incluir un resumen de las costas y gastos incurridos detallando cada uno de ellos en cada caso.

4.4. (M.3) METODOLOGÍA CUANTITATIVA: ENFOQUE DE BASILEA II

El enfoque cuantitativo tiene por objeto describir la gestión de riesgos operativos en una entidad financiera desde el punto de vista cuantitativo el cual tiene como finalidad calcular el requerimiento de capital teniendo como base los principios del Nuevo Acuerdo de Capitales Basilea II, así como la normativa local asociada y emitida por la SBS, para ello toda empresa deberá considerar que esta parte de la metodología considera el siguiente marco legal:

- Resolución SBS N° 037-2008 de fecha 10.01.2008 que aprueba el Reglamento de Gestión Integral de Riesgos.
- Resolución SBS No 2115 – 2009 de fecha 02.04.2009 que aprueba el Reglamento para el Requerimiento de Patrimonio Efectivo Por Riesgo Operacional (ver Anexo 1).
- Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.- Ley 26702 y sus modificatorias.

4.4.1. (M.3.1) Identificar los Métodos de cálculo del patrimonio efectivo por riesgo operacional.

Las empresas deberán destinar patrimonio efectivo para cubrir el riesgo operacional que enfrentan. El Reglamento establece tres modalidades para la determinación o cálculo del patrimonio efectivo por riesgo operacional, por ello se tendrá que aplicar alguno de los siguientes métodos:

a) ***Método del indicador básico***: Este método considera como base de cálculo el margen operacional bruto anualizado de la empresa.

b) ***Método estándar alternativo***: Este método considera como base de cálculo, una combinación de margen bruto y saldos de créditos, sobre la base de la identificación de 6 líneas de negocios de la empresa.

c) ***Métodos avanzados***: Este método permite que la empresa determine el procedimiento apropiado para establecer el requerimiento de patrimonio efectivo por riesgo operacional. Básicamente se aplica a empresas de gran tamaño y que cuentan con herramientas eficientes para la identificación y mitigación del riesgo operacional.

Asimismo, para la aplicación de los métodos b y c será necesario contar con autorización previa y expresa de la SBS, para ello, previamente deberán cumplirse los requisitos que dicho organismo exige.

Los métodos descritos a continuación para fines de entendimiento es una adapatación al contenido de la norma.

4.4.2. (M.3.2) Analizar los Requisitos y Condiciones de Implementación de cada método.

Las condiciones de implementación de cada método son los siguientes:

A. Método Del Indicador Básico

Para este método las entidades no necesitan cumplir ningún tipo de exigencia para calificar a este nivel, no requiere autorización de la SBS, aunque se les insta a cumplir con las llamadas buenas prácticas de gestión de riesgo operativo.

B. Método Estándar Alternativo

La elección de este método conlleva el cumplimiento de los siguientes requisitos:

- El Directorio y la Gerencia General deben participar activamente en la gestión del riesgo operativo.
- La empresa debe contar con una función de gestión del riesgo operativo cuyas responsabilidades se encuentren claramente especificadas, y que consideren como mínimo los aspectos señalados en el Reglamento para la Gestión del Riesgo Operativo.
- La entidad financiera debe contar con un programa de capacitación profesional dirigido a perfeccionar los conocimientos, aptitudes y otras competencias del personal especializado en la gestión del riesgo operativo.

- La entidad financiera debe contar con una metodología de gestión del riesgo operativo que sea conceptualmente sólida y que se encuentre implementada en su totalidad.
- La entidad financiera debe contar con recursos suficientes para aplicar su metodología de gestión de riesgo operativo, tanto en sus principales áreas de negocio como en sus áreas de apoyo y de control.
- La entidad financiera debe establecer reportes periódicos sobre su exposición al riesgo operativo, que incluyan las pérdidas importantes ocurridas, dirigidos a las gerencias de las unidades de negocio y de apoyo, gerencia general y al Directorio. La empresa debe establecer procedimientos para tomar acciones apropiadas según la información incluida en dichos reportes.
- La entidad financiera debe establecer procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operativo, y debe establecer políticas para tratar los casos de incumplimiento.
- La entidad financiera debe establecer incentivos monetarios y no monetarios a la apropiada gestión del riesgo operativo, incluidos en el sistema de evaluación de desempeño de la Gerencia y los principales participantes en dicha gestión.
- La entidad financiera debe contar con una base de datos de eventos de pérdida por riesgo operativo, con las características señaladas en la normativa vigente.

- La entidad financiera deberá implementar un sistema de gestión de la continuidad del negocio conforme a la normativa vigente, que tenga como objetivo asegurar un nivel aceptable de operatividad de sus procesos críticos, ante eventos que puedan afectar la continuidad de sus operaciones.
- La entidad financiera deberá contar con un sistema de gestión de la seguridad de la información conforme a la normativa vigente, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información.
- La evaluación de la gestión del riesgo operativo deberá contar con una revisión cuando menos anual, por parte de la Unidad de Auditoría Interna. Estas revisiones deben considerar las actividades de las áreas de negocio y de apoyo, así como la función de gestión del riesgo operativo, de acuerdo a su plan de trabajo.
- La evaluación de la gestión del riesgo operativo deberá contar con una revisión independiente por parte de una Sociedad de Auditoría Externa, al menos cada tres años. El informe independiente deberá ser realizado por una empresa auditora distinta o un equipo completamente distinto del que emitió el informe anual de evaluación de los estados financieros, sujetándose a las disposiciones de rotación conforme con el reglamento de auditoria externa.

C. Requisitos mínimos para el uso de métodos avanzados

Las entidades financieras que deseen emplear los métodos avanzados deberán cumplir con los requisitos cualitativos y cuantitativos descritos en los artículos 16° y 17° del Reglamento para el Requerimiento de Patrimonio Efectivo Por Riesgo Operacional.

C.1. Requisitos cualitativos

Las empresas deberán contar con los siguientes estándares cualitativos antes de realizar el cálculo del requerimiento de patrimonio efectivo por riesgo operativo basado en modelos internos:

a) La empresa deberá contar con una unidad especializada para la gestión del riesgo operativo.

b) El sistema de medición del riesgo operativo de la empresa deberá estar integrado a sus procesos habituales de gestión de riesgos. La información que se obtenga de dicho sistema deberá ser utilizada como parte integral del proceso de monitoreo y control del perfil de riesgo operativo de la empresa. En ese sentido, esta información deberá ser incorporada en los reportes sobre riesgos, reportes a la gerencia, la asignación de capital y el análisis de riesgos. La empresa deberá implantar técnicas para asignar capital por riesgo operativo a sus principales líneas de negocio y para establecer incentivos para la mejora de la gestión de estos riesgos en toda la entidad.

c) Deberá existir un reporte cuando menos trimestral sobre las exposiciones al riesgo operativo y la experiencia de pérdidas debidas a este riesgo, dirigido a las gerencias de las unidades de negocio, a la Gerencia General y al Directorio. La empresa deberá contar con procedimientos destinados a adoptar las acciones necesarias según la información contenida en dichos reportes de gerencia.

d) El sistema de gestión del riesgo operativo de la empresa deberá estar bien documentado. La empresa deberá contar con un mecanismo que le permita asegurar el cumplimiento de las políticas, controles y procedimientos internos referidos a la gestión del riesgo operativo, que deben estar documentados, y deberá establecer políticas para el tratamiento de los aspectos que no se cumplan.

e) Como parte de la revisión requerida a la Unidad de Auditoría Interna y a una Sociedad de Auditoría Externa, referida a las políticas y procedimientos empleados por la empresa para la gestión del riesgo operativo, debe incluirse una evaluación del sistema interno empleado por la empresa para la medición de este riesgo.

f) La revisión del sistema de medición del riesgo operativo que lleven a cabo los auditores externos deberá verificar que los procesos de validación interna operen de manera satisfactoria y

que el flujo y el procesamiento de datos asociados al sistema de medición del riesgo sean transparentes y accesibles.

g) En el caso de empresas con casa matriz en el exterior, la empresa deberá contar con la no objeción del supervisor bancario del país donde se ubica dicha casa matriz, respecto a la aplicación del método avanzado en la empresa.

h) Otros que determine la Superintendencia.

C.2. Requisitos cuantitativos

Los métodos avanzados utilizados para el cálculo del requerimiento de patrimonio efectivo por riesgo operativo deberán contar con los siguientes criterios cuantitativos mínimos:

C.2.1. Criterio de solidez

La empresa deberá ser capaz de demostrar que el método avanzado utilizado identifica eventos de pérdida situados en las colas de la distribución de probabilidad y que generan graves pérdidas. Con independencia del método utilizado, la empresa deberá demostrar que su medida del riesgo operativo satisface un criterio de solidez comparable a un intervalo de confianza del 99,9 por ciento, a lo largo de un periodo de un año.

C.2.2. Criterios detallados

El sistema interno de medición del riesgo operativo deberá ser consistente con el alcance de la definición de riesgo operativo señalada

en la normativa emitida por la Superintendencia, y con los tipos de eventos de pérdida definidos en el Anexo Nº 3 de la presente norma.

El cálculo del requerimiento patrimonial deberá incluir tanto la pérdida esperada (PE) como la pérdida no esperada (PNE), a menos que la empresa pueda demostrar que ya está recogiendo adecuadamente la PE en sus prácticas internas de negocio. Es decir, para que el requerimiento patrimonial se base sólo en la PNE, la empresa deberá poder demostrar, a satisfacción de la Superintendencia, que ha medido su exposición a la PE y que ha cubierto dicha pérdida.

El sistema de medición del riesgo de las empresas deberá identificar los principales factores de riesgo operativo que influyen en la forma de las colas de distribución de las estimaciones de pérdida.

Para calcular el requerimiento patrimonial, deben agregarse las mediciones obtenidas a partir de las diferentes estimaciones de riesgo operativo aplicadas. Sin embargo, la empresa podrá considerar las correlaciones existentes en las pérdidas por riesgo operativo, siempre que pueda demostrar a satisfacción de la Superintendencia que sus métodos para determinar las correlaciones son sólidos, se aplican con integridad y tienen en cuenta la incertidumbre asociada con dichas estimaciones de correlación. La empresa deberá validar sus supuestos de correlación usando técnicas cualitativas y cuantitativas adecuadas.

El sistema de medición de riesgo operativo deberá poseer elementos básicos que satisfagan el criterio de solidez enunciado en el literal a) del presente artículo. Estos elementos deberán incluir el uso de datos internos, de datos externos relevantes, de análisis de escenarios y de factores que reflejen el entorno del negocio y los sistemas de control interno.

La entidad financiera deberá contar con un proceso razonable, transparente, bien documentado y verificable acerca de la determinación de la importancia relativa asignada a cada uno de esos elementos fundamentales dentro de su sistema general de medición del riesgo operativo. El enfoque utilizado deberá ser consistente internamente y evitar la doble consideración de evaluaciones cualitativas o de coberturas del riesgo que ya se encuentren reconocidas en otros elementos del sistema de medición utilizado.

C.2.3. Datos internos

Las empresas deberán recopilar y analizar sus datos internos sobre eventos de pérdida por riesgo operativo e incorporarlos como parte del sistema interno de medición. Esto puede lograrse de diversas formas, incluyendo el uso de los datos internos de pérdida como base para las estimaciones de riesgos, como un método de validación de los datos de entrada y de salida del sistema de medición o como el enlace entre la experiencia de pérdidas y las decisiones de gestión y control de riesgos.

La empresa deberá contar con procedimientos documentados para evaluar la importancia de los datos históricos de pérdida, incluyendo los casos en que se utilicen juicios y opiniones, ajustes de escala u otros tipos de ajustes, el grado en que puedan introducirse dichos ajustes y el personal autorizado para tomar tales decisiones.

Las mediciones del riesgo operativo generadas internamente en la empresa y utilizadas para determinar el requerimiento patrimonial deberán estar basadas en un período mínimo de cinco (5) años de observación de datos internos de pérdida, ya sea que estos datos se empleen directamente para estimar las mediciones de pérdidas o para su validación.

Para efectos del requerimiento patrimonial, los procesos internos de recopilación de datos de pérdida de la empresa deberán satisfacer los siguientes criterios:

- La empresa deberá ser capaz de asignar sus datos internos de pérdida a las 6 líneas de negocio consideradas en el método estándar alternativo y a los tipos de eventos de pérdida señalados en el Anexo 3 de la presente norma, así como proporcionar dichos datos a la Superintendencia en caso de ser requeridos. La empresa deberá contar con criterios objetivos y documentados de asignación de las pérdidas a las líneas de negocio y a los tipos de eventos de pérdida especificados. Sin embargo, la empresa podrá decidir en qué medida desea aplicar

esa clasificación por categorías dentro de su sistema interno de medición.

- Los datos internos de pérdida de la empresa deberán ser completos, es decir, deben incluir la totalidad de las actividades y exposiciones importantes existentes en todos los subsistemas y todas las ubicaciones geográficas asociadas. La empresa deberá ser capaz de justificar que las actividades o exposiciones excluidas, tanto en forma individual como conjunta, no tienen un efecto significativo sobre las estimaciones generales de riesgo. La empresa deberá establecer un umbral mínimo adecuado de pérdida bruta para la recopilación de datos internos de pérdida.
- Además del dato referido al monto de la pérdida bruta, la empresa deberá recopilar datos sobre la fecha del evento de pérdida, cualquier recuperación del monto de la pérdida bruta, así como información descriptiva acerca de las causas del evento de pérdida. El nivel de detalle de la información descriptiva deberá estar en proporción con la cantidad de la pérdida bruta.
- La empresa deberá desarrollar criterios específicos para la asignación de datos de pérdidas procedentes de: (a) eventos sucedidos en una función centralizada (por ejemplo, en un departamento de tecnologías de información); (b) eventos relacionados con una actividad que incluya más de una línea de negocio; y (c) eventos relacionados a lo largo del tiempo.

Las pérdidas por riesgo operativo que estén relacionadas con el riesgo de crédito y que históricamente se hayan incluido en las bases de datos de riesgo de crédito con que cuentan las empresas (por ejemplo, fallos en la gestión de garantías) continuarán recibiendo el tratamiento de riesgo de crédito. En consecuencia, tales pérdidas no estarán sujetas al requerimiento patrimonial por riesgo operativo. Sin embargo, para efectos de la gestión del riesgo operativo, las empresas deberán identificar todas las pérdidas importantes por estos riesgos en forma consistente con el alcance de la definición de riesgo operativo señalada en la normativa emitida por la Superintendencia y los tipos de eventos de pérdida detallados en el Anexo 3, lo cual incluye los eventos de pérdida generados por riesgo operativo pero relacionados con el riesgo de crédito. Tales eventos deberán ser identificados separadamente en la base de datos de riesgo operativo de la empresa.

Las pérdidas por riesgo operativo que estén relacionadas con el riesgo de mercado deberán ser incluidas en el cálculo del requerimiento patrimonial por riesgo operativo.

C.2.4. Datos externos

El sistema de medición del riesgo operativo de la empresa deberá utilizar datos externos relevantes (ya sean datos públicos y/o datos agregados del sector), especialmente cuando existan motivos para creer que la empresa está expuesta a pérdidas poco frecuentes, pero potencialmente severas. Estos datos externos deberán incluir

información sobre el monto real de la pérdida, el volumen de operaciones de la entidad donde se produjo el evento de pérdida, las causas y circunstancias de los eventos de pérdida y cualquier otra información que permita evaluar la importancia del evento de pérdida para otras empresas. La empresa deberá contar con un proceso sistemático para determinar las situaciones en las que deberán utilizarse los datos externos y las metodologías utilizadas para incorporar estos datos (por ejemplo, aplicación de ajustes por tamaño, ajustes cualitativos o en el desarrollo de mejoras en el análisis de escenarios). Las condiciones y prácticas para el uso de los datos externos deberán ser revisadas anualmente, documentadas y sometidas a revisiones periódicas independientes a la empresa o su grupo de control.

C.2.5. Análisis de escenarios

La empresa deberá utilizar análisis de escenarios basados en las opiniones de expertos, junto con datos externos, para evaluar su exposición a pérdidas severas. Este enfoque se apoya en el conocimiento de gerentes experimentados y de expertos en gestión de riesgos para obtener evaluaciones razonables de las pérdidas severas que podría sufrir la entidad. Las evaluaciones realizadas por los expertos podrían ser expresadas como parámetros de una distribución estadística estimada de las pérdidas. Además, el análisis de escenarios debe utilizarse para evaluar el impacto de las desviaciones que se

produzcan respecto a los supuestos de correlación incorporados en el sistema de medición del riesgo operativo de la empresa, en particular, para evaluar las pérdidas potenciales procedentes de eventos simultáneos de pérdida. Estas evaluaciones deben ser validadas y revisadas a través de su comparación con la experiencia real de pérdidas, con el fin de asegurar su razonabilidad.

C.2.6. Factores del entorno de negocio y de control interno

Además de los datos de pérdida, ya sean reales o basados en escenarios, la metodología de evaluación de riesgos aplicada por la empresa debe capturar los factores clave de su entorno de negocio y de su control interno que puedan cambiar su perfil de riesgo operativo. Estos factores permitirán que las evaluaciones del riesgo que realice la empresa estén más orientadas hacia el futuro, reflejarán de forma más directa la calidad de los entornos operativos y de control de la empresa, ayudarán a alinear las asignaciones de patrimonio efectivo con los objetivos de la gestión de riesgos y permitirán reconocer de una manera más inmediata tanto las mejoras como los deterioros en los perfiles de riesgo operativo. Con el fin que sea aplicable para el cálculo del requerimiento patrimonial, el uso de estos factores dentro del sistema de medición del riesgo operativo de la empresa deberá satisfacer los siguientes criterios:

- La elección de cada factor deberá ser justificada por su influencia significativa en la exposición o mitigación del riesgo,

sobre la base de la experiencia e incluyendo la opinión experta del personal de las áreas de negocio afectadas. Cuando sea posible, los factores deben traducirse en medidas cuantitativas que permitan su verificación.

- Deberá considerarse adecuadamente la sensibilidad de las estimaciones de riesgo de la empresa ante variaciones en los factores y su peso relativo. Además de identificar las variaciones en el riesgo debido a mejoras en los controles, la metodología también debe identificar incrementos potenciales del riesgo atribuibles a una mayor complejidad de las actividades o a un incremento en el volumen de negocios.
- La metodología y cada elemento de su aplicación, incluidos los supuestos que sustenten cualquier ajuste a las estimaciones empíricas, deberán ser documentados y sometidos a revisiones independientes por parte de la empresa.
- El proceso y los resultados obtenidos deberán ser validados mediante su comparación con la experiencia real de pérdidas internas, con datos externos relevantes y con los ajustes oportunos introducidos.

C.2.7. Reconocimiento de los seguros

Las empresas que estén autorizadas a aplicar un método avanzado podrán reconocer el efecto reductor del riesgo que generan los seguros en el cálculo del requerimiento patrimonial por riesgo operativo. Dicho

reconocimiento se limitará al 20% del requerimiento patrimonial calculado con dicho método avanzado.

Para aplicar esta reducción en el requerimiento patrimonial, deberán cumplirse los siguientes requisitos:

a) El proveedor del seguro deberá contar con una clasificación de riesgo apropiada, y haber tenido dicha clasificación durante los dos semestres anteriores, de acuerdo con lo siguiente:
    - Si el proveedor del seguro se encuentra establecido en el país, la clasificación mínima aceptable será "A", otorgada por empresas debidamente registradas en la Superintendencia y en la Comisión Nacional Supervisora de Empresas y Valores (CONASEV).
    - Si el proveedor del seguro no se encuentra establecido en el país, la clasificación mínima aceptable será la "BBB-" de Standard & Poor's o equivalente, otorgada por empresas clasificadoras de riesgo del exterior de primera categoría que cuenten con autorización de funcionamiento en alguno de los países que conforman el G10.
    - Si existiera discrepancia entre diferentes clasificaciones otorgadas al proveedor del seguro, debe considerarse la más conservadora.
b) Los contratos de seguro a considerar deberán tener un plazo de vencimiento no menor de un año. Para contratos que tengan un

plazo residual de vencimiento inferior a un año, la empresa deberá aplicar los descuentos proporcionales necesarios que reflejen el plazo residual decreciente del contrato, hasta un recorte completo del 100% para contratos con un plazo residual de 90 días o menos.

c) Los contratos de seguro a considerar deberán contar con un periodo mínimo de preaviso para su cancelación de 90 días.

d) Los contratos de seguro a considerar no deberán tener exclusiones o limitaciones que dependan de acciones de la Superintendencia y otros organismos reguladores o, en el caso de liquidación de la empresa, que impidan a la empresa, al administrador o al liquidador recuperarse de los daños y perjuicios sufridos o gastos incurridos por la empresa, excepto en el caso de eventos que ocurran después de iniciado el procedimiento de liquidación de la empresa. No obstante, el contrato de seguro puede excluir la cobertura de multas u otras penalidades ocasionadas por la acción de la Superintendencia.

e) Los cálculos de la cobertura de riesgos considerando los seguros deberán ser realizados de una manera que resulte transparente y consistente con los datos de probabilidad e impacto de la pérdida utilizados por la empresa para calcular el requerimiento patrimonial por riesgo operativo.

f) El proveedor del seguro deberá ser un tercero. En el caso de seguros brindados por empresas del mismo grupo económico, la

exposición deberá estar reasegurada por un tercero independiente que satisfaga los criterios de admisión señalados anteriormente.

g) La metodología de reconocimiento del seguro deberá estar adecuadamente sustentada y documentada.

h) La empresa deberá incorporar como parte de la información de sustento que envíe a la Superintendencia la forma en que utiliza los seguros para mitigar sus riesgos.

La metodología de reconocimiento del seguro en el caso de una empresa que utilice un método avanzado deberá, también, tomar en consideración los siguientes aspectos mediante la aplicación de descuentos en la cantidad correspondiente al reconocimiento del seguro:

- El plazo de vencimiento residual del contrato, en caso de ser inferior a un año, conforme se establece en el literal b de la sección anterior.
- El plazo de cancelación del contrato, cuando sea inferior a un año.
- La incertidumbre del pago, así como los desfases existentes en la cobertura del seguro.

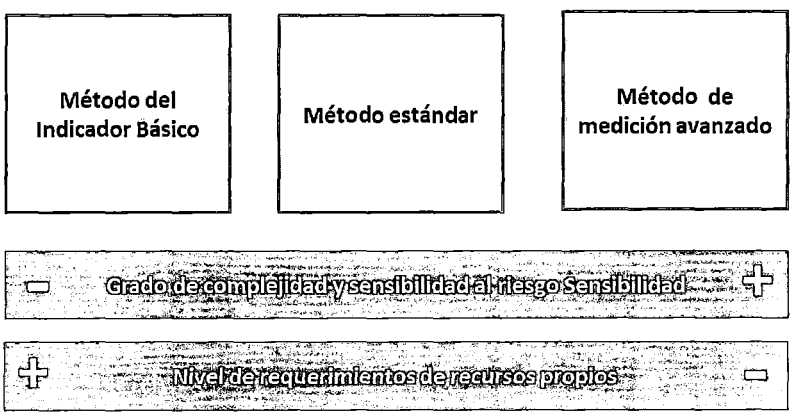
La Superintendencia podrá revisar posteriormente el límite establecido y los requisitos señalados para el reconocimiento de los seguros en el cálculo del requerimiento patrimonial por riesgo operativo, sobre la base de la experiencia acumulada.

Los dos primeros no se caracterizan por ser sensibles al riesgo, dado que determinan los requerimientos de capital en forma simplificada a través del producto entre los ingresos brutos anuales medios y el coeficiente de exigencia de capital. Ambos métodos son cuestionados, porque las entidades son penalizadas por el solo hecho de tener elevados ingresos brutos y porque el requerimiento de capital podría depender de las prácticas contables de cada país, posibilitando así el llamado arbitraje regulatorio.

4.4.3. (M.3.3) Comparar los método de cálculo y elegir alguno.

Los métodos se basan en tres enfoques de complejidad creciente que proporcionan incentivos para que las entidades se desplacen a entornos más precisos y sofisticados de medición y gestión del riesgo operacional, es decir si bien el método de indicador básico es menos complejo este involucra un mayor monto del nivel de requerimiento de recursos propios. La figura siguiente resume las dos principales diferencias.

Figura IV.12 Esquema para la Estimación de Riesgo Operativo



Fuente: El Tratamiento del Riesgo Operacional en Basilea II, Ángeles Nieto Giménez-Montesinos. Elaboración: Propia

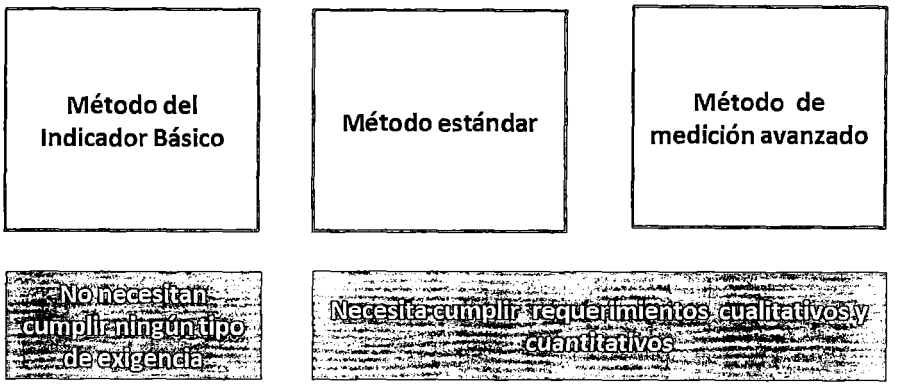
Por otra parte, tal como dijo el experto, Jordi García: la elección de un método u otro dependerá de lo siguiente:

"...cuan refinado sea su modelo, hay que tener en cuenta el grado de complejidad y exigencia, nótese que en caso del método estándar se incorpora el concepto de líneas de negocio y que además de que las entidades tienen que calificar para este modelo, tienen que cumplir no solo requisitos cuantitativos sino también requisitos cualitativos en donde resalta el hecho de tener una estructura que incentive y promueva la gestión del riesgo operativo. En cambio en el avanzado, la entidad utiliza su propio modelo interno de cálculo e igual tiene que calificar para el uso de su modelo",

En efecto, el método básico no necesita cumplir ningún tipo de exigencia para calificar a este nivel, no requiere autorización de la SBS, aunque se les insta a cumplir con las llamadas buenas prácticas de gestión de riesgo operativo; en cambio, los dos más complejos requieren autorización previa de la Superintendencia ya que el regulador valida el modelo además de cumplir requerimientos cualitativos y cuantitativos.

En conclusión, si bien existen estos factores que los diferencian y que propiciarína la elección de uno u otro método, tal como lo dice Basilea II en su documento de Buenas Prácticas de Riesgo Operacional, da a notar que el enfoque exacto elegido por cada entidad dependerá de una variedad de factores, incluyendo su tamaño y sofisticación y la naturaleza y complejidad de sus actividades.

Figura IV.13 Esquema para la Estimación de Riesgo Operativo



Fuente: El Tratamiento del Riesgo Operacional en Basilea II, Ángeles Nieto Giménez-Montesinos. Elaboración: Propia

Sin embargo, no obstante esas diferencias, se destaca la existencia de varios elementos que resultan cruciales para un esquema efectivo de Gestión de Riesgos Operativos para empresas de cualquier tamaño y alcance. Esos elementos son:

- Estrategias claramente definidas y su seguimiento por parte del consejo de administración y de la alta gerencia;
- Una sólida cultura de gestión del riesgos de operación y de control interno (incluyendo entre otras cosas, líneas claras de responsabilidad y segregación de funciones) y;
- Herramientas eficaces para la transmisión interna de información y planes de contingencia.

4.4.4. (M.3.4) Calcular el Requerimiento de capital

A. (M.3.4.1) Método Del Indicador Básico

Este método considera como indicador de exposición el "margen operativo bruto" de la entidad financiera, el cual se define como la suma de los ingresos financieros y los ingresos por servicios menos los gastos financieros y los gastos por servicios. En tal sentido, para calcular el margen operativo bruto, se utilizarán las siguientes cuentas contables:

Tabla IV.21 Cuentas para calcular el Margen Operativo Bruto

Composición del indicador	Cuentas del Manual de Contabilidad
(+) Ingresos	
Ingresos financieros	5100
Ingresos por servicios	5200 + 5700
(-) Gastos	
Gastos financieros	4100
Gastos por servicios	4200 + 4900

Fuente: SBS

A.1. (M.3.4.1.1) Leer los márgenes brutos

Para el cálculo del requerimiento patrimonial, se utilizará el saldo anualizado del margen operativo bruto, es decir, el total de margen obtenido durante los últimos 12 meses. Para ello, se utilizarán los saldos anualizados de las cuentas contables señaladas en el cuadro anterior. La anualización se deberá aplicar a los saldos de las cuentas de ingresos y gastos que se requieran para el cálculo del requerimiento de patrimonio efectivo por riesgo operativo según los métodos del Indicador Básico y

Estándar Alternativo, conforme a lo establecido en la presente norma. La fórmula es la siguiente:

Saldo anualizado (j, i) = Saldo (j,i) + Saldo (diciembre, i-1) – Saldo (j,i-1)
Dónde:
j: mes
i: año

Así por ejemplo, si en julio de 20012, se desea calcular los márgenes operativos brutos correspondientes a los últimos 3 años bajo el método del indicar básico, se deberán obtener previamente los saldos anualizados de las cuentas contables señaladas en el artículo 5° del presente Reglamento, de la siguiente manera:

Saldo anualizado (julio, 2012) = Saldo (julio, 2012) + Saldo (diciembre, 2012) – Saldo (julio, 2012)
Saldo anualizado (julio, 2011) = Saldo (julio, 2011) + Saldo (diciembre, 2011) – Saldo (julio, 2011)
Saldo anualizado (julio, 2010) = Saldo (julio, 2010) + Saldo (diciembre, 2010) – Saldo (julio, 2010)

A.2. (M.3.4.1.2) Calcular el requerimiento patrimonial

El requerimiento patrimonial por riesgo operativo según el método del indicador básico será equivalente al promedio de los saldos anualizados de los márgenes operativos brutos de la empresa, considerando los últimos 3 años, multiplicado por un factor fijo. Si el margen operativo bruto correspondiente a alguno de los tres últimos años es cero o es un número negativo, dicho(s) año(s) no debe(n) ser considerado(s) en el cálculo del promedio, en cuyo caso se calculará sobre la base del número de años cuyo margen operativo bruto sea positivo.

La fórmula de cálculo a utilizar es la siguiente:

$$R = \sum_{i=1}^{n} (MO_i \times \alpha) / n$$

Dónde:
R : Requerimiento patrimonial por riesgo operativo
MOi : Saldo anualizado del margen operativo bruto correspondiente al año i, en los casos que sea positivo
α : Factor fijo igual a 15%
n : Número de años en los que el saldo anualizado del margen operativo bruto fue positivo, considerando los 3 últimos años.

En el caso de las empresas con menos de 36 meses en operación realizarán el cálculo del requerimiento patrimonial por riesgo operativo según lo siguiente:

- Durante los primeros 12 meses de operación, el requerimiento patrimonial será equivalente al 15% del margen operativo bruto acumulado durante el periodo en que viene operando. La fórmula es la siguiente:

  $R = MO \times \alpha$

  Dónde:

  R : Requerimiento patrimonial por riesgo operativo
  MO : Margen operativo bruto acumulado durante el periodo que viene operando
  α : Factor fijo igual a 15%

- Si el margen operativo bruto acumulado es cero o negativo, el requerimiento patrimonial, según el método del indicador básico, será cero. No obstante, deberá tenerse en cuenta lo señalado en la Primera Disposición Final del presente Reglamento.
- A partir del mes 13 y hasta el mes 23 de operación, el requerimiento patrimonial por riesgo operativo será igual al 15%

del saldo anualizado del margen operativo bruto considerando sólo un período completo que incluya los últimos doce meses.

- A partir del mes 24 y hasta el mes 35 de operación, el requerimiento patrimonial por riesgo operativo será igual al promedio del saldo anualizado del margen operativo bruto considerando los dos últimos períodos de doce meses (dos años), multiplicado por 15%. Se utilizará la siguiente fórmula:

$$R = \sum_{i=1}^{n} (MO_i \times \alpha) / n$$

Dónde:
R : Requerimiento patrimonial por riesgo operativo
MOi : Saldo anualizado del margen operativo bruto correspondiente al año i, en los casos que sea positivo
α : Factor fijo igual a 15%
n : Número de años en los que el saldo anualizado del margen operativo bruto fue positivo, que será como máximo 2

Si el margen operativo bruto correspondiente a alguno de los dos años de operación es cero o es un número negativo, dicho(s) año(s) no debe(n) ser considerado(s) en el cálculo del promedio

B. (M.3.4.2) Método Estándar Alternativo

En este método existen dos tipos de indicadores de exposición para las líneas de negocio:

a) **Indicador de exposición para las líneas de negocio distintas a banca comercial y banca minorista**: Para estas líneas de negocio se utilizará como indicador de exposición al margen operativo

anualizado de cada línea. Para ello, debe utilizarse la siguiente fórmula:

$$IE_i = Ingresos_i - Gastos_i$$

Dónde:

IE_i : Indicador de exposición de la línea de negocio i
$Ingresos_i$: Ingreso anualizado de la línea de negocio i
$Gastos_i$: Gasto anualizado asignado a la línea de negocio i

El ingreso anualizado de cada línea de negocio se calculará como el total de los ingresos obtenidos en los últimos doce (12) meses. Asimismo, el gasto anualizado de cada línea de negocio se calculará como el total de los gastos obtenidos en los últimos doce (12) meses.

Para la determinación de los ingresos y gastos anualizados por líneas de negocio se considerarán las cuentas del Manual de Contabilidad de la siguiente manera:

- Para la información correspondiente al año 2009 y anteriores se utilizará la agrupación de cuentas establecida en el Anexo 2A de la norma.
- Para la información correspondiente al año 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo 2B de la norma.

b) **Indicador de exposición para las líneas de banca comercial y banca minorista:** Para estas líneas de negocio se utilizará como indicador de exposición el saldo de los créditos y las inversiones, multiplicado por un factor fijo. Para su cálculo, deberán considerarse

los saldos de créditos e inversiones durante los últimos 12 meses, conforme a la siguiente fórmula:

$$IE = m \times \sum_{i=1}^{12} Ci / 12$$

Dónde:

IE : Indicador de exposición anual para la línea de negocio banca comercial o banca minorista
M : 0,035 (Factor fijo)
Ci : Monto del saldo de créditos e inversiones para el mes i para Banca Comercial o Banca Minorista, según corresponda.

Para calcular el monto del saldo de créditos e inversiones correspondientes a Banca Comercial y Banca Minorista se utilizarán las cuentas del Manual de Contabilidad de la siguiente manera:

- Para la información correspondiente al año 2009 y anteriores se utilizará la agrupación de cuentas establecida en el Anexo 2A del presente Reglamento.
- Para la información correspondiente al año 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo 2B del presente Reglamento.

B.1. (M.3.4.2.1) Determinar las líneas de negocio

En este método, las actividades de la entidad financiera son divididas, por regulación SBS, en las siguientes líneas de negocio:

Tabla IV.22 Líneas de Negocio de la Entidad Financiera

Línea de negocio	Definición
Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización; underwriting; asesoramiento financiero a empresas corporativas, grandes y medianas empresas, así como al gobierno central y entidades del sector público; entre otras actividades de naturaleza similar.
Negociación y ventas	Operaciones de tesorería; compra y venta de títulos, monedas y commodities por cuenta propia; entre otras actividades de naturaleza similar.
Banca Minorista	Financiamiento a clientes minoristas incluyendo tarjetas de crédito, préstamo automotriz, entre otros.
Banca Comercial	Financiamiento a clientes no minoristas, incluyendo: factoring, descuento, arrendamiento financiero, entre otros.
Liquidación y pagos	Actividades relacionadas con pagos y cobranzas, transferencia interbancaria de fondos, compensación y liquidación, entre otras actividades de naturaleza similar.
Otros servicios	Servicios de custodia, fideicomisos, comisiones de confianza y otros servicios.

Fuente: SBS, Elaboración: Propia

B.1. (M.3.4.2.2) Determinar las líneas de negocio

Los factores de cada una de las líneas de negocio, por norma SBS, se presentan en el cuadro siguiente:

Tabla IV.23 Factor por Línea de Negocio

Líneas de Negocio	Valor del factor fijo
Finanzas corporativas (β_1)	18%
Negociación y ventas (β_2)	18%
Banca minorista (β_3)	12%
Banca comercial (β_4)	15%
Liquidación y pagos (β_5)	18%
Otros servicios (β_6)	15%

Fuente: SBS

B.2. (M.3.4.2.3) Calcular el Requerimiento de Capital

Los indicadores de exposición correspondientes a cada una de las líneas de negocio para los 3 últimos años son multiplicados por el factor fijo (β) asociado con cada línea de negocio. Luego, para cada uno de los

años se suman los valores obtenidos para cada línea de negocio (6 valores por cada año). Finalmente, se obtiene el promedio de las sumas obtenidas. El promedio resultante constituirá el requerimiento patrimonial por riesgo operativo. Si la suma de los productos para un año determinado resulta ser negativa, entonces se considerará el valor de 0 para ese año, en el cálculo del promedio.

El siguiente cuadro muestra el procedimiento de cálculo:

Tabla IV.24 Procedimiento de Cálculo de Requerimiento Patrimonial

Línea de negocio	Factor fijo	Indicador de exposición			Indicador * Factor fijo		
		Año 1	Año 2	Año 3	Año 1	Año 2	**Año 3**
Finanzas corporativas	18%	IE_{11}	IE_{12}	IE_{13}	R_{11}	R_{12}	R_{13}
Negociación y ventas	18%	IE_{21}	IE_{22}	IE_{23}	R_{21}	R_{22}	R_{23}
Banca minorista	12%	IE_{31}	IE_{32}	IE_{33}	R_{31}	R_{32}	R_{33}
Banca comercial	15%	IE_{41}	IE_{42}	IE_{43}	R_{41}	R_{42}	R_{43}
Liquidación y Pagos	18%	IE_{51}	IE_{52}	IE_{53}	R_{51}	R_{52}	R_{53}
Otros servicios	15%	IE_{61}	IE_{62}	IE_{63}	R_{61}	R_{62}	R_{63}
		Sumas anuales			S_1	S_2	S_3
		Requerimiento patrimonial			$\left[\sum_{i=1}^{3} \max(Si,0)\right] / 3$		

Dónde:

IE_{ij} : Indicador de exposición de la línea de negocio i en el año j
R_{ij} : Resultado de multiplicar el indicador de exposición por el factor fijo asociado a cada línea de negocio.
Si : Suma de los productos obtenidos para el año i

En el caso que la entidad financiera que cuente con menos de 36 meses de operación al momento de utilizar el método estándar alternativo, realizarán el cálculo del requerimiento patrimonial por riesgo operativo según lo siguiente:

a) Durante los primeros 12 meses de operación, los indicadores de exposición señalados en el artículo 10° deberán ser calculados considerando los datos correspondientes al periodo que la empresa viene operando, es decir:

- Para las líneas de negocio distintas a banca minorista y banca comercial, se utilizará el margen operativo acumulado de estas líneas.
- Para banca minorista y banca comercial, se utilizará el promedio de los saldos de las cuentas asociadas, multiplicado por un factor fijo (0,035)

En este caso, el requerimiento patrimonial será equivalente a la suma de los resultados del producto de los factores fijos (β) señalados en la tabla 6.4 por los indicadores de exposición calculados conforme a lo señalado al inicio de este párrafo. La fórmula es la siguiente:

$$R = \sum_{i=1}^{6} (IE_i x \beta_i)$$

Dónde:

R : Requerimiento patrimonial por riesgo operativo
IE_i : Indicador de exposición de la línea de negocio i
β_i : Factor fijo, asignado a la línea de negocio i.

b) A partir del mes 13 y hasta el mes 23 de operación, el requerimiento patrimonial por riesgo operativo se calculará considerando sólo un período completo que incluya los últimos doce (12) meses. Se utilizará el procedimiento y la fórmula señalados en el literal anterior.

c) A partir del mes 24 y hasta el mes 35 de operación, el requerimiento patrimonial por riesgo operativo se calculará conforme al procedimiento de cálculo señalado en el artículo 11° del Reglamento, pero aplicado a los dos últimos períodos de doce meses (dos años). Si la suma de los productos obtenidos para uno de los dos años resulta ser negativa, se considerará en el cálculo del promedio el valor de 0 para ese año.

C. (M.3.4.3) Método avanzado (el caso del Un Método de Medición Avanzada: Enfoque de Distribución de Pérdidas – LDA)

La entidad financiera autorizada a utilizar métodos avanzados calculará el requerimiento patrimonial por riesgo operativo mediante su sistema interno de medición del riesgo operativo.

La entidad financiera podrá ser autorizada a utilizar un método avanzado para una parte de sus operaciones y el método estándar alternativo en el resto de ellas, siempre que se satisfagan cada una de las condiciones siguientes:

- El uso de ambos métodos, en conjunto, tiene como alcance la totalidad de las operaciones de la empresa.
- Se satisfacen los requisitos para acceder a métodos avanzados para aquellas operaciones que serán consideradas en la aplicación del método avanzado seleccionado; de igual manera, se satisfacen los requisitos del método estándar alternativo a utilizar en las demás operaciones.

- La entidad financiera presenta a la SBS un plan que especifique el calendario a seguir para aplicar el método avanzado en todas las operaciones de la empresa (con excepción de aquellas poco significativas).
- En la fecha de aplicación del método avanzado, una parte significativa del riesgo operativo de la empresa está recogida en dicho método.

Uno de los métodos internos es el denominado LDA (Loss Distribution Approach o Enfoque de Distribución de Pérdidas), que se encuentra ampliamente difundido como modelo de cuantificación del riesgo operativo Este enfoque es una herramienta estadística heredada del ámbito actuarial, ampliamente utilizada en la industria aseguradora y que está convirtiéndose además en uno de los instrumentos más empleados en el ámbito bancario.

El método LDA tiene como objetivo la obtención de la función de distribución agregada de pérdidas operativos. Dicha distribución se obtiene de la acumulación de distribuciones de pérdidas para cada línea de negocio, para cada tipo de riesgo o para una combinación de ambas.

En consecuencia, se hace imprescindible mencionar aquí cuáles son las condiciones cruciales para que la metodología LDA arroje niveles de precisión aceptables:

- Una adecuada selección de las distribuciones de frecuencia e intensidad.

- Una apropiada parametrización de las distribuciones seleccionadas.

Consiguientemente, la modelización de la distribución de pérdidas será más robusta si está basada en agrupaciones con eventos de pérdida homogéneos.

Es en este sentido que cuanto más detallada sea la apertura de estas agrupaciones, más precisas serán las distribuciones de pérdida que describen el perfil de riesgo, debido a la mayor homogeneidad de los eventos de pérdida dentro de cada grupo.

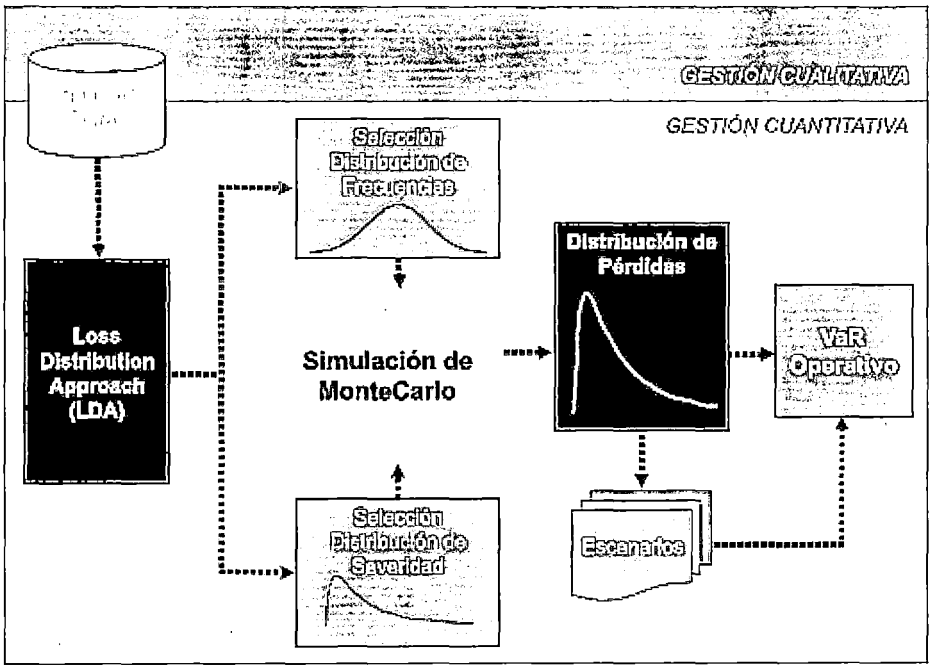
Por otro lado, cuanto mayor sea la apertura, menor será la cantidad de datos observados en cada agrupación, atentando contra la relevancia estadística del modelo. La decisión de cómo agrupar los datos conllevará un intercambio o trade-off entre el volumen de información para su modelización y el nivel de homogeneidad de los eventos bajo análisis.

El fenómeno de las pérdidas operativas puede ser desagregado en dos componentes: i) la frecuencia (que representa todas las cantidades posibles de eventos con su respectiva probabilidad) y ii) la intensidad (que representa todos los posibles valores de pérdida por evento y su probabilidad, una vez ocurrido el evento).

Por lo tanto, tal como se muestra en la Figura IV.14, la distribución de probabilidades de pérdidas también puede ser desagregada sobre la base de la estimación separada de frecuencia e intensidad, entendiendo que estos dos componentes tienen comportamientos específicos. Para volver a "unir" los dos componentes y explicar el fenómeno de las pérdidas

operativas se utilizan procesos de simulación. A efectos del cálculo, tanto la distribución de frecuencia como la distribución de intensidad deben ser estimadas en función de las pérdidas operativas observadas por la entidad y registradas en su base de pérdidas operativas. La figura a continuación esquematiza los pasos que deben seguirse en el proceso de estimación de la distribución de pérdidas operativas:

Figura IV.14 Esquema AMA la Estimación de Riesgo Operativo



Fuente y Elaboración: SBS

C.1. (M.3.4.3.1) Disponer de la Base de Datos

La base de datos es la "piedra fundamental" en la construcción o desarrollo de cualquier modelo de cuantificación. En forma particular, una base de datos poblada de pérdidas operativos históricas será el input fundamental del modelo de cuantificación

de riesgo operativo y permitirá el traspaso de un enfoque cualitativo a un enfoque integral (cualitativo cuantitativo).

Las entidades deben desarrollar sus bases de datos a partir de un proceso homogéneo de recolección de pérdidas y de asignación de éstas en función de las distintas áreas de negocios y de los diferentes tipos de riesgos, no sólo con el fin de registrar las pérdidas, sino también para entender sus causas.

C.2. (M.3.4.3.2) Determinar Frecuencia de Eventos

Con la finalidad de modelar la frecuencia de eventos con un horizonte determinado, se utiliza una distribución de conteo que explicita la probabilidad de ocurrencia de una determinada cantidad de eventos para dicho horizonte a partir de la población expuesta, es decir, de las pérdidas registradas por la entidad. Usualmente, la distribución seleccionada es la distribución de Poisson o la distribución Binomial, dadas sus características que permiten establecer de forma apropiada el número de eventos a partir de la media de la frecuencia de eventos observada en el pasado.

C.3. (M.3.4.3.3) Determinar la severidad (o intensidad) de eventos

Una vez estimada la distribución de frecuencias se debe proceder a estimar la distribución del monto de pérdida (o intensidad) de los eventos.

En virtud de eso es necesario estudiar la base de pérdidas operativos para "ajustar" la distribución paramétrica que mejor se adecue a los datos observados de montos de pérdidas.

En la práctica es usual que se utilicen distribuciones como Lognormal, Pareto y distribuciones de "cola larga"4, a efectos de no subestimar ésta por falta de información, dado que en los procesos de cuantificación de riesgo operativo debe prestarse especial atención a la estimación de la "cola" derecha de la distribución de intensidad, ya que allí se encuentran las pérdidas menos frecuentes pero las de mayor impacto para los resultados de la entidad.

Por eso es usual emplear distribuciones "mixtas" para recoger los potenciales eventos de pérdidas ubicados en la "cola" de la distribución.

C.4. (M.3.4.3.4) Realizar la Simulación de MonteCarlo

Por último, con la finalidad de generar la distribución de pérdidas se puede utilizar el método de simulación de MonteCarlo, una técnica que consiste en repetir el siguiente proceso:

- *Simular la cantidad de eventos de pérdidas operativos para el horizonte de tiempo determinado, para cada uno de estos eventos de pérdida se procede a simular el monto de pérdida asociado, luego, la pérdida total para el horizonte de tiempo es la suma de los montos de pérdida de cada uno de los eventos que se simularon en el punto anterior.*

De esta manera, el proceso estima la distribución de pérdidas utilizando un número suficiente de escenarios hipotéticos, generados aleatoriamente a partir de las estimaciones de las distribuciones de intensidad y frecuencia.

Cada una de estas repeticiones o escenarios hipotéticos -es decir, simulaciones- representa las pérdidas operativos para el período fijado como horizonte de tiempo. La cantidad de repeticiones o iteraciones debe ser elevada a fin de lograr estabilidad en los resultados de las simulaciones y lograr construir la distribución de pérdidas operativos.

La distribución de pérdidas agregadas puede ser construida a través de la convolución de las diferentes distribuciones de pérdidas de cada agrupación (correspondientes a cada línea de negocio, tipo de riesgo o a una combinación de ambas). Bajo el supuesto de correlación perfecta entre las pérdidas de cada agrupación, el requerimiento de capital total para la entidad puede ser determinado a través de la suma del valor en riesgo, obtenido de las distribuciones de pérdidas de cada agrupación realizada.

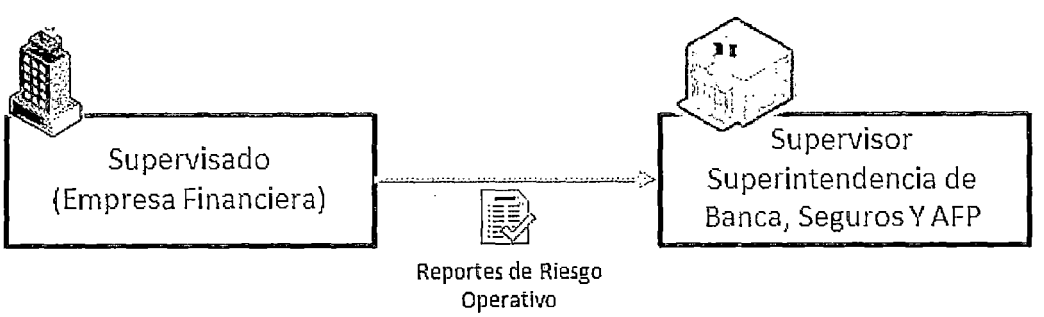
CAPÍTULO V

EJEMPLARIZACIÓN DE LA METODOLOGÍA PROPUESTA

El objetivo de este capítulo es explicar mediante ejemplos cómo una entidad financiera mide el riesgo utilizando la metodología propuesta en esta tesis. El objetivo de este capítulo es facilitar la comprensión y entendimiento de la metodología, mas no ser una prueba de concepto, ni una escenificación de de cada uno de los puntos de la metodología.

Tal como se aprecia en la Figura V.1, los actores de ejemplarización son el Supervisado (la Entidad Financiera) y el Supervisor (SBS), la entidad financiera mide el riesgo operativo y mediante un reporte de riesgo operativo envía a la SBS, quien analiza y valida esta información.

Figura V.1 Actores de la Aplicación de la Metodología de Riesgo Operativo



Fuente y Elaboración: Propia

Para el caso de los ejemplos se toman datos ficticios que corresponderían a una entidad financiera.

5.1. Enfoque Cualitativo del Riesgo Operativo

A continuación, a modo de preguntas y respuestas se plasman las técnicas utilizadas en el enfoque cualitativo:

5.1.1. ¿Cuáles son los pasos necesarios en la Autoevaluación de Riesgos?

Se deberá seguir los pasos del Procedimiento para la Autoevaluación de Riesgos (Figura IV.1). Del procedimiento, se resaltan los siguientes pasos claves:

1. Tener los procesos mapeados

Se deberá tener los procesos mapeados, respecto a dicho diagrama no existe una simbología homogénea, de hecho, existen esquemas distintos, a continuación, se presentan dos representaciones una gráfica y otra una tabla como ejemplo el proceso de Giros Nacionales y subproceso de Solicitud de Giro Nacional respectivamente, en teoría considerado como crítico.

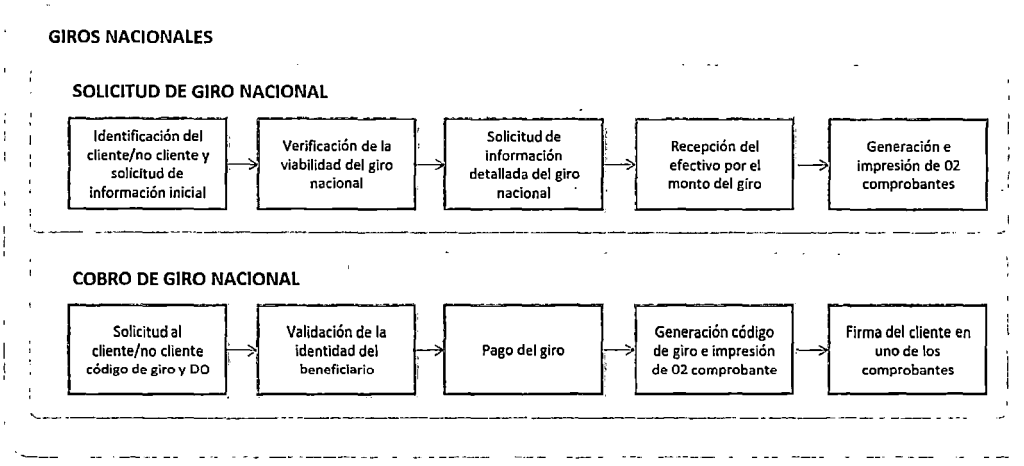
Tabla V.1 Ficha del Sub-proceso de Solicitud de Giro Nacional

Línea de Negocio: **Proceso: Solicitud de Giro Nacional**

Objetivo del Proceso: EL cliente/no cliente pueda realizar giros nacionales de manera eficiente, segura y oportuna	
Responsable del proceso: Gerente de Canales de Atención **Áreas y cargos clave del proceso:** Representante de Banca de Servicio Jefe de Banca de Servicio Supervisor de procesos y análisis operativos (Asistente de procesos y análisis operativos)	
Factores críticos de éxito: - Procedimientos actualizados y claros - Sistemas disponibles (Hardware, Software) - Personal capacitado - Recepción adecuada de la información	**Indicadores clave de desempeño utilizados:** Reclamos sobre giros nacionales
Comienzo del proceso: Cliente/no cliente se acerca a la ventanilla a solicitar un giro nacional	**Final del proceso:** Firma del beneficiario del giro en el refrendo y entrega del dinero
Procesos (o transformaciones clave):	
Entradas: Datos del solicitante y beneficiario. Monto del giro	**Salidas:** Refrendo firmado por el cliente
Productos relacionados:	**Sistemas de información utilizados:** Corporativo Reniec (Fuera del procedimiento normal)
Riesgos del proceso: Ver Matriz de Riesgos y Controles del Proceso	**Controles relacionados a los riesgos:** Ver Matriz de Riesgos y Controles del Proceso
Documentación existente relacionada: Proceso N 1000 Giros Nacionales	

Fuente y Elaboración: SBS

Figura V.2 Representación del Proceso de Giros Nacionales



Fuente y Elaboración: SBS

2. Identificar los riesgos del proceso

Se identifica los riesgos del sub-proceso de Giros Nacionales cuyos valores se plasman en una matriz, similar a la mostrada en la Tabla V.2:

Tabla V.2 Riesgos Identificados en el Proceso de Giros Nacionales

Subproceso	Cód.	Descripción Riesgo	Causas	Tipo de evento	Factor de riesgo
Giros nacionales	RGN-001	Pérdida de clientes que utilizan el servicio de giros nacionales	No contar con el efectivo para pagar el giro al beneficiario	7. Ejecución entrega y gestión de procesos	1. Procesos Internos
			Las alertas automáticas no están llegando al buzón del jefe de banca de servicios		
			La alerta no indica de qué agencia proviene el giro		
			Errores en ejecutar el procedimiento		
			Falta de capacitación al personal nuevo		
	RGN-002	Pérdida de clientes que utilizan el servicio de giros nacionales por fallas en el sistema	Caídas de línea	6. Interrupción del negocio / Fallos en el sistema	3. Tecnología de la Información
			Lentitud del sistema		
	RGN-003	Pagar el giro a una persona que no es el beneficiario del mismo	Error de digitación	7. Ejecución entrega y gestión de procesos	1. Procesos Internos
	RGN-004	Usurpación de identidad	No identificación correcta del beneficiario	2. Fraude Externo	4. Eventos Externos
	RGN-005	Fraude interno por parte de personal que tiene acceso a visualizar el código de giro	En la consulta de mayores movimientos diarios se puede visualizar el código de giro (Jefe de Banca de Servicio)	1. Fraude Interno	2. Recursos Humanos
			El área de procesos y análisis operativos puede visualizar el código del giro		
	RGN-006	Recibir sanciones de la SBS (puede incluir multas)	Para el caso de clientes que usan el servicio de giros, el personal del banco no aplique correctamente la política de conoce a tu cliente	7. Ejecución entrega y gestión de procesos	1. Procesos Internos

Fuente: SBS y Elaboración: Propia.

3. Evaluar los riesgos

En primer lugar se realiza la confección de la matriz del riesgo inherente, luego se realiza la confección del riesgo residual, para ello previamente se tiene que confeccionar la matriz de control, similar a la mostrada a las Tablas siguientes:

Tabla V.3 Evaluación de Riesgo Inherente

Subproceso	Cód.	Descripción Riesgo	Evaluación Riesgo Inherente					
			Probabilidad	Detalle Probabilidad	Impacto	Detalle Impacto	Cálculo (sólo cuantitativo)	Nivel Riesgo Inherente
Giros nacionales	RGN-001	Pérdida de clientes que utilizan el servicio de giros nacionales	1. Muy Baja	1.1 El evento puede ocurrir en menos del 5% de los casos	1. Muy Bajo	1.1 Impacto que reduzca el patrimonio efectivo en menos de 0,05% (menos US$ 62,767)	8 soles de comisión del giro x 10 clientes = 80 soles	
	RGN-002	Pérdida de clientes que utilizan el servicio de giros nacionales por fallas en el sistema	1. Muy Baja	1.1 El evento puede ocurrir en menos del 5% de los casos	1. Muy Bajo	1.1 Impacto que reduzca el patrimonio efectivo en menos de 0,05% (menos US$ 62,767)	8 soles de comisión del giro x 10 clientes = 80 soles	
	RGN-003	Pagar el giro a una persona que no es el beneficiario del mismo	1. Muy Baja	1.1 El evento puede ocurrir en menos del 5% de los casos	1. Muy Bajo	1.1 Impacto que reduzca el patrimonio efectivo en menos de 0,05% (menos US$ 62,767)		
	RGN-004	Usurpación de identidad	1. Muy Baja	1.1 El evento puede ocurrir en menos del 5% de los casos	1. Muy Bajo	1.1 Impacto que reduzca el patrimonio efectivo en menos de 0,05% (menos US$ 62,767)		
	RGN-005	Fraude interno por parte de personal que tiene acceso a visualizar el código de giro	1. Muy Baja	1.1 El evento puede ocurrir en menos del 5% de los casos	1. Muy Bajo	1.1 Impacto que reduzca el patrimonio efectivo en menos de 0,05% (menos US$ 62,767)		
	RGN-006	Recibir sanciones de la SBS (puede incluir multas)	5. Muy Alta	2.5 Nos podría ocurrir con cierta periodicidad (1 o más casos al mes)	4. Alto	7.4 Daño en la reputación con alcance nacional (medios masivos).		Extremo

Fuente: SBS y Elaboración: Propia.

Tabla V.4 Control de Riesgos

Subproceso	Cód.	Descripción Riesgo	Cód.	Descripción Control	Cargo Responsable		Tipo	Frecuencia	¿El Control se encuentra formalizado en una Norma?	Calificación control				
										Diseño	Ejecución	Total	¿Se desplaza la Probabilidad?	¿Se desplaza el Impacto?
Giros nacionales	RGN-001	Pérdida de clientes que utilizan el servicio de giros nacionales	1	Existen alertas automáticas que son enviadas a los Jefes de Banca de Servicios y a los analistas de abastecimiento de efectivo desde la agencia emisora del giro.	Jefe de Banca de Servicios	Eduardo Franco	Preventivo - Automático	Permanente	Si	3.Fuerte	2.Moderado	Moderado	No	No
			2	En las capacitaciones para Representantes de Banca de Servicios, se incluye el tema de giros nacionales	Jefe de Capacitación	Magda Zegarra	Preventivo - Manual	Esporádico / Sorpresivo	Si	2.Moderado	2.Moderado	Moderado	No	No
	RGN-002	Pérdida de clientes que utilizan el servicio de giros nacionales por fallas en el sistema												
	RGN-003	Pagar el giro a una persona que no es el beneficiario del mismo	3	Revisión del comprobante por parte del cliente, antes de firmarlo.	Jefe de Producto	Hugo Ortiz	Preventivo - Manual	Permanente	Si	2.Moderado	2.Moderado	Moderado	No	No
			4	El comprobante contiene un mensaje que le indica al cliente que debe revisar la información contenida en el mismo			Preventivo - Manual	Permanente	Si	2.Moderado	1.Débil	Débil	No	No
	RGN-004	Usurpación de identidad	5	El sistema solicita el N° de DNI y código del giro	Representante de Banca de Servicio	Eduardo Franco	Preventivo - Automático	Permanente	Si	3.Fuerte	3.Fuerte	Fuerte	No	No
			6	Solicitar el DNI al beneficiario y verificar su identidad	Representante de Banca de Servicio	Eduardo Franco	Preventivo - Manual	Permanente	Si	1.Débil	2.Moderado	Débil	No	No
			7	En caso de duda en la firma, el Jefe de Banca de Servicios debe consultar en poliweb la firma del beneficiario en caso que sea cliente, y en caso de no cliente a través de RENIEC, a partir de 3000 soles ó 1000 dólares	Jefe de Banca de Servicios	Eduardo Franco	Preventivo - Manual	Esporádico / Sorpresivo	Si	2.Moderado	2.Moderado	Moderado	No	No
	RGN-005	Fraude interno por parte de personal que tiene acceso a visualizar el código de giro												
	RGN-006	Recibir sanciones de la SBS (puede incluir multas)	8	Reportes de clientes por montos acumulados mayores a 50000 dólares	Oficial de UPLA	Ricardo Velásquez	Detectivo - Automático	Permanente	Si	2.Moderado	3.Fuerte	Moderado	Si	Si
			9	Capacitación al personal sobre las políticas de conoce a tu cliente	Oficial de UPLA	Ricardo Velásquez	Preventivo - Manual	Semestral	Si	3.Fuerte	3.Fuerte	Fuerte		
			10	Reporte de remesas (que incluye el concepto de giros nacionales)	Oficial de UPLA	Ricardo Velásquez	Preventivo - Automático	Mensual	No	2.Moderado	3.Fuerte	Moderado		

Fuente: SBS y Elaboración: Propia.

Tabla V.5 Evaluación de Riesgo Residual

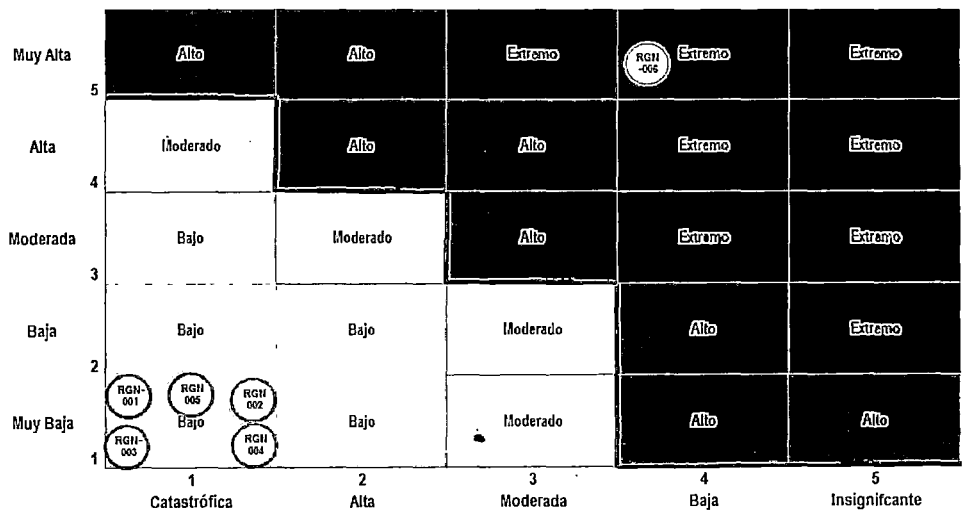
Subproceso	Cód.	Descripción Riesgo	Evaluación Riesgo Residual			Respuesta al Riesgo	Acciones propuestas / Oportunidades de mejora
			Probabilidad	Impacto	Nivel Riesgo Residual		
Giros nacionales	RGN-001	Pérdida de clientes que utilizan el servicio de giros nacionales	1. Muy Baja	1. Muy Bajo	Bajo	Mitigar	Para agilizar los extornos de giros nacionales, las alertas deben indicar de qué agencia provienen. Revisar porqué las alertas no están llegando al Jefe de Banca de servicios El Jefe de Banca de Servicios que autoriza el extorno de la agencia emisora, debe comunicar dicho extorno, vía correo electrónico, al Jefe de BS de la agencia destino y al analista de abastecimiento. Revisar el monto de la comisión por giros y evaluar si es necesario incluir el costo de la consulta por RENIEC, que se realiza para los clientes que no conocen la información completa del beneficiario.
	RGN-002	Pérdida de clientes que utilizan el servicio de giros nacionales por fallas en el sistema	1. Muy Baja	1. Muy Bajo	Bajo	Mitigar	Analizar si es necesario implementar procedimiento de contingencia para el pago del giro al beneficiario
	RGN-003	Pagar el giro a una persona que no es el beneficiario del mismo	1. Muy Baja	1. Muy Bajo	Bajo	Mitigar	Reforzar la comunicación al cliente, indicando que siempre debe revisar su comprobante
	RGN-004	Usurpación de identidad	1. Muy Baja	1. Muy Bajo	Bajo	Aceptar	
	RGN-005	Fraude interno por parte de personal que tiene acceso a visualizar el código de giro	1. Muy Baja	1. Muy Bajo	Bajo	Mitigar	Eliminar de la consulta de la agencia emisora, a la que accede el Jefe de Banca de Servicios, el número de operación del giro (código)
	RGN-006	Recibir sanciones de la SBS (puede incluir multas)	2. Baja	2. Bajo	Bajo	Aceptar	

Fuente: SBS y Elaboración: Propia.

4. Evaluar la Matriz de Riesgos Operacionales

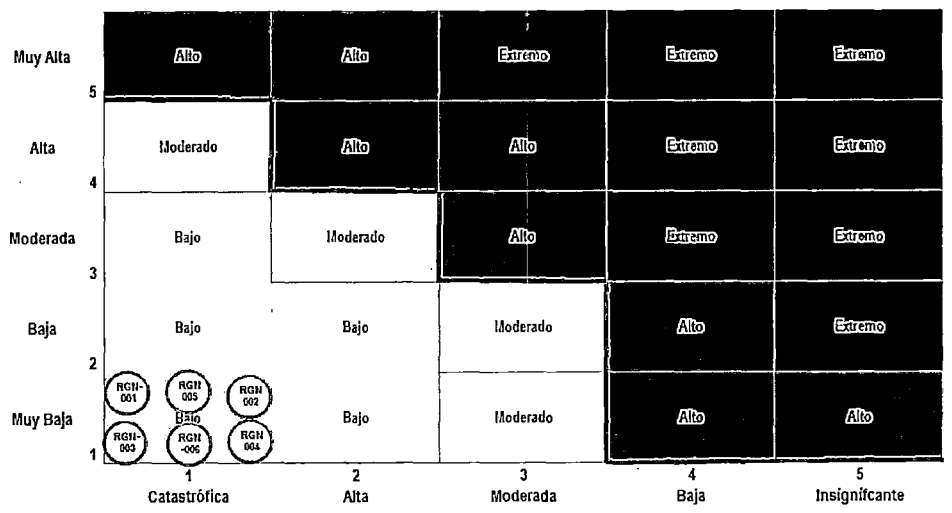
La información anterior se extrapola en una matriz de riesgos que nos permite visualizar, según la posición que ocupe el riesgo en la misma, se parte de la matriz de riesgo inherente para luego de aplicar los controles se llega a la matriz de riesgo residual.

Figura V.3 Matriz de Riesgo Inherente



Fuente y Elaboración: propias

Figura V.4 Matriz de Riesgo Residual



Fuente y Elaboración: propias

Un ejemplo de extrapolación es tal como el que se presenta a continuación

Tabla V.6 Extrapolación de Valores Impacto-Probabilidad

Evaluación			
Probabilidad	Impacto	Probabilidad-Impacto	Total
5. Muy Alta	5. Muy Alto	5. Muy Alta5. Muy Alto	Extremo
5. Muy Alta	4. Alto	5. Muy Alta4. Alto	Extremo
5. Muy Alta	3. Medio	5. Muy Alta3. Medio	Extremo
5. Muy Alta	2. Bajo	5. Muy Alta2. Bajo	Alto
5. Muy Alta	1. Muy bajo	5. Muy Alta1. Muy bajo	Alto
4. Alta	5. Muy Alto	4. Alta5. Muy Alto	Extremo
4. Alta	4. Alto	4. Alta4. Alto	Extremo
4. Alta	3. Medio	4. Alta3. Medio	Alto
4. Alta	2. Bajo	4. Alta2. Bajo	Alto
4. Alta	1. Muy bajo	4. Alta1. Muy bajo	Moderado
3. Media	5. Muy Alto	3. Media5. Muy Alto	Extremo
3. Media	4. Alto	3. Media4. Alto	Extremo
3. Media	3. Medio	3. Media3. Medio	Alto
3. Media	2. Bajo	3. Media2. Bajo	Moderado
3. Media	1. Muy bajo	3. Media1. Muy bajo	Bajo
2. Baja	5. Muy Alto	2. Baja5. Muy Alto	Extremo
2. Baja	4. Alto	2. Baja4. Alto	Alto
2. Baja	3. Medio	2. Baja3. Medio	Moderado
2. Baja	2. Bajo	2. Baja2. Bajo	Bajo
2. Baja	1. Muy bajo	2. Baja1. Muy bajo	Bajo
1. Muy Baja	5. Muy Alto	1. Muy Baja5. Muy Alto	Alto
1. Muy Baja	4. Alto	1. Muy Baja4. Alto	Alto
1. Muy Baja	3. Medio	1. Muy Baja3. Medio	Moderado
1. Muy Baja	2. Bajo	1. Muy Baja2. Bajo	Bajo
1. Muy Baja	1. Muy bajo	1. Muy Baja1. Muy bajo	Bajo

Fuente y Elaboración: propias

5.1.2. ¿Cuáles son los pasos necesarios en la Captura Eventos de Pérdida?

Se deberá seguir los pasos del Procedimiento para la Captura de Eventos de Pérdida (Figura 6.4), de ellos se resalta los pasos claves:

1. Ingresar la información del Evento de Pérdida

Ingresar la información con cualquiera de las tres formas: ya sea manual, semiautomática o automática del evento de pérdida, la idea en cualquiera de los casos es alimentar una base de datos centralizada, considerar los umbrales de la entidad y del regulador, también considerar las cuentas contables asociadas al evento. Esta información la ingresan los colaboradores.

Figura V.5 Registro o Ficha de Evento de Pérdida

Entidad Legal	Banco XXX						
Unidad	Banca Minorista					Nro de Evento	24/04/1907
SubUnidad	Red Oficinas					Fecha de Alta	15/06/2011
Proceso (N1)	RRHH					Proceso (N2)	Nóminas
Producto (N1)	N/A					Producto (N2)	NA
Clase de RO (N1)	Ejecución, entrega y gestión de procesos					Clase de RO (N2)	Error Humano
Referencia	247/10	Contabilización	40770			Ocurrencia	15/05/2011
Tipo de Evento		Ref Multiple	NA			Descubrimiento	15/04/2011
Importe	1,000,000			Cuenta	123456	Causa 1	Error humano
Importe Recuperado	200,000			Cuenta	9955	Causa 2	Falta de Capacitación
Recuperado por Seguro	0			Cuenta	NA	Causa 3	NA
Descripción Breve	error de cálculo					Riesgo de Crédito	N
Observaciones	Error en el cálculo de la retención de beneficios en especie practicada por el CAR						
Factor de Riesgo Identificado previamente				Conforme	S	Abierto/Cerrado	C
Categoria Nivel I	Ejecución de Procesos					Categoria Nivel	Ejecución de Procesos
Frecuencia Ajustada				Conforme	S	Evento Externo	N

Fuente: Curso Taller sobre de Base de Datos de Eventos por Riesgos Operativos, SBS, Elaboración: Propia

2. Analizar si amerita un plan de acción

Suponiendo que ya obtuvo el detalle contable y se realizaron los sustentos necesarios, el analista de Riesgos de Operación analiza si la pérdida amerita un plan de acción, esto es un trabajo uno a uno (pérdida por pérdida), suponiendo que los eventos son analizados en un mismo tiempo, los eventos de pérdida se mostraría en la tabla siguiente:

Tabla V.7 Matriz de Identificación de Eventos De Riesgo

N°	Evento de Riesgo	Fallo o Insuficiencia	Factor
1	Ejecución y administración de procesos, errores y omisiones en procesos, errores en la operativa.	En la agencia L, el 25.02.2010 el cliente Juana Pedro Arauco entregó US$ 1,100 ; la Asistente de Operaciones hizo una venta y dio el equivalente a S/.3,190. Con este dinero el cliente liquidó su crédito 99-01-6234327, llevándose una diferencia de 174,79 (debió ser compra y entregarle una diferencia sólo de S/.53,79)	Personal
2	Hurto y Fraude	En agencia O, realizó operación de retiro de efectivo en ventanilla de asistente, se detectó que realizó una suplantación del hermano de cliente Pedro Arias Moscoso se acercó a realizar un retiro de cuenta de ahorros, presentando el DNI del titular e intentando firmar como tal.	Procesos
3	Ejecución y administración de procesos, errores y omisiones en procesos, errores en la operativa.	En Oficina Especial A, cliente se acerca a depositar una orden de pago por S/ 1160 en su cuenta de ahorros, pero el asistente de operaciones realiza el depósito con la transacción 1220, depósito de cheques generando un descuadre en el cuadre contablede la agencia.	Personal
4	Fallas Tecnológicas	En agencia H, falla en las transacciones referentes a TARJETAS DE DEBITO , del aplicativo TXL, por un tiempo de 45 minutos aproximadamente.	Tecnología
...	...	...	...
N	Fallas Tecnológicas	En agencia G cambio de router sisco 2801 en horas de atención al público, sin previa coordinación.	Tecnología

Fuente y Elaboración: Propia

Tabla V.8 Matriz de Identificación de Eventos De Riesgo

N°	Evento de Riesgo	Fallo o Insuficiencia	Factor	Impacto	Probabilidad	Nivel de Riesgo	Plande Adecuación
1	Ejecución y administración de procesos, errores y omisiones en procesos, errores en la operativa.	En la agencia L, el 25.02.2010 el cliente Juana Pedro Arauco entregó US$ 1,100 ; la Asistente de Operaciones hizo una venta y dio el equivalente a S/.3,190. Con este dinero el cliente liquidó su crédito 99-01-6234327, llevándose una diferencia de 174,79 (debió ser compra y entregarle una diferencia sólo de S/.53,79)	Personal	Moderado	Moderado	Medio	No, se detectó el mismo día, genera plan de acción
2	Hurto y Fraude	En agencia O, realizó operación de retiro de efectivo en ventanilla de asistente, se detectó que realizó una suplantación del hermano de cliente Pedro Arias Moscoso se acercó a realizar un retiro de cuenta de ahorros, presentando el DNI del titular e intentando firmar como tal.	Procesos	Moderado	Moderado	Medio	No, se detectó el mismo día, genera plan de acción
3	Ejecución y administración de procesos, errores y omisiones en procesos, errores en la operativa.	En Oficina Especial A, cliente se acerca a depositar una orden de pago por S/ 1160 en su cuenta de ahorros, pero el asistente de operaciones realiza el depósito con la transacción 1220, depósito de cheques generando un descuadre en el cuadre contable de la agencia.	Personal	Moderado	Moderado	Medio	Se dio solución de forma inmediata. No genera plan de adecuación.
4	Fallas Tecnológicas	En agencia H, falla en las transacciones referentes a TARJETAS DE DEBITO , del aplicativo TXL, por un tiempo de 45 minutos aproximadamente.	Tecnología	Moderado	Moderado	Medio	No genera plan de adecuación.
N	Fallas Tecnológicas	En agencia G cambio de router sisco 2801 en horas de atención al público, sin previa coordinación.	Tecnología	Moderado	Moderado	Medio	No genera plan de adecuación dado que depende de la red de comunicaciones externa.

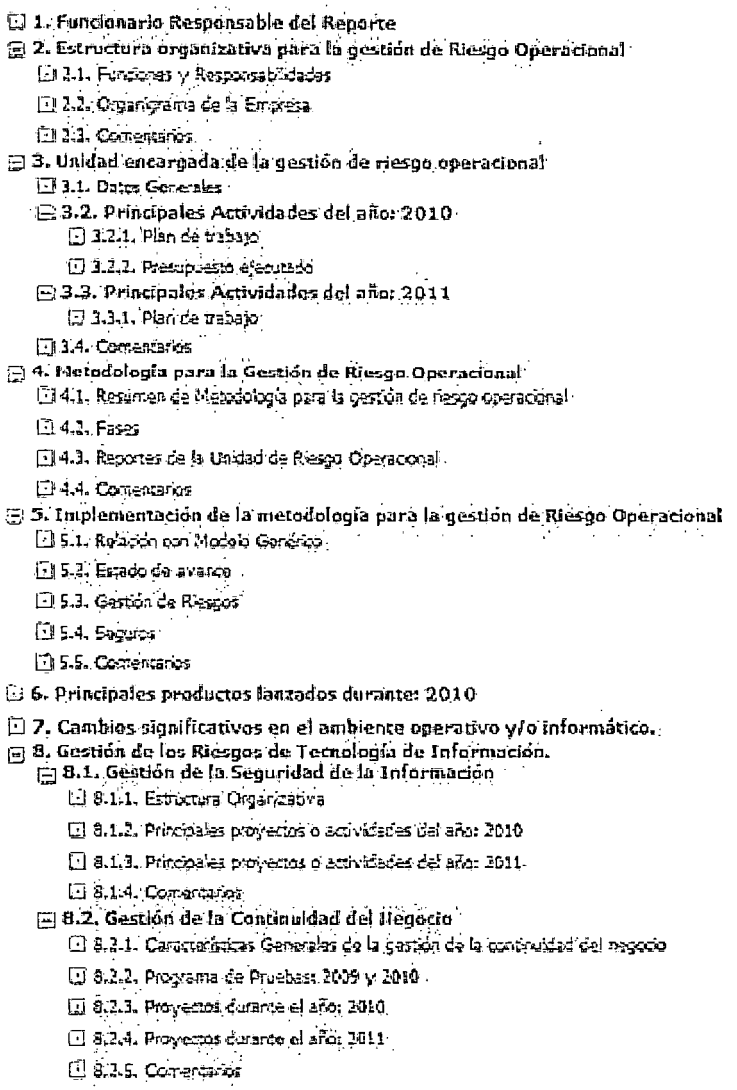
Fuente y Elaboración: Propia

5.1.3. ¿Qué informes solicita la SBS?

Las empresas deberán presentar a la Superintendencia informes anuales referidos a la gestión del riesgo operacional, a través del software IG-ROp, el cual se encontrará disponible en el "Portal del Supervisado". Dichos informes deberán ser remitidos a más tardar el 31 de enero del año siguiente al año de reporte. La Superintendencia podrá requerir, mediante Oficio, la actualización periódica de los informes.

A continuación se muestra la información solicitada.

Figura V.6 Información a ser enviada a la SBS



Fuente y Elaboración: SBS

Como se puede apreciar, la información que se remite a la SBS es sencilla, se puede adjuntar solo pruebas de que se está gestionando el riesgo o se puede detallar determinada información, ejemplos de información detallada se presenta a continuación:

Tabla V.9 Ejemplo: Eventos de Riesgo Operativo por Factor de Riesgo

Factor de Riesgo	Descripción	N° de Riesgos
Procesos	La Entidad Financiera debe gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.	4
Personal	La Entidad Financiera debe gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.	7
Tecnología	La Entidad Financiera debe gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.	9
Externos	La Entidad Financiera debe gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.	3
	Total de eventos de Riesgo Operativo	23

Fuente y Elaboración: Propias

Tabla V.10 Ejemplo: Faltantes reportados en ventanilla

Agencia	Fecha	Monto Soles	Monto Dólares
A	04.02.2010	49.54	0
B	18.02.2010	100.11	0
B	25.02.2010	999.46	0
C	16.02.2010	299.92	0
D	06.02.2010	250.03	0
E	05.02.2010	1,000.00	0

Fuente y Elaboración: Propia

Tabla V.11 Ejemplo: Faltantes reportados y compensados en Cajeros ingresados en una Cuenta

Fecha	Asiento	Debe / Haber	Importe (S/.)
27/02/2010	4021	H	405.77

24/02/2010	3270	D	4.90
23/02/2010	3089	D	0.20
22/02/2010	2908	D	12.20
15/02/2010	1939	D	5,000.00
11/02/2010	1481	D	7.37
06/02/2010	839	D	2.50
05/02/2010	707	D	18.00
04/02/2010	556	D	5.00
03/02/2010	415	D	13.80

Fuente y Elaboración: Propia

Tabla V.12 Ejemplo: Provisiones para eventos de Riesgo Legal (Cta. Ctble. 270202)

Despido por falta grave demandante	Materia	Monto Petitorio	Monto Reconocido	Depósito Judicial	Contingencia Legal
Persona 1	Pago de Beneficios Sociales	190,263.30	49,558.50	0	19,823.40
Persona 2	Pago de Beneficios Sociales	48,839.83	0	0	24,959.83
Persona 3	Indemnización por despido arbitrario	87,559.00	0	0	3,328.29
Persona 4	Indemnización por despido arbitrario	98,000.00	91,972.00	0	36,788.80
Persona 5	Indemnización por despido arbitrario	75,509.00	'0	0	75,509.00
Persona 6	Pago de Beneficios Sociales	28,920.00	0	0	14,460.00
Persona 7	Indemnización por despido arbitrario	37,609.38	6,078.64	0	2,431.46
Persona 8	Pago de Beneficios Sociales	21,904.00	965.00	10,440.79	10,498.21
Persona 9	Pago de Beneficios Sociales	10,233.00	820.00	0	9,413.00
Persona 10	Pago de Beneficios Sociales	10,229.00	648.00	0	1,220.61
Persona 11	Pago de Beneficios Sociales	13,242.00	1,237.00	10,440.79	1,564.21
Persona 12	Indemnización por despido arbitrario	20,903.33	0	0	20,903.33
	Total	643,211.84	151,279.14	20,881.58	220,810.84

Fuente: Entidad Financiera, Modificado por Autor de la Tesis

En este ejemplo las Provisiones para eventos de Riesgo Legal que Podrían Generar Provisiones para Litigios y Demandas, registradas contablemente (Cta. Ctble. 270202) son las posibles pérdidas o eventuales obligaciones en procesos iniciados por ex trabajadores contratados a plazo indeterminado y que representan riesgo legal como parte del riesgo operativo

5.2. Enfoque Cualitativo del Riesgo Operativo

A continuación, a modo de preguntas y respuestas se plasman las técnicas utilizadas en el enfoque cuantitativo:

5.2.1. ¿Cómo se realiza el cálculo de requerimiento de capital bajo el enfoque del indicador básico?

A sabiendas que el requerimiento patrimonial por riesgo operativo según el método del indicador básico será equivalente al promedio de los saldos anualizados de los márgenes operativos brutos de la empresa, considerando los últimos 3 años, se incluye un ejemplo en Excel utilizando las líneas de negocio

Figura V.7 Cálculo del Requerimiento de Capital - Enfoque del Indicador Básico

	A	B	C	D
1		Márgenes Operativos Brutos		
2	Linea de negocio	2007	2008	2009
3	Finanzas corporativas	20	30	40
4	Negociación y ventas	20	30	40
5	Banca Minorista	20	30	40
6	Banca Comercial	20	30	40
7	Liquidación y pagos	20	30	40
8	Otros servicios	20	30	40
9	Total	=SUMA(B3:B8)	=SUMA(C3:C8)	=SUMA(D3:D8)
10	Requerimiento de Capital		Promedio:	=PROMEDIO(B9:D9)
11			Factor Alfa:	0.15
12			Capital	=+D11*D10

	A	B	C	D
1		Márgenes Operativos Brutos		
2	Linea de negocio	2007	2008	2009
3	Finanzas corporativas	20	30	40
4	Negociación y ventas	20	30	40
5	Banca Minorista	20	30	40
6	Banca Comercial	20	30	40
7	Liquidación y pagos	20	30	40
8	Otros servicios	20	30	40
9	**Total**	120	180	240
10	Requerimiento de Capital		Promedio:	180
11			Factor Alfa:	15%
12			Capital	27

Fuente: Zenzi.org, Elaboración: Propia

5.2.2. ¿Cómo se realiza el cálculo de requerimiento de capital bajo el enfoque estándar alternativo?

Este método incorpora las líneas de negocio, los indicadores de exposición correspondientes a cada una de las líneas de negocio para los 3 últimos años, y luego éstos son multiplicados por un factor fijo se incluye un ejemplo en Excel utilizando las líneas de negocio

Figura V.8 Cálculo del Requerimiento de Capital - Enfoque Estándar

	A	B	C	D	E	F	G	H
1			Márgenes Operativos Brutos			Márgenes Operativos Brutos * Factor		
2	Linea de negocio	Factor	2007	2008	2009	2007	2008	2009
3	Finanzas corporativas	0.18	20	30	40	=+C3*B3	=+D3*B3	=+E3*B3
4	Negociación y ventas	0.18	20	30	40	=+C4*B3	=+D4*B3	=+E4*B3
5	Banca Minorista	0.12	20	30	40	=+C5*B3	=+D5*B3	=+E5*B3
6	Banca Comercial	0.15	20	30	40	=+C6*B3	=+D6*B3	=+E6*B3
7	Liquidación y pagos	0.18	20	30	40	=+C7*B3	=+D7*B3	=+E7*B3
8	Otros servicios	0.15	20	30	40	=+C8*B3	=+D8*B3	=+E8*B3
9						=SUMA(F3:F8)	=SUMA(G3:G8)	=SUMA(H3:H8)
10							Requerimiento de Capital	=PROMEDIO(F9:H9)

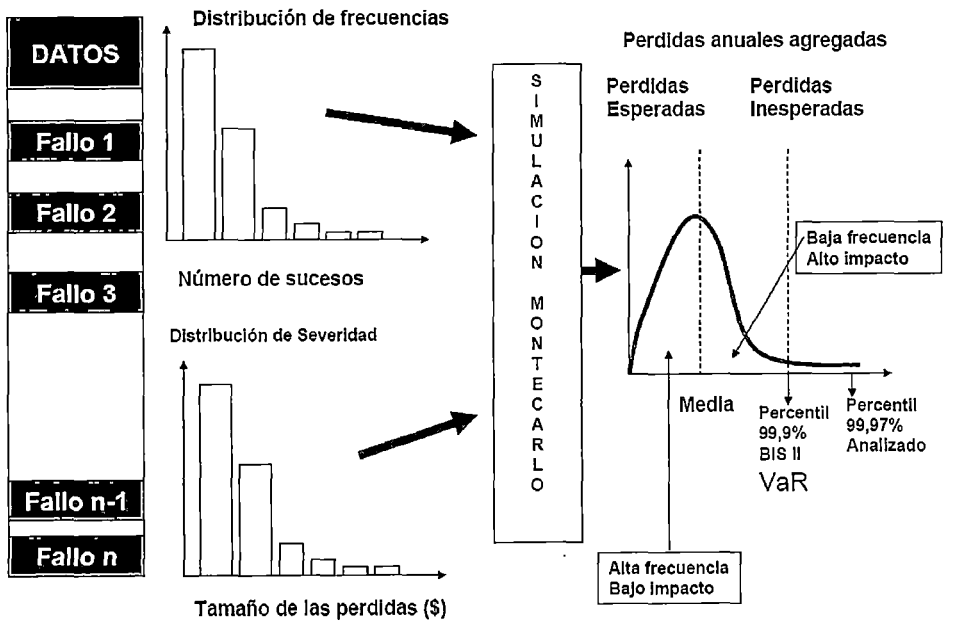
	A	B	C	D	E	F	G	H
1			Márgenes Operativos Brutos			Márgenes Operativos Brutos * Factor		
2	Linea de negocio	Factor	2007	2008	2009	2007	2008	2009
3	Finanzas corporativas	18%	20	30	40	3.6	5.4	7.2
4	Negociación y ventas	18%	20	30	40	3.6	5.4	7.2
5	Banca Minorista	12%	20	30	40	3.6	5.4	7.2
6	Banca Comercial	15%	20	30	40	3.6	5.4	7.2
7	Liquidación y pagos	18%	20	30	40	3.6	5.4	7.2
8	Otros servicios	15%	20	30	40	3.6	5.4	7.2
9						21.6	32.4	43.2
10							Requerimiento de Capital	32.4

Fuente: Zenzi.org, Elaboración: Propia

5.2.3. ¿Cómo se realiza el cálculo de requerimiento de capital bajo el enfoque medición avanzada?

Como se mencionó el método avanzado, dependerá del modelo interno de cada entidad y que este sea autorizado por la SBS autoriza, a continuación, se presente un enfoque

Figura V.9 Proceso de Medición del Método AMA



Fuente y Elaboración: SBS

En este escenario el fenómeno de las pérdidas operativas puede ser desagregado en dos componentes: i) la frecuencia (que representa todas las cantidades posibles de eventos con su respectiva probabilidad) y ii) la intensidad (que representa todos los posibles valores de pérdida por evento y su probabilidad, una vez ocurrido el evento). A efectos del cálculo, tanto la distribución de frecuencia como la distribución de intensidad deben ser estimadas en función de las pérdidas operativas observadas por la entidad y registradas en su base de pérdidas operativos.

A. Supuestos respecto a la Entidad Financiera:

- Determinada entidad financiera desea evaluar el capital necesario para cubrir su riesgo operativo en la línea de negocio de Banca Minorista y en el tipo de riesgo Gestión de Procesos.
- La entidad cuenta con una estadística propia que ha ido elaborando en los dos últimos años sobre el número de fallos que se han ido produciendo en esta línea, así como otra estadística que recoge la perdida que cada evento ha supuesto.
- La distribución de frecuencias de errores en la línea de negocio indica que se distribuye según una Binomial con una probabilidad del 4% (es decir, 4 fallos en la línea cada 100 operaciones realizadas)

- En cuanto a la evolución de la Severidad (LGD), los datos indican que las pérdidas por cada 100$ de transacción se pueden ajustar a una distribución de tipo Lognormal de media 2$ y desviación típica 1$.

B. Frecuencia de eventos y Percentiles

Con la finalidad de modelar la frecuencia de eventos con un horizonte determinado, se utiliza una distribución de conteo que explicita la probabilidad de ocurrencia de una determinada cantidad de eventos para dicho horizonte a partir de la población expuesta, es decir, de las pérdidas registradas por la entidad. La distribución seleccionada es la distribución Binomial cuyas formula es la siguiente:

$$f(x) = \binom{n}{x} p^x (1-p)^{n-x}$$

$$F(x) = \sum_{i=0}^{x} \binom{n}{i} p^i (1-p)^{n-i}$$

La distribución Binomial dadas sus características que permiten establecer de forma apropiada el número de eventos a partir de la media de la frecuencia de eventos observada en el pasado.

Tabla V.13 Frecuencia de Eventos

Numero Eventos	Probabilidad	Probabilidad Acumulada
0	1.69%	1.69%
1	7.03%	8.72%
2	14.50%	23.21%
3	19.73%	42.95%
4	19.94%	62.89%
5	15.95%	78.84%
6	10.52%	89.36%
7	5.89%	95.25%

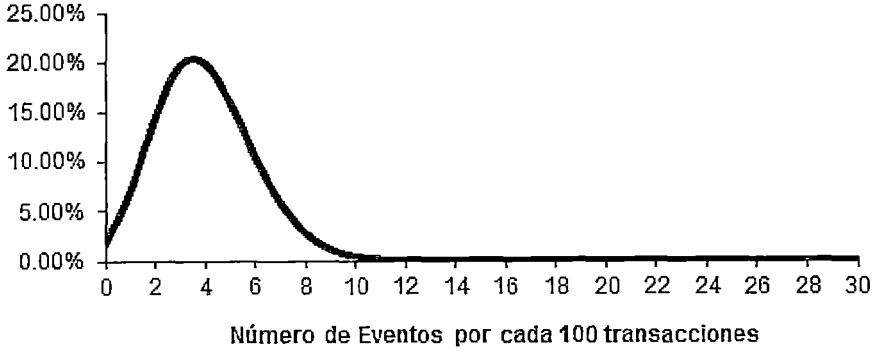
8	2.85%	98.10%	
9	1.21%	99.32%	
10	0.46%	99.78%	
11	0.16%	99.93%	
12	0.05%	99.98%	
13	0.01%	100.00%	
14	0.00%	100.00%	
15	0.00%	100.00%	
16	0.00%	100.00%	
17	0.00%	100.00%	
18	0.00%	100.00%	
19	0.00%	100.00%	
20	0.00%	100.00%	
...	...	...	
100	0.00%	100.00%	

n =	100	Media =	4
p =	0.04	Varianza =	3.84
q =	0.96		

Fuente y Elaboración: Propia

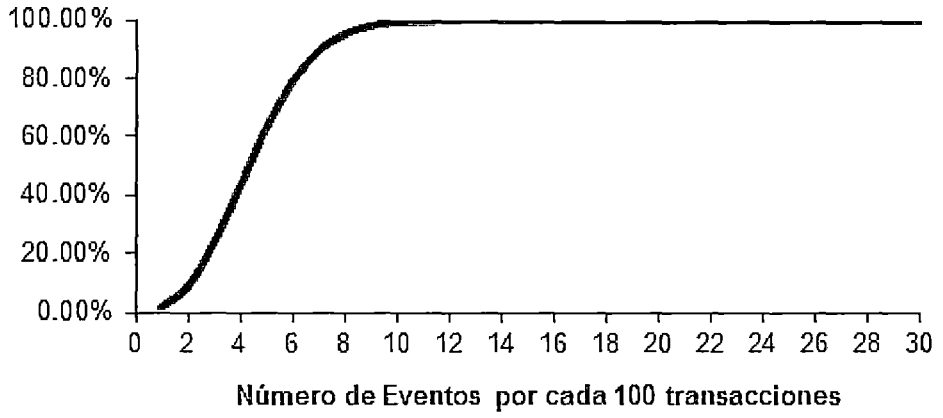
A partir de la información de los datos históricos de eventos de pérdidas y luego de haber calculado la probabilidades de frecuencias podemos generar unos gráficos similares a los siguientes:

Figura V.10 Distribución de Frecuencias de Eventos (Binomial (n,p))



Elaboración: el Autor de la Tesis

Figura V.11 Distribución Acumulada de Frecuencias de Eventos (Binomial (n,p))



Elaboración: el Autor de la Tesis

C. Severidad de la Pérdida (distribución de Severidad)

Una vez estimada la distribución de frecuencias se debe proceder a estimar la distribución del monto de pérdida (o intensidad) de los eventos. En virtud de eso es necesario estudiar la base de pérdidas operativos para "ajustar" la distribución paramétrica que mejor se adecue a los datos observados de montos de pérdidas.

En la práctica es usual que se utilicen distribuciones como Lognormal, cuya fórmula es la siguiente:

$$f(x) = \frac{1}{x\sqrt{2\pi\sigma'}} e^{-\frac{1}{2}\left[\frac{\ln x - \mu'}{\sigma'}\right]^2}$$

$$F(x) = \Phi\left(\frac{\ln x - \mu'}{\sigma'}\right)$$

$$\text{con } \mu' \equiv \ln\left[\frac{\mu^2}{\sqrt{\sigma^2 + \mu^2}}\right] \qquad \text{y} \qquad \sigma' \equiv \sqrt{\ln\left[1 + \left(\frac{\sigma}{\mu}\right)^2\right]}$$

A efectos de no subestimar ésta por falta de información, dado que en los procesos de cuantificación de riesgo operativo debe prestarse especial atención a la estimación de la "cola" derecha de la distribución de intensidad, ya que allí se encuentran las pérdidas menos frecuentes pero las de mayor impacto para los resultados de la entidad.

Tabla V.14 Probabilidades para Distribución de Severidad

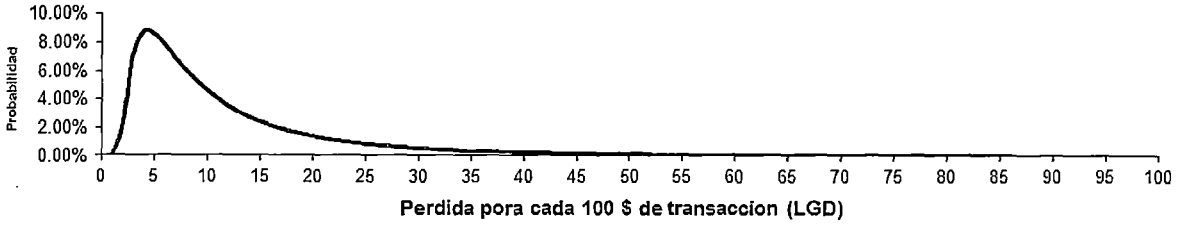
Valor X=LGD	Probabilidad Acumulada	Probabilidad
0.01	0.00%	0.00%
1	2.28%	2.28%
2	9.56%	7.29%
3	18.37%	8.81%
..	..	..
100	99.54%	0.01%

Media =	2	Valor inicial =	0.01
Desvia. Típica =	1	Cambio =	1

Fuente y Elaboración: el Autor de la Tesis

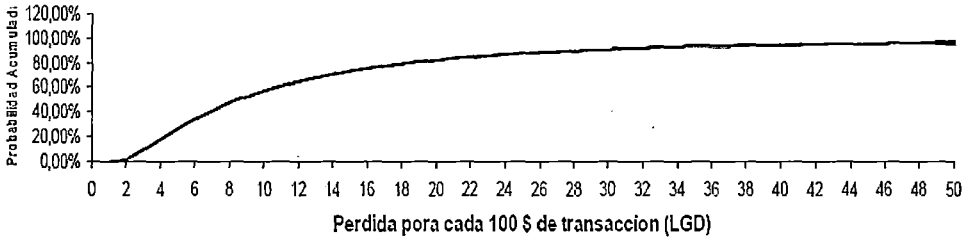
En forma similar que la distribución de frecuencias, a partir de la distribución de severidad generar unos gráficos similares a los siguientes:

Figura V.12 Distribución de Pérdidas LGD (LogNormal)



Elaboración: el Autor de la Tesis

Figura V.13 Distribución Acumulada de Pérdidas LGD (LogNormal)



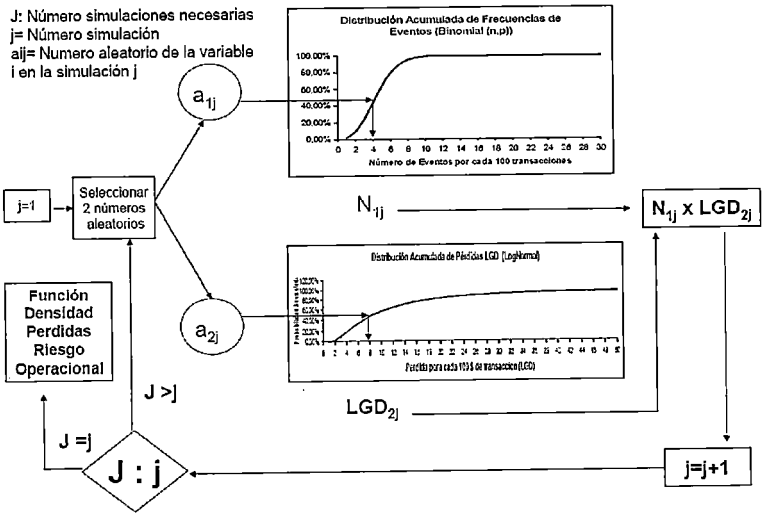
Elaboración: el Autor de la Tesis

D. Simulación de MonteCarlo

Por último, con la finalidad de generar la distribución de pérdidas se puede utilizar el método de simulación de MonteCarlo, el cual es una técnica de selección de números aleatorios a través de una o más distribuciones de probabilidad, para utilizarlas en una simulación. En este caso, el muestreo artificial o simulado trata de crear un universo teórico descrito completamente por una LEY DE PROBABILIDAD que se supone conocida o adecuada. Posteriormente, de este universo se obtiene una MUESTRA aleatoria mediante una sucesión de números aleatorios.

Para obtener una muestra del universo teórico que sea completamente aleatoria se deben haber realizado los pasos de cálculo de frecuencia y severidad.

Figura V.14 Interpretación de la Distribución Acumulada de Pérdidas LGD (LogNormal)



Elaboración: el Autor de la Tesis

Lo siguiente es la simular la cantidad de eventos de pérdidas operativos para el horizonte de tiempo determinado, para cada uno de estos eventos de pérdida se procede a simular el monto de pérdida asociado, luego, la pérdida total para el horizonte de tiempo es la suma de los montos de pérdida de cada uno de los eventos que se simularon en el punto anterior. De esta manera, el proceso estima la distribución de pérdidas utilizando un número suficiente de escenarios hipotéticos, generados aleatoriamente a partir de las estimaciones de las distribuciones de intensidad y frecuencia.

Cada una de estas repeticiones o escenarios hipotéticos -es decir, simulaciones- representa las pérdidas operativos para el período fijado como horizonte de tiempo. La cantidad de repeticiones o iteraciones debe ser elevada a fin de lograr estabilidad en los resultados de las

simulaciones y lograr construir la distribución de pérdidas operativos. Para efectos de escenificar estos datos se muestran los 100 primeros registros de un total de 1000.

Tabla V.15 Números Aleatorios y Simulación

NUMEROS ALEATORIOS			DATOS SIMULADOS	Distribución inversa		
Nº Simulación	Nº Eventos	LGD	DATO	Nº Eventos	LGD	PERDIDA
1	0.68	0.13	1	5.00	2	12
2	0.11	0.75	2	2.00	15	29
3	0.78	0.78	3	5.00	16	79
4	0.85	0.17	4	6.00	3	17
...	...	...	...	...	...	...
99	0.76	0.79	99	5.00	17	83
100	0.08	0.18	100	1.00	3	3

Elaboración: el Autor de la Tesis

La distribución de pérdidas agregadas puede ser construida a través de la convolución de las diferentes distribuciones de pérdidas. La siguiente tabla muestra la distribución de pérdidas generada.

Tabla V.16 Distribución de Pérdidas

PERDIDA	Frecuencia Perdidas	Probabilidad	Probabilidad Acumulada	PERDIDAxProbabilidad	(PERDIDAxProbabilidad)^2*Probabilidad
0	20	2.00%	2.00%	40.00%	4
1	5	0.50%	2.50%	2.50%	0
2	15	1.50%	4.00%	22.50%	0
3	15	1.50%	5.50%	22.50%	0
4	20	2.00%	7.50%	40.00%	0
...	...	...	...	...	...
540	1	0.10%	99.70%	0.10%	291
582	1	0.10%	99.80%	0.10%	339
700	**1**	**0.10%**	**99.90%**	0.10%	490
1,083	1	0.10%	100.00%	0.10%	1,172
Total Eventos	**1,000**	**100.00%**		**14**	**7,143**

Media =	14	Desviacion T.=	85

Fuente y Elaboración: el Autor de la Tesis

Bajo el supuesto de correlación perfecta entre las pérdidas de cada agrupación, el requerimiento de capital total para la entidad puede ser

determinado a través de la suma del VaR, obtenido de las distribuciones de pérdidas de cada agrupación realizada.

En este contexto, si la entidad financiera quiere cubrir un riesgo del 99,9%, es decir un Var (99,9%) la pérdida a cubrir sería de 700.

CAPÍTULO VI

BENEFICIOS DE LA METODOLOGÍA DE RIESGOS DE OPERACIÓN

El objetivo de este capítulo es dar a conocer los beneficios que tendría la entidad financiera en el caso adopte una metodología de riesgos operativos, se plantean beneficios cuantitativos y beneficios cualitativos

6.1. Beneficios Cualitativos

- El beneficio, que justifica la viabilidad legal y política, es que permite el cumplimiento del marco regulatorio exigido por la SBS.
- Permite la estandarización y el establecimiento de procedimientos, normas internas, plantillas, herramientas manuales y tecnológicas, para gestionar la gestión de riesgos, por ende se crea disciplina interna de gestión y control del riesgo operativo.
- Permite que la organización se involucre y comprometa con medidas permanentes de mejora continua, por ende es generador de cultura organizacional
- Dada la implementación de la metodología se llevará a cabo un mejor control del origen de los riesgos, se evitará errores en la

captura y tratamiento de los riesgos y por ende se generará confianza en las operaciones de negocio.

- Impulsa que se identifiquen tanto las brechas y riesgos de seguridad de información así como aquellos que puedan producir la no continuidad de los servicios u operaciones de la entidad financiera.
- A través de la aplicación de indicadores se podría realizar el seguimiento de los riesgos, ver el desempeño de aquellos que resulten claves para el negocio y por ende permitir la toma de decisiones.

6.2. Beneficios Cuantitativos

Si bien se entiende que la aplicación de la metodología se podría traducir en la generación de mecanismos que permitan la reducción de las pérdidas operativas o bien contribuir en el incremento del valor de los accionistas, lo cierto que el principal beneficio de la aplicación de la metodología, por ende realizar la gestión de riesgos operacionales, está ligados a otorgar una mejor disciplina financiera para la asignación de recursos. En efecto, el riesgo operativo y su evaluación cuantitativa (un porcentaje de los ingresos-llamado capital regulatorio exigido por la SBS) consume un porcentaje del capital económico de la entidad financiera, dicho porcentaje representa una medida de pérdidas no esperadas.

Si bien ese es el mayor beneficio, es necesario tener un entendimiento de los beneficios de implantar un modelo de gestión de riesgos de

operación (en el que disponer de una metodología como soporte básico y necesario al proceso de gestión) se realiza un análisis de flujo de caja de un proyecto para implantar un modelo de gestión de riesgos de operación.

6.2.1. Viabilidad Económica

Para realizar la viabilidad económica utilizaran métodos que consideran el valor del dinero en el tiempo, como son el Valor Actual Neto (VAN), utilizando una tasa de descuento de 10% anual y la Tasa Interna de Retorno (TIR), para ello se parte algunos datos precisos obtenidos del mercado y algunos otros basados en supuestos:

A. Información Obtenida del Mercado

A.1. Precio del Software

Teniendo como referencia, la ADJUDICACION DE MENOR CUANTIA AMC N° 0030-2010 "SISTEMA PARA LA GESTION DE RIESGOS OPERATIVOS" derivada de la (Derivada de la ADS N° 0069-2009-DL-BN) (información disponible en Internet debido a la Ley de Transparencia), por el cual el Banco de la Nación abre un proceso de adjudicación para la compra de un Aplicativo de Software Informático; que permita dar el soporte tecnológico a la Gestión de Riesgos Operativos de dicho Banco.

El análisis que el Banco de la Nación efectúa está basado en un análisis técnico y de costos que se muestran en la siguiente tabla y que sugiere un valor referencial de S/. 36,800 para 40 licencias de usuario.

Tabla VI.1 Cuadro de Evaluación de Herramientas Tecnológicas de Riesgo Operativo.

CUADRO DE VALOR REFERENCIAL
Sistema para la gestion de riesgos operativos

FUENTE 1: COTIZACIONES

COTIZACIÓN REFERENCIAL	COTIZACIÓN N° 3 Informatica Delta (Pragma)	COTIZACIÓN N° 1 Plus Technologies & Innovatios	COTIZACIÓN N° 4 Chase Cooper	COTIZACIÓN N° 5 AMS Risk Consulting	COTIZACIÓN N° 2 Price Waterhouse Coopers	Valor Referencial
Sistema para la gestion de riesgos operativos	Monto Total	Monto Total	Monto Total	Monto Total	Monto Total	Monto Total
Licencias	$ 31,000.00	$ 262,827.00	$ 85,000.00	$ 93,240.00	$ 116,000.00	$ 31,000.00
Consultorias				$ 13,445.38	$ 60,400.00	
Capacitacion			$ 25,000.00	$ 5,378.15		
Mantenimeinto		$ 37,561.86	$ 17,000.00			
Otros Gastos		$ 25,963.50		$ 7,563.03	$ 15,000.00	
Costo Neto	$ 31,000.00	$ 326,352.36	$ 127,000.00	$ 119,626.55	$ 191,400.00	$ 31,000.00
Impuestos	$ 5,890.00	$ 62,006.95	$ 24,130.00	$ 22,729.05	$ 36,366.00	$ 5,890.00
Costo Total	$ 36,890.00	$ 388,359.31	$ 151,130.00	$ 142,355.60	$ 227,766.00	$ 36,890.00
COSTO TOTAL	$ 36,890.00	$ 388,359.31	$ 151,130.00	$ 142,355.60	$ 227,766.00	$ 36,890.00
Cumple con los TR	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	
Tipo de proveedor	Domiciliado	No dominicialiado sin sede en el Peru	No dominicialiado sin sede en el Peru	Domiciliado	Domiciliado	

VALOR REFERENCIAL	$	36,890.00	(a)
VALOR SEACE	S/.	100,779.00	(b)

(a) El valor referencial es la menor cotización validada por el área usuaria, mediante EF/92.2410 Nº 0324-2010 y EF/92.2410 Nº 0372-2010
(b) En valor SEACE se esta considerando al ADS 1-2007 BCRP, el cua tiene un objeto de convocatoria símilar.
(c) El valor historico, No se ha adquirido anteriormente un sistema de gestion de riesgos operativos en el BN, es por ello que se ha desarrollado un base de datos manual
Tipo de Cambio de la SBS de 06/04/2010 2.839

FUENTE 2: VALOR SEACE

Valor Historico	ADS-1-2007-BCRPLIM "Software para evaluación de riesgos operacionales y tecnológicos"
COSTO TOTAL	S/. 100,779.00

Fuente y Elaboración: Banco de la Nación.

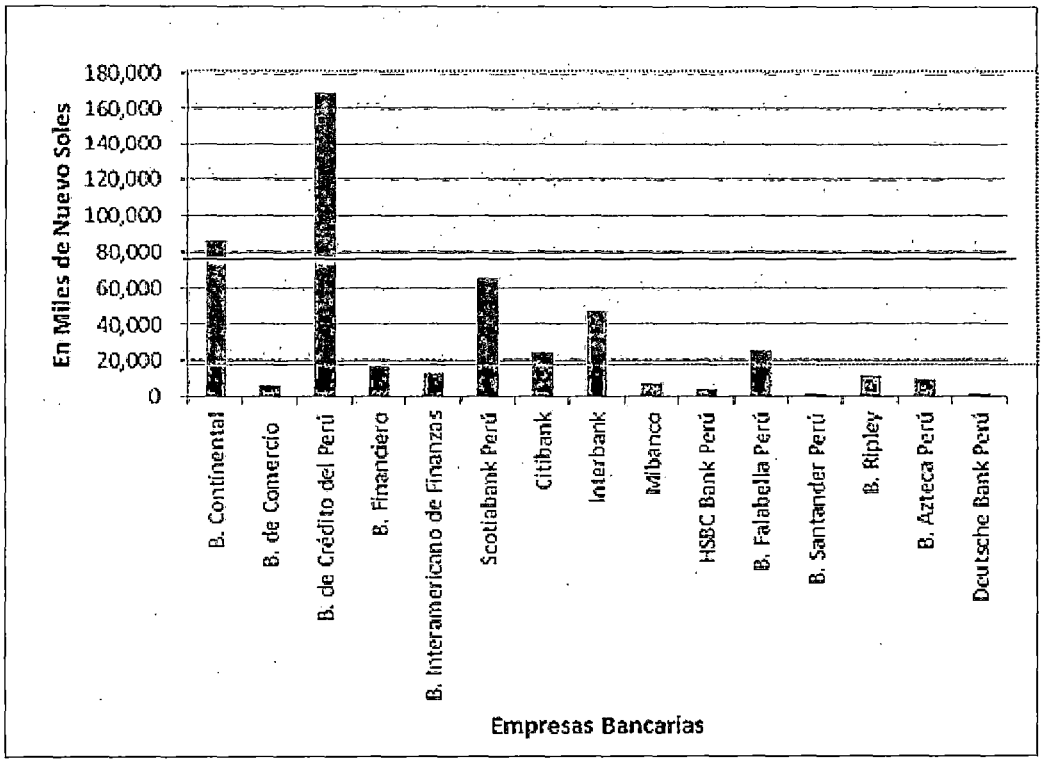
A.2. Cálculo de Requerimiento de Capital

Como se pudo analizar previamente el Requerimiento de Patrimonio Efectivo por Riesgo Operativo y se encuentra en proceso gradual de ajuste y que debe terminar a mediados de año del 2012. Es así que a diciembre del 2010, el 4.5% del total del patrimonio requerido al sistema financiera corresponde al riesgo operativo.

De esta manera, según la SBS y a Junio de 2011 el Requerimiento de Patrimonio Efectivo por Riesgo Operativo de las Empresas Bancarias asciende a un total de 495,427 miles de nuevos soles y en donde el Banco de Crédito se diferencia de las otras significativamente. Teniendo en cuenta que cuatro son los bancos con mayor

representatividad (75%) en cuanto a requerimiento de capital se ha calculado la media aproximada de 92,060 miles de nuevos soles

Figura VI.1 Requerimiento de Patrimonio Efectivo de Riesgo Operativo, Junio de 2011



Fuente: SBS, Elaboración: Propia

B. Flujo de Caja Económico

A continuación se presentan los supuestos siguientes:

- Ingresos totales de la entidad: 1"150,750 (en miles de nuevos soles) con tasa anual de crecimiento del sector de 5%
- Ingresos de la entidad a consecuencia de la implementación de la gestión de riesgos que utiliza la metodología propuesta: 13% de los ingresos

- Capital requerido sin metodología de riesgos 12% de los ingresos = 57537 (en miles de nuevos soles)
- Capital requerido sin metodología de riesgos 8% = 92,060 (en miles de nuevos soles), según cifra del mercado
- Inversión en software para 500 licencias = 460 (en miles de nuevos soles)
- Inversión en puesta en marcha = 100 (en miles de nuevos soles)
- Gastos en RRHH = 720 (en miles de nuevos soles)
- Otros Gastos = 100 (en miles de nuevos soles)
- Tasa de descuento: 10%
- IGV: 19%

Con esa información se obtiene la información de la Tabla 7.3 el cual presenta los indicadores estimados que hacen factible la realización de implantar un proyecto de gestión de riesgo operacional donde se aplique la metodología propuesta.

Tabla VI.2 Flujo de Caja de Proyecto de Riesgo Operativo.

	Año 0	Año 1	Año 2	Año 3
Ingresos		28,769	30,495	32,325
Ganancias por implantar gestión de riesgos operacional		28,769	30,495	32,325
Egresos		26,037	27,555	29,166
RR.HH.		720	720	720
Otros (incluye Requerimiento de Capital)		25,317	26,835	28,446
UAI		2,732	2,939	3,159
IGV a pagar		519	558	600
UDI		2,213	2,381	2,559
Inversión	2,920			
Gastos (software, puesta en parcha, publicidad)	2,920			
Préstamo	0			
Flujo	-2,920	2,213	2,381	2,559

Tasa	10%
VAN	2,711
TIR	61%

Elaboración: Propia

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

Las conclusiones de estas tesis son las siguientes:

- Se ha demostrado, a partir del cuestionario realizado a las entidades financieras que existe una carencia de componentes metodológicos cualitativos y cuantitativos y que en muchos casos la metodología no es lo suficientemente madura.
- Si bien el mercado de riesgo operativo aún está en etapa de desarrollo y madurez, lo cierto es que existen dificultades e inconvenientes en su implementación, entre los cuales se encuentra, después de la cultura de la empresa, la falta de un marco metodológico acorde.
- La base de una metodología de gestión de riesgos es el establecimiento de un Marco de Gestión Integral de Riesgo Operativo, el cual, debe considerar la composición de los elementos estratégicos y de organización entre los cuales destacan la estructura organizativa, la definición de un modelo general, así como las políticas y la metodología propiamente dicha.

- El enfoque metodológico cualitativo, en cuanto al uso de herramientas, no tiene una única receta para gestionar sus riesgos, es posible trabajar en un enfoque mixto en el que se conjuguen diversas herramientas como las autoevaluaciones, los mapas de riesgo e indicadores entre los principales.
- En el enfoque metodológico cuantitativo, según el marco legal, el método del indicador básico no tiene exigencias para su uso como si lo tienen los métodos estándar o avanzado y que requieren autorización previa del Supervisor, quien revisa el modelo, así como los requisitos cuantitativos y cualitativos como el hecho de hecho de tener una estructura organizativa que incentive y promueva la gestión del riesgo operativo.
- En el enfoque metodológico cuantitativo, los métodos van en complejidad creciente desde el indicador básico hasta el avanzado, y que es así justamente porque el propósito es proporcionar incentivos para que las entidades se desplacen a entornos más precisos y sofisticados de medición y gestión del riesgo operacional, es decir, si bien el método de indicador básico es menos complejo este es menos preciso y menos sofisticado. Posicionarse en un enfoque avanzado, significa ahorros de capital regulatorio. Las entidades que adopten este enfoque podrán calcular los recursos propios en función de su perfil real de riesgo, de los controles establecidos y del marco de gestión que hayan definido

- El enfoque o manera que tendrá la entidad para gestionar sus riesgos operacionales dependerá de una variedad de factores, incluyendo su tamaño y sofisticación y la naturaleza y complejidad de sus actividades.
- La Base de Datos de Pérdida Operacional resulta ser un elemento indispensable en la gestión tanto cualitativa como cuantitativa ya que la información de esta sirve para la modelización del riesgo, para el cálculo en riesgo y la gestión en general.
- El Riesgo Operativo va a evolucionar en la medida que evolucione la contabilidad, esto es, se requiere que los riesgos de operación tengan cuentas específicas de modo que el impacto económico de los diversos tipos de pérdidas se encuentren registrados en la cuentas específicas de riesgos de operación.

Recomendaciones:

Las recomendaciones de estas tesis son las siguientes:

- Establecer un Marco de Gestión Integral de Riesgo Operativo, el cual, debe considerar la composición de los elementos estratégicos y de organización entre los cuales destacan la estructura organizativa.
- Considerar la importancia de cultura organizacional como factor positivo o negativo cuando se requiera implementar la Gestión de Riesgo Operacional ya que esta alcanza a toda la empresa, por

ellos es importante que Alta Dirección acompañe en la estrategia de adopción.

- En cuanto al enfoque metodológico cualitativo y cuantitativo se recomienda
- En cuanto al enfoque metodológico cuantitativo, se recomienda planificar se desplacen progresivamente a entornos más precisos y sofisticados de medición como lo pueden ser los métodos avanzados.
- Se recomienda al Supervisor, elaborar un Plan de Contabilidad que tengan cuentas específicas de riesgo operacional de modo que el impacto económico de los diversos tipos de pérdidas se encuentren registrados en las cuentas específicas de riesgos de operación.
- La gestión de riesgo operativo no debe de ser una actividad orientada a la detección de riesgos, sino que permita a las entidades financieras lograr ventajas competitivas y llegar a un estado de madurez suficiente que impacten positivamente en aspectos relacionados con la mejora en la imagen y calidad de servicio, la reducción de pérdidas y la mejora en la capacidad de producción de la entidad financiera.

GLOSARIO DE TÉRMINOS

Basilea II Es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos

ERM COSO Es una metodología para gestionar los riesgos corporativos.

Evento de riesgo operacional Es un suceso o serie de sucesos, de origen interno o externo, que puede o no derivar en pérdidas financieras para la entidad.

Factor de riesgo operacional Es la causa primaria o el origen de un evento operacional.

ISO/IEC 17799 Es un estándar para la seguridad de la información. En Perú la ISO/IEC 17799:2000 es de uso obligatorio en todas las instituciones públicas desde agosto del 2004

Mapa de riesgos Es una herramienta que permite presentar una panorámica de los riesgos a los que está expuesta la entidad; independiente de la forma de su presentación, en el que se identifican y se ubican las áreas/actividades/activos (procesos) que podrían verse afectados durante la ocurrencia de un evento adverso. Permite ver las amenazas y medir la magnitud de cada riesgo (probabilidad e impacto económico). Son un instrumento gráfico de gestión de los riesgos que permite comparar los riesgos por su importancia relativa así como en conjunto, permitiendo a la entidad establecer niveles aceptables de riesgo.

Línea de negocio	Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios para atender un segmento de mercado objetivo.
Proceso	Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el usuario, sea interno o externo.
Riesgo inherente	Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
Riesgo residual	Nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han instrumentado los controles pertinentes para su tratamiento. En todo caso exige un permanente monitoreo para observar su evolución.
SBS	Iniciales de Superintendencia de Banca, Seguros y Administradoras de Fondo de Pensiones

BIBLIOGRAFÍA

LIBROS

[L-01] Fernández-Laviada, Ana, "*La Gestión de Riesgo Operativo: De la teoría a su aplicación*", LIMUSA Noriega Editores, 2007.

[L-02] Comité de Supervisión Bancaria de Basilea, *"Buenas prácticas para la Gestión y Supervisión del Riesgo Operativo"*, Secretaría del Comité de Supervisión Bancaria de Basilea c/o Bank for International Settlements, 2003.

[L-03] Jorion, Philippe, "*Valor en Riesgo: el nuevo paradigma para el control de riesgos con derivados*". LIMUSA Editores, México 2002.

[L-04] Jorion, Philippe, "*Value at Risk The New Benchmark for Managing Financial Risk*" Third Edition, Ed. McGrawHill- US 2007.

[L-05] Hernández Sampieri, Roberto, Fernández Collado, Carlos y Baptista Lucio, Pilar "*Metodología de la Investigación*" Cuarta Edición. Ed. McGrawHill- México, 2006.

[L-06] Gifman, Lawrence y Joehnk, Michael "*Fundamentos de Inversión*" Ed. Pearson- España 2005.

[L-07] Scheeser Study Notes, BOOK 5 "*Fixed Income, Derivvative and Alternative Investments*", CFA Institute, 2008.

[L-08] Ferreras Salagre, Alberto, "*Riesgo Operacional, Enfoque de distribución de pérdidas en la práctica*", Consejo Económico España, 2009.

[L-09] Jiménez Rodriguez, Enrique J. "*El Riesgo Operacional, Metodologías para su medición y Control*", Publicaciones Delta, 2010.

TESIS

[T-01] Giménez Martínez, José Ignacio "*Sistema de Medición Cuantitativa del Riesgo Operativo en Entidades financieras*", Universidad Pontificia Comillas Escuela técnica Superior de Ingeniería, Madrid, Junio 2006.

[T-02] Falen Lara, Wilson Paul, "*Gestión de Riesgos en las Casas de Bolsa. CASO: Sociedades Agentes de Bolsa en el Perú*" Universidad del Pacífico. Escuela De Postgrado. 2006.

[T-03] Dallagnol Filho, Valdemar Antonio "*Portfolio Management Using Value at Risk: A Comparison Between Genetic Algorithms and Particle Swarm Optimization*" Erasmus Univeristeit Rotterdam, 2006.

[T-04] Linares Vásquez, Mario "*Desarrollo de una Herramienta Computacional, Basada En Minería De Datos, Para Soporte Al Proceso De Selección De Portafolio"* Universidad Nacional de Colombia, Facultad de Ingeniería. Bogota, 2007.

[T-05] Bernales Silva, Alejandro Adrián, "*Metodología e Implementación de Métodos de "Value At Risk" en Mercados de Renta Fija con Baja Frecuencia de Transacciones*", Pontificia Universidad Católica de Chile, Escuela de Ingeniería, Chile, 2005.

[T-06] Dionne, Georges y Dahen, Hela "*What about Underevaluating Operational Value at Risk in the Banking Sector?*" Centre InterUniversitaire sur le Risque, les Politiques Economiques et l'Emploi., Montreal 2007.

MEMORIA

[M-01] Superintendencia de Banca, Seguros y AFP, Memoria Anual 2010

PAPERS

[P-01] Franco Arbeláez, Luis Ceferino *"El Valor en Riesgo Condicional-CVAR Como Medida Coherente De Riesgo"*, Ed. Madrid, 2005.

[P-02] Martín Mato, Miguel Ángel "*El Condicional Value at Risk en la Gestión de Carteras Latinoamericanas*", 2006.

[P-03] Carrillo Menéndez, Santiago "*El Riesgo de Mercado enla Práctica*", RiskLab- Madrid, 2000

[P-04] Cabrales M., Castillo, "*Diseño de una Metodología para la Medición y el Monitoreo del Riesgo de Liquidez en Instituciones Financieras Colombianas S.A.*" Universidad de los Andes, Bogotá, Colombia, 2004

[P-05] Suárez Rincón, Luz "*El Valor en Riesgo como Herramienta de Medición del Riesgo Financiero y su Uso En Colombia*" 2007.

[P-06] Morera Martinelli, Ana Patricia "*VaR: Una Opción para Medir el Riesgo de Mercado en los Fondos de Pensiones*", Departamento de Estudios Especiales y Valoración de Riesgo, Superintendencia de Pensiones, Agosto del 2002

REVISTAS

[R-01] Romero Meza, Rafael "*Medidas de Riesgo Financiero*", Revista Economía y Administración, Marzo / Abril 2005 Nº149, ISSN 076-4793

[R-02] Revista Electrónica CEO, "*Responsabilidad Social Corporativa*", Año 3 Edición Especial 2007.

ANEXOS

A1. RESOLUCIÓN SBS N° 2115-2009: Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operativo

Lima, 02 de abril de 2009

Resolución S.B.S.
N° 2115 -2009

El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, mediante el Decreto Legislativo N° 1028 se modificó la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702, en adelante Ley General, para permitir la implementación en nuestro país a partir del 1 de julio de 2009 de los estándares recomendados por el Comité de Supervisión Bancaria de Basilea referidos a medidas y normas de capital;

Que, la implementación en nuestro país de los estándares recomendados por el Comité de Supervisión Bancaria de Basilea permitirá adecuar los requerimientos de patrimonio efectivo al riesgo efectivamente asumido por las empresas;

Que, en el artículo 186° de la Ley General modificado por el Decreto Legislativo N° 1028 se establece que para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional, las empresas del sistema financiero utilizarán el método del indicador básico, el método estándar alternativo o métodos avanzados;

Que, en el artículo 194° de la Ley General modificado por el Decreto Legislativo N° 1028 se dispone que las empresas del sistema financiero podrán iniciar el cálculo del requerimiento de patrimonio efectivo por riesgo operacional mediante el método del indicador básico o el método estándar alternativo. No obstante, se precisa que para el uso del método estándar alternativo se requiere previa autorización de la Superintendencia según las normas que establezca este Organo de Control;

Que, asimismo, en el artículo 194° de la Ley General modificado por el Decreto Legislativo N° 1028 se señala que para hacer uso de los métodos avanzados se requiere, también, autorización previa de esta Superintendencia según las normas que establezca este Organo de Control;

Que, en consecuencia, resulta necesario establecer la metodología que deberá aplicarse, así como los requisitos que deberán cumplirse, para efectuar el cálculo del

requerimiento de patrimonio efectivo por riesgo operacional bajo el método del indicador básico, el método estándar alternativo o los métodos avanzados:

Que, mediante Resolución SBS N° 895-98 y sus normas modificatorias y complementarias se aprobó el Manual de Contabilidad para las Empresas del Sistema Financiero:

Que, resulta necesario modificar el Capítulo V "Información Complementaria" del Manual de Contabilidad para incorporar los Reportes correspondientes al cálculo de los requerimientos de patrimonio efectivo por riesgo operacional:

Estando a lo opinado por las Superintendencias Adjuntas de Banca y Microfinanzas, de Riesgos y de Asesoría Jurídica, así como por la Gerencia de Estudios Económicos; y,

En uso de las atribuciones conferidas en los numerales 7, 9 y 13 del artículo 349° de la Ley General,

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operacional que forma parte integrante de la presente Resolución.

Artículo Segundo.- Modifíquese el Manual de Contabilidad para las Empresas del Sistema Financiero en los siguientes términos:

Incorpórese en el Capítulo V "Información Complementaria" los Reportes N° 2-C1 y N° 2-C2 denominados "Requerimiento de Patrimonio Efectivo por Riesgo Operacional – Método del Indicador Básico" y "Requerimiento de Patrimonio Efectivo por Riesgo Operacional – Método Estándar Alternativo", respectivamente, conforme a los formatos señalados en los Anexos 4 y 5 del Reglamento aprobado por la presente Resolución.

La remisión de dichos reportes se efectuará por medio del Submódulo de Captura y Validación Externa (SUCAVE).

Artículo Tercero.- Los anexos que forman parte del Reglamento aprobado por la presente Resolución se publican en el Portal institucional (www.sbs.gob.pe), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS.

Artículo Cuarto.- Incorpórese el procedimiento N° 124 "Autorización para utilizar el método estándar alternativo para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional" en el Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia de Banca, Seguros y AFP aprobado mediante Resolución SBS N° 131-2002, cuyo texto se anexa a la presente Resolución y se publica conforme lo dispuesto en el Decreto Supremo N° 004-2008-PCM, reglamento de la Ley N° 29091. (Portal institucional: www.sbs.gob.pe).

Artículo Quinto.- La presente Resolución entrará en vigencia a partir del 1 de julio de 2009.

Regístrese, comuníquese y publíquese,

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

REGLAMENTO PARA EL REQUERIMIENTO DE PATRIMONIO EFECTIVO POR RIESGO OPERACIONAL

CAPITULO I
PRINCIPIOS GENERALES

Artículo 1°.- Alcance
Las disposiciones de la presente norma son aplicables a las empresas comprendidas en los literales A y B del artículo 16° de la Ley General, al Banco de la Nación, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco Agropecuario, al Fondo MIVIVIENDA S.A. y al Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), en adelante las empresas.

Artículo 2°.- Definiciones

Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Casa Matriz: Se refiere a la sociedad principal o a la que ejerza el control en un conglomerado financiero o mixto.
b. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
c. Evento de pérdida por riesgo operacional: El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.
d. Pérdida: Es un impacto negativo en los ingresos o en el valor patrimonial de la empresa.
e. Pérdida esperada: Expectativa de pérdida que se encuentra asociada a la marcha regular del negocio.
f. Pérdida no esperada: Es la diferencia entre la máxima pérdida que enfrentaría la empresa dado un nivel de confianza estadístico asociado, y la pérdida esperada.
g. Riesgo operacional: Es la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.
h. Superintendencia: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

Artículo 3°.- Requerimiento de patrimonio efectivo por riesgo operacional
Las empresas deberán destinar patrimonio efectivo para cubrir el riesgo operacional que enfrentan. Para el cálculo de dicho requerimiento patrimonial, las empresas deberán aplicar uno de los siguientes métodos:

a. Método del indicador básico
b. Método estándar alternativo
c. Métodos avanzados

El uso del método estándar alternativo o de los métodos avanzados requiere la autorización expresa de la Superintendencia.

En tanto no cuenten con la autorización señalada en el párrafo anterior, las empresas deberán aplicar el método del indicador básico.

Para hallar el equivalente a los activos ponderados por riesgo (APR) en el caso de riesgo operacional, se multiplicará el requerimiento patrimonial calculado según los métodos señalados al inicio de este artículo, por la inversa del límite global que establece la Ley General en el artículo 199° y la Vigésima Cuarta Disposición Transitoria.

Adicionalmente, el APR por riesgo operacional deberá ser multiplicado por un factor, cuyo valor corresponderá al indicado en la siguiente tabla:

Periodo	Factor de ajuste
Julio de 2009 - Junio de 2010	0,40
Julio de 2010 - Junio de 2011	0,40
Julio de 2011 – Junio de 2012	0,50
Julio de 2012 – En adelante	1,00

Artículo 4°.- Proceso de autorización ante la Superintendencia
Las empresas que deseen utilizar el método estándar alternativo o los métodos avanzados, deberán presentar a la Superintendencia una solicitud de autorización suscrita por el Gerente General, la cual deberá ir acompañada de los siguientes documentos:

- Copia certificada del acuerdo del Directorio u órgano social equivalente donde conste la decisión de solicitar la autorización correspondiente a la Superintendencia.
- Declaración de cumplimiento de los requisitos establecidos en el presente reglamento, adjuntando un informe que describa la forma en que la empresa cumple con cada requisito, según el método que solicite. Dicho informe deberá presentarse conforme al formato publicado por la Superintendencia en el Portal del Supervisado, debiendo mantenerse la correspondiente información de sustento a disposición de la Superintendencia.

En el caso del método estándar alternativo, luego de recibida la solicitud con los documentos requeridos, la Superintendencia emitirá su pronunciamiento en un plazo que no excederá de sesenta (60) días útiles.

En el caso de los métodos avanzados, luego de recibida la solicitud con los documentos requeridos, la Superintendencia iniciará un proceso de validación que podrá durar hasta dos (2) años, durante el cual se realizarán cálculos paralelos del requerimiento patrimonial. Luego de culminada la validación y habiendo obtenido la autorización de la SBS para el uso del método avanzado, las empresas autorizadas deberán aplicar durante los dos (2) primeros años pisos regulatorios para el cálculo de requerimiento patrimonial. Es decir, el requerimiento patrimonial por riesgo operacional no podrá ser menor que un porcentaje del requerimiento establecido antes de la aprobación del método avanzado. Los porcentajes a aplicar serán los siguientes: 90% durante el primer año y 80% durante el segundo año.

CAPITULO II
METODO DEL INDICADOR BÁSICO

Artículo 5°.- Definición del indicador de exposición por riesgo operacional
Este método de cálculo considera como indicador de exposición el 'margen operacional bruto' de la empresa, el cual se define como la suma de los ingresos financieros y los ingresos por servicios menos los gastos financieros y los gastos por servicios.

En tal sentido, para calcular el margen operacional bruto, se utilizarán las siguientes cuentas contables:

Composición del indicador	Cuentas del Manual de Contabilidad
(+) Ingresos	
Ingresos financieros	5100
Ingresos por servicios	5200 + 5700
(-) Gastos	
Gastos financieros	4100
Gastos por servicios	4200 + 4900

Para el cálculo del requerimiento patrimonial, se utilizará el saldo anualizado del margen operacional bruto, es decir, el total de margen obtenido durante los últimos 12 meses. Para ello, se utilizarán los saldos anualizados de las cuentas contables señaladas en el cuadro anterior. La anualización de los saldos se realizará conforme al procedimiento descrito en el Anexo 1.

Artículo 6°.- Cálculo del requerimiento patrimonial
El requerimiento patrimonial por riesgo operacional según el método del indicador básico será equivalente al promedio de los saldos anualizados de los márgenes operacionales brutos de la empresa, considerando los últimos 3 años, multiplicado por un factor fijo.

Si el margen operacional bruto correspondiente a alguno de los tres últimos años es cero o es un número negativo, dicho(s) año(s) no debe(n) ser considerado(s) en el cálculo del promedio, en cuyo caso se calculará sobre la base del número de años cuyo margen operacional bruto sea positivo.

La fórmula de cálculo a utilizar es la siguiente:

$$R = \alpha \sum_{i=1}^{n} (MO_i) \; / \; n$$

donde:
R : Requerimiento patrimonial por riesgo operacional
MO_i : Saldo anualizado del margen operacional bruto correspondiente al año i, en los casos que sea positivo
α : Factor fijo igual a 15%
n : Número de años en los que el saldo anualizado del margen operacional bruto fue positivo, considerando los 3 últimos años.

Las empresas deberán presentar a la Superintendencia el cálculo del requerimiento patrimonial por riesgo operacional según el método del indicador básico en el formato señalado en el Anexo 4. Esta información deberá ser remitida mensualmente vía SUCAVE en un plazo que no exceda de 15 días calendario de concluido el mes a que corresponde dicho cálculo.

Artículo 7°.- Consideraciones adicionales
Las empresas que cuenten con menos de 36 meses de operación realizarán el cálculo del requerimiento patrimonial por riesgo operacional según lo siguiente:

a) Durante los primeros 12 meses de operación, el requerimiento patrimonial será equivalente al 15% del margen operacional bruto acumulado durante el periodo en que viene operando.

La fórmula es la siguiente:

R = MO

Donde:

R : Requerimiento patrimonial por riesgo operacional
MO : Margen operacional bruto acumulado durante el periodo que viene operando
: Factor fijo igual a 15%

Si el margen operacional bruto acumulado es cero o negativo, el requerimiento patrimonial, según el método del indicador básico, será cero. No obstante, deberá tenerse en cuenta lo señalado en la Primera Disposición Final del presente Reglamento.

b) A partir del mes 13 y hasta el mes 23 de operación, el requerimiento patrimonial por riesgo operacional será igual al 15% del saldo anualizado del margen operacional bruto considerando sólo un periodo completo que incluya los últimos doce meses.

c) A partir del mes 24 y hasta el mes 35 de operación, el requerimiento patrimonial por riesgo operacional será igual al promedio del saldo anualizado del margen operacional bruto considerando los dos últimos periodos de doce meses (dos años), multiplicado por 15%. Se utilizará la siguiente fórmula:

$$R = \left(\sum_{i=1}^{n} MO_i \right) \alpha$$

Donde:

R : Requerimiento patrimonial por riesgo operacional
MO_i : Saldo anualizado del margen operacional bruto correspondiente al año i, en los casos que sea positivo
: Factor fijo igual a 15%
n : Número de años en los que el saldo anualizado del margen operacional bruto fue positivo, que será como máximo 2

Si el margen operacional bruto correspondiente a alguno de los dos años de operación es cero o es un número negativo, dicho(s) año(s) no debe(n) ser considerado(s) en el cálculo del promedio.

CAPITULO III
MÉTODO ESTANDAR ALTERNATIVO

Artículo 8°.- Requisitos mínimos para el uso del método estándar alternativo
Las empresas que deseen emplear el método estándar alternativo deberán cumplir con los siguientes requisitos:

a. El Directorio y la Gerencia General deben participar activamente en la gestión del riesgo operacional.

b. La empresa debe contar con una función de gestión del riesgo operacional cuyas responsabilidades se encuentren claramente especificadas, y que consideren como mínimo los aspectos señalados en el Reglamento para la Gestión del Riesgo Operacional.

c. La empresa debe contar con un programa de capacitación profesional dirigido a perfeccionar los conocimientos, aptitudes y otras competencias del personal especializado en la gestión del riesgo operacional.

d. La empresa debe contar con una metodología de gestión del riesgo operacional que sea conceptualmente sólida y que se encuentre implementada en su totalidad.

e. La empresa debe contar con recursos suficientes para aplicar su metodología de gestión de riesgo operacional, tanto en sus principales áreas de negocio como en sus áreas de apoyo y de control.

f. La empresa debe establecer reportes periódicos sobre su exposición al riesgo operacional, que incluyan las pérdidas importantes ocurridas, dirigidos a las gerencias de las unidades de negocio y de apoyo, gerencia general y al Directorio. La empresa debe establecer procedimientos para tomar acciones apropiadas según la información incluida en dichos reportes.

g. La empresa debe establecer procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional, y debe establecer políticas para tratar los casos de incumplimiento.

h. La empresa debe establecer incentivos monetarios y no monetarios a la apropiada gestión del riesgo operacional, incluidos en el sistema de evaluación de desempeño de la Gerencia y los principales participantes en dicha gestión.

i. La empresa debe contar con una base de datos de eventos de pérdida por riesgo operacional, con las características señaladas en la normativa vigente.

j. La empresa deberá implementar un sistema de gestión de la continuidad del negocio conforme a la normativa vigente, que tenga como objetivo asegurar un nivel aceptable de operatividad de sus procesos críticos, ante eventos que puedan afectar la continuidad de sus operaciones.

k. La empresa deberá contar con un sistema de gestión de la seguridad de la información conforme a la normativa vigente, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información.

l. La evaluación de la gestión del riesgo operacional deberá contar con una revisión cuando menos anual, por parte de la Unidad de Auditoría Interna. Estas revisiones deben considerar las actividades de las áreas de negocio y de apoyo, así como la función de gestión del riesgo operacional, de acuerdo a su plan de trabajo.

m. La empresa deberá contar con una revisión independiente de la gestión del riesgo operacional realizada por una sociedad de auditoría externa o una firma nacional o extranjera, que acredite contar con el conocimiento y experiencia requerida, que no se encuentre relacionada mediante vínculos de gestión o propiedad. Tratándose de una sociedad de auditoría externa, la revisión independiente deberá ser realizada por una sociedad o equipo distinto del que emitió el informe anual de los estados financieros, durante los dos años anteriores al inicio de la revisión. Cuando la revisión independiente sea efectuada por otras firmas distintas a las sociedades de auditoría externa, estas no deberán haber realizado actividades de consultoría relacionadas a la gestión del riesgo operacional en la empresa, durante los dos años anteriores al inicio de la revisión.

El Comité de Auditoría Interna de la empresa deberá aprobar la contratación de la sociedad de auditoría externa o firma encargada de la referida revisión.

La revisión deberá evaluar cuando menos los requisitos indicados en el presente artículo, y los criterios detallados en el informe a que hace referencia el artículo 4°, que deberá ser actualizado por la Gerencia, según la última versión publicada en el Portal del Supervisado a la fecha del inicio de la revisión.

La revisión independiente deberá efectuarse al menos cada tres años contados desde la fecha en que se emite la Resolución de Autorización para el uso del método estándar alternativo. Sólo en los años que se realizan dichas revisiones, se puede dejar sin efecto lo requerido en el artículo 18° del Reglamento para la Gestión del Riesgo Operacional.

Asimismo, las empresas deberán informar a la Superintendencia acerca de las revisiones independientes, cuando menos treinta (30) días antes del inicio de la revisión. La Superintendencia podrá solicitar que dicha revisión incluya procedimientos extendidos en las áreas que estime necesarias, asociadas a la gestión del riesgo operacional, de seguridad de información y de continuidad del negocio. Adicionalmente, podrá solicitar en cualquier momento, adelantar la revisión esperada dentro del ciclo de tres años previstos."[1]

Artículo 9°.- Determinación de líneas de negocio
En este método, las actividades de las empresas son divididas en las siguientes líneas de negocio:

Línea de negocio	Definición
Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización: underwriting; asesoramiento financiero a empresas corporativas, grandes y medianas empresas, así como al gobierno central y entidades del sector público; entre otras actividades de naturaleza similar.
Negociación y ventas	Operaciones de tesorería: compra y venta de títulos, monedas y commodities por cuenta propia; entre otras actividades de

[1] Literal modificado por la Resolución SBS N° 1855-2010 del 20-10-2010

	naturaleza similar.
Banca Minorista	Financiamiento a clientes minoristas incluyendo tarjetas de crédito, préstamo automotriz, entre otros.
Banca Comercial	Financiamiento a clientes no minoristas, incluyendo: factoring, descuento, arrendamiento financiero, entre otros.
Liquidación y pagos	Actividades relacionadas con pagos y cobranzas, transferencia interbancaria de fondos, compensación y liquidación, entre otras actividades de naturaleza similar.
Otros servicios	Servicios de custodia, fideicomisos, comisiones de confianza y otros servicios.

Artículo 10°.- Definición de los indicadores de exposición por riesgo operacional
Existen dos tipos de indicadores de exposición para las líneas de negocio:

a. **Indicador de exposición para las líneas de negocio distintas a banca comercial y banca minorista:**
Para estas líneas de negocio se utilizará como indicador de exposición al margen operacional anualizado de cada línea. Para ello, debe utilizarse la siguiente fórmula:

$IE_i = Ingresos_i - Gastos_i$

Donde:
IE_i : Indicador de exposición de la línea de negocio i
$Ingresos_i$: Ingreso anualizado de la línea de negocio i
$Gastos_i$: Gasto anualizado asignado a la línea de negocio i

El ingreso anualizado de cada línea de negocio se calculará como el total de los ingresos obtenidos en los últimos doce (12) meses. Asimismo, el gasto anualizado de cada línea de negocio se calculará como el total de los gastos obtenidos en los últimos doce (12) meses.

Para la determinación de los ingresos y gastos anualizados por líneas de negocio se considerarán las cuentas del Manual de Contabilidad de la siguiente manera:

Para la información correspondiente a enero-junio 2010, así como para la información correspondiente al año 2009 y anteriores se utilizará la agrupación de cuentas establecida en el Anexo 2A del presente Reglamento.
Para la información correspondiente a julio 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo 2B del presente Reglamento.[2]

b. **Indicador de exposición para las líneas de banca comercial y banca minorista:**
Para estas líneas de negocio se utilizará como indicador de exposición el saldo de los créditos y las inversiones, multiplicado por un factor fijo.

[2] Párrafo modificado por la Resolución SBS N° 14353-2009 del 30/10/2009

Para su cálculo, deberán considerarse los saldos de créditos e inversiones durante los últimos 12 meses, conforme a la siguiente fórmula:

$$IE = m \times \sum_{i=1}^{12} C_i \cdot 12$$

Donde:

IE: Indicador de exposición anual para la línea de negocio banca comercial o banca minorista

m: 0,035 (Factor fijo)

C_i: Monto del saldo de créditos e inversiones para el mes i para Banca Comercial o Banca Minorista, según corresponda.

Para la calcular el monto del saldo de créditos e inversiones correspondientes a Banca Comercial y Banca Minorista se utilizarán las cuentas del Manual de Contabilidad de la siguiente manera:

Para la información correspondiente a enero-junio 2010, así como para la información correspondiente al año 2009 y anteriores se utilizará la agrupación de cuentas establecida en el Anexo 2A del presente Reglamento.

Para la información correspondiente a julio 2010 y siguientes se utilizará la agrupación de cuentas establecida en el Anexo 2B del presente Reglamento.[3]

Artículo 11°.- Cálculo del requerimiento patrimonial

Se obtienen los indicadores de exposición correspondientes a cada una de las líneas de negocio para los 3 últimos años, y luego éstos son multiplicados por un factor fijo ( ) asociado con cada línea según se muestra en el siguiente cuadro:

Líneas de Negocio	Valor del factor fijo
Finanzas corporativas (1)	18%
Negociación y ventas (2)	18%
Banca minorista (3)	12%
Banca comercial (4)	15%
Liquidación y pagos (5)	18%
Otros servicios (6)	15%

Luego, para cada uno de los años se suman los valores obtenidos para cada línea de negocio (6 valores por cada año). Finalmente, se obtiene el promedio de las sumas obtenidas. El promedio resultante constituirá el requerimiento patrimonial por riesgo operacional.

Si la suma de los productos para un año determinado resulta ser negativa, entonces se considerará el valor de 0 para ese año, en el cálculo del promedio.

El siguiente cuadro muestra el procedimiento de cálculo:

[3] Párrafo modificado por la Resolución SBS N° 14353-2009 del 30/10/2009

Linea de negocio	Factor fijo	Indicador de exposición			Indicador * Factor fijo		
		Año 1	Año 2	Año 3	Año 1	Año 2	Año 3
Finanzas corporativas	18%	IE1	IE2	IE3	R1	R2	R3
Negociación y ventas	18%	IE4	IE5	IE6	R4	R5	R6
Banca minorista	12%	IE7	IE8	IE9	R7	R8	R9
Banca comercial	15%	IE10	IE11	IE12	R10	R11	R12
Liquidación y Pagos	18%	IE13	IE14	IE15	R13	R14	R15
Otros servicios	15%	IE16	IE17	IE18	R16	R17	R18
		Sumas anuales			S1	S2	S3

Requerimiento patrimonial $\max(S_1, S_2, S_3)$

Donde:

IE_i : Indicador de exposición de la línea de negocio i en el año j
R_i : Resultado de multiplicar el indicador de exposición por el factor fijo asociado a cada línea de negocio.
Si : Suma de los productos obtenidos para el año i

Las empresas deberán presentar a la Superintendencia el cálculo del requerimiento patrimonial por riesgo operacional según el método estándar alternativo en el formato señalado en el Anexo 5. Esta información deberá ser remitida mensualmente vía SUCAVE en un plazo que no exceda de 15 días calendario de concluido el mes a que corresponde dicho cálculo.

Artículo 12°.- Consideraciones adicionales
Las empresas que cuenten con menos de 36 meses de operación al momento de utilizar el método estándar alternativo, realizarán el cálculo del requerimiento patrimonial por riesgo operacional según lo siguiente:

a) Durante los primeros 12 meses de operación, los indicadores de exposición señalados en el artículo 10° deberán ser calculados considerando los datos correspondientes al periodo que la empresa viene operando, es decir:

- Para las líneas de negocio distintas a banca minorista y banca comercial, se utilizará el margen operacional acumulado de estas líneas.
- Para banca minorista y banca comercial, se utilizará el promedio de los saldos de las cuentas asociadas, multiplicado por un factor fijo (0,035)

En este caso, el requerimiento patrimonial será equivalente a la suma de los resultados del producto de los factores fijos ( ) señalados en el artículo 11° del presente Reglamento por los indicadores de exposición calculados conforme a lo señalado al inicio de este párrafo.

La fórmula es la siguiente:

$$R = \sum_{i=1}^{n} (IE_i \times \quad)$$

Donde:

R : Requerimiento patrimonial por riesgo operacional
IE_i : Indicador de exposición de la línea de negocio i
α_i : Factor fijo, asignado a la línea de negocio i.

b) A partir del mes 13 y hasta el mes 23 de operación, el requerimiento patrimonial por riesgo operacional se calculará considerando sólo un periodo completo que incluya los últimos doce (12) meses. Se utilizará el procedimiento y la fórmula señalados en el literal anterior.

c) A partir del mes 24 y hasta el mes 35 de operación, el requerimiento patrimonial por riesgo operacional se calculará conforme al procedimiento de cálculo señalado en el artículo 11° del Reglamento, pero aplicado a los dos últimos periodos de doce meses (dos años). Si la suma de los productos obtenidos para uno de los dos años resulta ser negativa, se considerará en el cálculo del promedio el valor de 0 para ese año.

CAPITULO IV
MÉTODOS AVANZADOS

Artículo 13°.- Métodos avanzados
La empresa autorizada a utilizar métodos avanzados calculará el requerimiento patrimonial por riesgo operacional mediante su sistema interno de medición del riesgo operacional.

Artículo 14°.- Uso parcial de los métodos avanzados
La empresa podrá ser autorizada a utilizar un método avanzado para una parte de sus operaciones y el método estándar alternativo en el resto de ellas, siempre que se satisfagan cada una de las condiciones siguientes:

El uso de ambos métodos, en conjunto, tiene como alcance la totalidad de las operaciones de la empresa.
Se satisfacen los requisitos para acceder a métodos avanzados para aquellas operaciones que serán consideradas en la aplicación del método avanzado seleccionado: de igual manera, se satisfacen los requisitos del método estándar alternativo a utilizar en las demás operaciones.
En la fecha de aplicación del método avanzado, una parte significativa del riesgo operacional de la empresa está recogida en dicho método.
La empresa presenta a la Superintendencia un plan que especifique el calendario a seguir para aplicar el método avanzado en todas las operaciones de la empresa (con excepción de aquellas poco significativas).

Artículo 15°.- Requisitos mínimos para el uso de métodos avanzados
Las empresas que deseen emplear los métodos avanzados deberán cumplir con los requisitos cualitativos y cuantitativos establecidos en los artículos 16° y 17° del presente Reglamento.

Artículo 16°.- Requisitos cualitativos
Las empresas deberán contar con los siguientes estándares cualitativos antes de realizar el cálculo del requerimiento de patrimonio efectivo por riesgo operacional basado en modelos internos:

a) La empresa deberá contar con una unidad especializada para la gestión del riesgo operacional.

b) El sistema de medición del riesgo operacional de la empresa deberá estar integrado a sus procesos habituales de gestión de riesgos. La información que se obtenga de dicho sistema deberá ser utilizada como parte integral del proceso de monitoreo y control del perfil de riesgo operacional de la empresa. En ese sentido, esta información deberá ser incorporada en los reportes sobre riesgos, reportes a la gerencia, la asignación de capital y el análisis de riesgos. La empresa deberá implantar técnicas para asignar capital por riesgo operacional a sus principales líneas de negocio y para establecer incentivos para la mejora de la gestión de estos riesgos en toda la entidad.

c) Deberá existir un reporte cuando menos trimestral sobre las exposiciones al riesgo operacional y la experiencia de pérdidas debidas a este riesgo, dirigido a las gerencias de las unidades de negocio, a la Gerencia General y al Directorio. La empresa deberá contar con procedimientos destinados a adoptar las acciones necesarias según la información contenida en dichos reportes de gerencia.

d) El sistema de gestión del riesgo operacional de la empresa deberá estar bien documentado. La empresa deberá contar con un mecanismo que le permita asegurar el cumplimiento de las políticas, controles y procedimientos internos referidos a la gestión del riesgo operacional, que deben estar documentados, y deberá establecer políticas para el tratamiento de los aspectos que no se cumplan.

e) Como parte de la revisión requerida a la Unidad de Auditoría Interna y a una Sociedad de Auditoría Externa, referida a las políticas y procedimientos empleados por la empresa para la gestión del riesgo operacional, debe incluirse una evaluación del sistema interno empleado por la empresa para la medición de este riesgo.

f) La revisión del sistema de medición del riesgo operacional que lleven a cabo los auditores externos deberá verificar que los procesos de validación interna operen de manera satisfactoria y que el flujo y el procesamiento de datos asociados al sistema de medición del riesgo sean transparentes y accesibles.

g) En el caso de empresas con casa matriz en el exterior, la empresa deberá contar con la no objeción del supervisor bancario del país donde se ubica dicha casa matriz, respecto a la aplicación del método avanzado en la empresa.

h) Otros que determine la Superintendencia.

Artículo 17°.- Requisitos cuantitativos

Los métodos avanzados utilizados para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional deberán contar con los siguientes criterios cuantitativos mínimos:

a) **Criterio de solidez**

La empresa deberá ser capaz de demostrar que el método avanzado utilizado identifica eventos de pérdida situados en las colas de la distribución de probabilidad y que generan graves pérdidas. Con independencia del método utilizado, la empresa deberá demostrar que su medida del riesgo operacional satisface un criterio de solidez comparable a un intervalo de confianza del 99,9 por ciento, a lo largo de un periodo de un año.

b) Criterios detallados

1. El sistema interno de medición del riesgo operacional deberá ser consistente con el alcance de la definición de riesgo operacional señalada en la normativa emitida por la Superintendencia, y con los tipos de eventos de pérdida definidos en el Anexo N° 3 de la presente norma.

2. El cálculo del requerimiento patrimonial deberá incluir tanto la pérdida esperada (PE) como la pérdida no esperada (PNE), a menos que la empresa pueda demostrar que ya está recogiendo adecuadamente la PE en sus prácticas internas de negocio. Es decir, para que el requerimiento patrimonial se base sólo en la PNE, la empresa deberá poder demostrar, a satisfacción de la Superintendencia, que ha medido su exposición a la PE y que ha cubierto dicha pérdida.

3. El sistema de medición del riesgo de las empresas deberá identificar los principales factores de riesgo operacional que influyen en la forma de las colas de distribución de las estimaciones de pérdida.

4. Para calcular el requerimiento patrimonial, deben agregarse las mediciones obtenidas a partir de las diferentes estimaciones de riesgo operacional aplicadas. Sin embargo, la empresa podrá considerar las correlaciones existentes en las pérdidas por riesgo operacional, siempre que pueda demostrar a satisfacción de la Superintendencia que sus métodos para determinar las correlaciones son sólidos, se aplican con integridad y tienen en cuenta la incertidumbre asociada con dichas estimaciones de correlación. La empresa deberá validar sus supuestos de correlación usando técnicas cualitativas y cuantitativas adecuadas.

5. El sistema de medición de riesgo operacional deberá poseer elementos básicos que satisfagan el criterio de solidez enunciado en el literal a) del presente artículo. Estos elementos deberán incluir el uso de datos internos, de datos externos relevantes, de análisis de escenarios y de factores que reflejen el entorno del negocio y los sistemas de control interno.

6. La empresa deberá contar con un proceso razonable, transparente, bien documentado y verificable acerca de la determinación de la importancia relativa asignada a cada uno de esos elementos fundamentales dentro de su sistema general de medición del riesgo operacional. El enfoque utilizado deberá ser consistente internamente y evitar la doble consideración de evaluaciones cualitativas o de coberturas del riesgo que ya se encuentren reconocidas en otros elementos del sistema de medición utilizado.

c) Datos internos

1. Las empresas deberán recopilar y analizar sus datos internos sobre eventos de pérdida por riesgo operacional e incorporarlos como parte del sistema interno de medición. Esto puede lograrse de diversas formas, incluyendo el uso de los datos internos de pérdida como base para las estimaciones de riesgos, como un método de validación de los datos de entrada y de salida del sistema de medición o como el enlace entre la experiencia de pérdidas y las decisiones de gestión y control de riesgos.

2. La empresa deberá contar con procedimientos documentados para evaluar la importancia de los datos históricos de pérdida, incluyendo los casos en que se utilicen juicios y opiniones, ajustes de escala u otros tipos de ajustes, el grado en que puedan introducirse dichos ajustes y el personal autorizado para tomar tales decisiones.

3. Las mediciones del riesgo operacional generadas internamente en la empresa y utilizadas para determinar el requerimiento patrimonial deberán estar basadas en un periodo mínimo de cinco (5) años de observación de datos internos de pérdida, ya sea que estos datos se empleen directamente para estimar las mediciones de pérdidas o para su validación.

4. Para efectos del requerimiento patrimonial, los procesos internos de recopilación de datos de pérdida de la empresa deberán satisfacer los siguientes criterios:

   La empresa deberá ser capaz de asignar sus datos internos de pérdida a las 8 líneas de negocio consideradas en el método estándar alternativo y a los tipos de eventos de pérdida señalados en el Anexo 3 de la presente norma, así como proporcionar dichos datos a la Superintendencia en caso de ser requeridos. La empresa deberá contar con criterios objetivos y documentados de asignación de las pérdidas a las líneas de negocio y a los tipos de eventos de pérdida especificados. Sin embargo, la empresa podrá decidir en qué medida desea aplicar esa clasificación por categorías dentro de su sistema interno de medición.

   Los datos internos de pérdida de la empresa deberán ser completos, es decir, deben incluir la totalidad de las actividades y exposiciones importantes existentes en todos los subsistemas y todas las ubicaciones geográficas asociadas. La empresa deberá ser capaz de justificar que las actividades o exposiciones excluidas, tanto en forma individual como conjunta, no tienen un efecto significativo sobre las estimaciones generales de riesgo. La empresa deberá establecer un umbral mínimo adecuado de pérdida bruta para la recopilación de datos internos de pérdida.

   Además del dato referido al monto de la pérdida bruta, la empresa deberá recopilar datos sobre la fecha del evento de pérdida, cualquier recuperación del monto de la pérdida bruta, así como información descriptiva acerca de las causas del evento de pérdida. El nivel de detalle de la información descriptiva deberá estar en proporción con la cantidad de la pérdida bruta.

   La empresa deberá desarrollar criterios específicos para la asignación de datos de pérdidas procedentes de: (a) eventos sucedidos en una función centralizada (por ejemplo, en un departamento de tecnologías de información); (b) eventos relacionados con una actividad que incluya más de una línea de negocio; y (c) eventos relacionados a lo largo del tiempo.

   Las pérdidas por riesgo operacional que estén relacionadas con el riesgo de crédito y que históricamente se hayan incluido en las bases de datos de riesgo de crédito con que cuentan las empresas (por ejemplo, fallos en la gestión de garantías) continuarán recibiendo el tratamiento de riesgo de crédito. En consecuencia, tales pérdidas no estarán sujetas al requerimiento patrimonial por riesgo operacional. Sin embargo, para efectos de la gestión del riesgo operacional, las empresas deberán identificar todas las pérdidas importantes por estos riesgos en forma consistente con el alcance de la definición de

riesgo operacional señalada en la normativa emitida por la Superintendencia y los tipos de eventos de pérdida detallados en el Anexo 3, lo cual incluye los eventos de pérdida generados por riesgo operativo pero relacionados con el riesgo de crédito. Tales eventos deberán ser identificados separadamente en la base de datos de riesgo operacional de la empresa.

Las pérdidas por riesgo operacional que estén relacionadas con el riesgo de mercado deberán ser incluidas en el cálculo del requerimiento patrimonial por riesgo operacional.

d) Datos externos

El sistema de medición del riesgo operacional de la empresa deberá utilizar datos externos relevantes (ya sean datos públicos y/o datos agregados del sector), especialmente cuando existan motivos para creer que la empresa está expuesta a pérdidas poco frecuentes, pero potencialmente severas. Estos datos externos deberán incluir información sobre el monto real de la pérdida, el volumen de operaciones de la entidad donde se produjo el evento de pérdida, las causas y circunstancias de los eventos de pérdida y cualquier otra información que permita evaluar la importancia del evento de pérdida para otras empresas. La empresa deberá contar con un proceso sistemático para determinar las situaciones en las que deberán utilizarse los datos externos y las metodologías utilizadas para incorporar estos datos (por ejemplo, aplicación de ajustes por tamaño, ajustes cualitativos o en el desarrollo de mejoras en el análisis de escenarios). Las condiciones y prácticas para el uso de los datos externos deberán ser revisadas anualmente, documentadas y sometidas a revisiones periódicas independientes a la empresa o su grupo de control.

e) Análisis de escenarios

La empresa deberá utilizar análisis de escenarios basados en las opiniones de expertos, junto con datos externos, para evaluar su exposición a pérdidas severas. Este enfoque se apoya en el conocimiento de gerentes experimentados y de expertos en gestión de riesgos para obtener evaluaciones razonables de las pérdidas severas que podría sufrir la entidad. Las evaluaciones realizadas por los expertos podrían ser expresadas como parámetros de una distribución estadística estimada de las pérdidas. Además, el análisis de escenarios debe utilizarse para evaluar el impacto de las desviaciones que se produzcan respecto a los supuestos de correlación incorporados en el sistema de medición del riesgo operacional de la empresa, en particular, para evaluar las pérdidas potenciales procedentes de eventos simultáneos de pérdida. Estas evaluaciones deben ser validadas y revisadas a través de su comparación con la experiencia real de pérdidas, con el fin de asegurar su razonabilidad.

f) Factores del entorno de negocio y de control interno

Además de los datos de pérdida, ya sean reales o basados en escenarios, la metodología de evaluación de riesgos aplicada por la empresa debe capturar los factores clave de su entorno de negocio y de su control interno que puedan cambiar su perfil de riesgo operacional. Estos factores permitirán que las evaluaciones del riesgo que realice la empresa estén más orientadas hacia el futuro, reflejarán de forma más directa la calidad de los entornos operativos y de control de la empresa, ayudarán a alinear las asignaciones de patrimonio efectivo con los objetivos de la gestión de riesgos y permitirán reconocer de una manera más inmediata tanto las mejoras como los deterioros en los perfiles de riesgo operacional. Con el fin que sea aplicable para el cálculo del requerimiento patrimonial, el uso de estos factores dentro del sistema de medición del riesgo operacional de la empresa deberá satisfacer los siguientes criterios:

La elección de cada factor deberá ser justificada por su influencia significativa en la exposición o mitigación del riesgo, sobre la base de la experiencia e incluyendo la opinión experta del personal de las áreas de negocio afectadas. Cuando sea posible, los factores deben traducirse en medidas cuantitativas que permitan su verificación.

Deberá considerarse adecuadamente la sensibilidad de las estimaciones de riesgo de la empresa ante variaciones en los factores y su peso relativo. Además de identificar las variaciones en el riesgo debido a mejoras en los controles, la metodología también debe identificar incrementos potenciales del riesgo atribuibles a una mayor complejidad de las actividades o a un incremento en el volumen de negocios.

La metodología y cada elemento de su aplicación, incluidos los supuestos que sustenten cualquier ajuste a las estimaciones empíricas, deberán ser documentados y sometidos a revisiones independientes por parte de la empresa.

El proceso y los resultados obtenidos deberán ser validados mediante su comparación con la experiencia real de pérdidas internas, con datos externos relevantes y con los ajustes oportunos introducidos.

Artículo 18°.- Reconocimiento de los seguros

Las empresas que estén autorizadas a aplicar un método avanzado podrán reconocer el efecto reductor del riesgo que generan los seguros en el cálculo del requerimiento patrimonial por riesgo operacional. Dicho reconocimiento se limitará al 20% del requerimiento patrimonial calculado con dicho método avanzado.

Para aplicar esta reducción en el requerimiento patrimonial, deberán cumplirse los siguientes requisitos:

a) El proveedor del seguro deberá contar con una clasificación de riesgo apropiada, y haber tenido dicha clasificación durante los dos semestres anteriores, de acuerdo con lo siguiente:

   Si el proveedor del seguro se encuentra establecido en el país, la clasificación mínima aceptable será "A", otorgada por empresas debidamente registradas en la Superintendencia y en la Comisión Nacional Supervisora de Empresas y Valores (CONASEV).
   Si el proveedor del seguro no se encuentra establecido en el país, la clasificación mínima aceptable será la "BBB-" de Standard & Poor's o equivalente, otorgada por empresas clasificadoras de riesgo del exterior de primera categoría que cuenten con autorización de funcionamiento en alguno de los países que conforman el G10.
   Si existiera discrepancia entre diferentes clasificaciones otorgadas al proveedor del seguro, debe considerarse la más conservadora.

b) Los contratos de seguro a considerar deberán tener un plazo de vencimiento no menor de un año. Para contratos que tengan un plazo residual de vencimiento inferior a un año, la empresa deberá aplicar los descuentos proporcionales necesarios que reflejen el plazo residual decreciente del contrato, hasta un recorte completo del 100% para contratos con un plazo residual de 90 días o menos.

c) Los contratos de seguro a considerar deberán contar con un periodo mínimo de preaviso para su cancelación de 90 días.

d) Los contratos de seguro a considerar no deberán tener exclusiones o limitaciones que dependan de acciones de la Superintendencia y otros organismos reguladores o, en el caso de liquidación de la empresa, que impidan a la empresa, al administrador o al liquidador recuperarse de los daños y perjuicios sufridos o gastos incurridos por la empresa, excepto en el caso de eventos que ocurran después de iniciado el procedimiento de liquidación de la empresa. No obstante, el contrato de seguro puede excluir la cobertura de multas u otras penalidades ocasionadas por la acción de la Superintendencia.

e) Los cálculos de la cobertura de riesgos considerando los seguros deberán ser realizados de una manera que resulte transparente y consistente con los datos de probabilidad e impacto de la pérdida utilizados por la empresa para calcular el requerimiento patrimonial por riesgo operacional.

f) El proveedor del seguro deberá ser un tercero. En el caso de seguros brindados por empresas del mismo grupo económico, la exposición deberá estar reasegurada por un tercero independiente que satisfaga los criterios de admisión señalados anteriormente.

g) La metodología de reconocimiento del seguro deberá estar adecuadamente sustentada y documentada.

h) La empresa deberá incorporar como parte de la información de sustento que envíe a la Superintendencia la forma en que utiliza los seguros para mitigar sus riesgos.

La metodología de reconocimiento del seguro en el caso de una empresa que utilice un método avanzado deberá, también, tomar en consideración los siguientes aspectos mediante la aplicación de descuentos en la cantidad correspondiente al reconocimiento del seguro:

El plazo de vencimiento residual del contrato, en caso de ser inferior a un año, conforme se establece en el literal b de la sección anterior.
El plazo de cancelación del contrato, cuando sea inferior a un año.
La incertidumbre del pago, así como los desfases existentes en la cobertura del seguro.

La Superintendencia podrá revisar posteriormente el límite establecido y los requisitos señalados para el reconocimiento de los seguros en el cálculo del requerimiento patrimonial por riesgo operacional, sobre la base de la experiencia acumulada.

DISPOSICIONES FINALES

Primera.- Requerimiento adicional
La Superintendencia podrá exigir a las empresas un requerimiento patrimonial mayor al calculado con el método al que la empresa ha sido autorizada a utilizar cuando los niveles de requerimiento de patrimonio efectivo no resulten adecuados a la naturaleza y escala de las operaciones, perfil de riesgo y sistema de gestión de riesgos de la empresa.

Segunda.- Revocatoria de autorización
Si la Superintendencia determina que una empresa que ha sido autorizada a utilizar el método estándar alternativo o los métodos avanzados, deja de satisfacer los requisitos de autorización asociados con dicho método, podrá revocar la autorización otorgada y exigirle que utilice un método más simple para algunas o todas sus operaciones, hasta que cumpla con las condiciones estipuladas por la Superintendencia para poder volver al método del que fuera revocado, lo que se comunicará mediante Oficio.

Tercera.- Vigencia
La presente norma entrará en vigencia el 1 de julio de 2009. Para la aplicación del método estándar alternativo a partir de dicha fecha, las empresas podrán presentar su solicitud de autorización de conformidad con lo señalado en la presente norma, a partir de su publicación.

ANEXO N° 1

ANUALIZACION DE SALDOS

La anualización se deberá aplicar a los saldos de las cuentas de ingresos y gastos que se requieran para el cálculo del requerimiento de patrimonio efectivo por riesgo operacional según los métodos del Indicador Básico y Estándar Alternativo, conforme a lo establecido en la presente norma.

La fórmula es la siguiente:

Saldo anualizado (j, i) = Saldo (j,i) + Saldo (diciembre, i-1) – Saldo (j,i-1)
Donde:
- j: mes
- i: año

Así por ejemplo, si en julio de 2009, se desea calcular los márgenes operacionales brutos correspondientes a los últimos 3 años bajo el método del indicar básico, se deberán obtener previamente los saldos anualizados de las cuentas contables señaladas en el artículo 5° del presente Reglamento, de la siguiente manera:

Saldo anualizado (julio, 2009) = Saldo (julio, 2009) + Saldo (diciembre, 2008) – Saldo (julio, 2008)

Saldo anualizado (julio, 2008) = Saldo (julio, 2008) + Saldo (diciembre, 2007) – Saldo (julio, 2007)

Saldo anualizado (julio, 2007) = Saldo (julio, 2007) + Saldo (diciembre, 2006) – Saldo (julio, 2006)

ANEXO N° 2A

CALCULO DE LOS INDICADORES DE EXPOSICION DE LAS LÍNEAS DE NEGOCIO
(Hasta el 31 de diciembre de 2009)[4]

Lineas de negocio distintas a banca comercial y banca minorista

Para obtener los ingresos y gastos de los últimos 12 meses por cada linea de negocio, deben sumarse los saldos anualizados de las siguientes cuentas del Manual de Contabilidad, según corresponda a cada linea de negocio[5]:

Ingresos

Linea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Finanzas corporativas	Intereses por créditos sindicados	5104 01 01 13
	Ing por op contingentes contratos de underwriting	5201 08 + 5202 24
	Ing por servicios financieros diversos suscripción y colocaciones garantizadas de valores	
	Ing por servicios financieros diversos asesoria financiera	5202 15
Negociación y ventas	Intereses por disponibles	5101
	Intereses y comisiones por fondos interbancarios	5102 + 5107 02
	Ingresos por inversiones a valor razonable con cambios en resultados y commodities	5103 01 + 5103 02 + 5103 06
	Diferencia de cambio	5108
	Reajuste por indexación	5109 01
	Ingresos por valorización de inversiones a valor razonable con cambios en resultados, commodities, productos financieros derivados y obligaciones relacionadas con inversiones negociables y a vencimiento	5109 11 + 5109 12 + 5109 15 + 5109 16 + 5109 17 + 5109 18
	Otros ingresos	5109 21 + 5109 24
	Ingresos por servicios financieros diversos compraventa de ME (spot y futuro)	5202 18 + 5202 19
	Ingresos por servicios financieros diversos otros inst. financieros derivados	5202 25
Liquidación y pagos	Ingresos por servicios financieros diversos cobranzas	5202 02

[4] En concordancia con lo establecido en la Resolución SBS N° 1435-2009 del 30/10/2009, el Anexo N° 2A tendrá vigencia hasta el 30 de junio de 2010

[5] El procedimiento para anualizar saldos es descrito en el Anexo N° 1 del presente Reglamento

Línea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Ingresos por servicios financieros diversos giros	5202 07
	Ingresos por servicios financieros diversos transferencias	5202 08
	Ingresos por servicios financieros diversos órdenes de pago	5202 12
	Ingresos por servicios financieros diversos cobro de tributos	5202 16
Otros servicios	Ingresos de cuentas por cobrar	5105
	Comisiones por cuentas por cobrar y otros	5107 05 + 5107 09
	Otros ingresos financieros diversos	5109 19
	Ingresos por operaciones contingentes litigios, demandas pendientes y otras contingencias	5201 09
	Ingresos por servicios financieros diversos custodia de valores, alquiler de cajas de seguridad	5202 03+5202 13
	Ingresos por servicios financieros diversos fideicomisos y comisiones de confianza	5202 04 + 5202 05
	Ing por servicios financieros diversos estudios técnicos y legales	5202 14
	Ingresos por servicios financieros diversos compraventa de valores	5202 17
	Ingresos por servicios financieros diversos servicios de caja	5202 21
	Otros ingresos por servicios financieros diversos	5202 29
	Ingresos por arrendamientos	5203
	Ventas de bienes y servicios	5700

Gastos

Línea de negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Negociación y ventas	Intereses y fluctuación de obligaciones relacionadas con inversiones negociables y a vencimiento	4101 05 + 4109 18
	Intereses por fondos interbancarios	4102
	Comisiones por fondos interbancarios	4107 02
	Diferencia de cambio y rendimiento aleatorio	4108 + 4109 02
	Reajuste por indexación	4109 01
	Gastos por valorización de inversiones a valor razonable con cambios en resultados y commodities	4109 11 + 4109 12 + 4109 15
	Fluctuación de valor de productos financieros derivados y otros	4109 16 + 4109 17 + 4109 21 + 4109 24
	Gastos por servicios financieros diversos compraventa de ME (spot y futuro)	4202 10 + 4202 11

Linea de negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Gastos por servicios financieros diversos otros instrumentos financieros derivados	4202 25

Para calcular los gastos de las demás lineas de negocio, se utilizará un factor de ponderación por cada linea, que permitirá obtener un monto aproximado de los gastos. Dicho factor se calculará de la siguiente manera:

$F_i = I_i / TI$

Donde:

F_i : Factor de ponderación de la linea i

I_i : Ingresos anualizados de la linea i, según distribución de cuentas contables señalada en la sección anterior.

TI : Total de ingresos calculados de la siguiente forma: Ingresos financieros (cuenta 5100) más los ingresos por servicios (cuentas 5200 + 5700) menos los ingresos de la linea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Para estimar los gastos de cada linea, se aplicará la siguiente formula:

$G_i = F_i * TG$

Donde:

G_i : Gastos anualizados de la linea i

F_i : Factor de ponderación de la linea i

TG : Total de gastos calculados de la siguiente forma: gastos financieros (cuenta 4100) más gastos por servicios (4200 + 4900) menos los gastos de la linea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Banca comercial

Banca Comercial	Cuentas
Créditos Comerciales	1401 01+ 1403 01 + 1404 01 + 1405 01+ 1406 01
Menos Sindicados	1401 01 13 + 1404 01 13 + 1405 01 13 + 1405 01 19 13 + 1406 01 13 + 1406 01 19 13
Menos Ingresos Diferidos	2901 01 +2901 02 + 2901 04 01 01 + 2901 04 01 04 + 2901 04 03 01 + 2901 04 03 04 + 2901 04 04 01 + 2901 04 04 04 + 2901 04 05 01 + 2901 04 05 04 + 2901 04 06 01 + 2901 04 06 04
Más Inversiones Disponibles para la Venta e Inversiones a Vencimiento	1303+1304+1305
Más Inversiones en Subsidiarias y Asociadas	1700

Banca minorista

Banca Minorista	Cuentas
Créditos MES, Consumo e Hipotecarios para Vivienda	1401 - 1401 01 + 1403 - 1403 01 + 1404 - 1404 01 + 1405 - 1405 01+ 1406 - 1406 01
Menos Ingresos Diferidos	2901 04 - 2901 04 01 01 - 2901 04 01 04 - 2901 04 03 01 - 2901 04 03 04 - 2901 04 04 01 - 2901 04 04 04 - 2901 04 05 01 - 2901 04 05 04 - 2901 04 06 01 - 2901 04 06 04

25

ANEXO N° 2B

CÁLCULO DE LOS INDICADORES DE EXPOSICION DE LAS LÍNEAS DE NEGOCIO[6]
(A partir del 01 de julio de 2010)

Lineas de negocio distintas a banca comercial y banca minorista

Para obtener los ingresos y gastos de los últimos 12 meses por cada línea de negocio, deben sumarse los saldos anualizados de las siguientes cuentas del Manual de Contabilidad, según corresponda a cada línea de negocio[7]:

Ingresos

Linea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Finanzas corporativas	Ing por financiación estructurada[8]	5104 01 10 30 + 5104 01 10 31 + 5104 01 10 32 + 5104 01 10 33 + 5104 01 10 34 + 5104 01 11 30 + 5104 01 11 31 + 5104 01 11 32 + 5104 01 11 33 + 5104 01 11 34 + 5104 01 12 30 + 5104 01 12 31 + 5104 01 12 32 + 5104 01 12 33 + 5104 01 12 34
	Ing por op contingentes: contratos de underwriting	5201 03 + 5202 24
	Ing por servicios financieros diversos suscripción y colocaciones garantizadas de valores	
	Ing por servicios financieros diversos asesoría financiera	5202 15
Negociación y ventas	Intereses por disponibles	5101
	Intereses y comisiones por fondos interbancarios	5102 + 5107 02
	Ingresos por inversiones a valor razonable con cambios en resultados y commodities	5103 01 + 5103 02 + 5103 06
	Diferencia de cambio	5108
	Reajuste por indexación	5109 01
	Ingresos por valorización de inversiones a valor razonable con cambios en resultados, commodities, productos financieros derivados y obligaciones relacionadas con inversiones negociables y a vencimiento	5109 11 + 5109 12 + 5109 15 + 5109 16 + 5109 17 + 5109 18
	Otros ingresos	5109 21 + 5109 24

[6] Denominación modificada por la Resolución SBS N° 14353-2009 del 30/10/2009
[7] El procedimiento para anualizar saldos es descrito en el Anexo N° 1 del presente Reglamento
[8] Subcuentas analíticas incorporadas por la Resolución SBS N° 14353-2009 del 30/10/2009

Linea de Negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Ingresos por servicios financieros diversos compraventa de ME (spot y futuro)	5202 18 + 5202 19
	Ingresos por servicios financieros diversos otros inst. financieros derivados	5202 25
Liquidación y pagos	Ingresos por servicios financieros diversos cobranzas	5202 02
	Ingresos por servicios financieros diversos giros	5202 07
	Ingresos por servicios financieros diversos transferencias	5202 08
	Ingresos por servicios financieros diversos órdenes de pago	5202 12
	Ingresos por servicios financieros diversos cobro de tributos	5202 16
Otros servicios	Ingresos de cuentas por cobrar	5105
	Comisiones por cuentas por cobrar y otros	5107 05 + 5107 09
	Otros ingresos financieros diversos	5109 19
	Ingresos por operaciones contingentes (fallos, demandas pendientes y otras contingencias	5201 09
	Ingresos por servicios financieros diversos custodia de valores, alquiler de cajas de seguridad	5202 03+5202 13
	Ingresos por servicios financieros diversos fideicomisos y comisiones de confianza	5202 04 + 5202 05
	Ing por servicios financieros diversos estudios técnicos y legales	5202 14
	Ingresos por servicios financieros diversos compraventa de valores	5202 17
	Ingresos por servicios financieros diversos servicios de caja	5202 21
	Otros ingresos por servicios financieros diversos	5202 29
	Ingresos por arrendamientos	5203
	Ventas de bienes y servicios	5700

Gastos

Linea de negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
Negociación y ventas	Intereses y fluctuación de obligaciones relacionadas con inversiones negociables y a vencimiento	4101 05 + 4109 18
	Intereses por fondos interbancarios	4102
	Comisiones por fondos interbancarios	4107 02
	Diferencia de cambio y rendimiento aleatorio	4108 + 4109 02
	Reajuste por indexación	4109 01

Linea de negocio	Cuentas Asociadas	Cuentas del Manual de Contabilidad
	Gastos por valorización de inversiones a valor razonable con cambios en resultados y commodities	4109 11 + 4109 12 + 4109 15
	Fluctuación de valor de productos financieros derivados y otros	4109 16 + 4109 17 + 4109 21 + 4109 24
	Gastos por servicios financieros diversos compraventa de ME (spot y futuro)	4202 10 + 4202 11
	Gastos por servicios financieros diversos otros instrumentos financieros derivados	4202 25

Para las demás líneas de negocio se deberá aplicar una fórmula que permita obtener un monto aproximado de los gastos. Para ello, se utilizará un factor de ponderación por cada línea, el cual se calculará de la siguiente manera:

$F_i = I_i / TI$

Donde:

F_i : Factor de ponderación de la línea i

I_i : Ingresos anualizados de la línea i, según distribución de cuentas contables señalada en la sección anterior.

TI : Total de ingresos calculados de la siguiente forma: Ingresos financieros (cuenta 5100) más los ingresos por servicios (cuentas 5200 + 5700) menos los ingresos de la línea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Para estimar los gastos de cada línea, se aplicará la siguiente fórmula:

$G_i = F_i * TG$

Donde:

G_i : Gastos anualizados de la línea i

F_i : Factor de ponderación de la línea i

TG : Total de gastos calculados de la siguiente forma: gastos financieros (cuenta 4100) más gastos por servicios (4200 + 4900) menos los gastos de la línea Negociación y ventas. Se utilizarán los saldos anualizados de las cuentas contables señaladas.

Banca comercial

Banca Comercial	Cuentas
Créditos a Bancos Multilaterales de Desarrollo	1401 05 + 1404 05 + 1405 05 + 1406 05
Créditos Soberanos	1401 06 + 1404 06 + 1405 06 + 1406 06
Créditos a Entidades del Sector Público	1401 07 + 1403 07 + 1404 07 + 1405 07 + 1406 07
Créditos a Intermediarios de Valores	1401 08 + 1403 08 + 1404 08 + 1405 08 + 1406 08

Créditos a Empresas del Sistema Financiero	1401 09 + 1404 09 + 1405 09 + 1406 09
Créditos Corporativos	1401 10 + 1403 10 + 1404 10 + 1405 10 + 1406 10
Créditos a Grandes Empresas	1401 11 + 1403 11 + 1404 11 + 1405 11 + 1406 11
Créditos a Medianas Empresas	1401 12 + 1403 12 + 1404 12 + 1405 12 + 1406 12
Menos Financiación Estructurada[9]	1401 10 30 + 1401 10 31 + 1401 10 32 + 1401 10 33 + 1401 10 34 + 1401 11 30 + 1401 11 31 + 1401 11 32 + 1401 11 33 + 1401 11 34 + 1401 12 30 + 1401 12 31 + 1401 12 32 + 1401 12 33 + 1401 12 34 + 1403 10 30 + 1403 10 31 + 1403 10 32 + 1403 10 33 + 1403 10 34 + 1403 11 30 + 1403 11 31 + 1403 11 32 + 1403 11 33 + 1403 11 34 + 1403 12 30 + 1403 12 31 + 1403 12 32 + 1403 12 33 + 1403 12 34 + 1404 10 30 + 1404 10 31 + 1404 10 32 + 1404 10 33 + 1404 10 34 + 1404 11 30 + 1404 11 31 + 1404 11 32 + 1404 11 33 + 1404 11 34 + 1404 12 30 + 1404 12 31 + 1404 12 32 + 1404 12 33 + 1404 12 34 + 1405 10 19 30 + 1405 10 19 31 + 1405 10 19 32 + 1405 10 19 33 + 1405 10 19 34 + 1405 10 30+ 1405 10 31 + 1405 10 32 + 1405 10 33 + 1405 10 34 + 1405 11 19 30 + 1405 11 19 31 + 1405 11 19 32 + 1405 11 19 33 + 1405 11 19 34 + 1405 11 30 + 1405 11 31 + 1405 11 32 + 1405 11 33 + 1405 11 34 + 1405 12 19 30 + 1405 12 19 31 + 1405 12 19 32 + 1405 12 19 33 + 1405 12 19 34 + 1405 12 22 30 + 1405 12 22 31 + 1405 12 22 32 + 1405 12 22 33 + 1405 12 22 34 + 1405 12 30 + 1405 12 31 + 1405 12 32 + 1405 12 33 + 1405 12 34+ 1406 10 19 30 + 1406 10 19 31 + 1406 10 19 32 + 1406 10 19 33 + 1406 10 19 34 + 1406 10 30+ 1406 10 31 + 1406 10 32 + 1406 10 33 + 1406 10 34 + 1406 11 19 30 + 1406 11 19 31 + 1406 11 19 32 + 1406 11 19 33 + 1406 11 19 34 + 1406 11 30 + 1406 11 31 + 1406 11 32 + 1406 11 33 + 1406 11 34 + 1406 12 19 30 + 1406 12 19 31 + 1405 12 19 32 + 1406 12 19 33 + 1406 12 19 34 + 1406 12 30 + 1406 12 31 + 1406 12 32 + 1406 12 33 + 1406 12 34
Menos Ingresos Diferidos	2901 01 +2901 02 + 2901 04 01 03 + 2901 04 01 04 +2901 04 01 05 + 2901 04 01 06 +2901 04 01 07 + 2901 04 01 08 + 2901 04 01 12 + 2901 04 01 13 +2901 04 01 14 + 2901 04 01 15 + 2901 04 01 16 + 2901 04 01 17 + 2901 04 03 03 + 2901 04 03 04 + 2901 04 03 05 + 2901 04 03 06 +2901 04 03 07 + 2901 04 03 08 + 2901 04 03 12 + 2901 04 03 13 +2901 04 03 14 + 2901 04 03 15 + 2901 04 03 16 + 2901 04 03 17 + 2901 04 04 03 + 2901 04 04 04 + 2901 04 04 05 + 2901 04 04 06 +2901 04 04 07 + 2901 04 04 08 + 2901 04 04 12 + 2901 04 04 13 +2901 04 04 14 + 2901 04 04 15 + 2901 04 04 16 + 2901 04 04 17 + 2901 04 05 03 + 2901 04 05 04 + 2901 04 05 05 + 2901 04 05 06 +2901 04 05 07 + 2901 04 05 08 + 2901 04 05 12 + 2901 04 05 13 +2901 04 05 14 + 2901 04 05 15 + 2901 04 05 16 + 2901 04 05 17 + 2901 04 06 03 + 2901 04 06 04 + 2901 04 06 05 + 2901 04 06 06 +2901 04 06 07 + 2901 04 06 08 + 2901 04 06 12 + 2901 04 06 13 +2901 04 06 14 + 2901 04 06 15 + 2901 04 06 16 + 2901 04 06 17
Más Inversiones Disponibles para la Venta e Inversiones a Vencimiento	1303+1304+1305
Más Inversiones en Subsidiarias y Asociadas	1700

[9] Cuentas analíticas y Subcuentas analíticas incorporadas por la Resolución SBS N° 14353-2009 del 30/10/2009

Banca minorista

Banca Minorista	Cuentas
Créditos a Microempresas	1401 02 + 1403 02 + 1404 02 + 1405 02 + 1406 02
Créditos de Consumo Revolventes y No-Revolventes	1401 03 + 1404 03 + 1405 03 + 1406 03
Créditos Hipotecarios para Vivienda	1401 04 + 1404 04 + 1405 04 + 1406 04
Créditos a Pequeñas Empresas	1401 13 + 1403 13 + 1404 13 + 1405 13 + 1406 13
Menos Ingresos Diferidos	2901 04 01 01 + 2901 04 01 02 + 2901 04 01 09 + 2901 04 01 10 + 2901 04 01 11 + 2901 04 01 18 + 2901 04 03 01 + 2901 04 03 09 + 2901 04 03 10 + 2901 04 03 18 + 2901 04 04 01 + 2901 04 04 02 + 2901 04 04 09 + 2901 04 04 10 + 2901 04 04 11 + 2901 04 04 18 + 2901 04 05 01 + 2901 04 05 02 + 2901 04 05 09 + 2901 04 05 10 + 2901 04 05 11 + 2901 04 05 18 + 2901 04 06 01 + 2901 04 06 02 + 2901 04 06 09 + 2901 04 06 10 + 2901 04 06 11 + 2901 04 06 18

ANEXO N° 3

TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Tipo de evento	Definición	Ejemplos
Fraude interno	Pérdidas derivadas de algun 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 implicado, al menos, un miembro de la empresa	Actividades no autorizadas (realizadas intencionalmente), robo, malversación, falsificación, soborno, apropiación de cuentas
Fraude externo	Pérdidas derivadas de algun tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero	Robo, falsificación, daños por ataques informáticos, robo de información
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 o discriminación	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Incumplimiento de los contratos con los clientes, divulgación de información privada de clientes, abuso de información confidencial, incumplimiento de las normas de conocimiento del cliente, prácticas restrictivas de la competencia, manipulación del mercado, lavado de dinero, publicidad impropia, defectos en el producto o servicio
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo)
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica
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	Ejecución errónea de modelos, errores contables, fallo en la gestión de las garantías, incumplimiento en el envío de reportes obligatorios, reportes inexactos, incumplimiento de normas tributarias, registros incorrectos de clientes, litigios con proveedores

A2. RESOLUCIÓN SBS N° 2116-2009: Reglamento para la Gestión de Riesgo Operativo

Lima, 02 de abril de 2009

Resolución S.B.S.
N° 2116 -2009

El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, mediante la Resolución SBS N° 37-2008 del 10 de enero de 2008, se aprobó el Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentra el riesgo operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

Que, mediante la Resolución SBS N° 006-2002 del 4 de enero de 2002 y sus modificatorias, se aprobó el Reglamento para la Administración de los Riesgos de Operación;

Que, en consecuencia, resulta necesario realizar modificaciones al Reglamento para la administración de los riesgos de operación, a fin que dicha norma sea consistente con las disposiciones del Reglamento de la Gestión Integral de Riesgos, así como con los desarrollos recientes sobre la materia;

Que, asimismo, resulta conveniente ampliar el alcance de la regulación referida a la gestión del riesgo operacional a las Administradoras Privadas de Fondos de Pensiones;

Estando a lo opinado por las Superintendencias Adjuntas de Banca y Microfinanzas, Seguros, Administradoras Privadas de Fondos de Pensiones, Riesgos y Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus modificatorias, y el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Gestión del Riesgo Operacional, que forma parte integrante de la presente Resolución.

Los anexos que forman parte del Reglamento aprobado por la presente Resolución se publican en el Portal institucional (http://www.sbs.gob.pe), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS.

Artículo Segundo.- Sustituir el artículo 117° del Título VI del Compendio de Normas de Superintendencia Reglamentarias del Sistema Privado de Administración de Fondos de Pensiones (SPP), por el texto siguiente:

"**Artículo 117°.- Riesgo Operacional.** Para administrar los riesgos operacionales asociados con el proceso de inversiones, las AFP se sujetarán a las disposiciones establecidas en el Reglamento para la Gestión del Riesgo Operacional.

Asimismo, como parte de las medidas para el tratamiento de este riesgo, las empresas deberán realizar lo siguiente:

a. Implementar procedimientos para que las operaciones de inversión cuenten con confirmaciones, ya sean escritas o por medios auditivos o electrónicos, suscritas por los intermediarios;
b. Implementar procedimientos para que las operaciones de inversión cumplan con las normas internas y externas aplicables y que las mismas se hayan realizado bajo condiciones de mercado, contando con los poderes y las firmas autorizadas;
c. Implementar planes de contingencia ante fallas técnicas en los sistemas de información o ante la ocurrencia de eventos de fuerza mayor que puedan afectar la gestión de las inversiones;
d. Establecer los procedimientos para el funcionamiento de sistemas de grabaciones de audio adecuados para la concertación de las operaciones de inversión, y el mantenimiento de dichas grabaciones por un mínimo de dos (2) años;
e. Establecer procedimientos relacionados a la concertación, registro, liquidación, guarda física y custodia de las operaciones de inversión y al mantenimiento y control de expedientes;
f. Establecer políticas y procedimientos que permitan una adecuada instrumentalización de convenios y contratos a fin de delimitar derechos y obligaciones contractuales tanto de las Carteras Administradas como de la AFP en aspectos vinculados con el proceso de inversión;
g. Establecer adecuados canales de difusión entre sus funcionarios de las disposiciones legales y administrativas aplicables a sus operaciones de inversión;
h. Evaluar y monitorear los efectos que habrán de producirse sobre los actos en materia de inversiones que realice la AFP, de conformidad con el régimen legal nacional o extranjero aplicable;
i. Evaluar y monitorear las implicancias jurídicas en caso de incumplimiento en el pago de una inversión realizada por parte de un emisor o contraparte y la factibilidad de ejecución de las garantías;
j. Establecer condiciones y requerimientos para el accionar diligente de los funcionarios en el proceso de inversión en resguardo de los recursos de las Carteras Administradas; y,
k. Asegurar un adecuado cumplimiento de las políticas sobre la conducta ética y las políticas orientadas a evitar conflictos de interés u otras irregularidades en la gestión de las inversiones de los recursos de las Carteras Administradas."

Artículo Tercero.- Incorpórese el procedimiento N° 122 "Autorizaciones especiales para la Gestión del Riesgo Operacional" y el procedimiento N° 123 "Autorización del Procesamiento Principal en el Exterior" en el Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia de Banca, Seguros y AFP aprobado mediante Resolución SBS N° 131-2002, cuyos textos se anexan a la presente Resolución y se publican conforme lo dispuesto en el Decreto Supremo N° 004-2008-PCM, reglamento de la Ley N° 29091. (Portal institucional: www.sbs.gob.pe).

Artículo Cuarto.- La presente Resolución entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010, fecha a partir de la cual quedarán sin efecto la Resolución SBS N° 006-2002 y sus normas modificatorias, la Circular G-130-2007, así como todas aquellas disposiciones que se le opongan de manera total o parcial.

Las Administradoras Privadas de Fondos de Pensiones tendrán un plazo de adecuación al Reglamento aprobado por la presente Resolución hasta el 30 de junio de 2010.

Regístrese, comuníquese y publíquese,

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

REGLAMENTO PARA LA GESTIÓN DEL RIESGO OPERACIONAL

CAPITULO I
DISPOSICIONES GENERALES

Artículo 1°.- Alcance
El presente Reglamento será de aplicación a las empresas señaladas en el artículo 16° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Las empresas de servicios complementarios y conexos señaladas en el artículo 17° de la Ley General se sujetarán, para la gestión de su riesgo operacional, a lo establecido en sus normas específicas. Asimismo, podrán tomar en consideración las disposiciones señaladas en el presente Reglamento en función a su tamaño y complejidad.

Artículo 2°.- Definiciones
Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Apetito por el riesgo: El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.
b. Directorio: Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
c. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
d. Evento de pérdida por riesgo operacional: El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.
e. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
f. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
g. Reglamento de la Gestión Integral de Riesgos: Reglamento de la Gestión Integral de Riesgos aprobado mediante la Resolución SBS N° 37-2008 del 10 de enero de 2008.
h. Riesgo legal: Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.
i. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.
j. Superintendencia: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
k. Tolerancia al riesgo: El nivel de variación que la empresa está dispuesta a asumir en caso de desviación de los objetivos empresariales trazados.

Artículo 3°.- Riesgo operacional

Entiéndase por riesgo operacional a la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Las empresas deben realizar una gestión adecuada del riesgo operacional que enfrentan, para lo cual observarán los criterios mínimos indicados en el presente Reglamento.

Artículo 4° Factores que originan el riesgo operacional

i) **Procesos internos**
Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

ii) **Personal**
Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.

iii) **Tecnología de información**
Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

iv) **Eventos externos**
Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

Artículo 5°.- Eventos de pérdida por riesgo operacional

Los eventos de pérdida por riesgo operacional pueden ser agrupados de la manera descrita a continuación:

a. Fraude interno.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

b. Fraude externo.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c. 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 reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d. Clientes, productos y prácticas empresariales.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

e. Daños a activos materiales.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f. Interrupción del negocio y fallos en los sistemas.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g. 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.

En el Anexo N° 1, se incluye una categorización de los tipos de eventos de pérdida aplicable según el sector al que pertenece la empresa.

CAPITULO II
ROLES Y RESPONSABILIDADES

Artículo 6°.- Responsabilidades del Directorio
El Directorio tiene las siguientes responsabilidades específicas respecto a la gestión del riesgo operacional:

a) Definir la política general para la gestión del riesgo operacional.
b) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.
c) Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.
d) Aprobar el manual de gestión del riesgo operacional.
e) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
f) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.
g) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

Artículo 7°.- Responsabilidades de la Gerencia
La gerencia general tiene la responsabilidad de implementar la gestión del riesgo operacional conforme a las disposiciones del Directorio.

Los gerentes de las unidades organizativas de negocios o de apoyo tienen la responsabilidad de gestionar el riesgo operacional en su ámbito de acción, dentro de las políticas, límites y procedimientos establecidos.

Artículo 8°.- Comité de riesgos

Las funciones del Comité de Riesgos señaladas en el Reglamento de la Gestión Integral de Riesgos, son de aplicación a la gestión del riesgo operacional en lo que corresponda.

Artículo 9°.- Unidad de riesgos
De conformidad con el Reglamento de la Gestión Integral de Riesgos, las empresas podrán contar con una Unidad de Riesgos centralizada o con unidades especializadas en la gestión de riesgos específicos.

En ese sentido, la Unidad de Riesgos de la empresa o, de ser el caso, la unidad especializada de gestión del riesgo operacional deberá cumplir con las siguientes funciones:

a. Proponer políticas para la gestión del riesgo operacional.
b. Participar en el diseño y permanente actualización del Manual de gestión del riesgo operacional.
c. Desarrollar la metodología para la gestión del riesgo operacional.
d. Apoyar y asistir a las demás unidades de la empresa para la aplicación de la metodología de gestión del riesgo operacional.
e. Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
f. Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.
g. Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.
h. Otras necesarias para el desarrollo de la función.

Las empresas deberán asignar recursos suficientes para la gestión del riesgo operacional, que les permita un adecuado cumplimiento de las funciones señaladas en el presente artículo y asegurar una adecuada independencia entre el área que asuma las funciones de gestión del riesgo operacional señaladas en el presente artículo y aquellas otras unidades de negocio o de apoyo.

Los bancos, las financieras, las empresas de seguros y las AFP deberán contar con una función especializada en riesgo operacional. De acuerdo al tamaño y complejidad de las operaciones que realice la empresa, la Superintendencia podrá requerir la creación de una unidad especializada.

CAPITULO III
LA GESTIÓN DEL RIESGO OPERACIONAL

Artículo 10°.- Manual de gestión del riesgo operacional
Las empresas deberán contar con un manual de gestión del riesgo operacional, el cual deberá contemplar por lo menos los siguientes aspectos:

a. Políticas para la gestión del riesgo operacional.
b. Funciones y responsabilidades asociadas con la gestión del riesgo operacional del Directorio, la Gerencia General, el Comité de Riesgos, la Unidad de Riesgos (o la unidad especializada, si corresponde) y las unidades de negocio y de apoyo.
c. Descripción de la metodología aplicada para la gestión del riesgo operacional.
d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición al riesgo operacional de la empresa y de cada unidad de negocio.

e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

Artículo 11°.- Metodología para la gestión del riesgo operacional
La metodología definida por la empresa para la gestión del riesgo operacional, cuando sea tomada en su conjunto, deberá considerar los componentes señalados en el artículo 4° del Reglamento de la Gestión Integral de Riesgos.

Asimismo, deberán cumplirse los siguientes criterios:

a. La metodología debe ser implementada en toda la empresa en forma consistente.
b. La empresa debe asignar recursos suficientes para aplicar su metodología en las principales líneas de negocio, y en los procesos de control y de apoyo.
c. La aplicación de la metodología debe estar integrada a los procesos de gestión de riesgos de la empresa.
d. Deben establecerse incentivos que permitan una mejora continua de la gestión del riesgo operacional.
e. La aplicación de la metodología de gestión del riesgo operacional debe estar adecuadamente documentada.
f. Deben establecerse procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional.

Artículo 12°.- Base de datos de eventos de pérdida
Las empresas deberán contar con una base de datos de los eventos de pérdida por riesgo operacional.

Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas, por lo cual las empresas deberán estar en capacidad de agrupar las pérdidas ocurridas por evento.

La base de datos deberá cumplir con los siguientes criterios:

a. Deben registrarse los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y entrenamiento al personal que interviene en el proceso.

b. Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

Código de identificación del evento.
Tipo de evento de pérdida (según tipos de eventos señalados en el Anexo 1 del presente Reglamento).
Línea de negocio asociada, según líneas señaladas en el Anexo 2 del presente Reglamento para las empresas del sistema financiero, Anexo 3 para las empresas de seguros y Anexo 4 para las AFP. Deberán considerarse los niveles 1 y 2 de los cuadros señalados en los anexos. Estos cuadros podrán ser actualizados por la Superintendencia mediante Circular.
Descripción corta del evento.
Descripción larga del evento.
Fecha de ocurrencia o de inicio del evento.
Fecha de descubrimiento del evento.
Fecha de registro contable del evento.

Monto(s) bruto(s) de la(s) pérdida(s), moneda y tipo de cambio.
Monto(s) recuperado(s) mediante coberturas existentes de forma previa al evento, moneda, tipo de cambio y tipo de cobertura aplicada.
Monto total recuperado, moneda y tipo de cambio.
Cuenta(s) contable(s) asociadas.
Identificación si el evento está asociado con el riesgo de crédito (para empresas del sistema financiero) o con el riesgo de seguros (para empresas del sistema de seguros).

En el caso de eventos con pérdidas múltiples, las empresas podrán registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que las originó.

De otro lado, podrá registrarse información parcial de un evento, en tanto se obtengan los demás datos requeridos. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

c. Deben definirse y documentarse criterios objetivos para asignar los eventos de pérdida a los tipos de evento señalados en el Anexo 1 del presente Reglamento, así como a las líneas de negocio señaladas en los Anexos 2, 3 y 4. Asimismo, deben definirse criterios específicos para aquellos casos en que un evento esté asociado a más de una línea de negocio.

d. Debe definirse un monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos. Al respecto, se fija un monto mínimo de 3 000 nuevos soles para los bancos, las financieras, las compañías de seguros y las AFP, y de 1 000 nuevos soles para el resto de empresas. Las empresas podrán establecer un monto mínimo inferior al indicado, teniendo en cuenta su volumen de operaciones y complejidad asociada. La Superintendencia podrá actualizar el monto mínimo definido por medio de Circular.

e. Debe definirse un monto mínimo de pérdida a partir del cual deberá contarse con un expediente físico o electrónico que contenga información adicional a la solicitada en el literal b. y que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado la empresa, incluyendo entre otras las mejoras o cambios requeridos en sus políticas o procedimientos. Dicho monto mínimo deberá ser aprobado por el Comité de Riesgos. La Superintendencia podrá establecer posteriormente un monto mínimo de carácter general.

Artículo 13°.- Gestión de la continuidad del negocio y de la seguridad de la información
Como parte de una adecuada gestión del riesgo operacional, las empresas deben implementar un sistema de gestión de la continuidad del negocio que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Asimismo, las empresas deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Para ello, las empresas deberán aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas.

Artículo 14°.- Subcontratación
Con el fin de gestionar los riesgos operacionales asociados a la subcontratación, las empresas deberán establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados. Dichas políticas y procedimientos deberán considerar:

a. El proceso de selección del proveedor del servicio
b. La elaboración del acuerdo de subcontratación
c. La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación
d. La implementación de un entorno de control efectivo
e. Establecimiento de planes de continuidad

Los acuerdos de subcontratación deberán formalizarse mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, y definir claramente las responsabilidades del proveedor y de la empresa.

CAPITULO IV
REQUERIMIENTOS DE INFORMACION

Artículo 15°.- Informe a la Superintendencia
Las empresas deberán presentar a la Superintendencia informes anuales referidos a la gestión del riesgo operacional, a través del software IG-ROp, el cual se encontrará disponible en el "Portal del Supervisado". Dichos informes deberán ser remitidos a más tardar el 31 de enero del año siguiente al año de reporte. La Superintendencia podrá requerir, mediante Oficio, la actualización periódica de los informes.

El contenido mínimo del referido informe, así como los aspectos operativos del IG-ROp, relacionados con las instrucciones, responsables y demás aspectos necesarios para su adecuado funcionamiento, se establecen en el "Manual del IG-ROp", el cual estará publicado en el "Portal del Supervisado" de la SBS. Asimismo, en el Portal, se publicarán instrucciones adicionales para el adecuado uso del sistema.

Las empresas supervisadas deberán designar un funcionario responsable por la información a ser reportada a través del IG-ROp, y tomarán las medidas necesarias para asegurar la veracidad de dicha información. El funcionario responsable deberá corresponder a cualquiera de las siguientes clasificaciones: Director, Gerente o Funcionario Principal, según las disposiciones de la Circular G-119-2004, referida a las normas para el registro de Directores, Gerentes y Principales Funcionarios – REDIR.

Artículo 16°.- Información adicional
La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión del riesgo operacional de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos mencionados por el presente Reglamento, así como los informes de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

CAPITULO V
COLABORADORES EXTERNOS

Artículo 17º.- Auditoría Interna
La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la gestión del riesgo operacional, así como de lo dispuesto en el presente Reglamento, de conformidad con lo establecido en el Reglamento de Auditoría Interna.

Artículo 18º.- Auditoría Externa
Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la gestión del riesgo operacional, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Artículo 19º.- Empresas Clasificadoras de Riesgo
Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la gestión del riesgo operacional en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

Primera.- Autorizaciones especiales
Las empresas podrán solicitar a la Superintendencia exoneración específica de alguno de los requerimientos normativos indicados en este Reglamento, adjuntando la documentación de sustento correspondiente, para lo cual serán de aplicación los requisitos señalados en la Primera Disposición Final y Transitoria del Reglamento de la Gestión Integral de Riesgos, en lo que sea aplicable a la gestión del riesgo operacional.

Segunda.- Régimen simplificado para las Edpymes
Las Edpymes no están obligadas a implementar la base de datos de eventos de pérdida requerida en el artículo 12° del presente Reglamento. No obstante, la Superintendencia podrá exigir la aplicación de dicho artículo a aquellas Edpymes que considere apropiadas, teniendo en consideración su tamaño, complejidad y volumen de operaciones.

Tercera.- Sanciones
En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Cuarta.- Transparencia
Como parte de la información que debe ser revelada en la Memoria Anual de las empresas, conforme a lo señalado en el Reglamento de la Gestión Integral de Riesgos, deben incluirse las características principales de la gestión del riesgo operacional implementada por la empresa.

Quinta.- Adecuación de las Administradoras Privadas de Fondos de Pensiones
En un plazo que no excederá de noventa (90) días calendario de haberse publicado el presente Reglamento, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la AFP respecto al cumplimiento de cada uno de los artículos del presente Reglamento, las acciones previstas para la total adecuación y el

cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

12

ANEXO N° 1

TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Tipo de evento (Nivel 1)	Definición	Tipo de evento (Nivel 2)	Ejemplos
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 implicado, al menos, un miembro de la empresa.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).
		Robo y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
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 o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Higiene y seguridad en el trabajo	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 empresarial 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 (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.
		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), lavado 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, exceso 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).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
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	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en el Delivery vs. Payment).
		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 proveedores.

ANEXO N° 2

LINEAS DE NEGOCIO GENÉRICAS PARA EMPRESAS DEL SISTEMA FINANCIERO

Nivel 1	Nivel 2	Definición
Finanzas corporativas	Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización; underwriting; asesoramiento financiero a empresas corporativas, grandes y medianas empresas, así como al gobierno central y entidades del sector público; entre otras actividades de naturaleza similar.
	Finanzas de administraciones públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Operaciones de tesorería; compra y venta de títulos, monedas y commodities por cuenta propia; entre otras actividades de naturaleza similar.
	Creación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Financiamiento a clientes minoristas incluyendo tarjetas de crédito, préstamo automotriz, entre otros.
Banca comercial	Banca comercial	Financiamiento a clientes no minoristas, incluyendo: factoring, descuento, arrendamiento financiero, entre otros.
Liquidación y pagos	Clientes externos	Actividades relacionadas con pagos y cobranzas, transferencia interbancaria de fondos, compensación y liquidación, entre otras actividades de naturaleza similar.
Otros servicios	Custodia	Servicios de custodia, fideicomisos, comisiones de confianza y otros servicios.
	Encargos de confianza	
	Fideicomisos	
	Otros servicios	

ANEXO N° 3

LINEAS DE NEGOCIO GENÉRICAS PARA EMPRESAS DE SEGUROS

NIVEL 1	NIVEL 2	Definición
Ramos generales	Incendio y Domiciliario	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Incendios - Lineas Aliadas Incendio - Lucro Cesante - Cristales - Terremoto - Domiciliario
	Ramos Técnicos	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Todo riesgo para contratistas - Rotura de maquinaria - Lucro cesante de Rotura de maquinaria - Montaje contra todo riesgo - Todo riesgo equipo electrónico - Todo riesgo equipo para contratistas - Calderas
	Robo, Bancos y 3D	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Robo y asalto - Deshonestidad frente a la empresa - Comprensivo contra deshonestidad - Seguro de Bancos
	Responsabilidad civil	Se refiere a pólizas emitidas por responsabilidad civil
	Cascos, Transportes y Aviación	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Transportes - Marítimo – Cascos - Aviación
	Autos y SOAT	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Vehículos - Lineas alladas vehículos - SOAT
	Accidentes personales	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Accidentes personales - Escolares
	Asistencia médica	Se refiere a pólizas emitidas por asistencia médica
	Otros	Se refiere a pólizas emitidas frente a los siguientes riesgos: - Cauciones - Crédito Interno - Crédito a la exportación - Multiseguros - Agrícola - Misceláneos - Animales
Ramos de vida	Seguros de Vida en Grupo	Se refiere a las siguientes pólizas: - Seguro de Vida en Grupo Particular - Seguro de Vida para Trabajadores - Seguro de Desgravamen - Seguro de Vida Individual de Corto Plazo

		- Sepelio de Corto Plazo
	Seguros de Vida Individual y Rentas	Se refiere a las siguientes pólizas: - Seguro de Vida Individual de Largo Plazo - Sepelio de Largo Plazo - Seguro de Vida para ex - Trabajadores - Renta Particular - Pensiones del Seguro Complementario de Trabajo de Riesgo - Renta de Jubilación - Pensión de Invalidez - Pensión de Sobrevivencia - Pensión de Invalidez-Régimen Temporal - Pensión de Sobrevivencia-Régimen Temporal
	Seguros Previsionales y SCTR	Se refiere a las siguientes pólizas: - Seguro Complementario de Trabajo de Riesgo - Invalidez - Sobrevivencia - Gastos de Sepelio
Finanzas corporativas	Finanzas corporativas	Deuda subordinada, emitir acciones, ofertas públicas iniciales y colocaciones en mercado secundario, fideicomiso
Negociación y ventas	Negociación y ventas	Renta fija, renta variable, divisas, posiciones propias en valores, operaciones con pacto de recompra.
Créditos	Créditos	Fianzas, créditos hipotecarios para trabajadores.

ANEXO N° 4

LINEAS DE NEGOCIO GENÉRICAS PARA AFP

Nivel 1	Nivel 2	Definición
Administración de fondos	Administración de aportes obligatorios	En la forma establecida en la Ley del SPP
	Administración de aportes voluntarios	En la forma establecida en la Ley del SPP

A3. CIRCULAR SBS N° G-139-2009: Gestión de la Continuidad del Negocio

Lima, 02 de abril de 2009

CIRCULAR N° G-139-2009

Ref.: Gestión de la continuidad del negocio

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones aprobado por el Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para la gestión de la continuidad del negocio, que forma parte de una adecuada gestión del riesgo operacional que enfrentan las empresas supervisadas, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el BS-25999, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance
Artículo 1°.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones
Artículo 2°.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. Grupos de interés: Personas u organizaciones que se ven impactadas por las operaciones de una empresa. Ejemplos: clientes, socios del negocio, empleados, proveedores, accionistas, entidades gubernamentales, entre otros.

c. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

d. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.

e. Periodo máximo tolerable de interrupción: Es el periodo de tiempo luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado.

f. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

g. Riesgo: La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.

h. Riesgo operacional: La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

i. Tiempo objetivo de recuperación: Es el tiempo establecido por la empresa para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

Gestión de la continuidad del negocio
Artículo 3º.- La gestión de la continuidad del negocio es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Las empresas deben realizar una gestión de la continuidad del negocio adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

Responsabilidad del Directorio
Artículo 4º.- El Directorio es responsable de establecer una adecuada gestión de la continuidad del negocio. Entre sus responsabilidades específicas están:

a. Aprobar una política general que defina el alcance, principios y guías que orienten la gestión de la continuidad del negocio.
b. Aprobar los recursos necesarios para el adecuado desarrollo de la gestión de la continuidad del negocio, a fin de contar con la infraestructura, metodología y personal apropiados.
c. Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión de la continuidad del negocio.

Responsabilidad de la Gerencia
Artículo 5º.- La gerencia general tiene la responsabilidad de implementar la gestión de la continuidad del negocio conforme a las disposiciones del Directorio. La gerencia podrá constituir comités para el cumplimiento de sus responsabilidades relacionadas con la gestión de la continuidad del negocio.

Responsabilidad de la Unidad de Riesgos

Artículo 6º.- La Unidad de Riesgos deberá asegurarse que la gestión de la continuidad del negocio que realice la empresa sea consistente con las políticas y procedimientos aplicados para la gestión de riesgos.

Función de continuidad del negocio
Artículo 7º.- Las empresas deberán contar con una función de continuidad del negocio, la cual tendrá a su cargo las siguientes responsabilidades:

a. Proponer las políticas, procedimientos y metodología apropiados para la gestión de la continuidad del negocio en la empresa, incluyendo la asignación de roles y responsabilidades;
b. Velar por una gestión de la continuidad del negocio competente;
c. Informar a la gerencia general y al comité de riesgos los aspectos relevantes de la gestión de la continuidad del negocio para una oportuna toma de decisiones.

En función a su tamaño y complejidad de operaciones y servicios, esta función será desempeñada por una unidad especializada o asignada a otra unidad de la empresa.

Fases de la gestión de la continuidad del negocio
Artículo 8º.- Las empresas deberán desarrollar como mínimo las siguientes fases como parte de la gestión de la continuidad del negocio:

8.1. Entendimiento de la organización

Esta fase consiste en conocer los objetivos y metas de la empresa; identificar los principales procesos, productos, servicios y proveedores, así como las actividades y recursos requeridos; evaluar los riesgos que podrían causar una interrupción de dichas actividades, y el impacto que podría tener dicha interrupción.

Las actividades mínimas a desarrollar durante esta fase son las siguientes:

a. Análisis de impacto: Consiste en determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios de la empresa. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera de la empresa, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, debe establecerse el periodo máximo tolerable de interrupción por cada uno de estos procesos.

   El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados.

b. Evaluación de riesgos: Consiste en identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deberá seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos que enfrenta la empresa.

La empresa debe definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.

8.2. Selección de la estrategia de continuidad

En esta fase, se determinan las estrategias de continuidad que permitirán mantener las actividades y procesos de negocio luego de ocurrido un evento de interrupción de operaciones.

Debe desarrollarse, como mínimo, la siguiente actividad:

a. Evaluación y selección de estrategias de continuidad por proceso: Se refiere a seleccionar las estrategias que permitirán mantener la continuidad de los procesos que soportan los principales productos y servicios de la empresa, dentro del tiempo objetivo de recuperación, definido para cada proceso. Las estrategias de continuidad deben tomar en cuenta los siguientes aspectos, según sea aplicable para cada proceso:
   - Seguridad del personal.
   - Habilidades y conocimientos asociados al proceso.
   - Instalaciones alternas de trabajo.
   - Infraestructura alterna de tecnología de información que soporte el proceso.
   - Seguridad de la información.
   - Equipamiento necesario para el proceso.

8.3. Desarrollo e implementación de la estrategia de continuidad

En esta fase, se deben desarrollar los planes de respuesta ante los eventos analizados en las fases previas, e implementar un modelo de respuesta flexible y escalable que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones. Para este fin, las empresas deberán implementar dos tipos de planes:

a. Plan de Gestión de Crisis: Consiste en preparar a la empresa para enfrentar la fase aguda de un evento de interrupción de operaciones, incluso de aquellos no esperados. Debe incluir los siguientes aspectos:
   - Propósito y alcance
   - Roles y responsabilidades
   - Criterios de invocación y activación
   - Responsable de su actualización
   - Planes de acción
   - Comunicaciones con el personal, familiares y contactos de emergencia
   - Interacción con los medios de comunicación
   - Comunicación con los grupos de interés
   - Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno)

b. Plan(es) de Continuidad del Negocio: Tiene(n) como objetivo dotar a la empresa de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos. Debe(n) considerar, como mínimo, los siguientes aspectos:
   - Propósito y alcance
   - Roles y responsabilidades
   - Criterios de invocación y activación
   - Responsable de su actualización
   - Planes de acción para reanudar los procesos conforme a la estrategia seleccionada.
   - Requerimiento de recursos

- Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, entre otros)

Se deben desarrollar planes específicos considerando, por lo menos, los siguientes:

Plan de Emergencia: Plan que tiene como objetivo salvaguardar la integridad física del personal.

Plan de Recuperación de los servicios de tecnología de información: Plan que busca inicialmente restaurar los servicios de tecnología de información dentro de los parámetros establecidos, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

8.4. Pruebas y actualización

Los planes de continuidad del negocio deberán ser probados cuando menos una vez al año. A continuación se detallan las actividades mínimas que deben ser aplicadas en esta fase:

a. Ejecución de pruebas: El alcance de las pruebas debe ser consistente con el alcance de los planes de continuidad del negocio. Cada prueba debe tener objetivos definidos y un reporte que resuma los resultados alcanzados y recomendaciones. Esta información debería ser usada para mejorar los planes de continuidad del negocio en forma oportuna. Pueden aplicarse diferentes tipos de prueba, desde las pruebas de escritorio hasta las simulaciones completas de escenarios de interrupción de operaciones.

   Las empresas deberán asegurarse que sus principales proveedores de servicios cuenten con planes de continuidad y que éstos cumplan con lo señalado en el presente numeral.

b. Actualización de los planes: Las empresas deben definir políticas y procedimientos para la actualización de los planes de gestión de la continuidad del negocio, de tal manera que cualquier cambio que impacte a la empresa (ya sea interno o externo) sea revisado en relación con la continuidad del negocio.

8.5. Integrar la gestión de la continuidad del negocio a la cultura organizacional

Las actividades mínimas a desarrollar en esta fase son las siguientes:

a. Evaluación del grado de conocimiento sobre la gestión de continuidad: Tiene como objetivo determinar el nivel de conocimiento actual y esperado sobre la gestión de continuidad del negocio, los procedimientos implementados, las tareas específicas señaladas en los planes de continuidad, entre otros aspectos.

b. Desarrollo y mejora de la cultura de continuidad: Diseñar e implementar planes de capacitación y entrenamiento, a fin de cubrir las deficiencias encontradas en la actividad previa.

c. Monitoreo permanente: Revisar periódicamente el nivel de entendimiento de la gestión de continuidad del negocio a fin de identificar requerimientos adicionales.

Documentación Sustentatoria
Artículo 9°.- Las empresas deberán mantener a disposición de la Superintendencia la documentación necesaria que permita sustentar el desarrollo de cada una de las fases y actividades descritas en el artículo anterior.

Los principales aspectos de la gestión de la continuidad del negocio, incluyendo el programa de pruebas de los planes de continuidad, serán reportados a través del aplicativo IG-ROp en el plazo establecido en el Reglamento para la Gestión del Riesgo Operacional.

Cambios significativos
Artículo 10°.- Las empresas analizarán el impacto que tienen los cambios significativos sobre la continuidad del negocio.

Los cambios significativos podrán considerar entre otros: cambio de la infraestructura tecnológica que soporta los principales productos y/o servicios, fusión con otra empresa, implementación de un nuevo producto, cambio de un proveedor principal, cambio de oficina principal, entre otros.

Auditoría Interna
Artículo 11°.- La Unidad de Auditoría Interna evaluará el cumplimiento de lo dispuesto en la presente norma de acuerdo a su plan de trabajo.

Plan de Adecuación
Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las empresas deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la empresa respecto al cumplimiento de cada uno de los artículos de la presente Circular, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Vigencia y Plazo de Adecuación
Artículo 13°.- La presente Circular entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010. A partir de dicha fecha, queda derogado el artículo 83° del Título III del Compendio de Normas de Superintendencia Reglamentarias del Sistema Privado de Administración de Fondos de Pensiones, referido a Gestión Empresarial.

Atentamente,

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

A4. CIRCULAR SBS N° G-140-2009: Gestión de Seguridad de la Información

Lima, 02 de abril de 2009

CIRCULAR N° G-140-2009

Ref.: Gestión de la seguridad de la información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance
Artículo 1°.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones
Artículo 2°.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. Factor de autenticación: Información utilizada para verificar la identidad de una persona. Pueden clasificarse de la siguiente manera:
   Algo que el usuario conoce (por ejemplo: una clave de identificación)

Algo que el usuario posee (por ejemplo: una tarjeta)
Algo que el usuario es (por ejemplo: características biométricas)

c. Incidente de seguridad de información: Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

d. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

e. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.

f. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

   I. Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
   II. Integridad: La información debe ser completa, exacta y válida.
   III. Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

g. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.

h. Subcontratación significativa: Aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.

Sistema de gestión de la seguridad de la información
Artículo 3º.- Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

a. Definición de una política de seguridad de información aprobada por el Directorio.
b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Estructura organizacional
Artículo 4°.- Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.

Asimismo, deben asegurarse que se desarrollen las siguientes funciones, ya sea a través de una unidad especializada o a través de alguna de las áreas de la empresa:

a. Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.
b. Coordinar y monitorear la implementación de los controles de seguridad de información.
c. Desarrollar actividades de concientización y entrenamiento en seguridad de información.
d. Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas.

La Superintendencia podrá requerir la creación de una unidad especializada en gestión de la seguridad de información en empresas que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Controles de seguridad de información
Artículo 5°.- Como parte de su sistema de gestión de la seguridad de información, las empresas deberán considerar, como mínimo, la implementación de los controles generales que se indican en el presente artículo.

5.1 Seguridad lógica

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
b) Revisiones periódicas sobre los derechos concedidos a los usuarios.
c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
f) Controles especiales sobre usuarios remotos y computación móvil.

5.2 Seguridad de personal

a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.
b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.
c) Concientización y entrenamiento.
d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.
e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

5.3 Seguridad física y ambiental

a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.
b) Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

5.4 Inventario de activos y clasificación de la información

a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.
b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5.5. Administración de las operaciones y comunicaciones

a) Procedimientos documentados para la operación de los sistemas.
b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
c) Separación de funciones para reducir el riesgo de error o fraude.
d) Separación de los ambientes de desarrollo, pruebas y producción.
e) Monitoreo del servicio dado por terceras partes.
f) Administración de la capacidad de procesamiento.
g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.
j) Seguridad sobre canales electrónicos.
k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente.
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.
f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.

5.7. Procedimientos de respaldo

a) Procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.

b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.

5.8. Gestión de incidentes de seguridad de información

Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las empresas deberán considerar los siguientes aspectos:

a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.
b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

5.9. Cumplimiento normativo

Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

5.10. Privacidad de la información

Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.

Seguridad en operaciones de transferencia de fondos por canales electrónicos
Artículo 6°.- En el caso de las operaciones de transferencia de fondos a terceros ofrecidas por las empresas para su realización a través de canales electrónicos, las empresas deberán implementar un esquema de autenticación de los clientes basado en dos factores como mínimo. Para el caso en que el canal electrónico sea Internet, uno de los factores de autenticación deberá ser de generación o asignación dinámica. Las empresas podrán utilizar otros factores de autenticación, en tanto éstos proporcionen un nivel de seguridad equivalente o superior respecto a los dos factores señalados, en particular cuando se trate de operaciones importantes según los límites que el banco determine de acuerdo a las características del producto o servicio ofrecido.

La empresa deberá tomar en cuenta los riesgos operacionales asociados, en el diseño de los procedimientos, las definiciones de límites y las consideraciones de seguridad e infraestructura requeridas para un funcionamiento seguro y apropiado en las operaciones de transferencia de fondos.

Subcontratación
Artículo 7°.- Las empresas son responsables y deben verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en el artículo 21° del Reglamento de la Gestión Integral de Riesgos. Asimismo, las empresas deben asegurarse que el procesamiento y la información objeto de la subcontratación, se encuentre efectivamente aislada en todo momento.

En caso que las empresas deseen realizar una subcontratación significativa de su procesamiento de datos, de tal manera que éste sea realizado en el exterior, requerirán de la autorización previa y expresa de la Superintendencia. Para ello, la empresa debe asegurar un adecuado cumplimiento de la presente Circular, en lo que sea aplicable al servicio de procesamiento contratado.

La Superintendencia podrá requerir cuando así lo considere apropiado que el proveedor del servicio en el exterior se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio.

En el Anexo A que forma parte de la presente norma y se publica en el Portal electrónico institucional (www.sbs.gob.pe), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS, se detalla la información que debe remitir la empresa adjunta a su solicitud de autorización. Una vez recibida la documentación completa, dentro de un plazo que no excederá de sesenta (60) días útiles, la Superintendencia emitirá la resolución que autoriza o el oficio que deniega la solicitud presentada por la empresa.

Las empresas que obtengan la autorización para realizar su procesamiento de datos en el exterior, deberán asegurar, con una frecuencia anual, que el servicio subcontratado sea sometido a un examen de auditoría independiente, por una empresa auditora de prestigio, que guarde conformidad con el estándar SAS 70 emitido por el Instituto Americano de Contadores Públicos Certificados (AICPA). En tal sentido, las empresas deberán remitir a la Superintendencia el Reporte de Auditoría de Tipo II considerado en dicho estándar, el cual entre otros aspectos considera la evaluación de los controles implementados y las pruebas de su efectividad.

Información a la Superintendencia
Artículo 8°.- Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la gestión del riesgo operacional, emitido por la SBS, las empresas deberán incluir información sobre la gestión de la seguridad de la información.

Información adicional
Artículo 9°.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión de la seguridad de la información de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos a que hace mención la presente Circular, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

Sanciones
Artículo 10°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Vigencia
Artículo 11°.- Las disposiciones de la presente Circular entran en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano", otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010, fecha a partir de la cual quedará sin efecto la Circular SBS N°G-105-2002.
Adecuación de las AFP
Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la AFP respecto al cumplimiento de cada uno de los artículos de la presente Circular, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Atentamente,

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

ANEXO A

DOCUMENTACIÓN A REMITIR JUNTO CON LA SOLICITUD DE AUTORIZACIÓN PARA REALIZAR PROCESAMIENTO PRINCIPAL EN EL EXTERIOR

Documento	Contenido mínimo requerido
1. Información general del proveedor y del servicio	Razón social del proveedor. Giro del negocio y años de experiencia. Indicar a qué empresas brinda servicios actualmente. Estados Financieros del proveedor correspondientes a los dos últimos años. Relación de accionistas del proveedor y funcionarios principales. Relación con la empresa supervisada (indicar si pertenecen al mismo grupo económico). Servicios que serán provistos por el proveedor y el tipo de información a ser procesada. Ubicación (país y ciudad) del centro de procesamiento principal. Razones para seleccionar al proveedor.
2. Borrador del Contrato	Aspectos a considerar: Acuerdos de niveles de servicio. Procedimientos de monitoreo. Procedimientos de contingencia. Cumplimiento de las normas sobre secreto bancario y confidencialidad de la información. Prestación del servicio en regímenes especiales (vigilancia, intervención, liquidación). El proveedor debe seguir brindando el servicio como mínimo un año después de que la empresa ha ingresado a un régimen especial. Compromiso de cumplimiento de la normativa de la Superintendencia. Aseguramiento del acceso adecuado a la información con fines de supervisión, en tiempos razonables y a solo requerimiento, por parte de la Superintendencia, Auditoría Interna y Externa, en condiciones normales de operación y en regímenes especiales. Este aspecto debe ser aplicable sobre cualquier otra empresa que el proveedor subcontrate para brindar servicios a la entidad supervisada. Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y la Superintendencia.
3. Informe de la Plataforma Tecnológica	Aspectos a considerar: (Señalar qué equipos y aplicaciones estarán a cargo del proveedor) Inventario de equipos de cómputo. Inventario de software base. Herramientas y/o manejadores de base de datos. Aplicaciones críticas. Esquema de comunicaciones a ser implementado entre el proveedor y la empresa supervisada.
4. Informe de Comunicación con	Descripción de la forma de envío de información a la Superintendencia luego de que se implemente el servicio de procesamiento en el exterior. Asimismo,

	la Superintendencia (SUCAVE, RCD, otros)	indicar los cambios que se aplicarán sobre los procedimientos asociados a la generación, consolidación y reporte de dicha información.
5.	Informe de Evaluación de Riesgos	Evaluación de los riesgos de operación asociados con el esquema propuesto por la empresa, realizada por la Unidad de Riesgos.
6.	Gestión de la seguridad de información	Política de seguridad de información de la empresa. Estructura organizativa para la gestión de la seguridad de información. Asignación de responsabilidades asociadas con la seguridad de información en la entidad y el proveedor. Forma en que se aislará el procesamiento y la información objeto de la subcontratación. Procedimientos y controles a implementar, considerando el procesamiento en el exterior, en los siguientes aspectos: - Seguridad lógica. - Seguridad de personal. - Seguridad física y ambiental. - Administración de las operaciones y comunicaciones. - Desarrollo y mantenimiento de los sistemas informáticos. - Administración de las copias de respaldo.
7.	Gestión de continuidad de negocios	Plan de Contingencia del proveedor, para asegurar la continuidad del servicio de procesamiento informático. Señalar la prioridad asignada al procesamiento de la información de la empresa supervisada respecto al resto de clientes del proveedor. Señalar la forma en que se dará aviso a la empresa supervisada, y las acciones que deberá desarrollar la empresa en caso de una contingencia en el proveedor. Frecuencia y alcance de las pruebas al Plan de Contingencia del proveedor.
8.	Plan de Auditoría de Sistemas	Señalar el alcance, forma y periodicidad de las revisiones de auditoría de sistemas considerando el nuevo esquema de procesamiento principal de la empresa.
9.	Gestión del proyecto	Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control. Costo estimado de implementación del proyecto.

A5. CUESTIONARIO DE RIESGO OPERACIONAL

ENCUESTA SOBRE RIESGO OPERACIONAL

Trabajo de Investigación de Riesgo Operativo

DEFINCIÓN Y MOTIVOS DE ADOPCION

1 ¿Cuáles son los Motivos por los cuales se comenzó a trabajar en la gestión de Riesgo Operacional?

- ☐ Motivos Regulatorios
- ☐ Control y Reducción de Pérdidas Operacionales
- ☐ Concientización de alta dirección
- ☐ Requerimientos de Auditoría

TIPOS DE EVENTO

2 ¿Cuáles son los Tipos de Evento más Importantes de Riesgo Operacional en las Entidades Financieras? (marque todas las que corresponda)

- ☐ Fraude interno
- ☐ Fraude externo
- ☐ Relaciones laborales y seguridad en el puesto de trabajo
- ☐ Clientes, productos y prácticas empresariales
- ☐ Daños a activos materiales
- ☐ Interrupción del negocio y fallos en los sistemas
- ☐ Ejecución, entrega y gestión de procesos

LINEAS DE NEGOCIO

3 ¿Cuáles son las Lineas de Negocio más Importantes de Riesgo Operacional en su Entidad? (marque todas las que corresponda)

- ☐ Finanzas corporativas
- ☐ Negociación y ventas
- ☐ Banca Minorista
- ☐ Banca Comercial
- ☐ Liquidación y pagos
- ☐ Otros servicios

ORGANIZACION: AREA INDEPENDIENTE DE RIESGOS DE OPERACION

4 ¿Cuentan con un área independiente de Riesgos de Operacion en su Entidad? (marque solo una)

- ☐ Si
- ☐ No
- ☐ En Desarrollo

Si su respuesta es "Si" cuantas personas laboran en dicha área: _____

HERRAMIENTAS

5 ¿Cuáles son los Herramientas de Gestión de Riesgo Operacional que emplea en su Entidad? (marque todas las que corresponda)

- ☐ Cuadro de mando
- ☐ Mapas de riesgos
- ☐ Autoevaluación
- ☐ Alertas
- ☐ Indicadores de riesgo
- ☐ Bases de datos de pérdidas

METODOS DE MEDICION

6 ¿Cuáles es el Método de Medición del Requerimiento de Patrimonio Efectivo por Riesgo Operacional que su entidad esta empleando? (marque sólo una)

- ☐ Requerimiento según Método del Indicador Básico
- ☐ Requerimiento según Método Estándar Alternativ
- ☐ Requerimiento según Métodos Avanzados

DEFINCIÓN Y MOTIVOS DE ADOPCION

7 ¿Cuáles es Nivel de cumplimiento de Metodología Cualitativa de Riesgo Operacional según Principios de Basilea II en su entidad? (ingrese un valor aproximado en porcentaje)

Tener un sistema de gestión del Riesgo Operativo (RO) que asigne responsabilidades claras a la unidad de gestión del RO.	
Tener un sistema de evaluación del RO perfectamente integrado dentro de los procesos de gestión del riesgo de la entidad.	
Analizar de forma sistemática la información sobre el RO, incluidas las perdidas relevantes sufridas en cada una de las líneas.	
Contar con un sistema periódico de información sobre las exposiciones al RO, incluidas las pérdidas operacionales más relevantes, dirigido al Consejo de Administración, la Alta Dirección y las diferentes unidades de negocio.	
Contar con un sistema periódico de información sobre el historial de pérdidas por RO, dirigido al Consejo de Administración, la Alta Dirección y las diferentes unidades de negocio.	
Definir procedimientos destinados a adoptar las acciones necesarias según la información aportada por los informes de la gestión del RO.	
Documentar correctamente todo el sistema de gestión del RO.	
Validar y examinar de forma periódica e independiente los procesos de gestión y el sistema de evaluación del RO.	
Que los auditores internos y/o externos realicen exámenes periódicos de los procesos de gestión y de los sistemas de evaluación del RO.	
Implantar técnicas que asignen los ingresos brutos o el capital, según el método, a las diferentes líneas de negocio y que generen incentivos para la mejora de la gestión del RO en toda la entidad.	

PRINCIPALES DIFUCULTADES PARA GESTIONAR EL RIESGO OPERACIONAL

8 ¿Cuáles son las Principales Dificultades para Gestionar el riesgo Operacional I? (marque todas las que corresponda)

- [ ] Falta de Marco metodológico acorde.
- [ ] Falta de conocimientos técnicos
- [ ] Compromiso/cultura de la empresa
- [ ] Falta/uso de software adecuado
- [ ] Disponibilidad de datos internos

COMPONENTES DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS

9 Brinde uno aproximación del uso de componentes de gestión de riesgos que su entidad emplea (En porcentajes)

	Incluye componentes	Carece de algun componente
CUALITATIVOS: Comprende la estructura organizativa, modelo general, políticas, requisitos, marco legal, mapeo de procesos, herramientas informáticas (softw are) y documentales que cubren las diferentes etapas de gestión de riesgos cualitativo, identificación de eventos de pérdida..		
CUANTITATIVOS: Metodos de medición de cálculo para los diferentes tipos de riesgo, Integrado con el sistema financiero y contable de empresa, softw are		

A6. PAUTAS PARA EL RECONOCIMIENTO DE EVENTOS DE PÉRDIDA

a) Se reconoce un evento de pérdida cuando la respuesta a una de las siguientes interrogantes es afirmativa:
¿El suceso tiene como causa raíz o causa principal, una falla de procesos, personas o sistemas?
¿El evento se debió a que se incumplió un control o se realizo una excepción a las políticas?
¿Se podría considerar que el origen del evento fue ocasionado por procesos o sistemas o que los controles de éstos, se consideran inadecuados para soportar el producto?
¿El evento incumple leyes, reglamentos o contratos con terceros (marcas de tarjetas, clientes u otras instituciones)?
¿Se pudo o podría verse afectado negativamente a la empresa, por fallas en procesos con soporte de terceros? Este caso incluye eventos accidentales, fallas de procesos o sistemas (inclusive en su diseño), fallas que perjudican a la empresa y fraude del personal del proveedor.
¿Se han dañado los activos de la empresa? ¿Ocurrió un hurto/robo de bienes de la empresa o bajo su custodia?
¿El evento tiene su origen en fallas de equipos que soportan el proceso, como por ejemplo: computadoras, lectores de medios magnéticos, etc.?
¿Es un robo o fraude realizado por terceros en perjuicio de la empresa?, ¿incluye estafas en créditos y operaciones de mercado? Por ejemplo, suplantación, falsificación de firmas, etc.
¿Es un fraude realizado por colaboradores de la empresa o con la participación de los mismos? Por ejemplo, aquellos casos donde se retira al empleado por intento de engaño, o por incumplimiento del proceso con intención de beneficio propio.
b) Algunos eventos de pérdida cumplen con lo siguiente:
En caso de pérdidas por riesgos asociados al crédito, estas tienen relación u origen con causas vinculadas a procesos, sistemas o personas que ejecutaron inoportunamente o erróneamente sus actividades.
En caso de pérdidas asociadas a operaciones de mercado (riesgo de mercado / liquidez), estas tienen relación u origen con causas vinculadas a procesos, sistemas o personas que ejecutaron inoportunamente o erróneamente sus actividades.
Los daños en cajeros, monederos y otros equipos de la empresa.
Los daños en oficinas, tiendas y locales de la empresa realizados por terceros.
Es un siniestro que afecta a los activos de la empresa o su personal en las oficinas, como por ejemplo: sismos, incendios, accidentes, etc.
Es una sanción de entidades gubernamentales por acciones realizadas u omitidas por la empresa.
Los juicios laborales o demandas de trabajadores por despidos improcedentes, discriminación, acoso que afectan a la empresa.
Multas o indemnizaciones consecuencia de incumplimiento de normas laborales, condiciones de seguridad e higiene en el trabajo, accidentes laborales.
Demandas civiles, multas o sanciones consecuencia de eventos accidentales que afectan a clientes u otras personas no vinculadas a la empresa.

A7. TIPOS DE EVENTOS DE PÉRDIDA

Tipo de evento (Nivel 1)	Definición	Tipo de evento (Nivel 2)	Ejemplos
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 implicado, al menos, un miembro de la empresa.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).
		Robo y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
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 o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Higiene y seguridad en el trabajo	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 empresarial 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 (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.

		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), lavado 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, exceso 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).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
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	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en el Delivery vs. Payment).
		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 proveedores.

Fuente: SBS

A8. CATEGORÍAS DE RIESGO OPERACIONAL

CATEGORÍA	SUBCATEGORÍA	RIESGO
Evento Externo	Actividades criminales	Acciones enmascaradas.
		Apertura fraudulenta de cuenta por un cliente
		Chantaje
		Daños físicos a la propiedad
		Fraudes externos / fraude con cheques / falsificación.
		Hurto o robo
		Incendio provocado
		Interrupción del negocio
		Lavado de dinero
		Otros.
		Terrorismo / bombas
	Desastres y fallas en la infraestructura de servicios básicos	Desastres civiles.
		Fallas de energía
		Fallas de transporte.
		Fallas en telecomunicaciones externas.
		Fuego.
		Inaccesibilidad a las instalaciones.
		Interrupción en suministro de agua
		Inundación.
		Otros desastres naturales (geológicas / meteorológicas).
		Otros.
	Legales / publico	Incumplimiento regulación ambiental.
	Responsabilidad	Incumplimiento de la responsabilidad del fiduciario o de la agencia.
		Interpretación de la ley
		Otros.
		Tergiversación.
	Riesgo de proveedores	Bancarrota del proveedor.
		Contratos inadecuados.
		Fallas del acuerdo del nivel de servicio.
		Fallas en la entrega.
		Inadecuada administración de servicios o proveedores.

		Incumplimiento de responsabilidades (mal uso de data confidencial).
		Otros.
	Riesgo político / de gobierno.	Bloqueo / interrupción del negocio.
		Cambio del régimen de impuestos.
		Expropiación de activos.
		Guerra.
		Otros cambios en la ley
		Otros
	Riesgos de regulación	Cambios en las regulaciones de la industria / país.
	Riesgos de Servicios internos	Actividades no autorizadas / Rogue Trading
Personas	Actividades no autorizadas / Rogue Trading	Mal uso de información privilegiada.
	Fechorias de Empleados	Actividades con contrapartidas no autorizadas.
		Actividades dirigidas para especular con los precios de los portafolios.
		Actividades en productos no autorizados.
		Actividades fuera del alcance de los acuerdos pactados.
		Ignorar deliberadamente los procesos.
		Incumplimiento de límites.
		Manipulación de mercado.
		Modelos incorrectos (cambios intencionales y no autorizados en los parámetros).
		Sobre estimar un contrato para apropiarse de una comisión.
		Tácticas de ventas ilegales / negligentes / desleales.
	Fraude / malicia del empleado (criminal)	Fraude de programación.
		Hurto o robo de propiedad intelectual.
		Hurto o robo físico.
		Lavado de dinero (Deliberado).
		Malversación.
		Sabotaje de la reputación del banco (Deliberado).
	Interrupción de labores	Acción Industrial (Huelga/ paro de los trabajadores de la empresa).
	Leyes Laborales	Despido injusto.
		Discriminación / Igual oportunidad.
		Hostigamiento.
		No-adherencia a otras leyes laborales.
		No-adherencia a regulaciones de salud y seguridad.
	Pérdida o carencia de personal clave	Carencia de empleados adecuados.
		Perdida de personal clave.
Procesos	Cumplimiento	Breach of Chinese walls
		Incumplimiento de procedimientos externos.
		Incumplimiento de procedimientos internos.
	Documentación o Riesgos contractuales	Documentos no completados apropiadamente.
		Expedientes de ventas inadecuados.
		Fallas en el due diligence.
		Inadecuadas cláusulas / términos del contrato.
		Otros.
		Términos de contratos inapropiados.
	Pagos / Acuerdos	Fallas o inadecuados procesos internos de pagos

	Reportes internos y externos	Errores en la información contable / Data inadecuada.
		Inadecuados reportes de activos financieros / títulos valores y stock de cambio.
		Inadecuados reportes de administración del riesgo.
		Inadecuados reportes de excepción.
		Inadecuados reportes de impuestos.
		Inadecuados reportes financieros.
		Inadecuados reportes regulatorios.
		No aplicación de leyes de información confidencial / secreto bancario.
		Otros.
	Riesgo de entrega	Errores en la entrega de activos financieros / títulos valores.
		Incumplimiento de límites.
		Insuficiente capacidad de recursos para hacer frente a los volumenes de operaciones
		Otros.
		Pérdidas por errores en la conciliación.
	Riesgos de proyectos / Administración del cambio	Inadecuado planeamiento del proyecto.
		Inadecuados procesos de productos nuevos.
		Incumplimiento en los plazos y costos planeados.
		Otros.
	Riesgos de ventas	Asesoría limitada sobre productos financieros (incluye títulos valores).
		Complejidad de producto.
		Otros.
		Selección inadecuada de productos.
	Valoración / Tasación	Error en el registro de datos.
		Otros.
		Riesgo del modelo.
Sistemas	Brechas de seguridad en los sistemas	Brechas de seguridad externa.
		Brechas de seguridad interna.
		Fraude de programación. (por terceros)
		Otros.
		Virus informáticos.
	Capacidad de sistemas	Inadecuada planificación de la capacidad.
		Otros.
		Software inadecuado
	Desarrollo e Implementación de sistemas.	Errores de programación (internos y externos)
		Exceder costos / tiempo.
		Falla de los sistemas para adecuarse a los requerimientos funcionales.
		Falla en la integración y/o migración con/de los sistemas existentes.
		Inadecuada administración del proyecto.
		Otros.
	Fallas en los sistemas	Fallas de hardware
		Fallas de interfase
		Fallas de software
		Fallas internas de telecomunicaciones.
		Fallo de la red.
		Otros.

		Riesgo de la interdependencia de sistemas.
	Riesgo de inversión tecnológica	Arquitectura inadecuada.
		Inadecuada definición de requerimientos del funcionales.
		Incompatibilidad con los sistemas existentes
		Obsolescencia del hardware
		Obsolescencia del software
		Otros.
		Riesgo estratégico (plataforma/proveedores).